Nations Unies ECE/TRANS/SC.1/GE.21/2018/1/Rev.1

Conseil économique et social

Distr. générale
13 avril 2021
Français
Original : anglais

Commission économique pour l'Europe

Comité des transports intérieurs

Groupe de travail des transports routiers

Groupe d'experts de l'Accord européen relatif au travail des équipages des véhicules effectuant des transports internationaux par route (AETR)

Vingt-sixième session
Genève, 14 juin 2021
Point 2 b) de l'ordre du jour provisoire
Programme de travail : Appendice 1C

Appendice 1C

Soumis par le Gouvernement du Portugal*

Dans l'annexe du présent document, soumis par le Portugal (qui assure la présidence du Conseil de l'Union européenne), figurent des propositions d'amendements à l'annexe 1C visant à adapter les spécifications de l'Union européenne relatives au tachygraphe intelligent au cadre juridique de l'AETR.

* Les modifications apportées à ce document figurent en caractères gras pour les ajouts et biffés pour les suppressions.

Dans le souci de préserver l'interopérabilité des logiciels des équipements définis dans le présent appendice et ses sous-appendices, certains sigles, termes ou expressions de programmation informatique ont été maintenus dans la langue originale de rédaction du texte, à savoir l'anglais. Des traductions littérales ont toutefois été accolées, pour information, entre parenthèses derrière certaines de ces expressions, afin d'en faciliter la compréhension.

Annexe

Table des matières

Introduction

Le tachygraphe numérique de première génération est déployé ~~depuis le 1er mai 2006~~ **sur le territoire des Parties contractantes**. Il peut servir jusqu'à la fin de sa durée de vie pour le transport national. ~~En revanche, pour le transport international, il est impératif que 15 ans après l'entrée en vigueur du présent règlement de la Commission, tous les véhicules soient équipés d'un tachygraphe intelligent de deuxième génération conforme au sens du présent règlement.~~

Le tachygraphe de première génération est conforme aux exigences de l'appendice 1B du présent Accord, tandis que le tachygraphe de deuxième génération, également appelé tachygraphe intelligent, est conforme aux exigences du présent appendice. L~~a~~**e** présent ~~annexe~~ **appendice** contient les exigences applicables aux appareils de contrôle et aux cartes tachygraphiques de deuxième génération.

À partir de leur date de lancement, l**es** appareil**s** de contrôle de deuxième génération**, version 2,** devr**ont** être installé**s** dans les véhicules **visés par le présent Accord** ~~immatriculés pour la première fois~~ et des cartes tachygraphiques de deuxième génération**, version 2,** devront être délivrées. Afin de favoriser une mise en service sans heurts du tachygraphe de deuxième génération :

- Les cartes tachygraphiques de deuxième génération**, version 2,** doivent être conçues pour être utilisées également dans les unités embarquées de première génération **et de deuxième génération, version 1 ;**
- Le remplacement des cartes tachygraphiques de première génération **et de deuxième génération, version 1,** en cours de validité à la date de lancement ne sera pas exigé.

Cela permettra aux conducteurs de garder leur carte de conducteur individuelle et de l'utiliser dans les deux systèmes.

Toutefois, les appareils de contrôle de deuxième génération ne doivent être étalonnés qu'au moyen de cartes d'atelier de deuxième génération.

Le présent ~~annexe~~ **appendice** contient toutes les exigences relatives à l'interopérabilité entre les tachygraphes de première et de deuxième générations.

~~L'appendice~~ **Le sous-appendice** 15 donne des précisions supplémentaires sur la façon dont la coexistence des deux **générations** ~~systèmes~~**, y compris des différentes versions de la deuxième génération,** doit être gérée.

Liste des ~~appendices~~ **sous-appendices**

App 1 : DICTIONNAIRE DE DONNÉES

App 2: SPÉCIFICATION DES CARTES TACHYGRAPHIQUES

App 3 : PICTOGRAMMES

App 4 : TIRAGES PAPIER

App 5 : AFFICHAGE

App 6 : CONNECTEUR FRONTAL POUR L'ÉTALONNAGE ET LE TÉLÉCHARGEMENT

App 7 : PROTOCOLES DE TÉLÉCHARGEMENT DES DONNÉES

App 8 : PROTOCOLE D'ÉTALONNAGE

App 9 : HOMOLOGATION − LISTE DES ESSAIS MINIMAUX REQUIS

App 10 : EXIGENCES EN MATIÈRE DE SÉCURITÉ

App 11 : MÉCANISMES DE SÉCURITÉ COMMUNS

App 12 : POSITIONNEMENT BASÉ SUR LE SYSTÈME MONDIAL DE NAVIGATION PAR SATELLITE (GNSS)

App 13 : INTERFACE STI

1. Définitions

Dans le présent ~~annexe~~ **appendice**, on entend par :

a) « activation » :
la phase au cours de laquelle le tachygraphe devient pleinement opérationnel et toutes les fonctions sont mises en œuvre, y compris les fonctions de sécurité, au moyen d'une carte d'atelier ;

b) « authentification » :
une fonction destinée à établir et vérifier une identité déclarée ;

c) « authenticité » :
le fait qu'une information provient d'une partie dont l'identité peut être vérifiée ;

d) « test intégré » :
des essais exécutables sur demande, par une action de l'opérateur ou d'un dispositif externe ;

e) « jour civil » :
une journée comprise entre 00 h 00 et 24 h 00. Tous les jours civils sont liés à l'heure universelle coordonnée (UTC) ;

f) « étalonnage d'un tachygraphe intelligent » :
la mise à jour ou la confirmation des paramètres du véhicule à conserver en mémoire. Les paramètres du véhicule comprennent l'identification du véhicule (numéro d'identification du véhicule (VIN), numéro d'immatriculation du véhicule (VRN) et ~~État membre~~ **Partie contractante** d'immatriculation) et les caractéristiques du véhicule (w, k, l, taille des pneumatiques, réglage du limiteur de vitesse (le cas échéant), heure UTC, kilométrage, **type de chargement par défaut**). Pendant l'étalonnage d'un appareil de contrôle, les types et les identifiants des scellements pertinents à des fins d'homologation doivent également être stockés en mémoire ;

Toute mise à jour ou confirmation de l'heure UTC uniquement est considérée comme une remise à l'heure et non comme un étalonnage, à condition qu'elle ne s'oppose pas à l'exigence 409 ;

L'étalonnage d'un appareil de contrôle nécessite l'utilisation d'une carte d'atelier ;

g) « numéro de carte » :
un code alphanumérique à 16 positions constituant le numéro d'identification unique d'une carte tachygraphique dans ~~un État membre~~ **une Partie contractante**. Ce numéro comprend l'**identification du conducteur ou du propriétaire de la carte accompagnée d'un** indice séquentiel ~~(le cas échéant)~~, d'un indice de remplacement et d'un indice de renouvellement de la carte ;

Chaque carte est ainsi identifiable par son numéro et par le code de ~~l'État membre~~ **la Partie contractante** qui l'a délivrée ;

h) « indice séquentiel de la carte » :
le 14e caractère alphanumérique du numéro de carte, utilisé pour différencier les cartes délivrées à une entreprise, un atelier ou une autorité de contrôle habilité à recevoir plusieurs cartes tachygraphiques. L'entreprise, l'atelier ou l'autorité de contrôle est identifié par les 13 premières positions du numéro de carte ;

i) « indice de renouvellement de la carte » :
le 16e caractère alphanumérique du numéro de carte, incrémenté à chaque renouvellement de la carte tachygraphique **correspondant à un numéro d'identification donné c'est-à-dire l'identification du conducteur ou du propriétaire de la carte accompagnée d'un indice séquentiel ;**

j) « indice de remplacement de la carte » :
le 15e caractère alphanumérique du numéro de carte, incrémenté à chaque remplacement de la carte tachygraphique **correspondant à un numéro d'identification donné, c'est-à-dire l'identification du conducteur ou du propriétaire de la carte accompagnée d'un indice séquentiel** ;

k) « coefficient caractéristique du véhicule » :

la caractéristique numérique donnant la valeur du signal de sortie émis par la partie du véhicule qui relie celui-ci à l'appareil de contrôle (arbre de sortie de la boîte de vitesses ou essieu) pendant que le véhicule se déplace sur une distance d'un kilomètre dans les conditions normales d'essai définies à l'exigence 414. Le coefficient caractéristique est exprimé en impulsions par kilomètre (w = … imp/km) ;

l) « carte d'entreprise » :

une carte tachygraphique délivrée par les autorités d'un**e** ~~État membre~~ **Partie contractante** à une entreprise de transport tenue d'utiliser des véhicules équipés d'un tachygraphe, ladite carte permettant l'identification de l'entreprise de transport ainsi que l'affichage, le téléchargement et l'impression des données stockées dans le tachygraphe, lesquelles ont été verrouillées par cette même entreprise ;

m) « constante de l'appareil de contrôle » :

Le nombre donnant la valeur du signal d'entrée nécessaire pour indiquer et enregistrer une distance parcourue d'un kilomètre. Cette constante est exprimée en impulsions par kilomètre (k = … imp/km) ;

n) « temps de conduite continue » calculé par l'appareil de contrôle[1] :

la somme des temps de conduite accumulés par un conducteur donné depuis la fin de sa dernière période de DISPONIBILITÉ ou d'INTERRUPTION/REPOS ou INCONNUE[2] de 45 minutes ou plus (cette période peut avoir été divisée comme prévu ~~dans le règlement (CE) n° 561/2006~~ **dans le présent Accord**). Les calculs tiennent compte, en tant que de besoin, des activités antérieures enregistrées sur la carte de conducteur. Lorsque le conducteur n'a pas inséré sa carte, les calculs se fondent sur les données enregistrées dans la mémoire pour la période en cours où aucune carte n'a été insérée et se rapportant au lecteur pertinent ;

o) « carte de contrôleur » :

une carte tachygraphique délivrée par les autorités d'un**e** ~~État membre~~ **Partie contractante** à une autorité nationale de contrôle compétente, qui permet l'identification de l'organisme de contrôle et, éventuellement, de l'agent de contrôle, ainsi que l'accès aux données stockées dans la mémoire ou sur les cartes de conducteur et, éventuellement, sur les cartes d'atelier, pour lecture, impression et/ou téléchargement ;

Elle donne également accès à la fonction de contrôle routier d'étalonnage et aux données du lecteur de communication à distance à des fins de détection précoce ;

p) « temps d'interruption cumulé » calculé par l'appareil de contrôle[1] :

la somme des périodes de DISPONIBILITÉ ou d'INTERRUPTION/REPOS ou INCONNUE[2] de 15 minutes ou plus accumulées par un conducteur donné, depuis la fin de sa dernière période de DISPONIBILITÉ ou d'INTERRUPTION/REPOS ou INCONNUE[2] de 45 minutes ou plus (cette période peut avoir été divisée conformément au ~~règlement (CE) n° 561/2006~~ **présent Accord**).

Les calculs tiennent compte, en tant que de besoin, des activités antérieures enregistrées sur la carte de conducteur. Les périodes inconnues de durée négative (début de la période inconnue > fin de la période inconnue) en raison de chevauchements temporels entre deux appareils de contrôle différents ne sont pas prises en compte dans les calculs.

Lorsque le conducteur n'a pas inséré sa carte, les calculs se fondent sur les données enregistrées dans la mémoire concernant la période en cours où aucune carte n'a été insérée et le lecteur approprié ;

---

[1] Ce mode de calcul du temps de conduite continu et du temps d'interruption cumulé permet à l'appareil de contrôle de lancer en temps voulu l'avertissement relatif au temps de conduite continu. Il ne préjuge pas l'interprétation légale de ces temps. D'autres modes de calcul du temps de conduite continu et du temps d'interruption cumulé peuvent être utilisés pour remplacer ceux prévus dans ces définitions si celles-ci ont été rendues obsolètes par la mise à jour d'autres instruments législatifs applicables.

[2] Les périodes marquées INCONNU correspondent à des périodes où la carte de conducteur n'a pas été insérée dans l'appareil de contrôle et pour lesquelles aucune saisie manuelle des activités du conducteur n'a été effectuée.

q) « mémoire » :

un dispositif de stockage de données électroniques installé dans l'appareil de contrôle ;

r) « signature numérique » :

les données attachées à un bloc de données, ou une transformation cryptographique de celui-ci, permettant à son destinataire d'avoir la preuve de son authenticité et de son intégrité ;

s) « téléchargement » :

la copie, avec signature numérique, d'une partie ou de la totalité d'un ensemble de fichiers de données enregistrés dans la mémoire de l'unité embarquée sur le véhicule ou dans la mémoire d'une carte tachygraphique, pour autant que ce processus ne modifie ni ne supprime aucune des données stockées ;

Les fabricants d'unités embarquées de tachygraphes intelligents et les fabricants d'équipements conçus pour télécharger des fichiers de données doivent prendre toutes les dispositions appropriées, dans la mesure du raisonnable, pour garantir que les entreprises de transport ou les conducteurs puissent procéder au téléchargement de ces données dans les meilleurs délais ;

Il se peut que le téléchargement du fichier contenant les relevés de la vitesse instantanée ne soit pas nécessaire pour établir la conformité avec ~~le règlement (CE) n° 561/2006~~ **le présent Accord**, mais il peut servir à d'autres fins, notamment à des fins d'enquête dans le cadre d'un accident ;

t) « carte de conducteur » :

une carte tachygraphique délivrée par les autorités d'un**e** ~~État membre~~ **Partie contractante** à un conducteur donné, qui permet l'identification du conducteur et le stockage des données relatives à son activité ;

u) « circonférence effective des pneumatiques » :

la moyenne des distances parcourues par chacune des roues entraînant le véhicule (roues motrices) lors d'une rotation complète. La mesure de ces distances est effectuée dans les conditions normales d'essai telles que définies à l'exigence 414 et est exprimée sous la forme « l = … mm ». Les constructeurs de véhicules peuvent remplacer la mesure de ces distances par un calcul théorique tenant compte de la répartition du poids du véhicule sur les essieux, à vide, **c'est-à-dire avec liquide de refroidissement, lubrifiants, carburant, outillage, roue de secours et conducteur,** et en ordre de marche[3]. Les méthodes suivies pour effectuer ce calcul théorique doivent être approuvées par une autorité compétente de ~~l'État membre~~ **la Partie contractante** et ne peuvent s'appliquer qu'avant l'activation du tachygraphe ;

v) « événement » :

une opération anormale détectée par le tachygraphe intelligent et pouvant résulter d'une tentative de fraude ;

w) « dispositif GNSS externe » :

un dispositif contenant le récepteur GNSS lorsque l'unité embarquée sur le véhicule n'est pas une unité intégrée, ainsi que les autres composants nécessaires à la protection de la communication des données de position au reste de l'unité embarquée ;

x) « anomalie » :

une opération anormale détectée par le tachygraphe intelligent et pouvant résulter d'un dysfonctionnement ou d'une panne de l'appareil ;

y) « récepteur GNSS » :

un dispositif électronique qui reçoit et traite numériquement les signaux émis par un ou plusieurs systèmes mondiaux de navigation par satellite (GNSS, abréviation de *Global Navigation Satellite System*) afin de fournir des informations sur la position, la vitesse et l'heure ;

[3] ~~Règlement (UE) n° 1230/2012 concernant les masses et dimensions de certaines catégories de véhicules à moteur et de leurs remorques et modifiant la directive 2007/46/CE, tel que modifié en dernier lieu.~~

z) « installation » :
le montage d'un tachygraphe dans un véhicule ;

aa) « interopérabilité » :
la capacité des systèmes et des processus sous-jacents à échanger des données et à partager des informations ;

bb) « interface » :
un dispositif mis en place entre les systèmes, qui leur permet de communiquer et d'interagir ;

cc) « position » :
les coordonnées géographiques du véhicule à un moment donné ;

dd) « capteur de mouvement » :
un composant du tachygraphe émettant un signal représentatif de la vitesse du véhicule et/ou de la distance parcourue par celui-ci ;

ee) « carte non valable » :
une carte considérée comme défectueuse, dont l'authentification ~~initiale~~ a échoué, dont la date de début de validité n'a pas encore été atteinte ou dont la date d'expiration est passée.

Une carte est aussi considérée comme non valable par l'unité embarquée sur le véhicule :

- **Si une carte délivrée par la même Partie contractante, avec le même numéro d'identification, c'est-à-dire la même identification de conducteur ou de propriétaire accompagnée d'un indice séquentiel, mais avec un indice de renouvellement plus élevé, a déjà été insérée dans l'unité embarquée ; ou**
- **Si une carte délivrée par la même Partie contractante, avec le même numéro d'identification, c'est-à-dire la même identification de conducteur ou de détenteur accompagnée d'un indice séquentiel et d'un indice de renouvellement, mais avec un indice de remplacement plus élevé, a déjà été insérée dans l'unité embarquée ;**

ff) « norme ouverte » :
une norme définie dans une spécification normalisée librement accessible ou disponible contre une somme symbolique, qu'il est permis de copier, de diffuser ou d'utiliser gratuitement ou pour une somme symbolique ;

gg) « hors champ » :
tous les cas où l'utilisation de l'appareil **de contrôle** n'est pas requise, conformément au ~~règlement (CE) n° 561/2006~~ **présent Accord ;**

hh) « excès de vitesse » :
le dépassement de la vitesse autorisée pour le véhicule, pendant toute période de plus de 60 secondes au cours de laquelle la vitesse mesurée du véhicule dépasse la limite fixée pour le réglage du dispositif limiteur de vitesse dans ~~la directive 92/6/CEE du Conseil du 10 février 1992 relative à l'installation et à l'utilisation, dans la Communauté, de limiteurs de vitesse sur certaines catégories de véhicules à moteur[4], telle que modifiée en dernier lieu~~ **le Règlement ONU nº 89 ;**

ii) « inspection périodique » :
une série d'opérations de contrôle réalisées pour s'assurer que le tachygraphe fonctionne correctement, que ses réglages correspondent aux paramètres du véhicule et qu'aucun dispositif de manipulation n'est adjoint au tachygraphe ;

jj) « imprimante » :
un composant de l'appareil de contrôle qui permet d'imprimer les données stockées ;

kk) « communication de détection précoce à distance » :
la communication entre le dispositif de communication à distance à des fins de détection précoce et le lecteur de communication à distance à des fins de détection précoce lors de

~~[4] JO L 57 du 2.3.1992, p. 27.~~

contrôles routiers ciblés afin de détecter à distance une éventuelle manipulation ou mauvaise utilisation de l'appareil de contrôle ;

ll) « dispositif de communication à distance », « module de communication à distance » ou « dispositif de détection précoce à distance » :
l'équipement de l'unité embarquée sur le véhicule utilisé pour effectuer des contrôles routiers ciblés ;

mm) « lecteur de communication à distance à des fins de détection précoce » :
le système utilisé par les agents de contrôle pour les contrôles routiers ciblés ;

nn) « renouvellement de la carte » :
la délivrance d'une nouvelle carte tachygraphique lorsqu'une carte arrive à expiration ou ne fonctionne pas correctement et a été retournée à l'autorité qui l'a délivrée ~~; le renouvellement suppose la certitude que deux cartes en cours de validité ne coexistent pas~~ ;

oo) « réparation » :
toute réparation d'un capteur de mouvement, d'une unité embarquée ou d'un câble qui impose de le ou de la déconnecter de son alimentation électrique ou d'autres composants du tachygraphe, ou d'ouvrir le capteur de mouvement ou l'unité embarquée ;

pp) « remplacement de la carte » :
la délivrance d'une **nouvelle** carte tachygraphique en remplacement d'une carte existante qui a été déclarée perdue, volée ou défectueuse, et n'a pas été retournée à l'autorité qui l'a délivrée ~~; le remplacement comporte toujours le risque que deux cartes en cours de validité coexistent~~ ;

qq) « certification de sécurité » :
le processus par lequel un organisme de certification Critères communs certifie que l'appareil de contrôle (ou le composant de cet appareil) ou la carte tachygraphique objet de la procédure satisfait aux exigences de sécurité définies dans les profils de protection correspondants ;

rr) « autotest » :
des tests automatiques effectués périodiquement par l'appareil de contrôle afin de déceler les anomalies ;

ss) « mesure du temps » :
un enregistrement numérique en continu de la date et du temps universel coordonné (UTC) ;

tt) « remise à l'heure » :
un réglage ~~automatique~~ de l'heure actuelle**, qui peut être exécuté de manière automatique** ~~à intervalles réguliers et dans la limite d'une tolérance maximale d'une minute~~ **sur la base de l'heure fournie par le récepteur GNSS**, ou être effectué ~~un réglage pendant l'~~ **en mode** étalonnage ;

uu) « dimension des pneumatiques » :
la désignation des dimensions des pneumatiques (roues motrices externes) conformément ~~à la directive 92/23/CEE du 31 mars 1992[5], telle que modifiée en dernier lieu~~ **au Règlement ONU nº 54** ;

vv) « identification du véhicule » :
les numéros permettant d'identifier le véhicule : numéro d'immatriculation du véhicule (VRN) avec indication de ~~l'État membre~~ **la Partie contractante** d'immatriculation et numéro d'identification du véhicule (VIN) ;

ww) « semaine » pour les calculs dans l'appareil de contrôle :
la période comprise entre 00 h 00 le lundi et 24 h 00 le dimanche (heure UTC) ;

xx) « carte d'atelier » :
une carte tachygraphique délivrée par les autorités d'un**e** ~~État membre~~ **Partie contractante** à certains membres du personnel d'un fabricant de tachygraphes, d'un installateur, d'un constructeur de véhicules ou d'un atelier, homologué par cet**te** ~~État membre~~ **Partie contractante**. La carte d'atelier indique l'identité du détenteur et permet de procéder à

~~[5] JO L 129 du 14.5.1992, p. 95.~~

l'essai, à l'étalonnage et à l'activation des tachygraphes, et/ou au téléchargement à partir de ceux-ci ;

yy) « adaptateur » :

un dispositif qui émet un signal permanent représentatif de la vitesse du véhicule et/ou de la distance parcourue, autre que celui utilisé pour la détection indépendante du mouvement, et qui est :

- Installé et utilisé uniquement sur les véhicules des catégories M1 et N1 (tels que définis ~~à l'annexe II de la directive 2007/46/CE du Conseil, telle que modifiée en dernier lieu) mis en circulation pour la première fois après le 1er mai 2006,~~ **dans la Résolution d'ensemble sur la construction des véhicules (R.E.3), révision 6, du 11 juillet 2017, ECE/TRANS/WP.29/78/Rev.6) ;**
- Installé lorsqu'il n'est pas mécaniquement possible d'installer un autre type de capteur de mouvement par ailleurs conforme aux dispositions ~~de la~~ **du** présent~~e annexe~~ **appendice** et de ses **sous-**appendices 1 à 15 ;
- Installé entre l'unité embarquée sur le véhicule et le point d'où les impulsions de distance et de vitesse sont générées par des capteurs intégrés ou d'autres interfaces.
- L'adaptateur a le même fonctionnement qu'un capteur de mouvement, conforme aux dispositions **due** ~~la~~ présent~~e annexe~~ **appendice** et de ses **sous-**appendices 1 à 16, connecté à l'unité embarquée sur le véhicule.

L'utilisation d'un tel adaptateur dans les véhicules décrits ci-dessus permet l'installation et l'utilisation correcte d'une unité embarquée conforme à l'ensemble des exigences ~~de la~~ **du** présent~~e annexe~~ **appendice.** Pour ces véhicules, le tachygraphe intelligent comprend des câbles, un adaptateur et une unité embarquée ;

zz) « intégrité des données » :

la précision et la cohérence des données stockées, indiquées par l'absence de toute modification des données entre deux mises à jour d'un enregistrement de données. L'intégrité implique que les données soient la copie exacte de leur version originale et qu'elles n'aient par exemple pas été altérées lors des processus d'écriture sur une carte tachygraphique ou un dispositif dédié et de lecture à partir de ceux-ci, ou lors de leur transmission via un canal de communication quel qu'il soit ;

~~**aaa) « confidentialité des données » :**~~

les ~~mesures techniques globales prises pour assurer la bonne mise en œuvre des principes énoncés dans la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, ainsi que de ceux énoncés dans la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;~~

aaa) réservé

bbb) « tachygraphe intelligent » :

l'appareil de contrôle, les cartes tachygraphiques et l'ensemble des équipements qui interagissent directement ou indirectement au cours de leur fabrication, de leur installation, de leur utilisation, des essais et des contrôles, tels que les cartes, les lecteurs de communication à distance et tout autre équipement servant au téléchargement, à l'analyse de données, à l'étalonnage, de même qu'à la conception, à la gestion ou à la mise en œuvre d'éléments de sécurité, etc. ;

Les tachygraphes intelligents sont des appareils de contrôle conformes à l'appendice 1C du présent Accord.

ccc) « date de lancement » :

~~36 mois après l'entrée en vigueur des dispositions détaillées visées à l'article 11 du règlement (UE) n° 165/2014.~~

~~*Il s'agit de l*~~***1***~~*a*~~ *date à partir de laquelle les véhicules immatriculés pour la première fois* ***doivent être équipés d'un tachygraphe conformément au présent Accord ;~~*~~***:**

~~— doivent être équipés d'un tachygraphe connecté à un service de positionnement s'appuyant sur un système de navigation par satellite,~~

— doivent ~~être capables, lorsque le véhicule est en mouvement, de communiquer des données aux autorités de contrôle compétentes à des fins de contrôles routiers ciblés,~~

~~— et peuvent être équipés d'une interface normalisée permettant l'utilisation en mode opérationnel, par un dispositif extérieur, des données enregistrées ou produites par le tachygraphe ;~~

ddd) « profil de protection » :
un document utilisé dans le cadre d'un processus de certification selon les Critères communs, qui définit, indépendamment de toute mise en œuvre, les exigences en matière de sécurité et de garantie de l'information ;

eee) « précision GNSS » :
dans le cadre de l'enregistrement de la position fournie par le système mondial de navigation par satellite (GNSS) par les tachygraphes, la valeur du coefficient d'affaiblissement de la précision du positionnement horizontal (HDOP) calculée comme la minimale des valeurs HDOP recueillies par les systèmes GNSS disponibles.

fff) « temps de conduite accumulé » :
une valeur représentant le nombre total de minutes de conduite accumulées par un véhicule donné.

Le temps de conduite accumulé est un décompte libre de toutes les minutes considérées comme de la CONDUITE par la fonction de suivi des activités de conduite de l'appareil de contrôle, et n'est employé que pour déclencher l'enregistrement de la position du véhicule, chaque fois qu'un multiple de trois heures de temps de conduite accumulé est atteint. L'accumulation commence dès l'activation de l'appareil de contrôle. Elle n'est pas influencée par d'autres conditions, telles que les conditions hors champ ou trajet en ferry/train. Le temps de conduite accumulé n'est pas destiné à être affiché, imprimé ou téléchargé ;

ggg) « masse à vide du véhicule en état de marche » :

a) Dans le cas d'un véhicule à moteur :
la masse du véhicule, avec son ou ses réservoirs à carburant remplis à au moins 90 % de leur capacité, y compris la masse du conducteur, du carburant et des liquides, muni de l'équipement de série tel que spécifié par le constructeur et, lorsqu'ils sont montés, de la carrosserie, de la cabine, de l'attelage et de la ou des roues de secours, ainsi que de l'outillage de bord ;

b) Dans le cas d'une remorque :
la masse du véhicule, y compris le carburant et les liquides, muni de l'équipement de série tel que spécifié par le constructeur et, lorsqu'ils sont montés, la masse de la carrosserie, du ou des attelages additionnels, de la ou des roues de secours, ainsi que de l'outillage de bord ;

hhh) « numéro d'identification du véhicule » :
une combinaison de caractères fixe attribuée à chaque véhicule par le constructeur et constituée de deux parties : la première, composée de six caractères au maximum (lettres ou chiffres), indique les caractéristiques générales du véhicule, en particulier le type et le modèle ; la seconde, composée de huit caractères dont les quatre premiers peuvent être des lettres ou des chiffres et les quatre autres uniquement des chiffres, permet, en association avec la première partie, d'identifier clairement un véhicule donné.

2. Caractéristiques générales et fonctions de l'appareil de contrôle

2.1 Caractéristiques générales

La fonction de l'appareil de contrôle est d'enregistrer, de stocker, d'afficher, d'imprimer et de produire des données concernant les activités du conducteur.

Tout véhicule équipé d'un appareil de contrôle conforme aux dispositions ~~de la~~ **du** présente ~~annexe~~ **appendice** doit comporter un indicateur de vitesse et un compteur kilométrique. Ces fonctions peuvent être intégrées dans l'appareil de contrôle.

1) L'appareil de contrôle comprend des câbles, un capteur de mouvement et une unité embarquée.

2) L'interface entre les capteurs de mouvement et les unités embarquées doivent être conformes aux exigences d~~e l'appendice~~ **du sous-appendice** 11.

3) L'unité embarquée sur le véhicule doit être connectée à un ou plusieurs systèmes mondiaux de navigation par satellite, comme spécifié ~~à l'appendice~~ **au sous-appendice** 12.

4) L'unité embarquée sur le véhicule (ci-après UEV, avec comme équivalent anglais VU pour « Vehicle Unit ») doit communiquer avec des lecteurs de communication à distance à des fins de détection précoce, comme spécifié ~~à l'appendice~~ **au sous-appendice** 14.

5) L'unité embarquée sur le véhicule ~~peut~~ **doit** comporter une interface STI, dont les caractéristiques sont définies ~~à l'appendice~~ **au sous-appendice** 13. L'appareil de contrôle peut être relié à d'autres équipements par l'intermédiaire d'interfaces supplémentaires et/ou de l'interface STI ~~facultative~~.

6) Toute insertion ou connexion de toute fonction ou de tout dispositif, homologué ou non, dans ou à l'appareil de contrôle, ne doit pas interférer ou être susceptible d'interférer avec le fonctionnement correct et sûr de l'appareil de contrôle, ni avec les dispositions du présent ~~règlement~~ **Accord**. Les utilisateurs de l'appareil de contrôle s'identifient dans l'appareil à l'aide de cartes tachygraphiques.

7) L'appareil de contrôle ouvre des droits d'accès sélectifs aux données et aux fonctions, selon le type et/ou l'identité de l'utilisateur. L'appareil de contrôle enregistre et stocke des données dans sa mémoire, dans le dispositif de communication à distance et sur les cartes tachygraphiques.

~~Ces fonctions sont assurées dans le respect de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[6], de la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[7] et en conformité avec l'article 7 du règlement (UE) n° 165/2014.~~

2.2 Fonctions

8) L'appareil de contrôle doit assurer les fonctions suivantes :

- Contrôle des insertions et retraits de cartes ;
- Mesure de la vitesse, de la distance parcourue et de la position ;
- Mesure du temps ;
- Suivi des activités du conducteur ;
- Suivi de la situation de conduite ;

~~[6] JO L 281 du 23.11.1995, p. 31.~~

~~[7] JO L 201 du 31.7.2002, p. 37.~~

- Saisie manuelle de données par le conducteur :
  - Lieu de début et/ou de fin des périodes de travail journalières ;
  - Saisie manuelle des activités du conducteur **et consentement du conducteur pour l'interface STI** ;
  - Saisie des conditions particulières ;
  - **Saisie des opérations de chargement/déchargement ;**
- Gestion des verrouillages d'entreprise ;
- Suivi des activités de contrôle ;
- Détection des événements et/ou des anomalies ;
- Autotests et tests intégrés ;
- Lecture des données stockées dans la mémoire ;
- Enregistrement et stockage de données dans la mémoire ;
- Lecture des cartes tachygraphiques ;
- Enregistrement et stockage de données sur les cartes tachygraphiques ;
- Affichage ;
- Impression ;
- Avertissement ;
- Téléchargement de données vers des supports externes ;
- Communication à distance pour les contrôles routiers ciblés ;
- Envoi de données vers d'autres dispositifs externes ;
- Étalonnage ;
- Contrôle routier d'étalonnage ;
- Remise à l'heure ;
- **Surveillance des passages de frontières ;**
- **Mise à jour logicielle.**

2.3 Modes de fonctionnement

9) L'appareil de contrôle doit disposer de quatre modes de fonctionnement :

- Mode opérationnel ;
- Mode contrôle ;
- Mode étalonnage ;
- Mode entreprise.

10) L'appareil de contrôle doit basculer dans les modes de fonctionnement suivants selon la carte tachygraphique valable insérée dans l'interface destinée aux cartes. La génération de la carte tachygraphique n'entre pas en compte dans la sélection du mode de fonctionnement, pour autant que la carte insérée soit valable. Une carte d'atelier de première génération doit toujours être considérée comme non valable lorsqu'elle est insérée dans une UEV de deuxième génération.

Mode de fonctionnement		Lecteur « conducteur »				
		Pas de carte	Carte de conducteur	Carte de contrôleur	Carte d'atelier	Carte d'entreprise
Lecteur « co-conducteur »	Pas de carte	Opérationnel	Opérationnel	Contrôle	Étalonnage	Entreprise
	Carte de conducteur	Opérationnel	Opérationnel	Contrôle	Étalonnage	Entreprise
	Carte de contrôleur	Contrôle	Contrôle	Contrôle(*)	Opérationnel	Opérationnel
	Carte d'atelier	Étalonnage	Étalonnage	Opérationnel	Étalonnage(*)	Opérationnel
	Carte d'entreprise	Entreprise	Entreprise	Opérationnel	Opérationnel	Entreprise(*)

(*) En pareil cas, l'appareil de contrôle utilise uniquement la carte tachygraphique insérée dans le lecteur « conducteur ».

11) L'appareil de contrôle doit refuser les cartes non valables, sauf pour l'affichage, l'impression ou le téléchargement des données présentes sur une carte périmée, qui doivent demeurer possibles.

12) Toutes les fonctions énumérées à la section 2.2 doivent être disponibles dans tous les modes de fonctionnement, à l'exception de :

- La fonction d'étalonnage, accessible uniquement en mode étalonnage ;
- La fonction de contrôle routier d'étalonnage, accessible uniquement en mode contrôle ;
- La fonction de gestion des verrouillages d'entreprise, accessible uniquement en mode entreprise ;
- Le suivi des activités de contrôle, accessible uniquement en mode contrôle ;
- La fonction de téléchargement, inaccessible en mode opérationnel, ~~(sauf dans les cas prévus à l'exigence 193),~~ à l'exception :
  - Conformément à l'exigence 193 ;
  - Du téléchargement d'une carte de conducteur lorsqu'aucun autre type de carte n'est insérée dans l'UEV.

13) L'appareil de contrôle peut extraire toute donnée pour affichage, impression ou téléchargement vers des interfaces externes, sauf dans les cas suivants :

- En mode opérationnel, toute donnée d'identification personnelle (nom et prénom(s)) ne correspondant pas à la carte tachygraphique insérée doit être masquée, et tout numéro de carte ne correspondant pas à la carte tachygraphique insérée doit être partiellement masqué (un caractère sur deux, de gauche à droite) ;
- En mode entreprise, les données relatives au conducteur (exigences 102, 105**,** ~~et~~ 108**, 133a et 133e**) peuvent être extraites seulement pour les périodes où aucun verrouillage n'existe ou où aucune autre entreprise (telle qu'identifiée par les 13 premiers chiffres du numéro de la carte d'entreprise) ne détient de verrouillage ;
- Lorsqu'aucune carte n'est insérée dans l'appareil de contrôle, seules peuvent être extraites les données relatives au conducteur pour le jour même et les 8 jours civils précédents ;
- Les données à caractère personnel **enregistrées et produites par le tachygraphe ou les cartes tachygraphiques** ~~provenant de l'UEV~~ ne doivent pas être extraites par l'intermédiaire de l'interface STI de l'UEV sans que le consentement du conducteur auquel elles se rapportent soit vérifié ;

– Les unités embarquées ont une période de validité opérationnelle normale de 15 ans, à partir de la date de **prise d'effet de** ~~délivrance de~~ leurs certificats, mais peuvent être utilisées pendant 3 mois supplémentaires, uniquement aux fins du téléchargement de données.

2.4 Sécurité

La sécurité du système vise à protéger la mémoire de manière à empêcher l'accès non autorisé aux données et leur manipulation, et à détecter toutes tentatives en ce sens, à préserver l'intégrité et l'authenticité des données échangées entre le capteur de mouvement et l'unité embarquée sur le véhicule, entre l'appareil de contrôle et les cartes tachygraphiques et**, le cas échéant,** entre l'appareil de contrôle et le dispositif GNSS externe, à préserver la confidentialité, l'intégrité et l'authenticité des données échangées dans le cadre de la communication de détection précoce à distance à des fins de contrôle, et enfin à vérifier l'intégrité et l'authenticité des données téléchargées.

14) Afin de garantir la sécurité du système, les composants suivants doivent satisfaire aux exigences définies dans leur profil de protection respectif, comme prévu ~~à l'appendice~~ **au sous-appendice** 10 :

– L'unité embarquée sur le véhicule ;

– La carte tachygraphique ;

– Le capteur de mouvement ;

– Le dispositif GNSS externe (ce profil n'est nécessaire et applicable que pour la variante externe du **dispositif** GNSS).

3. Exigences de construction et de fonctionnement applicables à l'appareil de contrôle

3.1 Contrôle des cartes ~~l'insertion~~ et des retraits ~~des cartes~~

15) L'appareil de contrôle doit assurer le suivi des insertions et retraits de carte.

16) Lors de l'insertion d'une carte **(ou de son authentification à distance)**, l'appareil de contrôle vérifie que la carte tachygraphique est valable **au sens de la définition ee) de la section 1,** et, si c'est le cas, détermine son type et la génération à laquelle elle appartient.

Si ~~une carte portant le même numéro de carte et un indice de renouvellement supérieur a déjà été insérée dans l'appareil de contrôle, la carte est déclarée non valable. Si une carte portant le même numéro de carte et le même indice de renouvellement, mais un indice de remplacement supérieur, a déjà été insérée dans l'appareil de contrôle, la carte est déclarée non valable.~~

Pour vérifier si une carte a déjà été insérée, l'appareil de contrôle doit utiliser les données relatives aux cartes tachygraphiques qui sont stockées dans sa mémoire, comme indiqué à l'exigence 133.

17) Les cartes tachygraphiques de première génération doivent être considérées comme non valables par l'appareil de contrôle après que la possibilité d'utiliser des cartes tachygraphiques de première génération a été supprimée par un atelier, conformément ~~à l'appendice~~ **au sous-appendice** 15 (exigence ~~MIG003~~ **MIG_003**).

18) Les cartes d'atelier de première génération qui sont insérées dans l'appareil de contrôle de deuxième génération doivent être considérées comme non valables.

19) L'appareil de contrôle doit être conçu de telle manière que les cartes tachygraphiques soient verrouillées en position lorsqu'elles sont correctement insérées dans l'interface destinée aux cartes.

20) Le retrait d'une carte tachygraphique n'est possible que lorsque le véhicule est à l'arrêt, et après que les données pertinentes ont été enregistrées sur la carte. Le retrait de la carte nécessite une action concrète de l'utilisateur.

3.2 Mesure de la vitesse, de la position et de la distance parcourue

21) Le capteur de mouvement (éventuellement intégré dans l'adaptateur) est le principal instrument de mesure de la vitesse et de la distance parcourue.

22) Cette fonction assure la mesure et l'affichage en continu de la valeur kilométrique correspondant à la distance totale parcourue par le véhicule en utilisant les impulsions envoyées par le capteur de mouvement.

23) Cette fonction assure la mesure et l'affichage en continu de la vitesse du véhicule en utilisant les impulsions envoyées par le capteur de mouvement.

24) La fonction de mesure de la vitesse doit également indiquer si le véhicule est en mouvement ou à l'arrêt. Le véhicule est considéré en mouvement dès que la fonction détecte plus de 1 imp/s pendant au moins 5 secondes en provenance du capteur de mouvement, et dans le cas contraire, le véhicule est considéré comme à l'arrêt.

25) Les dispositifs indicateurs de vitesse (compteur de vitesse) et de distance totale parcourue (compteur kilométrique) installés sur tout véhicule muni d'un appareil de contrôle conforme aux dispositions du présent ~~règlement~~ **Accord** doivent satisfaire aux exigences concernant les tolérances maximales (voir points 3.2.1 et 3.2.2) énoncées dans ~~la~~ **le** présente ~~annexe~~ **appendice**.

26) Pour détecter la manipulation des données de mouvement, les informations provenant du capteur de mouvement sont corroborées par les informations relatives au mouvement du véhicule provenant du récepteur GNSS et ~~éventuellement~~ d'une ou plusieurs autres sources indépendantes du capteur de mouvement. **Au moins une autre source indépendante d'informations sur le mouvement du véhicule doit être intégrée à l'UEV sans qu'une interface externe soit nécessaire.**

27) Cette fonction doit mesurer la position du véhicule afin de permettre l'enregistrement ~~automatique~~ :

- Des positions correspondant aux lieux où le conducteur et/ou le co-conducteur commencent leur période de travail journalière ;
- Des positions correspondant aux lieux où le temps de conduite ~~continue~~ **accumulé** ~~du conducteur~~ atteint un multiple de trois heures ;
- **Des positions correspondant aux lieux où le véhicule a franchi la frontière d'un pays ;**
- **Des positions correspondant aux lieux où des opérations de chargement ou de déchargement ont été effectuées ;**
- Des positions correspondant aux lieux où le conducteur et/ou le co-conducteur terminent leur période de travail journalière.

3.2.1 Mesure de la distance parcourue

28) La distance parcourue peut être mesurée de manière :

- Soit à cumuler les mouvements en marche avant et en marche arrière ;
- Soit à prendre uniquement en compte les mouvements en marche avant.

29) L'appareil de contrôle mesure la distance parcourue de 0 à 9 999 999,9 km.

30) La distance mesurée doit respecter les tolérances suivantes (distances d'au moins 1 000 m) :

- ±1 % avant installation ;

– ±2 % lors de l'installation et des inspections périodiques ;

– ±4 % en service.

Les tolérances ne doivent pas être utilisées pour modifier intentionnellement la distance mesurée.

31) La distance mesurée doit avoir une résolution égale à 0,1 km ou meilleure.

3.2.2 Mesure de la vitesse

32) L'appareil de contrôle mesure la vitesse de 0 à 220 km/h.

33) Afin de garantir une tolérance maximale sur la vitesse affichée de ±6 km/h en service, et compte tenu :

– D'une tolérance de ±2 km/h pour les variations du signal entrant (variations dues aux pneumatiques, entre autres) ; et

– D'une tolérance de ±1 km/h sur les mesures effectuées au cours de l'installation et des inspections périodiques,

l'appareil de contrôle doit, pour les vitesses comprises entre 20 et 180 km/h et pour des coefficients caractéristiques du véhicule compris entre **2** 400~~0~~ et 25 000 imp/km, mesurer la vitesse avec une tolérance de ±1 km/h (à vitesse constante).

Remarque : la résolution des données stockées entraîne une tolérance additionnelle de ±0,5 km/h sur la vitesse stockée par l'appareil de contrôle.

34) La vitesse doit être mesurée correctement dans les tolérances normales et dans les 2 secondes qui suivent la fin d'un changement de vitesse lorsque la vitesse a changé à un rythme allant jusqu'à 2 m/s².

35) La mesure de la vitesse doit avoir une résolution égale à 1 km/h ou meilleure.

3.2.3 Mesure de la position

36) L'appareil de contrôle mesure la position absolue du véhicule à l'aide du récepteur GNSS.

37) La position absolue ~~est~~ **doit être** mesurée sous forme de coordonnées géographiques en degrés et minutes de latitude et de longitude, avec une résolution d'un dixième de minute.

3.3 Mesure du temps

38) La fonction de mesure du temps assure une mesure en continu et un affichage numérique de la date et de l'heure UTC.

39) La date et l'heure UTC sont utilisées pour dater les données à l'intérieur de l'appareil de contrôle (enregistrements, échange de données) et pour tous les tirages papier spécifiés ~~à l'appendice~~ **au sous-appendice** 4 (Impressions).

40) Afin de visualiser l'heure locale, il doit être possible de changer le décalage horaire de l'heure affichée par paliers d'une demi-heure. Aucun décalage horaire autre qu'un multiple positif ou négatif de la demi-heure n'est autorisé.

41) La dérive temporelle ne doit pas excéder ±~~2~~**21** seconde~~s~~ par jour, dans **des conditions de température** ~~les conditions d'homologation~~ **conformes à l'exigence 213**, en l'absence de toute remise à l'heure.

41a) Lorsque le réglage de l'heure est effectué en atelier conformément à l'exigence 212, l'heure doit être établie avec une précision de 3 secondes ou mieux.

41b) L'unité embarquée sur le véhicule doit comporter un compteur de dérive qui calcule la dérive temporelle maximale depuis le dernier réglage de l'heure effectué conformément au point 3.23. La dérive temporelle maximale est définie par le fabricant

de l'unité embarquée et ne doit pas dépasser 1 seconde par jour, comme indiqué à l'exigence 41.

41c) Le compteur de dérive doit être remis à 1 seconde après chaque réglage de l'heure de l'appareil de contrôle conformément au point 3.23, y compris :

- **Les réglages automatiques de l'heure ;**
- **Les réglages de l'heure effectués en mode étalonnage.**

42) La mesure du temps doit avoir une résolution égale à 1 seconde ou meilleure.

43) La mesure du temps ne doit pas être affectée par une coupure de l'alimentation électrique externe d'une durée inférieure à 12 mois dans les conditions d'homologation.

3.4 Suivi des activités du conducteur

44) Cette fonction assure une surveillance permanente et séparée des activités d'un conducteur et d'un co-conducteur.

45) L'activité du conducteur doit être l'une des activités suivantes : CONDUITE, TRAVAIL, DISPONIBILITÉ ou INTERRUPTION/REPOS.

46) Il doit être possible au conducteur et/ou au co-conducteur de sélectionner manuellement les activités TRAVAIL, DISPONIBILITÉ ou INTERRUPTION/REPOS.

47) Lorsque le véhicule est en mouvement, l'activité CONDUITE doit être automatiquement sélectionnée pour le conducteur, et l'activité DISPONIBILITÉ doit être automatiquement sélectionnée pour le co-conducteur.

48) Lorsque le véhicule s'arrête, l'activité TRAVAIL doit être automatiquement sélectionnée pour le conducteur.

49) Le premier changement d'activité vers **INTERRUPTION/**REPOS ou DISPONIBILITÉ intervenant dans les 120 secondes qui suivent la sélection automatique de l'activité TRAVAIL en raison de l'arrêt du véhicule doit être considéré comme étant intervenu au moment de l'arrêt du véhicule (et peut par conséquent annuler le passage à l'activité TRAVAIL).

50) Cette fonction doit transmettre les changements d'activité vers les fonctions d'enregistrement avec une résolution d'une minute.

51) Étant donné une minute civile, si l'activité CONDUITE est enregistrée tant au cours de la minute qui précède que de la minute qui suit immédiatement, la minute entière est comptabilisée comme de la CONDUITE.

52) Étant donné une minute civile qui n'est pas comptabilisée comme de la CONDUITE en application de l'exigence 51, la minute entière sera considérée comme relevant de la même activité que l'activité continue la plus longue survenue dans la minute (ou de la plus récente dans le cas de plusieurs activités de même durée).

53) Cette fonction doit également permettre le suivi permanent du temps de conduite continu et du temps d'interruption cumulé du conducteur.

3.5 Suivi de la situation de conduite

54) Cette fonction assure en permanence et automatiquement le suivi de la situation de conduite.

55) La situation de conduite ÉQUIPAGE doit être sélectionnée lorsque deux cartes de conducteur en cours de validité sont insérées dans l'appareil, et la situation de conduite SEUL doit être sélectionnée dans tous les autres cas.

3.6 Saisie par le conducteur

3.6.1 Saisie du lieu de début et/ou de fin de la période de travail journalière

56) Cette fonction doit permettre la saisie des lieux où, selon le conducteur et/ou le co-conducteur, leurs périodes de travail journalières commencent et/ou se terminent.

57) On entend par « lieu » le pays et, le cas échéant, la région~~, qui sont saisis ou confirmés manuellement~~.

58) Lors du retrait d'une carte de conducteur **(ou d'atelier)**, l'appareil de contrôle **affiche la position actuelle du véhicule sur la base des informations fournies par le récepteur GNSS et par la carte numérique stockées conformément au point 3.12.19, et demande au détenteur de la carte de confirmer ou de rectifier manuellement la position** ~~inviter le conducteur/co-conducteur à saisir le «lieu où s'achève la période de travail journalière»~~.

59) **Le lieu saisi conformément à l'exigence 58 doit être considéré comme le lieu où se termine la période de travail journalière. Il est enregistré temporairement sur la carte de conducteur (ou d'atelier) correspondante, et pourra être écrasé ultérieurement** ~~conducteur renseigne alors l'emplacement actuel du véhicule, ce qui est considéré comme la saisie temporaire~~.

Dans les conditions suivantes, la saisie temporaire effectuée lors du dernier retrait de la carte est validée (c'est-à-dire qu'elle ne peut plus être écrasée) :

- La saisie d'un lieu où débute la période de travail journalière en cours lors de la saisie manuelle en application de l'exigence 61 ;
- La saisie suivante d'un lieu où débute la période de travail journalière en cours si le détenteur de la carte **ne** renseigne **aucun** lieu de début ou de fin de la période travail lors de la saisie manuelle en application de l'exigence 61.

Dans les conditions suivantes, la saisie temporaire effectuée lors du dernier retrait de la carte est écrasée et la nouvelle saisie est validée :

- La saisie suivante du lieu où s'achève la période de travail en cours si le détenteur de la carte ne renseigne aucun lieu de début ou de fin de la période de travail lors de la saisie manuelle en application de l'exigence 61.

60) Il doit être possible de saisir le lieu de début et/ou de fin d'une période de travail journalière au moyen de commandes se trouvant dans les menus. Si plusieurs saisies de ce type sont effectuées au cours d'une minute civile, seuls le dernier lieu de début et le dernier lieu de fin saisis pendant cette durée sont gardés enregistrés.

L'appareil de contrôle affiche la position actuelle du véhicule sur la base des informations fournies par le récepteur GNSS et par la carte numérique stockée conformément au point 3.12.19, et demande au conducteur de confirmer ou de rectifier manuellement la position.

3.6.2 Saisie manuelle des activités du conducteur et consentement du conducteur pour l'interface STI

61) Lors de l'insertion d'une carte de conducteur (ou d'atelier), et seulement à ce moment, l'appareil de contrôle doit permettre la saisie manuelle d'activités. La saisie manuelle d'activités est effectuée en indiquant la date et l'heure locale du fuseau horaire (décalage UTC) sélectionné pour l'unité embarquée.

Lors de l'insertion de la carte de conducteur ou d'atelier, les informations suivantes sont rappelées au détenteur de la carte :

- La date et l'heure du dernier retrait de la carte ;
- Facultativement, le décalage de l'heure locale sélectionné pour l'unité embarquée.

Lors de la première insertion d'une carte de conducteur ou d'atelier qui est encore inconnue de l'unité embarquée, le détenteur est invité à donner son accord pour que les données personnelles liées au tachygraphe puissent être extraites par l'intermédiaire de l'interface STI

~~facultative~~. **Pour vérifier si une carte a déjà été insérée, l'appareil de contrôle doit utiliser les données relatives aux cartes tachygraphiques stockées dans sa mémoire, comme indiqué à l'exigence 133.**

Le consentement du conducteur/de l'atelier peut être activé ou désactivé à tout moment par des commandes se trouvant dans le menu, à condition que la carte du conducteur/de l'atelier soit insérée.

Il doit être possible de saisir des activités, moyennant les restrictions suivantes :

- Le type d'activité doit être TRAVAIL, DISPONIBILITÉ ou INTERRUPTION/ REPOS ;
- Les heures de début et de fin pour chaque activité doivent se situer exclusivement dans la période séparant le dernier retrait de l'insertion actuelle de la carte ;
- Les activités ne doivent pas se chevaucher dans le temps.

Il doit être possible d'effectuer des saisies manuelles, si nécessaire, lors de la première insertion d'une carte de conducteur (ou d'atelier) encore inutilisée.

La procédure de saisie manuelle d'activités comprend autant d'étapes consécutives que nécessaire pour permettre la sélection d'un type, d'une heure de début et d'une heure de fin pour chaque activité. Pour toute partie de la période séparant le dernier retrait de la carte de son insertion actuelle, le détenteur a le choix de ne déclarer aucune activité.

Dans le cadre des saisies manuelles associées à l'insertion de la carte, le détenteur de celle-ci a, le cas échéant, la possibilité de saisir :

- Un lieu où s'est achevée une période de travail journalière précédente, associé à l'heure correspondante (modifiant ainsi la saisie effectuée lors du dernier retrait de la carte **et la validant**) ;
- Le lieu où débute la période de travail journalière en cours, associé à l'heure correspondante **(validant ainsi une saisie temporaire effectuée lors du dernier retrait de la carte)**.

En ce qui concerne le lieu de début de la période de travail journalière en cours saisi à l'insertion de la carte, l'appareil de contrôle affiche la position actuelle du véhicule sur la base des informations fournies par le récepteur GNSS et par la ou les cartes numériques stockées conformément au point 3.12.19, et demande au conducteur de la confirmer ou de la rectifier manuellement.

Si le détenteur de la carte ne renseigne aucun lieu de début ou de fin de la période de travail lors des saisies manuelles associées à l'insertion de la carte, le logiciel considère qu'il s'agit d'une déclaration de période de travail identique à celle associée au précédent retrait de la carte. La saisie suivante d'un lieu où s'est achevée une période de travail journalière précédente se substitue alors à la saisie temporaire effectuée lors du dernier retrait de la carte.

En cas de saisie d'un lieu, celui-ci est enregistré sur la carte tachygraphique appropriée.

La saisie manuelle est interrompue :

- Si la carte est retirée ; ou
- Si le véhicule est mis en mouvement alors que la carte se trouve dans le lecteur réservé au conducteur.

D'autres interruptions sont autorisées, par exemple une temporisation après une certaine période d'inactivité de l'utilisateur. En cas d'interruption de la saisie manuelle, l'appareil de contrôle valide toute saisie complète de lieu et d'activité déjà effectuée (indiquant sans ambiguïté un lieu et une heure, ou un type d'activité, une heure de début et une heure de fin).

Si une seconde carte de conducteur ou d'atelier est insérée alors que la saisie manuelle d'activités est en cours pour une carte insérée auparavant, la saisie concernant cette première carte doit pouvoir être achevée avant le début de la saisie manuelle concernant la seconde carte.

Le détenteur de la carte a la possibilité d'effectuer une saisie manuelle selon la procédure minimale suivante :

- La saisie manuelle des activités s'effectue par ordre chronologique pour la période allant du dernier retrait de la carte à son insertion actuelle ;
- L'heure de début de la première activité est fixée à l'heure du retrait de la carte. Pour chaque saisie ultérieure, l'heure de début présélectionnée suit immédiatement l'heure de fin de la saisie précédente. Un type d'activité et une heure de fin doivent être sélectionnés pour chaque activité.

La procédure se termine lorsque l'heure de fin d'une activité saisie manuellement correspond à l'heure d'insertion de la carte.

L'appareil de contrôle doit permettre aux conducteurs et aux ateliers d'effectuer successivement des saisies manuelles qui doivent être introduites au cours de la procédure par l'intermédiaire de l'interface STI spécifiée au sous-appendice 13 et, éventuellement, par l'intermédiaire d'autres interfaces.

L'appareil de contrôle ~~peut~~ **doit** ~~alors, à titre facultatif,~~ permettre au détenteur de la carte de modifier toute activité saisie manuellement, jusqu'à sa validation par la sélection d'une commande particulière. Par la suite, toute modification de ce type est interdite.

3.6.3 Saisie de conditions particulières

62) L'appareil de contrôle doit permettre au conducteur de saisir en temps réel les deux conditions particulières suivantes :

- « HORS CHAMP » (début, fin) ;
- « TRAJET EN FERRY/TRAIN » (début, fin).

Un « TRAJET EN FERRY/TRAIN » ne ~~peut~~ **doit pas** survenir lorsque la condition « HORS CHAMP » est ouverte. **Si une condition « HORS CHAMP » est ouverte, l'appareil de contrôle ne doit pas permettre aux utilisateurs de pointer le début d'un « TRAJET EN FERRY/TRAIN ».**

Une condition « HORS CHAMP » ouverte doit impérativement être fermée automatiquement par l'appareil de contrôle en cas de retrait ou d'insertion d'une carte de conducteur.

Une condition « HORS CHAMP » ouverte doit empêcher les événements et avertissements suivants :

- Conduite sans carte appropriée ;
- Avertissements liés à un temps de conduite continue.

Le **conducteur doit entrer** le marqueur de début de TRAJET EN FERRY/TRAIN ~~doit être pointé avant l'arrêt du moteur~~ **immédiatement après avoir sélectionné la condition INTERRUPTION/REPOS** à son arrivée sur le ferry ou le train.

L'appareil de contrôle doit impérativement clôturer une condition « TRAJET EN FERRY/TRAIN » ouverte ~~doit se terminer~~ lorsque l'une des situations suivantes se présente :

- Le conducteur met fin manuellement au TRAJET EN FERRY/TRAIN **à l'arrivée à destination du ferry ou du train, avant de quitter le véhicule ;**
- **Une condition « HORS CHAMP » est ouverte ;**
- Le conducteur éjecte sa carte ;
- **L'activité du conducteur est comptabilisée comme de la CONDUITE pendant une minute civile conformément au point 3.4.**

Si plusieurs conditions particulières d'un même type sont saisies au cours d'une minute civile, seule la dernière est gardée enregistrée.

~~Un TRAJET EN FERRY/TRAIN ouvert prend fin lorsqu'il n'est plus valable selon les règles énoncées dans le règlement (CE) n° 561/2006**de le présent Accord**.~~

3.6.4 *Saisie des opérations de chargement/déchargement*

62a) L'appareil de contrôle doit permettre au conducteur de saisir et de confirmer, en temps réel, toute information *indiquant* que le véhicule est en train d'être chargé ou déchargé, ou qu'une opération de chargement/déchargement simultanés est en cours.

Si plusieurs opérations de chargement/déchargement de même type sont saisies au cours d'une minute civile, seule la dernière est gardée enregistrée.

62b) Les opérations de chargement, de déchargement ou de chargement/déchargement simultanés doivent être enregistrées comme des événements séparés.

62c) Les informations relatives aux opérations de chargement/déchargement doivent être saisies avant que le véhicule ne quitte le lieu où les opérations sont effectuées.

3.7 Gestion des verrouillages d'entreprise

63) Cette fonction doit permettre la gestion des verrouillages placés par une entreprise en vue de restreindre à elle seule l'accès aux données en mode entreprise.

64) Les verrouillages d'entreprise consistent en une date et une heure de début (verrouillage) et une date et une heure de fin (déverrouillage), associées à l'identification de l'entreprise par le numéro de la carte d'entreprise correspondante (lors du verrouillage).

65) Le verrouillage et le déverrouillage ne sont possibles qu'en temps réel.

66) Le déverrouillage ne peut être effectué que par l'entreprise qui a procédé au verrouillage (identifiée par les 13 premiers chiffres du numéro de la carte d'entreprise).

67) Le déverrouillage est automatique lorsqu'une autre entreprise verrouille l'accès aux données.

68) Dans le cas où une entreprise procède à un verrouillage et que le verrouillage précédent concerne cette même entreprise, on supposera que le verrouillage précédent n'a pas été déverrouillé et qu'il est toujours en fonction.

3.8 Suivi des activités de contrôle

69) Cette fonction assure le suivi des activités d'AFFICHAGE, d'IMPRESSION, de TÉLÉCHARGEMENT depuis l'unité embarquée sur le véhicule ou la carte, et de contrôle routier d'ÉTALONNAGE, menées en mode contrôle.

70) Cette fonction assure également le suivi des activités de CONTRÔLE DE VITESSE en mode contrôle. Un contrôle de vitesse est supposé avoir eu lieu lorsqu'en mode contrôle, le message « excès de vitesse » a été envoyé sur l'imprimante pour impression ou affiché à l'écran, ou lorsque des données « événements et anomalies » ont été téléchargées depuis la mémoire de la UEV.

3.9 Détection d'événements et/ou d'anomalies

71) Cette fonction détecte les événements et/ou anomalies qui suivent.

3.9.1 Événement « insertion d'une carte non valable »

72) Cet événement est déclenché par l'insertion d'une carte non valable, par l'insertion d'une carte de conducteur déjà remplacée et/ou lorsqu'une carte valable insérée arrive à expiration.

3.9.2 Événement « conflit de cartes »

73) Cet événement est déclenché pour chacune des combinaisons de cartes marquées d'une croix dans le tableau suivant :

Conflit de cartes		Lecteur « conducteur »				
		Pas de carte	Carte de conducteur	Carte de contrôleur	Carte d'atelier	Carte d'entreprise
Lecteur « co-conducteur »	Pas de carte					
	Carte de conducteur				X	
	Carte de contrôleur			X	X	X
	Carte d'atelier		X	X	X	X
	Carte d'entreprise			X	X	X

3.9.3 Événement « chevauchement temporel »

74) Cet événement est déclenché lorsque la date et l'heure du dernier retrait d'une carte de conducteur, telles qu'elles apparaissent sur la carte, sont postérieures à la date et à l'heure actuelle de l'appareil de contrôle dans lequel la carte est insérée.

3.9.4 Événement « conduite sans carte appropriée »

75) Cet événement est déclenché pour toute combinaison de cartes tachygraphiques valables marquée d'une croix dans le tableau suivant, lorsque l'activité du conducteur passe en CONDUITE, ou en cas de changement de mode de fonctionnement lorsque l'activité du conducteur est CONDUITE :

Conduite sans carte appropriée		Lecteur « conducteur »				
		Pas de carte (ou carte non valable)	Carte de conducteur	Carte de contrôleur	Carte d'atelier	Carte d'entreprise
Lecteur « co-conducteur »	Pas de carte (ou carte non valable)	X		X		X
	Carte de conducteur	X		X	X	X
	Carte de contrôleur	X	X	X	X	X
	Carte d'atelier	X	X	X		X
	Carte d'entreprise	X	X	X	X	X

3.9.5 Événement « insertion d'une carte en cours de conduite »

76) Cet événement est déclenché lorsqu'une carte tachygraphique est insérée dans un lecteur quelconque alors que l'activité du conducteur est CONDUITE.

3.9.6 Événement « clôture incorrecte de la dernière session »

77) Cet événement est déclenché lorsque l'appareil de contrôle détecte à l'insertion de la carte que, malgré les dispositions de la section 3.1, la session précédente n'a pas été correctement clôturée (la carte a été retirée avant que toutes les données nécessaires aient été enregistrées sur la carte). Cet événement ne peut concerner que les cartes de conducteur et d'atelier.

3.9.7 Événement « excès de vitesse »

78) Cet événement est déclenché à chaque excès de vitesse.

3.9.8 Événement « interruption de l'alimentation électrique »

79) Cet événement est déclenché, en mode autre qu'étalonnage ou contrôle, en cas d'interruption pendant plus de 200 millisecondes de l'alimentation électrique du capteur de mouvement et/ou de l'unité embarquée sur le véhicule. Le seuil d'interruption est fixé par le fabricant. La rupture de l'alimentation électrique due au démarrage du moteur du véhicule ne doit pas déclencher cet événement.

3.9.9 Événement « erreur de communication avec le dispositif de communication à distance »

80) Cet événement est déclenché, en mode autre qu'étalonnage, lorsque le dispositif de communication à distance ne confirme pas la bonne réception de données de communication à distance envoyées par l'unité embarquée sur le véhicule à plus de trois reprises.

3.9.10 Événement « absence d'informations de positionnement en provenance du récepteur GNSS »

81) Cet événement est déclenché, en mode autre qu'étalonnage, lorsque le récepteur GNSS (interne ou externe) ne fournit aucune information sur la position pendant plus de trois heures de conduite consécutives.

3.9.11 Événement « erreur de communication avec le dispositif GNSS externe »

82) Cet événement est déclenché, en mode autre qu'étalonnage, lorsque la communication entre le dispositif GNSS externe et l'unité embarquée sur le véhicule est interrompue pendant plus de 20 minutes consécutives et que le véhicule est en mouvement.

3.9.12 Événement « erreur sur les données de mouvement »

83) Cet événement est déclenché, en mode autre qu'étalonnage, en cas d'interruption du flux normal de données entre le capteur de mouvement et l'unité embarquée sur le véhicule et/ou en cas d'erreur d'intégrité ou d'authentification des données au cours de l'échange de données entre le capteur de mouvement et l'UEV. **Il est également déclenché, en mode autre qu'étalonnage, si la vitesse calculée à partir des impulsions émises par le capteur de mouvement passe de 0 à plus de 40 km/h en 1 seconde, puis reste supérieure à 40 km/h pendant au moins 3 secondes.**

3.9.13 Événement « conflit concernant le mouvement du véhicule »

84) C**omme spécifié au sous-appendice 12, c**et événement est déclenché, en mode autre qu'étalonnage, lorsque des informations relatives au mouvement calculées par le capteur de mouvement entrent en conflit avec les informations de mouvement en provenance du récepteur GNSS interne**,** ~~ou~~ du dispositif GNSS externe~~, voire~~ **ou** d'autres sources indépendantes, conformément à **l'exigence 26** ~~l'appendice 12~~. Cet événement n'est pas déclenché pendant un trajet en ferry/train~~, en condition HORS DE PORTÉE ou lorsque les informations de positionnement fournies par le récepteur GNSS ne sont pas disponibles~~.

3.9.14 Événement « tentative d'atteinte à la sécurité »

85) Cet événement est déclenché par tout autre événement affectant la sécurité du capteur de mouvement, de l'unité embarquée sur le véhicule et/ou du dispositif GNSS externe, conformément aux dispositions ~~de l'appendice~~ **du sous-appendice** 10, dans les modes autres qu'étalonnage.

3.9.15 Événement « conflit temporel »

86) Cet événement est déclenché, en mode autre qu'étalonnage, lorsque l'UEV détecte un écart ~~de plus d'une minute~~ entre l'heure fournie par sa fonction de mesure du temps et l'heure **provenant des positions authentifiées transmises** par le récepteur GNSS **ou par le dispositif GNSS externe**. **Un « écart temporel » est détecté si la différence entre ces deux valeurs est supérieure à ±3 secondes, ce qui correspond à la précision temporelle définie à l'exigence 41a, augmentée de la dérive temporelle maximale par jour.** Cet événement

~~est~~ **doit être** enregistré avec la valeur de l'horloge interne **de l'appareil de contrôle** ~~de l'unité embarquée sur le véhicule et s'accompagne d'une remise à l'heure automatique. Après le déclenchement d'un événement «Conflit temporel», l'UEV ne générera plus d'autres événements «Conflit temporel» pendant les 12 heures suivantes. Cet événement n'est pas déclenché lorsqu'aucun signal GNSS valable n'a pu être détecté par le récepteur GNSS au cours des 30 derniers jours~~. **L'UEV vérifie que l'événement « conflit temporel » a été déclenché avant de remettre automatiquement à l'heure son horloge interne, conformément à l'exigence 211.** ~~Cependant, lorsque les informations de positionnement fournies par le récepteur GNSS sont à nouveau disponibles, la remise à l'heure automatique sera effectuée.~~

3.9.16 Anomalie « carte »

87) Cette anomalie est déclenchée en cas de fonctionnement anormal d'une carte tachygraphique en cours d'utilisation.

3.9.17 Anomalie « appareil de contrôle »

88) Cette anomalie est déclenchée dans le cas des anomalies suivantes, dans les modes autres qu'étalonnage :

- Anomalie interne de l'UEV ;
- Anomalie de l'imprimante ;
- Anomalie de l'affichage ;
- Anomalie de téléchargement ;
- Anomalie du capteur ;
- Anomalie du récepteur GNSS ou du dispositif GNSS externe ;
- Anomalie du dispositif de communication à distance ;
- **Anomalie de l'interface STI** ~~**(le cas échéant)**~~**.**

3.9.18 Événement « anomalie GNSS »

88a) Cet événement est déclenché, en mode autre qu'étalonnage, lorsque le récepteur GNSS détecte une attaque, ou lorsque l'authentification des messages de navigation a échoué, comme spécifié au sous-appendice 12. Après le déclenchement de l'événement « anomalie GNSS », l'UEV ne générera plus d'autres événements de ce type pendant les 10 minutes suivantes.

3.10 Autotests et tests intégrés

89) L'appareil de contrôle détecte ~~lui-même~~ les anomalies par des autotests et des tests intégrés, selon le tableau suivant :

Élément à tester	*Autotest*	*Test intégré*
Logiciels		Intégrité
Mémoire	Accès	Accès, intégrité des données
Dispositifs d'interface carte	Accès	Accès
Clavier		Contrôle manuel
Imprimante	(au choix du fabricant)	Impression
Affichage		Contrôle visuel

Élément à tester	*Autotest*	*Test intégré*
Téléchargement (effectué uniquement lors du téléchargement)	Fonctionnement correct	
Capteur	Fonctionnement correct	Fonctionnement correct
Dispositif de communication à distance	Fonctionnement correct	Fonctionnement correct
Dispositif GNSS	Fonctionnement correct	Fonctionnement correct
Interface STI ~~(optionnel)~~	**Fonctionnement correct**	

3.11 Lecture de la mémoire

90) L'appareil de contrôle doit pouvoir lire toutes les données stockées dans sa mémoire.

3.12 Enregistrement et stockage dans la mémoire

Aux fins de la présente section,

- On entend par « 365 jours » 365 jours civils d'activité moyenne de conducteurs dans un véhicule. L'activité moyenne par jour dans un véhicule est définie comme au moins 6 conducteurs ou co-conducteurs, 6 cycles d'insertion/retrait de cartes et 256 changements d'activités, de sorte que « 365 jours » comprennent au moins 2 190 (co-)conducteurs, 2 190 cycles d'insertion/retrait de carte et 93 440 changements d'activité ;
- **Le nombre moyen de saisies de lieux par jour est fixé à au moins 6 saisies correspondant aux lieux où commence la période de travail journalière et 6 saisies correspondant aux lieux où elle s'achève, de sorte que « 365 jours » comprennent au moins 4 380 saisies ;**
- Le nombre moyen de positions **où le temps de conduite accumulé atteint un multiple de 3 heures** par jour **est fixé à au moins 6 positions, de sorte que « 365 jours » comprennent au moins 2 190 positions**~~où commence la période de travail journalière, 6 positions correspondant aux lieux où le temps de conduite continue du conducteur atteint un multiple de trois heures et 6 positions correspondant aux lieux où se termine la période de travail journalière, de sorte qu'au moins 6 570 positions sont comprises dans ces «365 jours»~~ ;
- **Le nombre moyen de passages de frontières par jour est fixé à au moins 20 passages, de sorte que « 365 jours » comprennent au moins 7 300 passages de frontières ;**
- **Le nombre moyen d'opérations de chargement/déchargement par jour est fixé à au moins 25 opérations (tous types confondus), de sorte que « 365 jours » comprennent au moins 9 125 opérations de chargement/déchargement ;**
- Les heures sont enregistrées à la minute près, sauf indication contraire ;
- Le kilométrage est enregistré au kilomètre près ;
- Les vitesses sont enregistrées au kilomètre/heure près ;
- Les positions (latitudes et longitudes) sont enregistrées en degrés et en minutes, au dixième de minute près, et sont accompagnées de la précision GNSS et de l'heure d'acquisition**, ainsi que d'un drapeau indiquant si la position a été authentifiée**.

91) Les données enregistrées dans la mémoire ne doivent pas être affectées par une coupure de l'alimentation électrique externe d'une durée inférieure à douze mois dans les conditions d'homologation. En outre, les données stockées dans le dispositif externe de communication à distance, tel que défini ~~à l'appendice~~ **au sous-appendice** 14, ne doivent pas être affectées par les coupures d'alimentation de moins de 28 jours.

92) L'appareil de contrôle doit pouvoir enregistrer et stocker implicitement ou explicitement dans sa mémoire les données suivantes.

3.12.1 Données d'identification de l'équipement

3.12.1.1 Données d'identification de l'unité embarquée sur le véhicule

93) L'appareil de contrôle doit pouvoir stocker dans sa mémoire les données suivantes pour l'identification de l'unité embarquée sur le véhicule :

- Nom du fabricant ;
- Adresse du fabricant ;
- Numéro de pièce ;
- Numéro de série ;
- Génération de l'UEV ;
- Possibilité d'utiliser des cartes tachygraphiques de première génération ;
- Numéro de version du logiciel ;
- Date d'installation de la version du logiciel ;
- Année de fabrication de l'appareil ;
- Numéro d'homologation ;
- **Identificateur de version de la carte numérique (exigence 133l).**

94) Les données d'identification de l'unité embarquée sur le véhicule sont enregistrées et stockées une fois pour toutes par le fabricant de l'unité embarquée, à l'exception des données ~~concernant le logiciel et le numéro d'homologation,~~ qui peuvent être modifiées en cas ~~d'évolution~~ **de mise à jour** du logiciel et de celles concernant la possibilité d'utiliser des cartes tachygraphiques de première génération.

3.12.1.2 Données d'identification du capteur de mouvement

95) Le capteur de mouvement doit pouvoir stocker dans sa mémoire les données d'identification suivantes :

- Nom du fabricant ;
- Numéro de série ;
- Numéro d'homologation ;
- Identificateur du composant de sécurité intégré (numéro de série du microprocesseur interne, par exemple) ;
- Identificateur du système d'exploitation (numéro de version du logiciel, par exemple).

96) Les données d'identification du capteur de mouvement sont enregistrées et stockées une fois pour toutes sur le capteur par son fabricant.

97) L'unité embarquée sur le véhicule doit pouvoir enregistrer et stocker dans sa mémoire les données suivantes concernant les 20 appariements de capteurs de mouvement ayant abouti les plus récents (si plusieurs appariements ont eu lieu en un jour civil, seuls le premier et le dernier de la journée sont conservés) :

Les données suivantes doivent être enregistrées pour chacun de ces appariements :

- Données d'identification du capteur de mouvement :
  - Numéro de série ;
  - Numéro d'homologation ;
- Données d'appariement du capteur de mouvement :
  - Date de l'appariement.

3.12.1.3 Données d'identification des systèmes mondiaux de navigation par satellite (GNSS)

98) Le dispositif GNSS externe doit pouvoir stocker dans sa mémoire les données d'identification suivantes :

- Nom du fabricant ;
- Numéro de série ;
- Numéro d'homologation ;
- Identificateur du composant de sécurité intégré (numéro de série du microprocesseur interne, par exemple) ;
- Identificateur du système d'exploitation (numéro de version du logiciel, par exemple).

99) Les données d'identification sont enregistrées et stockées une fois pour toutes sur le dispositif GNSS externe par son fabricant.

100) L'unité embarquée sur le véhicule doit pouvoir enregistrer et stocker dans sa mémoire les données suivantes associées aux 20 couplages de dispositifs GNSS externes ayant abouti les plus récents (si plusieurs couplages ont eu lieu en un jour civil, seuls le premier et le dernier de la journée sont conservés).

Les données suivantes doivent être enregistrées pour chacun de ces couplages :

- Données d'identification du dispositif GNSS externe :
  - Numéro de série ;
  - Numéro d'homologation ;
- Données de couplage du dispositif GNSS externe :
  - Date de couplage.

3.12.2 Clés et certificats

101) L'appareil de contrôle doit pouvoir stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié ~~à l'appendice~~ **au sous-appendice** 11, parties A et B.

3.12.3 Données concernant l'insertion et le retrait de carte de conducteur ou d'atelier

102) Pour chaque cycle d'insertion-retrait d'une carte de conducteur ou d'atelier, l'appareil de contrôle enregistre et stocke dans sa mémoire :

- Les nom et prénom(s) du détenteur de la carte tels qu'ils sont stockés sur la carte ;
- Le numéro de la carte, ~~l'État membre~~ **la Partie contractante** qui l'a délivrée et la date d'expiration tels qu'ils sont stockés sur la carte ;
- La génération de la carte ;
- La date et l'heure d'insertion ;
- Le kilométrage du véhicule au moment de l'insertion de la carte ;
- Le lecteur dans lequel est insérée la carte ;
- La date et l'heure du retrait ;

– Le kilométrage du véhicule au moment du retrait de la carte ;

– Les informations suivantes concernant le dernier véhicule utilisé par le conducteur, telles qu'elles sont stockées sur la carte :

– Le numéro d'immatriculation et ~~l'État membre~~ **la Partie contractante** d'immatriculation ;

– La génération de l'UEV (si disponible) ;

– La date et l'heure du retrait de la carte ;

– Un marqueur indiquant si le détenteur de la carte a saisi manuellement des activités lors de l'insertion de la carte ou non.

103) La mémoire doit pouvoir conserver ces données pendant au moins 365 jours.

104) Lorsque la capacité de stockage est épuisée, les données nouvelles remplacent les données les plus anciennes.

3.12.4 Données relatives aux activités du conducteur

105) L'appareil de contrôle enregistre et stocke dans sa mémoire pour tout changement d'activité du conducteur et/ou du co-conducteur, tout changement de la situation de conduite et/ou toute insertion ou tout retrait d'une carte de conducteur ou d'atelier :

– La situation de conduite (ÉQUIPAGE, SEUL) ;

– Le lecteur (CONDUCTEUR, CO-CONDUCTEUR) ;

– La situation de la carte dans le lecteur (INSÉRÉE, NON INSÉRÉE) ;

– L'activité (CONDUITE, DISPONIBILITÉ, TRAVAIL, INTERUPTION/REPOS) ;

– La date et l'heure du changement.

Remarque : INSÉRÉE signifie qu'une carte de conducteur ou d'atelier en cours de validité est insérée dans le lecteur. NON INSÉRÉE signifie le contraire, c'est-à-dire qu'aucune carte de conducteur ou d'atelier en cours de validité n'est insérée dans le lecteur (par exemple, une carte d'entreprise est insérée ou aucune carte n'est insérée).

Les données relatives aux activités saisies manuellement par un conducteur ne sont pas enregistrées dans la mémoire.

106) La mémoire doit pouvoir conserver les données relatives à l'activité du conducteur pendant au moins 365 jours.

107) Lorsque la capacité de stockage est épuisée, les données nouvelles remplacent les données les plus anciennes.

3.12.5 Positions et lieux où les périodes de travail journalières débutent et se terminent et/ou 3 heures de temps de conduite ~~continue~~ accumulé sont atteintes

108) L'appareil de contrôle enregistre et stocke dans sa mémoire :

– Les lieux et positions où le conducteur et/ou le co-conducteur commencent leur période de travail journalière ;

– Les positions où le temps de conduite ~~continue~~ **accumulé** ~~du conducteur~~ atteint un multiple de trois heures ;

– Les lieux et positions où le conducteur et/ou le co-conducteur terminent leur période de travail journalière.

109) Lorsque le récepteur GNSS ne peut pas communiquer la position du véhicule à ces instants précis, l'appareil de contrôle doit utiliser la dernière position disponible, ainsi que la date et l'heure correspondantes.

110) Pour chaque lieu ou pour chaque position, l'appareil de contrôle doit enregistrer et stocker dans sa mémoire :

- Le numéro de la carte du (co-)conducteur et ~~l'État membre~~ **la Partie contractante** qui l'a délivrée ;
- La génération de la carte ;
- La date et l'heure de la saisie ;
- Le type de saisie (début, fin ou 3 heures de temps de conduite ~~continue~~**accumulé**) ;
- La précision GNSS, la date et l'heure correspondantes, le cas échéant ;
- Le kilométrage du véhicule ;
- **Un marqueur indiquant si la position a été authentifiée.**

110a) Pour les lieux de début ou de fin de la période de travail journalière saisis dans le cadre de la procédure de saisie manuelle à l'insertion de la carte conformément à l'exigence 61, le kilométrage et la position du véhicule doivent être enregistrés.

111) La mémoire doit être en mesure de conserver pendant au moins 365 jours les lieux et les positions où les périodes de travail journalières commencent et se terminent, et/ou où les 3 heures de temps de conduite ~~continue~~ **accumulé** sont atteintes.

112) Lorsque la capacité de stockage est épuisée, les données nouvelles remplacent les données les plus anciennes.

3.12.6 Kilométrage

113) L'appareil de contrôle enregistre dans sa mémoire le kilométrage du véhicule et la date correspondante, chaque jour civil à minuit.

114) La mémoire doit pouvoir conserver les relevés quotidiens à minuit du compteur kilométrique pendant au moins 365 jours.

115) Lorsque la capacité de stockage est épuisée, les données nouvelles remplacent les données les plus anciennes.

3.12.7 Données relatives à la vitesse du véhicule

116) L'appareil de contrôle enregistre et stocke dans sa mémoire la vitesse instantanée du véhicule, ainsi que la date et l'heure correspondantes, à chaque seconde des 24 dernières heures au moins au cours desquelles le véhicule a été conduit.

3.12.8 Données relatives aux événements

Aux fins du présent point, l'heure est enregistrée à la seconde près.

117) L'appareil de contrôle enregistre et stocke dans sa mémoire les données énumérées ci-dessous pour chaque événement détecté, selon les règles de stockage suivantes :

Événement	*Règles de stockage*	*Données à enregistrer pour chaque événement*
Insertion d'une carte non valable	- les 10 événements les plus récents	- date et heure de l'événement - type, numéro et génération de la carte ou des cartes à l'origine de l'événement et ~~État membre~~ **Partie contractante** l'ayant délivrée - nombre d'événements semblables survenus le même jour

Événement	*Règles de stockage*	*Données à enregistrer pour chaque événement*
Conflit de carte	- les 10 événements les plus récents	- date et heure de début de l'événement - date et heure de fin de l'événement - type, numéro et génération de chacune des deux cartes à l'origine du conflit et ~~État membre~~ **Partie contractante** les ayant délivrées
Conduite sans carte appropriée	- l'événement le plus long pour chacun des 10 derniers jours d'occurrence - les 5 événements les plus longs enregistrés au cours des 365 derniers jours	- date et heure de début de l'événement - date et heure de fin de l'événement - type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et ~~État membre~~ **Partie contractante** l'ayant délivrée - nombre d'événements semblables survenus le même jour
Insertion d'une carte en cours de conduite	- le dernier événement pour chacun des 10 derniers jours d'occurrence	- date et heure de l'événement - type, numéro et génération de la carte et ~~État membre~~ **Partie contractante** l'ayant délivrée - nombre d'événements semblables survenus le même jour
Clôture incorrecte de la dernière session	- les 10 événements les plus récents	- date et heure de l'insertion - type, numéro et génération de la carte et ~~État membre~~ **Partie contractante** l'ayant délivrée - données relatives à la dernière session telles qu'elles figurent sur la carte : - date et heure de l'insertion ~~- le numéro d'immatriculation, la Partie contractante d'immatriculation et la génération de l'UEV .~~

Événement	*Règles de stockage*	*Données à enregistrer pour chaque événement*
Excès de vitesse (1)	- l'événement le plus grave (c'est-à-dire celui présentant la vitesse moyenne la plus élevée) pour chacun des 10 derniers jours d'occurrence - les 5 événements les plus graves enregistrés au cours des 365 derniers jours - le premier événement survenu après le dernier étalonnage	- date et heure de début de l'événement - date et heure de fin de l'événement - vitesse maximale mesurée au cours de l'événement - vitesse moyenne arithmétique mesurée au cours de l'événement - type, numéro et génération de la carte de conducteur (le cas échéant) et ~~État membre~~ **Partie contractante** l'ayant délivrée - nombre d'événements semblables survenus le même jour
Interruption de l'alimentation électrique (2)	- l'événement le plus long pour chacun des 10 derniers jours d'occurrence - les 5 événements les plus longs enregistrés au cours des 365 derniers jours	- date et heure de début de l'événement - date et heure de fin de l'événement - type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et ~~État membre~~ **Partie contractante** l'ayant délivrée - nombre d'événements semblables survenus le même jour
Erreur de communication avec le dispositif de communication à distance	- l'événement le plus long pour chacun des 10 derniers jours d'occurrence - les 5 événements les plus longs enregistrés au cours des 365 derniers jours	- date et heure de début de l'événement - date et heure de fin de l'événement - type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et ~~État membre~~ **Partie contractante** l'ayant délivrée - nombre d'événements semblables survenus le même jour
Absence d'informations de positionnement en provenance du récepteur GNSS	- **l'événement le plus long pour chacun des 10 derniers jours d'occurrence** - **les 5 événements les plus longs enregistrés au cours des 365 derniers jours**	- **date et heure de début de l'événement** - **date et heure de fin de l'événement** - **type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et Partie contractante l'ayant délivrée** - **nombre d'événements semblables survenus le même jour**

Événement	*Règles de stockage*	*Données à enregistrer pour chaque événement*
Erreur de communication avec le dispositif GNSS externe	- l'événement le plus long pour chacun des 10 derniers jours d'occurrence - les 5 événements les plus longs enregistrés au cours des 365 derniers jours	- date et heure de début de l'événement - date et heure de fin de l'événement - type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et Partie contractante l'ayant délivrée - nombre d'événements semblables survenus le même jour
Erreur sur les données de mouvement	- l'événement le plus long pour chacun des 10 derniers jours d'occurrence - les 5 événements les plus longs enregistrés au cours des 365 derniers jours	- date et heure de début de l'événement - date et heure de fin de l'événement - type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et ~~État membre~~ **Partie contractante** l'ayant délivrée - nombre d'événements semblables survenus le même jour
Conflit concernant le mouvement du véhicule	- l'événement le plus long pour chacun des 10 derniers jours d'occurrence - les 5 événements les plus longs enregistrés au cours des 365 derniers jours	- date et heure de début de l'événement - date et heure de fin de l'événement - type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et ~~État membre~~ **Partie contractante** l'ayant délivrée - nombre d'événements semblables survenus le même jour
Tentative d'atteinte à la sécurité	- les 10 événements les plus récents pour chaque type d'événement	- date et heure de début de l'événement - date et heure de fin de l'événement (le cas échéant) - type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et ~~État membre~~ **Partie contractante** l'ayant délivrée - type d'événement

Événement	*Règles de stockage*	*Données à enregistrer pour chaque événement*
Conflit temporel	- l'événement le plus ~~long~~ **grave (c'est-à-dire celui où l'écart entre la date et l'heure de l'appareil de contrôle et la date et l'heure GNSS est le plus grand)** pour chacun des 10 derniers jours d'occurrence - les 5 événements les plus ~~longs~~ **graves** enregistrés au cours des 365 derniers jours	- date et heure de l'appareil de contrôle - date et heure GNSS - type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et ~~État membre~~ **Partie contractante** l'ayant délivrée - nombre d'événements semblables survenus le même jour
Anomalie GNSS	- **l'événement le plus long pour chacun des 10 derniers jours d'occurrence** - **les 5 événements les plus longs enregistrés au cours des 365 derniers jours**	- **date et heure de début de l'événement** - **date et heure de fin de l'événement** - **type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et Partie contractante l'ayant délivrée** - **nombre d'événements semblables survenus le même jour**

1) L'appareil de contrôle doit également enregistrer et stocker dans sa mémoire :

- La date et l'heure du dernier CONTRÔLE D'EXCÈS DE VITESSE ;
- La date et l'heure du premier excès de vitesse survenu après ce CONTRÔLE D'EXCÈS DE VITESSE ;
- Le nombre d'événements de type « excès de vitesse » survenus depuis le dernier CONTRÔLE D'EXCÈS DE VITESSE.

2) Ces données peuvent être enregistrées uniquement lors du rétablissement de l'alimentation électrique, les heures pouvant être connues avec une précision d'une minute.

3.12.9 Données relatives aux anomalies

Aux fins du présent point, l'heure est enregistrée à la seconde près.

118) L'appareil de contrôle doit essayer d'enregistrer et de stocker dans sa mémoire les données énumérées ci-dessous pour chaque anomalie détectée, selon les règles de stockage suivantes :

Anomalie	*Règles de stockage*	*Données à enregistrer pour chaque anomalie*
Anomalie de la carte	- les 10 dernières anomalies de la carte de conducteur	- date et heure de début de l'anomalie - date et heure de fin de l'anomalie - type, numéro et génération de la carte et ~~État membre~~ **Partie contractante** l'ayant délivrée
Anomalies de l'appareil de contrôle	- les 10 anomalies les plus récentes pour chaque type d'anomalie - la première anomalie survenue après le dernier étalonnage	- date et heure de début de l'anomalie - date et heure de fin de l'anomalie - type d'anomalie - type, numéro et génération de toute carte insérée au début et/ou à la fin de l'anomalie et ~~État membre~~ **Partie contractante** l'ayant délivrée

3.12.10 Données d'étalonnage

119) L'appareil de contrôle enregistre et stocke dans sa mémoire les données se rapportant :

- Aux paramètres d'étalonnage connus au moment de l'activation ;
- Au tout premier étalonnage après son activation ;
- À son premier étalonnage dans le véhicule où il se trouve actuellement (tel qu'identifié par le numéro d'identification du véhicule) ;
- Les 20 étalonnages les plus récents (lorsque plusieurs étalonnages interviennent le même jour civil, seuls le premier et le dernier sont conservés).

120) Les données suivantes doivent être enregistrées pour chacun de ces étalonnages :

- L'objet de l'étalonnage (activation, première installation, installation, inspection périodique) ;
- Le nom et l'adresse de l'atelier ;
- Le numéro de la carte d'atelier, ~~l'État membre~~ **la Partie contractante** l'ayant délivrée et sa date d'expiration ;
- L'identification du véhicule ;
- Les paramètres mis à jour ou confirmés, à savoir w, k, l, taille des pneumatiques, réglage du limiteur de vitesse, compteur kilométrique (valeurs nouvelle et ancienne), date et heure (valeurs nouvelle et ancienne) ;
- Les types et les identifiants de tous les scellements en place ;
- **Les numéros de série du capteur de mouvement, du dispositif GNSS externe (le cas échéant) et du dispositif externe de communication à distance (le cas échéant) ;**
- **Le type de chargement par défaut associé au véhicule (marchandises ou passagers) ;**
- **Le pays dans lequel l'étalonnage a été effectué, ainsi que la date et l'heure auxquelles la position utilisée pour déterminer ce pays a été fournie par le récepteur GNSS.**

121) En outre, l'appareil de contrôle enregistre et stocke dans sa mémoire des données concernant la possibilité d'utiliser les cartes tachygraphiques de première génération (encore activées ou non).

122) Le capteur de mouvement enregistre et stocke dans sa mémoire les données suivantes concernant son installation :

- Première connexion à une UEV (date, heure, numéro d'homologation et numéro de série de l'UEV) ;
- Dernière connexion à une UEV (date, heure, numéro d'homologation et numéro de série de l'UEV).

123) Le dispositif GNSS externe enregistre et stocke dans sa mémoire les données suivantes concernant son installation :

- Premier couplage avec une UEV (date, heure, numéro d'homologation et numéro de série de l'UEV) ;
- Dernier couplage avec une UEV (date, heure, numéro d'homologation et numéro de série de l'UEV).

3.12.11 Données relatives à la remise à l'heure

124) L'appareil de contrôle enregistre et stocke dans sa mémoire les données pertinentes concernant les remises à l'heure exécutées en mode étalonnage, hors du cadre d'un étalonnage périodique (voir définition f)) :

- La plus récente remise à l'heure ;
- Les 5 plus grandes corrections.

125) Les données suivantes doivent être enregistrées pour chacune de ces remises à l'heure :

- Date et heure (anciennes valeurs) ;
- Date et heure (nouvelles valeurs) ;
- Nom et adresse de l'atelier ;
- Numéro, génération et date d'expiration de la carte d'atelier et ~~État membre~~ **Partie contractante** l'ayant délivrée.

3.12.12 Données relatives aux activités de contrôle

126) L'appareil de contrôle enregistre et stocke dans sa mémoire les données suivantes ayant trait aux 20 dernières activités de contrôle :

- La date et l'heure du contrôle ;
- Le numéro et la génération de la carte de contrôleur et ~~l'État membre~~ **la Partie contractante** qui l'a délivrée ;
- Le type de contrôle (affichage et/ou impression et/ou téléchargement à partir de l'UEV et/ou téléchargement à partir de la carte et/ou contrôle routier d'étalonnage).

127) En cas de téléchargement, les dates de la journée la plus ancienne et de la journée la plus récente téléchargées sont également enregistrées.

3.12.13 Données relatives aux verrouillages d'entreprise

128) L'appareil de contrôle enregistre et stocke dans sa mémoire les données suivantes ayant trait aux 255 plus récents verrouillages d'entreprise :

- La date et l'heure du verrouillage ;
- La date et l'heure du déverrouillage ;
- Le numéro et la génération de la carte d'entreprise et ~~l'État membre~~ **la Partie contractante** qui l'a délivrée ;
- Le nom et l'adresse de l'entreprise.

Les données précédemment verrouillées dont le verrouillage a été supprimé de la mémoire en raison de la limite précitée sont considérées comme étant non verrouillées.

3.12.14 Données relatives au téléchargement

129) L'appareil de contrôle enregistre et stocke dans sa mémoire les données suivantes ayant trait au dernier téléchargement de la mémoire vers des médias extérieurs en mode entreprise ou étalonnage :

- La date et l'heure du téléchargement ;
- Le numéro de la carte d'entreprise ou d'atelier, ~~l'État membre~~ **la Partie contractante** qui a délivré la carte et la génération de la carte ;
- Le nom de l'entreprise ou de l'atelier.

3.12.15 Données relatives aux conditions particulières

130) L'appareil de contrôle enregistre dans sa mémoire les données suivantes ayant trait aux conditions particulières :

- La date et l'heure de la saisie ;
- Le type de condition particulière.

131) La mémoire doit pouvoir conserver les données relatives aux conditions particulières pendant au moins 365 jours (en supposant qu'en moyenne une condition est ouverte et fermée par jour). Lorsque la capacité de stockage est épuisée, les données nouvelles remplacent les données les plus anciennes.

3.12.16 Données relatives aux cartes tachygraphiques

132) L'appareil de contrôle doit pouvoir stocker les données suivantes relatives aux différentes cartes tachygraphiques ayant été utilisées dans l'UEV :

- Le numéro de la carte tachygraphique et son numéro de série ;
- Le fabricant de la carte tachygraphique ;
- Le type de carte tachygraphique ;
- La version de la carte tachygraphique.

133) L'appareil de contrôle doit pouvoir stocker au moins 88 enregistrements de ce type.

3.12.17 Passages de frontières

133a) L'appareil de contrôle enregistre et stocke dans sa mémoire les informations suivantes concernant les passages de frontières :

- **Le pays que le véhicule quitte ;**
- **Le pays dans lequel le véhicule entre ;**
- **La position correspondant au lieu où le véhicule a franchi la frontière.**

133b) Avec les pays et la position, l'appareil de contrôle enregistre et stocke dans sa mémoire :

- **Le numéro de la carte du (co-)conducteur et la Partie contractante qui l'a délivrée ;**
- **La génération de la carte ;**
- **La précision GNSS, la date et l'heure correspondantes ;**
- **Un marqueur indiquant si la position a été authentifiée ;**
- **Le kilométrage du véhicule au moment du passage de frontière.**

133c) La mémoire doit pouvoir stocker les données relatives aux passages de frontières pendant au moins 365 jours.

133d) Lorsque la capacité de stockage est épuisée, les données nouvelles remplacent les données plus anciennes.

3.12.18 Opérations de chargement/déchargement

133e) L'appareil de contrôle enregistre et stocke dans sa mémoire les informations suivantes concernant les opérations de chargement et de déchargement du véhicule :

- **Le type d'opération (chargement, déchargement ou chargement/déchargement simultanés) ;**
- **La position correspondant au lieu où l'opération de chargement/déchargement s'est déroulée.**

133f) Lorsque le récepteur GNSS n'est pas en mesure de fournir la position du véhicule au moment du chargement ou du déchargement, l'appareil de contrôle doit utiliser la dernière position disponible, ainsi que la date et l'heure correspondantes.

133g) Avec le type d'opération et la position, l'appareil de contrôle enregistre et stocke dans sa mémoire :

- **Le numéro de la carte du conducteur et/ou du co-conducteur et la Partie contractante qui l'a délivrée ;**
- **La génération de la carte ;**
- **La date et l'heure de l'opération de chargement/déchargement ;**
- **La précision GNSS, la date et l'heure correspondantes, le cas échéant ;**
- **Un marqueur indiquant si la position a été authentifiée ;**
- **Le kilométrage du véhicule.**

133h) La mémoire doit pouvoir stocker les données relatives aux opérations de chargement/déchargement pendant au moins 365 jours.

133i) Lorsque la capacité de stockage est épuisée, les données nouvelles remplacent les données plus anciennes.

3.12.19 Carte numérique

133j) Afin d'enregistrer la position du véhicule lors du franchissement de la frontière d'un pays, l'appareil de contrôle stocke dans sa mémoire une carte numérique.

133k) Les cartes numériques pouvant être utilisées en appui à la fonction de surveillance des passages de frontières de l'appareil de contrôle sont mises à disposition par le laboratoire chargé des essais d'interopérabilité pour téléchargement à partir d'un site Web sécurisé prévu à cet effet, sous différents formats.

133l) Pour chacune de ces cartes, un identificateur de version et une valeur de hachage sont disponibles sur le site Web.

133m) Les cartes doivent comporter :

- **Un niveau de définition correspondant au niveau 0 de la nomenclature des unités territoriales statistiques (NUTS) ;**
- **Une échelle de 1:1 million.**

133n) Les fabricants de tachygraphes doivent sélectionner une carte sur le site Web sécurisé et la télécharger.

133o) Les fabricants de tachygraphes ne doivent utiliser une carte téléchargée à partir du site Web qu'après avoir vérifié son intégrité en utilisant la valeur de hachage de la carte.

133p) Le fabricant de l'appareil de contrôle importe la carte sélectionnée dans l'appareil dans un format adapté, mais la sémantique de la carte importée doit rester inchangée.

133q) Le fabricant doit aussi enregistrer l'identificateur de version de la carte utilisée dans l'appareil de contrôle.

133r) Il doit être possible de mettre à jour la carte numérique stockée ou de la remplacer par une nouvelle carte mise à disposition par le laboratoire chargé des essais d'interopérabilité.

133s) Les mises à jour des cartes numériques doivent être effectuées conformément aux mécanismes de mise à jour logicielle prévus par le fabricant, en application des exigences 226d et 226e, de sorte que l'appareil de contrôle puisse vérifier l'authenticité et l'intégrité de la nouvelle carte importée, avant de l'enregistrer et de remplacer la carte précédente.

133t) Les fabricants de tachygraphes peuvent ajouter des informations supplémentaires à la carte de base visée à l'exigence 133m) à des fins autres que l'enregistrement des passages de frontières, telles que les frontières des régions des Parties contractantes, à condition que la sémantique de la carte de base reste inchangée.

3.13 Lecture des cartes tachygraphiques

134) L'appareil de contrôle doit pouvoir lire sur les cartes tachygraphiques de première et de deuxième génération, le cas échéant, les données nécessaires pour :

- Identifier le type de la carte, le détenteur de la carte, le véhicule utilisé précédemment, la date et l'heure du dernier retrait et l'activité sélectionnée à ce moment ;
- Vérifier que la dernière session a été correctement clôturée ;
- Calculer le temps de conduite continue du conducteur, le temps d'interruption cumulé et les temps de conduite **ac**cumulés pour la semaine précédente et la semaine en cours ;
- Donner suite aux demandes d'impression de données enregistrées sur une carte de conducteur ;
- Télécharger une carte de conducteur sur un média externe.

Cette exigence s'applique aux cartes tachygraphiques de première génération uniquement si leur utilisation n'a pas été rendue impossible par un atelier.

135) En cas d'erreur de lecture, l'appareil de contrôle fait une nouvelle tentative, à trois reprises au maximum, et en cas d'échec répété, déclare la carte défaillante et non valable.

135a) La structure de l'application « TACHO_G2 » dépend de la version de la carte. Les cartes de la version 2 contiennent des fichiers élémentaires (EF) supplémentaires par rapport à celles de la version 1, notamment :

- **Dans les cartes de conducteur et d'atelier :**
  - **EF Places_Authentication doit contenir l'état d'authentification des positions du véhicule stockées dans EF Places. Chaque état d'authentification doit être accompagné d'une date et d'une heure, qui doivent correspondre exactement à la date et à l'heure stockées avec la position correspondante dans EF Places ;**
  - **EF GNSS_Places_Authentication doit contenir l'état d'authentification des positions du véhicule stockées dans EF GNSS_Places. Chaque état d'authentification doit être accompagné d'une date et d'une heure, qui doivent correspondre exactement à la date et à l'heure stockées avec la position correspondante dans EF GNSS_Places ;**

- **EF Border_Crossings, EF Load_Unload_Operations et EF Load_Type_Entries doivent contenir des données relatives aux passages de frontières, aux opérations de chargement/déchargement et aux types de chargement ;**

- **Dans les cartes d'atelier :**
  - **EF Calibration_Add_Data doit contenir des données d'étalonnage supplémentaires par rapport à celles stockées dans EF Calibration. Les anciennes date et heure et au numéro d'identification du véhicule doivent être stockés avec chaque enregistrement de données d'étalonnage supplémentaire, et doivent correspondre exactement aux anciennes date et heure et au numéro d'identification du véhicule stockés avec les données d'étalonnage correspondantes dans EF Calibration ;**

- **Dans toutes les cartes tachygraphiques :**
  - **EF VU_Configuration doit contenir les paramètres spécifiques du tachygraphe du détenteur de la carte.**

L'unité embarquée sur le véhicule ne doit pas tenir compte des états d'authentification qui se trouvent dans EF Places_Authentication ou EF GNSS_Places_Authentifcation, lorsqu'aucune position présentant le même horodatage n'est trouvée dans EF Places ou EF GNSS_Places.

L'unité embarquée sur le véhicule doit ignorer le fichier élémentaire EF VU_Configuration dans toutes les cartes, dans la mesure où aucune règle spécifique n'a encore été fournie concernant l'utilisation de ce fichier élémentaire. Ces règles seront établies par un amendement de l'appendice 1C, qui comprendra la modification ou la suppression du présent paragraphe.

3.14 Enregistrement et stockage sur les cartes tachygraphiques

3.14.1 Enregistrement et stockage sur les cartes tachygraphiques de première génération

136) À condition que l'utilisation de cartes tachygraphiques de première génération n'ait pas été rendue impossible par un atelier, l'appareil de contrôle doit enregistrer et stocker les données exactement comme le ferait un appareil de contrôle de première génération.

137) L'appareil de contrôle règle les « données de session » sur la carte de conducteur ou d'atelier immédiatement après l'insertion de la carte.

138) L'appareil de contrôle met à jour les données stockées sur une carte de conducteur, d'atelier, d'entreprise et/ou de contrôleur en cours de validité, avec toutes les données nécessaires concernant la période d'insertion de la carte et le détenteur de la carte. Les données enregistrées sur ces cartes sont spécifiées au chapitre 4.

139) L'appareil de contrôle met à jour les données relatives à l'activité du conducteur et aux lieux (spécifiées aux points 4.5.3.1.9 et 4.5.3.1.11) stockées sur les cartes de conducteur et/ou d'atelier en cours de validité, avec les données relatives à l'activité et aux lieux saisies manuellement par le détenteur de la carte.

140) Tous les événements **et anomalies** qui ne sont pas définis pour l'appareil de contrôle de première génération ne sont pas stockés sur les cartes de conducteur et d'atelier **de première génération**.

141) La mise à jour des données enregistrées sur les cartes tachygraphiques est réalisée de telle manière que, lorsque cela est nécessaire compte tenu de la capacité réelle de stockage de la carte, les données les plus récentes remplacent les données les plus anciennes.

142) En cas d'erreur d'écriture, l'appareil de contrôle fait une nouvelle tentative, à trois reprises au maximum, et en cas d'échec répété, déclare la carte défaillante et non valable.

143) Avant le retrait d'une carte de conducteur **ou d'atelier**, et après que toutes les données pertinentes ont été enregistrées sur la carte, l'appareil de contrôle remet à zéro les « données de session ».

3.14.2 Enregistrement et stockage sur les cartes tachygraphiques de deuxième génération

144) Les cartes tachygraphiques de deuxième génération doivent contenir deux applications de carte différentes, la première devant être rigoureusement identique à l'application TACHO des cartes tachygraphiques de première génération, la seconde étant l'application « TACHO_G2 » spécifiée dans le chapitre 4 ~~de l'appendice~~ **du sous-appendice** 2.

La structure de l'application « TACHO_G2 » dépend de la version de la carte. Les cartes de la version 2 contiennent des fichiers élémentaires supplémentaires par rapport à celles de la version 1.

145) L'appareil de contrôle règle les « données de session » sur la carte de conducteur ou d'atelier immédiatement après l'insertion de la carte.

146) L'appareil de contrôle met à jour les données stockées sur les deux applications des cartes de conducteur, d'atelier, d'entreprise et/ou de contrôleur en cours de validité avec toutes les données nécessaires concernant la période d'insertion de la carte et le détenteur de la carte. Les données enregistrées sur ces cartes sont spécifiées au chapitre 4.

147) L'appareil de contrôle met à jour les données relatives aux lieux d'activité du conducteur et aux positions (spécifiées aux points 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 et 4.5.3.2.11) stockées sur les cartes de conducteur et/ou d'atelier en cours de validité, avec les données relatives aux lieux et aux activités saisies manuellement par le détenteur de la carte.

147a) Lors de l'insertion d'une carte de conducteur ou d'atelier, l'appareil de contrôle enregistre sur la carte le type de chargement par défaut du véhicule.

147b) Lors de l'insertion d'une carte de conducteur ou d'atelier, et après la procédure de saisie manuelle, l'appareil de contrôle vérifie le dernier lieu de début ou de fin de la période de travail journalière stocké sur la carte. Ce lieu peut être temporaire, comme indiqué à l'exigence 59. Si ce lieu est situé dans un pays différent de celui où se trouve actuellement le véhicule, l'appareil de contrôle doit stocker sur la carte un passage de frontière, ainsi que :

- **Le pays que le conducteur a quitté (ou la mention « aucune information disponible ») ;**
- **Le pays dans lequel le conducteur est entré (ou le pays où se trouve actuellement le véhicule) ;**
- **La date et l'heure auxquelles le conducteur a franchi la frontière (ou l'heure d'insertion de la carte) ;**
- **La position du conducteur lorsque la frontière a été franchie (ou la mention « aucune information disponible ») ;**
- **Le kilométrage du véhicule (ou la mention « aucune information »).**

148) La mise à jour des données enregistrées sur les cartes tachygraphiques est réalisée de telle manière que, lorsque cela est nécessaire compte tenu de la capacité réelle de stockage de la carte, les données les plus récentes remplacent les données les plus anciennes.

149) En cas d'erreur d'écriture, l'appareil de contrôle fait une nouvelle tentative, à trois reprises au maximum, et en cas d'échec répété, déclare la carte défaillante et non valable.

150) Avant le retrait d'une carte de conducteur, et après que toutes les données pertinentes ont été enregistrées sur les deux applications de la carte, l'appareil de contrôle remet à zéro les « données de session ».

150a) L'unité embarquée sur le véhicule doit ignorer le fichier EF VU_Configuration dans toutes les cartes, dans la mesure où aucune règle spécifique n'a encore été fournie concernant l'utilisation de ce fichier élémentaire. Ces règles seront établies par un

amendement de l'appendice 1C, qui comprendra la modification ou la suppression du présent paragraphe.

3.15 Affichage

151) L'affichage doit comporter au moins 20 caractères.

152) La taille des caractères doit être d'au moins 5 mm de hauteur et 3,5 mm de largeur.

153) Le dispositif d'affichage doit prendre en charge les caractères spécifiés au chapitre 4 (Jeux de caractères) ~~de l'appendice~~ **du sous-appendice** 1. L'affichage peut utiliser des graphies simplifiées (par exemple, les caractères accentués peuvent être affichés sans accent ou les minuscules peuvent être affichées en majuscules).

154) L'affichage doit être muni d'un éclairage non éblouissant.

155) Les indications doivent être visibles à l'extérieur de l'appareil de contrôle.

156) L'appareil de contrôle doit pouvoir afficher :

- Des données par défaut ;
- Des données relatives aux avertissements ;
- Des données relatives à l'accès aux menus ;
- D'autres données demandées par l'utilisateur.
- Des informations supplémentaires peuvent être affichées par l'appareil de contrôle, à condition qu'elles soient clairement distinctes des informations précitées.

157) L'affichage de l'appareil de contrôle doit utiliser les pictogrammes ou les combinaisons de pictogrammes présentés ~~à l'appendice~~ **au sous-appendice** 3. D'autres pictogrammes ou combinaisons de pictogrammes peuvent également être utilisés, pour autant qu'ils soient clairement distincts des pictogrammes ou combinaisons de pictogrammes précités.

158) Le dispositif d'affichage doit toujours être allumé lorsque le véhicule est en mouvement.

159) L'appareil de contrôle peut comporter une fonction manuelle ou automatique qui coupe le dispositif d'affichage lorsque le véhicule est à l'arrêt.

Le format d'affichage est spécifié ~~à l'appendice~~ **au sous-appendice** 5.

3.15.1 Affichage par défaut

160) Lorsque l'affichage d'aucune autre information n'est requis, l'appareil de contrôle affiche, par défaut :

- L'heure locale (heure UTC + décalage fixé par le conducteur) ;
- Le mode de fonctionnement ;
- L'activité en cours du conducteur et du co-conducteur ;
- Des informations relatives au conducteur :
  - Si son activité en cours est la CONDUITE, son temps de conduite continue et son temps d'interruption cumulé ;
  - Si son activité en cours n'est pas la CONDUITE, la durée de cette activité (depuis sa sélection) et le temps d'interruption cumulé.

161) L'affichage des données concernant chaque conducteur doit être clair, simple et dépourvu d'ambiguïté. Lorsque les informations relatives au conducteur et au co-conducteur ne peuvent pas être affichées en même temps, l'appareil de contrôle doit afficher par défaut les informations ayant trait au conducteur et doit permettre à l'utilisateur d'afficher les informations concernant le co-conducteur.

162) Lorsque la largeur d'affichage n'est pas suffisante pour afficher par défaut le mode de fonctionnement, l'appareil de contrôle doit afficher brièvement le nouveau mode de fonctionnement à chaque changement de mode.

163) L'appareil de contrôle doit afficher brièvement le nom du détenteur de la carte lors de l'insertion d'une carte.

164) Lorsqu'une condition HORS CHAMP ou TRAJET EN FERRY/TRAIN est ouverte, le pictogramme approprié doit apparaître pour indiquer que la condition en question est ouverte (l'activité du conducteur en cours peut ne pas être affichée en même temps).

3.15.2 Affichage des avertissements

165) L'appareil de contrôle utilise principalement, pour les avertissements, les pictogrammes figurant ~~à l'appendice~~ **au sous-appendice** 3, complétés au besoin par des informations sous forme de code numérique. Un message d'avertissement dans la langue choisie par le conducteur peut également être ajouté.

3.15.3 Menu d'accès

166) L'appareil de contrôle doit comporter les commandes nécessaires dans un menu approprié.

3.15.4 Autres affichages

167) Il doit être possible d'afficher au choix et sur demande :

- La date et l'heure UTC et le décalage de l'heure locale ;
- Le contenu ~~d'un des six~~ **des** tirages papier ~~correspondants~~ **visés à l'exigence 169**, dans le même format que les tirages eux-mêmes ;
- Le temps de conduite continue et le temps d'interruption **ac**cumulé du conducteur ;
- Le temps de conduite continue et le temps d'interruption **ac**cumulé du co-conducteur ;
- Le temps de conduite **ac**cumulé du conducteur pour la semaine précédente et pour la semaine en cours ;
- Le temps de conduite **ac**cumulé du co-conducteur pour la semaine précédente et pour la semaine en cours ;
- Et à titre facultatif :
- La durée actuelle de l'activité du co-conducteur (depuis sa sélection) ;
- Le temps de conduite **ac**cumulé du conducteur pour la semaine en cours ;
- Le temps de conduite **ac**cumulé du co-conducteur pour la période de travail journalière en cours ;
- Le temps de conduite **ac**cumulé du conducteur pour la période de travail journalière en cours.

168) L'affichage du contenu du tirage papier est séquentiel, ligne par ligne. Si la largeur d'affichage est inférieure à 24 caractères, l'utilisateur peut visualiser l'ensemble des informations par un moyen approprié (plusieurs lignes, affichage déroulant…). Les lignes du tirage papier prévues pour les informations manuscrites peuvent être omises.

3.16 Impression

169) L'appareil de contrôle doit pouvoir imprimer des informations stockées dans sa mémoire et/ou sur des cartes tachygraphiques, de manière à obtenir les sept tirages papier suivants :

- Tirage quotidien des activités du conducteur stockées sur la carte ;

- Tirage quotidien des activités du conducteur stockées dans la mémoire de l'unité embarquée sur le véhicule ;
- Tirage des événements et anomalies stockés sur la carte ;
- Tirage des événements et anomalies stockés dans la mémoire de l'unité embarquée sur le véhicule ;
- Tirage des données techniques ;
- Tirage des données relatives aux excès de vitesse ;
- Tirage de l'historique des données de la carte tachygraphique pour une UEV donnée (voir chap. 3, point 12.16).
- Le détail du format à respecter et du contenu de ces tirages papier est spécifié ~~à l'appendice~~ **au sous-appendice** 4.

Des données additionnelles peuvent figurer à la fin des tirages papier.

D'autres tirages papier peuvent également être obtenus à partir de l'appareil de contrôle, pour autant qu'ils soient clairement distincts des sept précités.

170) Les activités quotidiennes du conducteur ainsi que les événements et anomalies stockés sur la carte ne peuvent être imprimés que lorsqu'une carte de conducteur ou d'atelier est insérée dans l'appareil de contrôle. L'appareil de contrôle met à jour les données stockées sur la carte concernée avant de lancer l'impression.

171) Afin d'imprimer quotidiennement les activités du conducteur ou les événements et anomalies stockés sur la carte, l'appareil de contrôle doit :

- Soit sélectionner automatiquement la carte de conducteur ou la carte d'atelier si une seule de ces cartes est insérée ;
- Soit comporter une commande permettant de sélectionner la carte source ou de sélectionner la carte insérée dans le lecteur « conducteur» si deux de ces cartes sont insérées dans l'appareil de contrôle.

172) L'imprimante doit pouvoir imprimer 24 caractères par ligne.

173) La taille des caractères doit être d'au moins 2,1 mm de hauteur et 1,5 mm de largeur.

174) L'imprimante doit prendre en charge les caractères spécifiés au chapitre 4 (Jeux de caractères) d~~e l'appendice~~ **du sous-appendice** 1.

175) Les imprimantes doivent être conçues de telle manière que la définition des tirages papier soit suffisante pour éviter toute ambiguïté à la lecture.

176) Les tirages papier doivent conserver leurs dimensions et leur contenu dans les conditions normales d'humidité (10-90 %) et de température.

177) Le papier homologué utilisé par l'appareil de contrôle doit porter la marque d'homologation appropriée et une indication du (ou des) type(s) d'appareil(s) de contrôle avec le(s)quel(s) il peut être utilisé.

178) Les tirages papier doivent rester facilement lisibles et identifiables dans les conditions normales de stockage, en ce qui concerne l'intensité lumineuse, l'humidité et la température, pendant au moins deux ans.

179) Les tirages papier doivent au minimum être conformes aux spécifications d'essai définies ~~à l'appendice~~ **au sous-appendice** 9.

180) Il doit être également possible d'écrire à la main sur ces documents, par exemple pour la signature du conducteur.

181) En cas de rupture de l'alimentation en papier en cours d'impression, et après rechargement en papier, l'appareil de contrôle doit soit recommencer l'impression au début, soit la reprendre là où elle s'était interrompue, en faisant clairement référence à la partie imprimée auparavant.

3.17 Avertissements

182) L'appareil de contrôle doit avertir le conducteur lorsqu'il détecte un événement et/ou une anomalie.

183) L'avertissement concernant une interruption de l'alimentation électrique peut être retardé jusqu'au rétablissement du courant.

184) L'appareil de contrôle prévient le conducteur 15 minutes avant et au moment du dépassement du temps de conduite continue maximal autorisé.

185) Les avertissements doivent être visuels. Des avertissements sonores peuvent également être produits en plus des avertissements visuels.

186) Les avertissements visuels doivent être clairement identifiables par l'utilisateur, doivent apparaître dans le champ de vision du conducteur et doivent être facilement lisibles aussi bien de jour que de nuit.

187) Les avertissements visuels peuvent être intégrés à l'appareil de contrôle et/ou être extérieurs à celui-ci.

188) Dans ce dernier cas, ils doivent comporter le symbole « T ».

189) Les avertissements doivent durer au moins 30 secondes, sauf si l'utilisateur en accuse réception en appuyant sur une ou plusieurs touches spécifiques de l'appareil de contrôle. Ce premier accusé de réception ne doit pas effacer l'affichage de la cause de l'avertissement visé au point suivant.

190) La cause de l'avertissement doit être affichée sur l'appareil de contrôle et rester visible jusqu'à ce que l'utilisateur en accuse réception à l'aide d'une touche ou d'une commande spécifique sur l'appareil de contrôle.

191) Des avertissements additionnels peuvent être prévus, pour autant qu'ils ne prêtent pas à confusion avec ceux définis précédemment.

3.18 Téléchargement de données vers des supports externes

192) L'appareil de contrôle doit permettre le téléchargement à la demande de données stockées dans sa mémoire ou sur une carte de conducteur vers des supports de stockage externes, par l'intermédiaire du connecteur de téléchargement/d'étalonnage. L'appareil de contrôle met à jour les données stockées sur la carte concernée avant de lancer le téléchargement.

193) En outre, et en option, l'appareil de contrôle peut, dans tout mode de fonctionnement, télécharger des données par l'intermédiaire de n'importe quel**le** ~~autre moyen~~ **interface** vers une entreprise authentifiée par ce canal. En pareil cas, les données ainsi téléchargées sont soumises aux droits d'accès applicables en mode entreprise.

194) Le téléchargement ne doit ni modifier ni effacer les données stockées.

195) L'interface électrique du connecteur de téléchargement/d'étalonnage est spécifiée ~~à l'appendice~~ **au sous-appendice** 6.

196) Les protocoles de téléchargement sont spécifiés ~~à l'appendice~~ **au sous-appendice** 7.

196a) Toute entreprise de transport exploitant des véhicules équipés d'un appareil de contrôle conforme au présent appendice doit veiller à ce que toutes les données soient téléchargées depuis l'unité embarquée sur le véhicule et les cartes de conducteur.

La période maximale pendant laquelle les données pertinentes peuvent être téléchargées ne doit pas dépasser :

- **90 jours pour les données de l'unité embarquée ;**
- **28 jours pour les données de la carte de conducteur.**

196b) Les entreprises de transport conservent les données téléchargées à partir de l'unité embarquée sur le véhicule et des cartes de conducteur pendant au moins 12 mois après leur enregistrement.

3.19 Communication à distance pour les contrôles routiers ciblés

197) Lorsque le contact est mis, l'unité embarquée sur le véhicule enregistre, toutes les 60 secondes, dans le dispositif de communication à distance, les données les plus récentes nécessaires aux fins des contrôles routiers ciblés. Ces données sont chiffrées et signées, conformément aux dispositions des **sous-**appendices 11 et 14.

198) Les données qui doivent être contrôlées à distance sont mis à la disposition des lecteurs de communication à distance par communication sans fil, comme indiqué ~~à l'appendice~~ **au sous-appendice** 14.

199) Les données nécessaires aux fins des contrôles routiers ciblés ont trait aux événements suivants :

- Dernière tentative d'atteinte à la sécurité ;
- Interruption de l'alimentation électrique la plus longue ;
- Anomalie du capteur ;
- Erreurs sur les données de mouvement ;
- Conflits concernant le mouvement du véhicule ;
- Conduite sans carte en cours de validité ;
- Insertion de carte en cours de conduite ;
- Données relatives à la remise à l'heure ;
- Données d'étalonnage, y compris les dates des deux derniers étalonnages enregistrés ;
- Numéro d'immatriculation du véhicule ;
- Vitesse enregistrée par le tachygraphe ;
- **Position du véhicule ;**
- **Indication quant à la possibilité que le conducteur ne respecte pas les temps de conduite.**

3.20 Échanges de ~~D~~données ~~transmises à~~ avec d'autres dispositifs externes

200) L'appareil de contrôle ~~peut~~ **doit** également être équipé **d'une** interface~~s~~ ~~normalisées~~ **STI conforme aux dispositions du sous-appendice 13,** qui permet l'utilisation, par un dispositif externe, ~~en mode opérationnel ou «étalonnage»,~~ des données enregistrées ou produites par le tachygraphe **ou les cartes tachygraphiques.**

En mode opérationnel, le consentement du conducteur est requis pour la transmission de données à caractère personnel par l'intermédiaire de l'interface STI. Toutefois, cette exigence ne s'applique pas aux données du tachygraphe ou de la carte tachygraphique consultées en mode contrôle, entreprise ou étalonnage. Pour ces modes, les droits d'accès aux données et aux fonctions sont spécifiés dans les exigences 12 et 13.

Les exigences suivantes sont applicables aux données mises à disposition par l'intermédiaire de l'interface STI :

- **Les données à caractère personnel ne sont disponibles que sous réserve du consentement vérifiable du conducteur, qui accepte que ses données personnelles puissent quitter le réseau du véhicule ;**

Le sous-appendice 13 présente une sélection de données existantes qui peuvent être disponibles par l'intermédiaire de l'interface STI, ainsi que la classification de ces données en tant que données « à caractère personnel » ou « sans caractère personnel ». Des données supplémentaires peuvent être produites en plus de celles spécifiées au sous-appendice 13. Le fabricant de l'unité embarquée doit classer ces données dans les catégories « à caractère personnel » ou « sans caractère personnel », l'exigence relative au consentement du conducteur s'appliquant aux données de la catégorie « à caractère personnel » ;

- **Le consentement du conducteur peut être activé ou désactivé à tout moment à l'aide de commandes se trouvant dans le menu, à condition que sa carte soit insérée ;**
- **En aucun cas, la présence de l'interface STI ne doit perturber ou affecter le bon fonctionnement et la sécurité de l'unité embarquée sur le véhicule.**

D'autres interfaces d'unité embarquée peuvent coexister, à condition qu'elles respectent pleinement les exigences du sous-appendice 13 en ce qui concerne le consentement du conducteur. L'appareil de contrôle permet de communiquer le statut du consentement du conducteur aux autres plateformes faisant partie du réseau du véhicule ainsi qu'aux dispositifs externes.

En ce qui concerne les données à caractère personnel introduites dans le réseau du véhicule, puis traitées hors de ce réseau, il ne relève pas de la responsabilité du fabricant du tachygraphe de veiller à ce que leur traitement soit conforme à la législation applicable dans l'UE en matière de protection des données.

L'interface STI doit aussi permettre au conducteur et au co-conducteur de saisir des données dans le cadre de la procédure de saisie manuelle, conformément à l'exigence 61.

L'interface STI peut aussi être utilisée pour saisir, en temps réel, des informations supplémentaires, notamment :

- **L'activité sélectionnée par le conducteur, conformément à l'exigence 46 ;**
- **Des lieux, conformément à l'exigence 56 ;**
- **Des conditions particulières, conformément à l'exigence 62 ;**
- **Des opérations de chargement/déchargement, conformément à l'exigence 62a.**

Ces informations peuvent également être saisies par l'intermédiaire d'autres interfaces.

~~Dans l'appendice~~**le sous-appendice** ~~13, une interface STI facultative est spécifiée et normalisée. D'autres interfaces similaires peuvent coexister, à condition qu'elles respectent pleinement les exigences de l'appendice~~ **du sous-appendice** ~~13 en termes de liste minimale de données, de sécurité et de consentement du conducteur.~~

~~**Le consentement du conducteur n'est pas applicable aux données transmises au réseau du véhicule par l'appareil de contrôle. Dans le cas où les données à caractère personnel injectées dans le réseau du véhicule sont ensuite traitées en dehors de ce réseau, il incombe au constructeur du véhicule de faire en sorte que le traitement de ces données soit conforme à la législation en matière de protection des données personnelles applicable sur le territoire des Parties contractantes et à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Le consentement du conducteur n'est pas non plus applicable au téléchargement de données tachygraphiques par une entreprise extérieure (exigence 193), cette situation étant régie par le droit d'accès de la carte d'entreprise.**~~

~~Les exigences suivantes sont applicables aux données ITS mises à disposition par l'intermédiaire de cette interface:~~

- ~~ces données constituent un ensemble de données existantes sélectionnées qui proviennent du dictionnaire de données du tachygraphe (appendice~~ **sous-appendice** ~~1),~~

~~— un sous-ensemble de ces données sélectionnées constitue des «données à caractère personnel»,~~

~~— ce sous-ensemble de «données à caractère personnel» n'est disponible que si le consentement vérifiable du conducteur, qui accepte que ses données personnelles puissent quitter le réseau du véhicule, est activé,~~

~~— l'accord du conducteur peut être activé ou désactivé à tout moment,à l'aide de commandes se trouvant dans le menu, à condition que la carte du conducteur soit insérée,~~

~~— l'ensemble et le sous-ensemble de données seront diffusés via le protocole sans fil Bluetooth dans le rayon de la cabine du véhicule, avec une fréquence de rafraîchissement d'une minute,~~

~~— le couplage du dispositif externe avec l'interface ITS sera protégé par un code PIN dédié et aléatoire d'au moins 4 chiffres, enregistré et affichable dans chaque VU,~~

~~— en aucun cas la présence de l'interface ITS ne peut perturber ou affecter le fonctionnement correct et la sécurité de l'UEV .~~

~~D'autres données peuvent également être transmises en plus de l'ensemble de données existantes sélectionnées, considérées comme la liste minimale, à condition qu'elles ne puissent pas être considérées comme des données à caractère personnel.~~

~~L'appareil de contrôle doit~~ **~~pouvoir~~** ~~informer les autres dispositifs~~ **~~faisant partie du réseau du véhicule~~** ~~du consentement du conducteur.~~

~~Lorsque le contact du véhicule est en position MARCHE, ces données sont transmises en permanence.~~

201) L'interface de liaison série spécifiée à ~~l'annexe~~ **l'appendice** 1B du ~~règlement (CEE) n° 3821/85~~**présent Accord**, tel que modifié en dernier lieu, peut continuer à équiper les tachygraphes afin d'assurer leur compatibilité avec les équipements de génération antérieure. **La liaison série fait partie du réseau du véhicule, conformément à l'exigence 200** ~~Quoi qu'il en soit, le consentement du conducteur est toujours nécessaire lorsque des données personnelles sont transmises~~.

3.21 Étalonnage

202) La fonction d'étalonnage permet :

- Le couplage automatique du capteur de mouvement avec l'UEV ;
- Le couplage automatique du dispositif GNSS externe avec l'UEV, le cas échéant ;
- L'adaptation numérique de la constante (k) de l'appareil de contrôle au coefficient caractéristique du véhicule (w) ;
- La remise à l'heure pendant la période de validité de la carte d'atelier insérée ;
- L'ajustement du kilométrage ;
- La mise à jour des données d'identification du capteur de mouvement stockées dans la mémoire ;
- La mise à jour, le cas échéant, des données d'identification du dispositif GNSS externe stockées dans la mémoire ;
- La mise à jour des types et des identifiants de tous les scellements en place ;
- La mise à jour ou la confirmation d'autres paramètres connus par l'appareil de contrôle : identification du véhicule, w, l, taille des pneumatiques et réglages du limiteur de vitesse le cas échéant**, et type de chargement par défaut ;**
- **Le stockage automatique du pays dans lequel l'étalonnage a été effectué, ainsi que la date et l'heure auxquelles la position utilisée pour déterminer ce pays a été fournie par le récepteur GNSS.**

203) En outre, la fonction d'étalonnage doit rendre impossible l'utilisation de cartes tachygraphiques de première génération dans l'appareil de contrôle, pour autant que les conditions spécifiées ~~à l'appendice~~ **au sous-appendice** 15 soient remplies.

204) Le couplage du capteur de mouvement à l'UEV consiste au moins en :

- La mise à jour des données d'installation du capteur de mouvement détenues par le capteur de mouvement (si nécessaire) ;
- La copie dans la mémoire de l'UEV des données d'identification nécessaires du capteur de mouvement.

205) Le couplage du dispositif GNSS externe avec l'UEV consiste au moins en :

- La mise à jour des données d'installation du dispositif GNSS externe contenues dans le dispositif GNSS externe (si nécessaire) ;
- La copie dans la mémoire de l'UEV, à partir du dispositif GNSS externe, des données d'identification nécessaires du dispositif GNSS externe, y compris son numéro de série.

~~Le couplage doit être suivi par la vérification des informations de positionnement du GNSS~~.

206) La fonction d'étalonnage doit permettre la saisie des données nécessaires par l'intermédiaire de la connexion de téléchargement/étalonnage conformément au protocole d'étalonnage défini ~~à l'appendice~~ **au sous-appendice** 8. La fonction d'étalonnage peut également permettre la saisie des données nécessaires par d'autres moyens.

3.22 Contrôles routiers d'étalonnage

207) La fonction de contrôle routier d'étalonnage doit permettre la lecture des numéros de série du capteur de mouvement (qui peut être intégré dans l'adaptateur) et du dispositif GNSS externe (le cas échéant) qui sont connectés à l'UEV au moment de la demande.

208) Cette lecture doit au moins être possible sur l'unité embarquée au moyen de commandes se trouvant dans les menus.

209) La fonction de contrôle routier d'étalonnage doit également permettre le contrôle de la sélection du mode d'entrée/sortie de la ligne de signalisation d'entrée/sortie du connecteur d'étalonnage spécifié ~~à l'appendice~~ **au sous-appendice** 6, par l'intermédiaire de l'interface avec la ligne K. Cela doit être réalisé dans le cadre de la session de réglage ECUAdjustmentSession, comme spécifié dans la section 7 (Contrôle des impulsions d'essai − Unité fonctionnelle de contrôle des entrées/sorties) ~~de l'appendice~~ **du sous-appendice** 8.

Lorsque le mode d'entrée/sortie de la ligne de signalisation d'entrée/sortie du connecteur d'étalonnage est actif conformément à la présente exigence, l'avertissement « conduite sans carte appropriée » (exigence 75) ne doit pas être déclenché par l'unité embarquée sur le véhicule.

3.23 Remise à l'heure

210) La fonction de remise à l'heure doit permettre le réglage automatique de l'heure. Deux sources de données temporelles sont utilisées par l'appareil de contrôle pour la remise à l'heure : 1) l'horloge interne de l'UEV et 2) le récepteur GNSS.

211) L'heure de l'horloge interne de l'UEV est réglée automatiquement **à des intervalles de temps variables** ~~toutes les 12 heures au maximum~~. **La remise à l'heure automatique est déclenchée entre 72 h et 168 h après le réglage précédent, et après que l'UEV a pu accéder à l'heure GNSS par l'intermédiaire d'un message de position authentifiée valide, conformément au sous-appendice 12. Néanmoins, le réglage de l'heure ne doit jamais entraîner un réajustement supérieur à la dérive temporelle maximale accumulée par jour, telle que calculée par le fabricant de l'UEV en application de l'exigence 41b. Si la différence entre l'heure de l'horloge interne de l'UEV et celle du récepteur GNSS est supérieure à la dérive temporelle maximale accumulée par jour, il conviendra de**

rapprocher autant que possible l'heure de l'horloge interne de l'UEV de celle du récepteur GNSS. Le réglage de l'heure ne peut être effectué que si l'heure fournie par le récepteur GNSS est obtenue par l'intermédiaire des messages de position authentifiée, comme indiqué au sous-appendice 12. ~~Lorsque ce délai a expiré et **que le réajustement n'est pas possible car** le signal GNSS n'est pas disponible, le réglage de l'heure se fait dès que l'UEV est en mesure d'accéder à une heure valable fournie par le récepteur GNSS, selon les conditions d'allumage du véhicule.~~ **L'heure indiquée dans le message de position authentifiée** est la base temps pour le réglage automatique de l'horloge interne de l'UEV ~~déterminée à partir du récepteur GNSS~~. ~~Un événement «Conflit temporel» est déclenché si l'heure courante dévie de plus d'une (1) minute par rapport à l'information temps fournie par le récepteur GNSS.~~

212) La fonction de remise à l'heure doit également permettre de déclencher le réglage de l'heure courante, en mode étalonnage.

Les ateliers peuvent régler l'heure :

- **Soit en introduisant une valeur temporelle dans l'UEV, en utilisant le service WriteDataByIdentifier, conformément à la section 6.2 du sous-appendice 8 ;**
- **Soit en demandant la synchronisation de l'horloge de l'UEV avec l'heure fournie par le récepteur GNSS. Le réglage de l'heure ne peut être effectué que si l'heure fournie par le récepteur GNSS est obtenue par l'intermédiaire des messages de position authentifiée. Dans ce dernier cas, le service RoutineControl doit être utilisé comme prévu au chapitre 8 du sous-appendice 8.**

3.24 Caractéristiques de performance

213) L'unité embarquée sur le véhicule et le dispositif GNSS externe doivent pouvoir fonctionner correctement dans une gamme de températures comprise entre -20 °C et 70 °C, et le capteur de mouvement dans une gamme de températures comprise entre -40 °C et 135 °C. Le contenu de la mémoire doit être conservé jusqu'à des températures de -40 °C.

214) Le tachygraphe doit pouvoir fonctionner correctement dans une gamme d'humidité comprise entre 10 % et 90 %.

215) Les scellements utilisés dans le tachygraphe intelligent doivent résister aux mêmes conditions que celles applicables aux composants du tachygraphe sur lesquels ils sont apposés.

216) L'appareil de contrôle doit être protégé contre les surtensions, l'inversion de la polarité de son alimentation électrique et les courts-circuits.

217) Les capteurs de mouvement doivent :

- Soit réagir à un champ magnétique qui perturbe la détection des mouvements du véhicule. Dans ces circonstances, l'unité embarquée enregistrera et stockera une anomalie du capteur (exigence 88) ;
- Soit posséder un élément de détection protégé des champs magnétiques ou insensible à ceux-ci.

218) L'appareil de contrôle et le dispositif GNSS externe doivent être conformes ~~à la réglementation internationale R10 de l'ECE-ONU~~ **au Règlement ONU nº 10** et être protégés contre les décharges électrostatiques et les variations électrostatiques transitoires.

3.25 Matériaux

219) Tous les éléments constituant l'appareil de contrôle doivent être faits de matériaux d'une stabilité et d'une résistance mécanique suffisantes, et présenter des caractéristiques électriques et magnétiques stables.

220) Toutes les parties internes de l'appareil doivent être protégées contre l'humidité et la poussière dans les conditions normales d'utilisation.

221) L'unité embarquée sur le véhicule et le dispositif GNSS externe doivent satisfaire au niveau de protection IP 40, et le capteur de mouvement au niveau de protection IP 64, selon la norme CEI 60529:1989, y compris les amendements A1:1999 et A2:2013.

222) L'appareil de contrôle doit être conforme aux spécifications techniques applicables en matière de conception ergonomique.

223) L'appareil de contrôle doit être protégé contre les détériorations accidentelles.

3.26 Inscriptions

224) Si l'appareil de contrôle affiche la vitesse et le kilométrage du véhicule, les détails suivants doivent apparaître :

- À côté du chiffre indiquant la distance parcourue, l'unité de mesure de cette distance, indiquée par l'abréviation « km » ;
- À côté du chiffre indiquant la vitesse, l'indication « km/h ».

L'appareil de contrôle peut également être commuté de manière à afficher la vitesse en miles par heure, auquel cas l'unité de mesure de la vitesse sera indiquée par l'abréviation « mph ». L'appareil de contrôle peut également être commuté de manière à afficher la distance en miles, auquel cas l'unité de mesure de la distance sera indiquée par l'abréviation « mi ».

225) Une plaque signalétique doit être fixée sur chaque composant séparé de l'appareil de contrôle et doit comporter les indications suivantes :

- Nom et adresse du fabricant ~~de l'appareil~~ ;
- Numéro de référence du fabricant et année de fabrication ~~de l'appareil~~ ;
- Numéro de série ~~de l'appareil~~ ;
- Marque d'homologation ~~de l'appareil~~.

226) Lorsque l'espace disponible est insuffisant pour faire figurer l'ensemble des indications précitées, la plaque signalétique doit indiquer au moins : le nom ou le logo du fabricant, et le numéro de la pièce ~~de l'appareil~~.

3.27 Surveillance des passages de frontières

226a) Cette fonction permet de détecter, lorsque le véhicule a franchi la frontière d'un pays, le pays de provenance et le pays de destination.

226b) La détection du passage de frontière se fonde sur la position mesurée par l'appareil de contrôle et sur la carte numérique stockées conformément au point 3.12.19.

226c) Lorsque le véhicule est présent dans un pays pour une durée inférieure à 120 s, les passages de frontières associés ne doivent pas être enregistrés.

3.28 Mise à jour logicielle

226d) L'unité embarquée sur le véhicule doit comporter une fonction assurant la mise à jour des logiciels lorsque celle-ci ne nécessite pas de ressources matérielles autres que celles prévues à l'exigence 226f et que les autorités d'homologation autorisent les mises à jour logicielle sur la base de l'unité embarquée existante homologuée conformément au présent Accord.

226e) La fonction de mise à jour logicielle est conçue pour prendre en charge les fonctionnalités suivantes, lorsqu'elles sont légalement requises :

- **La modification des fonctions visées au point 2.2, à l'exception de la fonction de mise à jour logicielle elle-même ;**
- **L'ajout de nouvelles fonctions directement liées à l'application de la législation de l'UE sur le transport par route ;**
- **La modification des modes de fonctionnement visés au point 2.3 ;**
- **La modification de la structure des fichiers, par exemple l'ajout de nouvelles données ou l'augmentation de la taille des fichiers ;**
- **Le déploiement de correctifs logiciels pour remédier aux défauts des logiciels ainsi qu'aux failles de sécurité ou encore pour contrer les attaques signalées contre les fonctions de l'appareil de contrôle.**

226f) L'unité embarquée sur le véhicule doit fournir gratuitement au moins 35 % des ressources matérielles nécessaires à la mise à jour des logiciels et des données en application de l'exigence 226e) et au moins 65 % des ressources matérielles nécessaires à la mise à jour de la carte numérique sur la base des ressources requises pour la version 2021 de la carte de niveau NUTS 0.

4. Exigences de fabrication et de fonctionnement applicables aux cartes tachygraphiques

4.1 Données visibles

Le recto de la carte doit comporter :

227) Les mots « carte de conducteur », « carte de contrôleur », « carte d'atelier » ou « carte d'entreprise » imprimés en majuscules dans la ou les langues officielles de ~~l'État membre~~ **la Partie contractante** qui a délivré la carte, selon le type de carte ;

228) Le nom de ~~l'État membre~~ **la Partie contractante** qui a délivré la carte (facultatif) ;

229) **Pour les États membres de l'UE**, le signe distinctif de l'État membre qui a délivré la carte, imprimé en négatif dans un rectangle bleu et entouré de 12 étoiles jaunes. Les signes distinctifs sont les suivants :

B	Belgique	LV	Lettonie
BG	Bulgarie	L	Luxembourg
CZ	République tchèque	LT	Lituanie
CY	Chypre	M	Malte
DK	Danemark	NL	Pays-Bas
D	Allemagne	A	Autriche
EST	Estonie	PL	Pologne
GR	Grèce	P	Portugal
		RO	Roumanie
		SK	Slovaquie
		SLO	Slovénie
E	Espagne	FIN	Finlande

B	Belgique	LV	Lettonie
BG	Bulgarie	L	Luxembourg
CZ	République tchèque	LT	Lituanie
CY	Chypre	M	Malte
F	France	S	Suède
HR	Croatie		
H	Hongrie		
IRL	Irlande	UK	Royaume-Uni
I	Italie		

Pour les Parties contractantes non membres de l'UE, le signe distinctif de la Partie contractante qui a délivré la carte. Les signes distinctifs des Parties contractantes non membres de l'Union européenne sont ceux définis dans la Convention de Vienne sur la circulation routière de 1968 et dans la Convention de Genève sur la circulation routière de 1949.

230) Des indications particulières concernant la carte délivrée, numérotées comme suit :

	Carte de conducteur	*Carte de contrôleur*	*Carte d'entreprise ou d'atelier*
1.	nom du conducteur	nom de l'organisme de contrôle	nom de l'entreprise ou de l'atelier
2.	prénom(s) du conducteur	nom du contrôleur (le cas échéant)	nom du détenteur de la carte (le cas échéant)
3.	date de naissance du conducteur	prénom(s) du contrôleur (le cas échéant)	prénom(s) du détenteur de la carte (le cas échéant)
4.a	date de début de validité de la carte		
4.b	date d'expiration de la carte		
4.c	la désignation de l'autorité qui a délivré la carte (peut être imprimée au verso)		
4.d	un numéro différent de celui indiqué au point 5, à des fins administratives (facultatif)		
5.a	numéro du permis de conduire (à la date de délivrance de la carte de conducteur)	-	-
5.b	numéro de la carte		
6.	photographie du conducteur	photographie du contrôleur (facultatif)	photographie du monteur (facultatif)
7.	signature du détenteur (facultatif)		
8.	lieu habituel de résidence, ou adresse postale du détenteur (facultatif)	adresse postale de l'organisme de contrôle	adresse postale de l'entreprise ou de l'atelier

231) Les dates sont indiquées sous la forme « jj/mm/aaaa » ou « jj.mm.aaaa » (jour, mois, année).

Le verso de la carte doit comporter :

232) Une légende des numéros indiqués au recto ;

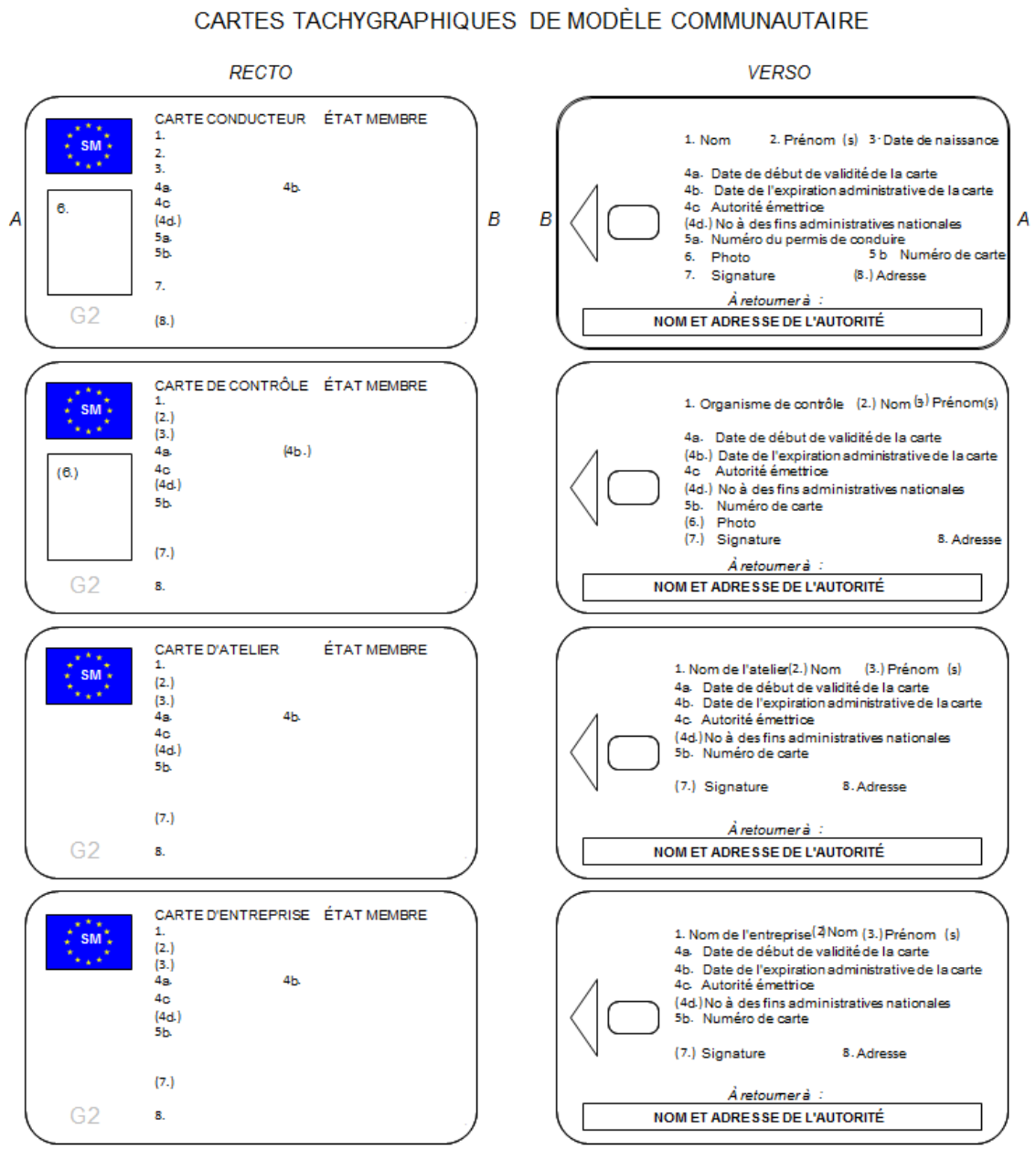
233) Avec l'accord écrit exprès du détenteur, des informations non liées à l'administration de la carte peuvent également être indiquées, pour autant qu'elles ne modifient en rien l'utilisation du modèle comme carte tachygraphique.

234) Les cartes tachygraphiques doivent être imprimées sur les fonds de couleur suivants :

- Carte de conducteur : blanc ;
- Carte de contrôleur : bleu ;
- Carte d'atelier : rouge ;
- Carte d'entreprise : jaune.

235) Les cartes tachygraphiques présentent au moins les éléments de protection contre la contrefaçon et la manipulation suivants :

- Impression de fond de sécurité finement guillochée et irisée ;
- Chevauchement de l'impression de fond de sécurité et de la photographie ;
- Au moins une ligne bicolore micro-imprimée.



~~Après consultation de la Commission, les États membres~~

~~Bernardo vérifiera la nécessité de fournir les modèles en double comme dans l'original.~~

236) ~~Après consultation de la Commission, L~~es ~~États membres~~ **Parties contractantes** peuvent ajouter des couleurs et des inscriptions, tels que des symboles nationaux et des éléments de sécurité, sans préjudice des autres dispositions ~~de la présente annexe~~ **du présent appendice**.

~~Les cartes temporaires visées à l'article 26, paragraphe 4, du règlement (UE) n° 165/2014 doivent être conformes aux dispositions de la présente annexe.~~

237) **Réservé.**

4.2 Sécurité

La sécurité du système vise à protéger l'intégrité et l'authenticité des données échangées entre les cartes et l'appareil de contrôle, ainsi que l'intégrité et l'authenticité des données téléchargées à partir des cartes, en autorisant uniquement certaines opérations d'inscription

sur les cartes par l'appareil de contrôle, en décryptant certaines données, en excluant toute possibilité de falsification des données stockées sur les cartes, en empêchant les manipulations et en détectant toute tentative en ce sens.

238) Afin de garantir la sécurité du système, les cartes tachygraphiques doivent satisfaire aux exigences de sécurité définies dans les ~~appendices~~ **sous-appendices** 10 et 11.

239) Les cartes tachygraphiques doivent pouvoir être lues par d'autres appareils, tels que des micro-ordinateurs.

4.3 Normes

240) Les cartes tachygraphiques doivent être conformes aux normes suivantes :

- ISO/CEI 7810 Cartes d'identification − Caractéristiques physiques ;
- ISO/CEI 7816 Cartes d'identification − Cartes à circuit intégré :
  - Partie 1 : caractéristiques physiques ;
  - Partie 2 : dimensions et emplacement des contacts (ISO/CEI 7816-2:2007) ;
  - Partie 3 : interface électrique et protocoles de transmission (ISO/CEI 7816-3:2006) ;
  - Partie 4 : organisation, sécurité et commandes pour les échanges (ISO/CEI 7816-4:2013 + Cor 1:2014) ;
  - Partie 6 : éléments de données intersectoriels pour les échanges (ISO/CEI 7816-6:2004 + Cor 1:2006) ;
  - Partie 8 : commandes pour des opérations de sécurité (ISO/CEI 7816-8:2004).

Les cartes tachygraphiques doivent être testées conformément à la norme ISO/CEI 10373-3:2010 « Cartes d'identification − Méthodes d'essai − Partie 3 : cartes à circuit(s) intégré(s) à contacts et dispositifs d'interface assimilés ».

4.4 Spécifications environnementales et électriques

241) Les cartes tachygraphiques doivent pouvoir fonctionner correctement dans toutes les conditions climatiques normalement observées sur le territoire ~~communautaire~~ **des Parties contractantes**, et au minimum dans une gamme de température comprise entre -25 °C et +70 °C, avec des pointes occasionnelles à +85 °C, « occasionnelles » signifiant d'une durée inférieure ou égale à 4 heures et survenant au maximum à 100 reprises au cours de la durée de vie de la carte.

242) Les cartes tachygraphiques doivent pouvoir fonctionner correctement dans une gamme d'humidité comprise entre 10 % et 90 %.

243) Les cartes tachygraphiques doivent pouvoir fonctionner correctement pendant une période de cinq ans si elles sont utilisées conformément aux spécifications environnementales et électriques.

244) En fonctionnement, les cartes tachygraphiques doivent satisfaire au Règlement ONU n° 10, relatif à la compatibilité électromagnétique, et doivent être protégées contre les décharges électrostatiques.

4.5 Stockage des données

Aux fins du présent paragraphe,

- Les heures sont enregistrées à la minute près, sauf indication contraire ;
- Le kilométrage est enregistré au kilomètre près ;
- Les vitesses sont enregistrées au kilomètre/heure près ;

– Les positions (latitudes et longitudes) sont enregistrées en degrés et en minutes, au dixième de minute près.

Les fonctions, les commandes et les structures logiques des cartes tachygraphiques, qui satisfont aux exigences en matière de stockage des données, sont spécifiées ~~à l'appendice~~ **au sous-appendice** 2.

Sauf indication contraire, le stockage de données sur les cartes tachygraphiques doit être organisé de telle manière que les données nouvelles remplacent les données stockées les plus anciennes dans les cas où la capacité de mémoire prévue pour les enregistrements concernés est épuisée.

245) Le présent paragraphe précise la capacité minimale de stockage des divers fichiers d'application. Les cartes tachygraphiques doivent pouvoir indiquer à l'appareil de contrôle la capacité réelle de stockage de ces fichiers.

246) ~~Toutes les~~ Des données supplémentaires ~~qui~~ peuvent être stockées sur les cartes tachygraphiques, **à condition que leur stockage soit conforme à la législation applicable en matière de protection des données**~~liées à d'autres applications éventuellement présentes sur la carte, doivent être stockées conformément à la directive 95/46/CE du 24 octobre 1995 **relative à la protection des données à caractère personnel applicable sur le territoire des Parties contractantes, et à la Convention** relative à la protection des personnes physiques à l'égard du traitement **automatique** des données à caractère personnel et à la libre circulation de ces données[8], à la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [9] et en conformité avec l'article 7 du règlement (UE) n° 165/2014~~.

247) Chaque fichier maître (MF) d'une carte tachygraphique doit contenir jusqu'à cinq fichiers élémentaires (EF) pour la gestion de la carte, l'application et les identifications de puce, ainsi que les deux fichiers spécialisés (DF) suivants :

– DF Tachograph, qui contient l'application accessible aux unités embarquées de première génération et est également présent sur les cartes tachygraphiques de première génération ;

– DF Tachograph_G2, qui contient l'application uniquement accessible aux unités embarquées de deuxième génération et est seulement présent sur les cartes tachygraphiques de deuxième génération.

Remarque : la version 2 des cartes de deuxième génération contient des fichiers élémentaires supplémentaires dans DF Tachograph_G2.

La structure des cartes tachygraphiques est présentée en détail ~~à l'appendice~~ **au sous-appendice** 2.

4.5.1 Fichiers élémentaires pour l'identification et la gestion des cartes

4.5.2 Identification des cartes à circuit intégré

248) Les cartes tachygraphiques doivent pouvoir stocker les données suivantes pour l'identification des cartes intelligentes :

– Arrêt d'horloge (clockstop) ;

– Numéro de série de la carte (y compris les références de fabrication) ;

– Numéro d'homologation de la carte ;

– Identification personnelle de la carte ;

– Identification de l'intégrateur ;

~~[8] JO L 281 du 23.11.1995, p. 31.~~

~~[9] JO L 201 du 31.7.2002, p. 37.~~

– Identificateur du circuit intégré.

4.5.2.1 Identification du microprocesseur

249) Les cartes tachygraphiques doivent pouvoir stocker les données suivantes pour l'identification des circuits intégrés :

– Numéro de série du circuit intégré ;

– Références de fabrication du circuit intégré.

4.5.2.2 DIR (présent uniquement sur les cartes tachygraphiques de deuxième génération)

250) Les cartes tachygraphiques doivent pouvoir stocker les objets de données pour l'identification des applications spécifiés dans ~~l'appendice~~ **le sous-appendice** 2.

4.5.2.3 Informations ATR (conditionnelles, présentes uniquement sur les cartes tachygraphiques de deuxième génération)

251) Les cartes tachygraphiques doivent pouvoir stocker l'objet de données contenant les informations de longueur étendue spécifié dans ~~l'appendice~~ **le sous-appendice** 2, lorsque la carte de tachygraphe prend en charge les zones de longueur étendue.

4.5.2.4 Informations de longueur étendue (conditionnelles, présentes uniquement sur les cartes tachygraphiques de deuxième génération)

252) Les cartes tachygraphiques doivent pouvoir stocker les objets de données contenant les informations de longueur étendue spécifiés dans ~~l'appendice~~ **le sous-appendice** 2, lorsque la carte de tachygraphe prend en charge les zones de longueur étendue.

4.5.3 Carte de conducteur

4.5.3.1 Application tachygraphique (accessible aux unités embarquées de première et deuxième générations)

4.5.3.1.1 Identification des applications

253) La carte de conducteur doit permettre le stockage des données suivantes pour l'identification des applications :

– Identification de l'application tachygraphique ;

– Identification du type de carte tachygraphique.

4.5.3.1.2 Clés et certificats

254) La carte de conducteur doit pouvoir stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié ~~à l'appendice~~ **au sous-appendice** 11, partie A.

4.5.3.1.3 Identification de la carte

255) La carte de conducteur doit pouvoir stocker les données suivantes pour l'identification de la carte :

– Numéro de la carte ;

– ~~État membre~~ **Partie contractante** qui a délivré la carte, nom de l'autorité de délivrance, date de délivrance ;

– Date de début de validité de la carte et date d'expiration.

4.5.3.1.4 Identification du détenteur de la carte

256) La carte de conducteur doit permettre le stockage des données suivantes pour l'identification du détenteur de la carte :

– Nom du détenteur ;

– Prénom(s) du détenteur ;

– Date de naissance ;

– Langue habituelle.

4.5.3.1.5 Téléchargement d'une carte

257) La carte de conducteur doit permettre le stockage des données suivantes concernant le téléchargement d'une carte :

– Date et heure du dernier téléchargement de la carte (à d'autres fins que le contrôle).

258) La carte de conducteur doit permettre le stockage d'un enregistrement de ce type.

4.5.3.1.6 Renseignements concernant le permis de conduire

259) La carte de conducteur doit pouvoir stocker les données suivantes concernant le permis de conduire :

– ~~État membre~~ **Partie contractante** qui a délivré le permis, nom de l'autorité de délivrance ;

– Numéro du permis de conduire (à la date de délivrance de la carte).

4.5.3.1.7 Données relatives aux événements

Aux fins du présent point, l'heure est enregistrée à la seconde près.

260) La carte de conducteur doit permettre le stockage des données liées aux événements suivants détectés par l'appareil de contrôle alors que la carte est insérée :

– Chevauchement temporel (lorsque la carte est la cause de l'événement) ;

– Insertion d'une carte en cours de conduite (lorsque cet événement concerne la carte) ;

– Clôture incorrecte de la dernière session (lorsque cet événement concerne la carte) ;

– Interruption de l'alimentation électrique ;

– Erreur sur les données de mouvement ;

– Tentatives d'atteinte à la sécurité.

261) La carte de conducteur doit permettre le stockage des données suivantes concernant ces événements :

– Code de l'événement ;

– Date et heure du début de l'événement (ou de l'insertion de la carte dans le cas où l'événement était en cours à ce moment-là) ;

– Date et heure de la fin de l'événement (ou du retrait de la carte dans le cas où l'événement était en cours à ce moment-là) ;

– Numéro et ~~État membre~~ **Partie contractante** d'immatriculation du véhicule dans lequel l'événement est survenu.

Remarque concernant l'événement « chevauchement temporel » :

– La date et l'heure du début de l'événement doivent correspondre à la date et à l'heure du retrait de la carte du véhicule précédent ;

– La date et l'heure de la fin de l'événement doivent correspondre à la date et à l'heure de l'insertion de la carte dans le véhicule actuel ;

– Les données relatives au véhicule doivent correspondre au véhicule où l'événement est apparu.

Remarque concernant l'événement « clôture incorrecte de la dernière session » :

– La date et l'heure du début de l'événement doivent correspondre à la date et à l'heure de l'insertion de la carte correspondant à la session incorrectement clôturée ;

– La date et l'heure de la fin de l'événement doivent correspondre à la date et à l'heure de l'insertion de la carte pour la session au cours de laquelle l'événement a été détecté (session en cours) ;

– Les données relatives au véhicule doivent correspondre au véhicule dans lequel la session a été incorrectement clôturée.

262) La carte de conducteur doit permettre le stockage des données relatives aux six derniers événements de chaque type (soit 36 événements).

4.5.3.1.8 Données relatives aux anomalies

Aux fins du présent point, l'heure est enregistrée à la seconde près.

263) La carte de conducteur doit permettre le stockage des données relatives aux anomalies suivantes détectées par l'appareil de contrôle alors que la carte est insérée :

– Anomalie de la carte (lorsque la carte est l'objet de l'~~événement~~**anomalie**) ;

– Anomalie ~~de l'appareil de contrôle~~ ;

– **Anomalie de l'appareil de contrôle.**

264) La carte de conducteur doit permettre le stockage des données suivantes concernant ces anomalies :

– Code de l'anomalie ;

– Date et heure du début de l'anomalie (ou de l'insertion de la carte dans le cas où l'anomalie était en cours à ce moment-là) ;

– Date et heure de la fin de l'anomalie (ou du retrait de la carte dans le cas où l'anomalie était en cours à ce moment-là) ;

– Numéro et ~~État membre~~ **Partie contractante** d'immatriculation du véhicule dans lequel l'anomalie est survenue.

~~265) La carte de conducteur doit permettre le stockage des données relatives aux douze dernières anomalies de chaque type (soit 24 anomalies).~~ **La carte de conducteur doit permettre le stockage des données relatives aux 12 dernières anomalies de chaque type (soit 24 anomalies).**

4.5.3.1.9 Données relatives à l'activité du conducteur

266) La carte de conducteur doit pouvoir stocker, pour chaque jour civil au cours duquel la carte a été utilisée ou pour lequel le conducteur a saisi des activités manuellement, les données suivantes :

– Date ;

– Compteur de présence journalière (ajout d'une unité pour chacun de ces jours civils) ;

– Distance totale parcourue par le conducteur pendant cette journée ;

– Situation du conducteur à 00 h 00 ;

– En cas de changement d'activité du conducteur et/ou de changement de la situation de conduite et/ou d'insertion ou retrait de la carte de conducteur :

– Situation de conduite (ÉQUIPAGE, SEUL) ;

– Lecteur (CONDUCTEUR, CO-CONDUCTEUR) ;

– Situation de la carte (INSÉRÉE, NON INSÉRÉE) ;

– Activité (CONDUITE, DISPONIBILITÉ, TRAVAIL, INTERRUPTION/ REPOS) ;

– Heure du changement.

267) La mémoire de la carte de conducteur doit permettre le stockage des données relatives à l'activité du conducteur pendant au moins 28 jours (l'activité moyenne d'un conducteur est définie comme 93 changements d'activité par jour).

268) Les données énumérées aux exigences 261, 264 et 266 doivent être stockées d'une manière permettant de retrouver les activités dans l'ordre de leur occurrence, même en cas de chevauchement temporel.

4.5.3.1.10 Données concernant les véhicules utilisés

269) La carte de conducteur doit pouvoir stocker, pour chaque jour civil où la carte a été utilisée, et pour chaque période d'utilisation d'un véhicule donné ce jour-là (une période d'utilisation comprend tous les cycles consécutifs d'insertion/retrait de la carte dans le véhicule, en se plaçant du point de vue de la carte), les données suivantes :

– Date et heure de la première utilisation du véhicule (c'est-à-dire de la première insertion de la carte pour cette période d'utilisation du véhicule, ou 00 h 00 si la période d'utilisation est en cours à cette heure-là) ;

– Kilométrage du véhicule à ce moment ;

– Date et heure de la dernière utilisation du véhicule (c'est-à-dire le dernier retrait de la carte pour cette période d'utilisation du véhicule, ou 23 h 59 si la période d'utilisation est en cours à cette heure-là) ;

– Kilométrage du véhicule à ce moment ;

– Numéro et ~~État membre~~ **Partie contractante** d'immatriculation du véhicule.

270) La carte de conducteur doit pouvoir stocker au moins 84 enregistrements de ce type.

4.5.3.1.11 Lieux de début et/ou de fin des périodes de travail journalières

271) La carte de conducteur doit permettre le stockage des données suivantes relatives aux lieux de début et/ou de fin des périodes de travail journalières, saisis par le conducteur :

– Date et heure de la saisie (ou date/heure associée à la saisie, si celle-ci est réalisée au cours de la procédure de saisie manuelle) ;

– Type de saisie (début ou fin, condition de saisie) ;

– Pays et région saisis ;

– Kilométrage du véhicule.

272) La mémoire de la carte de conducteur doit pouvoir stocker au moins 42 paires d'enregistrements de ce type.

4.5.3.1.12 Données de session pour chaque carte

273) La carte de conducteur doit permettre le stockage des données suivantes concernant le véhicule dans lequel s'est ouverte la session en cours :

– Date et heure d'ouverture de la session (c'est-à-dire de l'insertion de la carte), à la seconde près ;

– Numéro et ~~État membre~~ **Partie contractante** d'immatriculation du véhicule.

4.5.3.1.13 Données relatives aux activités de contrôle

274) La carte de conducteur doit permettre le stockage des données suivantes relatives aux activités de contrôle :

– Date et heure du contrôle ;

– Numéro de la carte de contrôleur et ~~État membre~~ **Partie contractante** qui l'a délivrée ;

– Type de contrôle (affichage et/ou impression, et/ou téléchargement à partir de l'UEV et/ou de la carte (voir remarque)) ;

– Période téléchargée, le cas échéant ;

– Numéro et ~~État membre~~ **Partie contractante** d'immatriculation du véhicule dans lequel le contrôle a été effectué.

Remarque : le téléchargement d'une carte ne sera enregistré que s'il est effectué par l'intermédiaire d'un appareil de contrôle.

275) La carte de conducteur doit permettre le stockage d'un enregistrement de ce type.

4.5.3.1.14 Données relatives aux conditions particulières

276) La carte de conducteur doit permettre le stockage des données suivantes relatives aux conditions particulières saisies alors que la carte est insérée (quel que soit le lecteur) :

– Date et heure de la saisie ;

– Type de condition particulière.

277) La carte de conducteur doit pouvoir stocker au moins 56 enregistrements de ce type.

4.5.3.2 Application tachygraphique de deuxième génération (non accessible aux unités embarquées de première génération**, accessible aux unités embarquées de deuxième génération, versions 1 et 2**)

4.5.3.2.1 Identification des applications

278) La carte de conducteur doit pouvoir stocker les données suivantes pour l'identification des applications :

– Identification de l'application tachygraphique ;

– Identification du type de carte tachygraphique.

4.5.3.2.1.1 Identification des applications supplémentaires (non accessible aux unités embarquées de deuxième génération, version 1)

278a) La carte de conducteur doit pouvoir stocker des données pour l'identification des applications supplémentaires (applicable uniquement pour la version 2).

4.5.3.2.2 Clés et certificats

279) La carte de conducteur doit pouvoir stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié ~~à l'appendice~~ **au sous-appendice** 11, partie B.

4.5.3.2.3 Identification de la carte

280) La carte de conducteur doit pouvoir stocker les données suivantes pour l'identification de la carte :

– Numéro de la carte ;

– ~~État membre~~ **Partie contractante** qui a délivré la carte, nom de l'autorité de délivrance, date de délivrance ;

– Date de début de validité de la carte et date d'expiration.

4.5.3.2.4 Identification du détenteur de la carte

281) La carte de conducteur doit pouvoir stocker les données suivantes pour l'identification du détenteur de la carte :

– Nom du détenteur ;

– Prénom(s) du détenteur ;

– Date de naissance ;

– Langue habituelle.

4.5.3.2.5 Téléchargement d'une carte

282) La carte de conducteur doit permettre le stockage des données suivantes relatives au téléchargement d'une carte :

– Date et heure du dernier téléchargement de la carte (à d'autres fins que le contrôle).

283) La carte de conducteur doit permettre le stockage d'un enregistrement de ce type.

4.5.3.2.6 Renseignements concernant le permis de conduire

284) La carte de conducteur doit pouvoir stocker les données suivantes concernant le permis de conduire :

– ~~État membre~~ **Partie contractante** qui a délivré le permis, nom de l'autorité de délivrance ;

– Numéro du permis de conduire (à la date de la délivrance de la carte).

4.5.3.2.7 Données relatives aux événements

Aux fins du présent point, l'heure est enregistrée à la seconde près.

285) La carte de conducteur doit permettre le stockage des données liées aux événements suivants détectés par l'appareil de contrôle alors que la carte est insérée :

– Chevauchement temporel (lorsque la carte est la cause de l'événement) ;

– Insertion d'une carte en cours de conduite (lorsque cet événement concerne la carte) ;

– Clôture incorrecte de la dernière session (lorsque cet événement concerne la carte) ;

– Interruption de l'alimentation électrique ;

– Erreur de communication avec le dispositif de communication à distance ;

– Absence d'informations de positionnement en provenance du récepteur GNSS ;

– Erreur de communication avec le dispositif GNSS externe ;

– Erreur sur les données de mouvement ;

– Conflit concernant le mouvement du véhicule ;

– Tentatives d'atteinte à la sécurité ;

– Conflit temporel.

286) La carte de conducteur doit permettre le stockage des données suivantes concernant ces événements :

– Code de l'événement ;

– Date et heure du début de l'événement (ou de l'insertion de la carte dans le cas où l'événement était en cours à ce moment-là) ;

– Date et heure de la fin de l'événement (ou du retrait de la carte dans le cas où l'événement était en cours à ce moment-là) ;

– Numéro et ~~État membre~~ **Partie contractante** d'immatriculation du véhicule dans lequel l'événement est survenu.

Remarque concernant l'événement « chevauchement temporel » :

– La date et l'heure du début de l'événement doivent correspondre à la date et à l'heure du retrait de la carte du véhicule précédent ;

– La date et l'heure de la fin de l'événement doivent correspondre à la date et à l'heure de l'insertion de la carte dans le véhicule actuel ;

– Les données relatives au véhicule doivent correspondre au véhicule où l'événement est apparu.

Remarque concernant l'événement « clôture incorrecte de la dernière session » :

– La date et l'heure du début de l'événement doivent correspondre à la date et à l'heure de l'insertion de la carte correspondant à la session incorrectement clôturée ;

– La date et l'heure de la fin de l'événement doivent correspondre à la date et à l'heure de l'insertion de la carte pour la session au cours de laquelle l'événement a été détecté (session en cours) ;

– Les données relatives au véhicule doivent correspondre au véhicule dans lequel la session a été incorrectement clôturée.

287) La carte de conducteur doit permettre le stockage des données relatives aux ~~six~~ **12** derniers événements de chaque type (soit ~~66~~ **132** événements).

4.5.3.2.8 Données relatives aux anomalies

Aux fins du présent point, l'heure est enregistrée à la seconde près.

288) La carte de conducteur doit permettre le stockage des données relatives aux anomalies suivantes détectées par l'appareil de contrôle alors que la carte est insérée :

– Anomalie de la carte (lorsque la carte est l'objet de l'~~événement~~**anomalie**) ;

– **Anomalie de l'appareil de contrôle**.

289) La carte de conducteur doit permettre le stockage des données suivantes pour ces anomalies :

– Code de l'anomalie ;

– Date et heure du début de l'anomalie (ou de l'insertion de la carte dans le cas où l'anomalie était en cours à ce moment-là) ;

– Date et heure de la fin de l'anomalie (ou du retrait de la carte dans le cas où l'anomalie était en cours à ce moment-là) ;

– Numéro et ~~État membre~~ **Partie contractante** d'immatriculation du véhicule dans lequel l'anomalie est survenue.

290) La carte de conducteur doit permettre le stockage des données relatives aux ~~12~~ **24** dernières anomalies de chaque type (soit ~~24~~ **48** anomalies).

4.5.3.2.9 Données relatives à l'activité du conducteur

291) La carte de conducteur doit pouvoir stocker, pour chaque jour civil au cours duquel la carte a été utilisée ou pour lequel le conducteur a saisi des activités manuellement, les données suivantes :

– Date ;

– Compteur de présence journalière (ajout d'une unité pour chacun de ces jours civils) ;

– Distance totale parcourue par le conducteur pendant cette journée ;

– Situation du conducteur à 00 h 00 ;

  – En cas de changement d'activité du conducteur et/ou de changement de la situation de conduite et/ou d'insertion ou retrait de la carte de conducteur :

  – Situation de conduite (ÉQUIPAGE, SEUL) ;

  – Lecteur (CONDUCTEUR, CO-CONDUCTEUR) ;

  – Situation de la carte (INSÉRÉE, NON INSÉRÉE) ;

- Activité (CONDUITE, DISPONIBILITÉ, TRAVAIL, INTERRUPTION/ REPOS) ;
- Heure du changement.

292) La mémoire de la carte de conducteur doit permettre le stockage des données relatives à l'activité du conducteur pendant au moins ~~28~~**56** jours (**aux fins de la présente exigence,** l'activité moyenne d'un conducteur est définie comme ~~93~~**117** changements d'activité par jour).

293) Les données énumérées aux exigences 286, 289 et 291 doivent être stockées d'une manière permettant de retrouver les activités dans l'ordre de leur occurrence, même en cas de chevauchement temporel.

4.5.3.2.10 Données concernant les véhicules utilisés

294) La carte de conducteur doit pouvoir stocker, pour chaque jour civil où la carte a été utilisée, et pour chaque période d'utilisation d'un véhicule donné ce jour-là (une période d'utilisation comprend tous les cycles consécutifs d'insertion/retrait de la carte dans le véhicule, en se plaçant du point de vue de la carte), les données suivantes :

- Date et heure de la première utilisation du véhicule (c'est-à-dire de la première insertion de la carte pour cette période d'utilisation du véhicule, ou 00 h 00 si la période d'utilisation est en cours à cette heure-là) ;
- Kilométrage du véhicule au moment de cette première utilisation ;
- Date et heure de la dernière utilisation du véhicule (c'est-à-dire le dernier retrait de la carte pour cette période d'utilisation du véhicule, ou 23 h 59 si la période d'utilisation est en cours à cette heure-là) ;
- Kilométrage du véhicule au moment de cette dernière utilisation ;
- Numéro et ~~État membre~~ **Partie contractante** d'immatriculation du véhicule ;
- Numéro d'identification du véhicule (VIN).

295) La carte de conducteur doit pouvoir stocker ~~au moins 84~~**200** enregistrements de ce type.

4.5.3.2.11 Positions et lieux de début et/ou de fin des périodes de travail journalières

296) La carte de conducteur doit permettre le stockage des données suivantes relatives aux lieux de début et/ou de fin des périodes de travail journalières, saisis par le conducteur :

- Date et heure de la saisie (ou date/heure associée à la saisie, si celle-ci est réalisée au cours de la procédure de saisie manuelle) ;
- Type de saisie (début ou fin, condition de saisie) ;
- Pays et région saisis ;
- Kilométrage du véhicule ;
- Position du véhicule ;
- Précision GNSS, date et heure de détermination de la position.

297) La mémoire de la carte de conducteur doit pouvoir stocker ~~au moins 84 paires~~ **112** enregistrements de ce type.

4.5.3.2.12 Données de session pour chaque carte

298) La carte de conducteur doit permettre le stockage des données suivantes relatives au véhicule dans lequel s'est ouverte la session en cours :

- Date et heure d'ouverture de la session (c'est-à-dire de l'insertion de la carte), à la seconde près ;

– Numéro et ~~État membre~~ **Partie contractante** d'immatriculation du véhicule.

4.5.3.2.13 Données relatives aux activités de contrôle

299) La carte de conducteur doit permettre le stockage des données suivantes relatives aux activités de contrôle :

– Date et heure du contrôle ;

– Numéro de la carte de contrôleur et ~~État membre~~ **Partie contractante** qui l'a délivrée ;

– Type de contrôle (affichage et/ou impression, et/ou téléchargement à partir de l'UEV et/ou de la carte (voir remarque)) ;

– Période téléchargée, le cas échéant ;

– Numéro et ~~État membre~~ **Partie contractante** d'immatriculation du véhicule dans lequel le contrôle a été effectué.

Remarque : conformément aux exigences de sécurité, le téléchargement d'une carte ne sera enregistré que s'il est effectué par l'intermédiaire d'un appareil de contrôle.

300) La carte de conducteur doit permettre le stockage d'un enregistrement de ce type.

4.5.3.2.14 Données relatives aux conditions particulières

301) La carte de conducteur doit permettre le stockage des données suivantes relatives aux conditions particulières saisies alors que la carte est insérée (quel que soit le lecteur) :

– Date et heure de la saisie ;

– Type de condition particulière.

302) La carte de conducteur doit pouvoir stocker ~~au moins 56~~ **112** enregistrements de ce type.

4.5.3.2.15 Données concernant les unités embarquées utilisées

303) La carte de conducteur doit permettre le stockage des données suivantes concernant les différentes unités embarquées sur le véhicule dans lesquelles la carte a été utilisée :

– Date et heure du début de la période d'utilisation de l'unité embarquée (c'est-à-dire de la première insertion de la carte dans l'unité embarquée pour cette période) ;

– Fabricant de l'unité embarquée ;

– Type d'unité embarquée ;

– Numéro de version du logiciel de l'unité embarquée.

304) La carte de conducteur doit pouvoir stocker ~~au moins 84~~ **200** enregistrements de ce type.

4.5.3.2.16 Données relatives aux lieux où trois heures de temps de conduite ~~continue~~ **accumulé** sont atteintes

305) La carte de conducteur doit permettre le stockage des données suivantes relatives à la position du véhicule lorsque le temps de conduite ~~continue~~ **accumulé** ~~du conducteur~~ atteint un multiple de trois heures :

– Date et heure auxquelles le temps de conduite ~~continue~~ **accumulé** ~~du détenteur de la carte~~ atteint un multiple de trois heures ;

– Position du véhicule ;

– Précision GNSS, date et heure de détermination de la position ;

– **Kilométrage du véhicule**.

306) La carte de conducteur doit pouvoir stocker ~~au moins 252~~ **336** enregistrements de ce type.

4.5.3.2.17 État d'authentification des positions correspondant aux lieux de début et/ou de fin des périodes de travail journalières (non accessible aux unités embarquées de deuxième génération, version 1)

306a) La carte de conducteur doit permettre le stockage de données supplémentaires se rapportant aux lieux de début et/ou de fin des périodes de travail journalières, saisies par le conducteur conformément au point 4.5.3.2.11 :

- **La date et l'heure de la saisie, lesquelles doivent correspondre exactement à la date et à l'heure stockées dans EF Places sous DF Tachographe_G2 ;**
- **Un marqueur indiquant si la position a été authentifiée.**

306b) La mémoire de la carte de conducteur doit pouvoir stocker 112 enregistrements de ce type.

4.5.3.2.18 État d'authentification des positions correspondant aux lieux où les trois heures de temps de conduite accumulé sont atteintes (non accessible aux unités embarquées de deuxième génération, version 1)

306c) La carte de conducteur doit permettre le stockage de données supplémentaires se rapportant à la position du véhicule correspondant au lieu où le temps de conduite accumulé atteint un multiple de trois heures conformément au point 4.5.3.2.16 :

- **La date et l'heure auxquelles le temps de conduite accumulé atteint un multiple de trois heures, lesquelles doivent correspondre exactement à la date et à l'heure stockées dans EF GNSS_Places sous DF Tachograph_G2 ;**
- **Un marqueur indiquant si la position a été authentifiée.**

306d) La carte de conducteur doit pouvoir stocker 336 enregistrements de ce type.

4.5.3.2.19 Passages de frontières (non accessible aux unités embarquées de deuxième génération, version 1)

306e) La carte de conducteur doit pouvoir stocker les données suivantes concernant les passages de frontières soit lors de l'insertion de la carte conformément à l'exigence 147b, soit alors que la carte est déjà insérée :

- **Le pays que le véhicule quitte ;**
- **Le pays dans lequel le véhicule entre ;**
- **La date et l'heure auxquelles le véhicule a franchi la frontière ;**
- **La position du véhicule au moment du franchissement de la frontière ;**
- **La précision GNSS ;**
- **Un marqueur indiquant si la position a été authentifiée ;**
- **Le kilométrage du véhicule.**

306f) La carte de conducteur doit permettre le stockage de 1 120 enregistrements de ce type.

4.5.3.2.20 Opérations de chargement/déchargement (non accessible aux unités embarquées de deuxième génération, version 1)

306g) La carte de conducteur doit permettre le stockage des données suivantes concernant les opérations de chargement/déchargement :

- **Le type d'opération (chargement, déchargement ou chargement/déchargement simultanés) ;**
- **La date et l'heure de l'opération de chargement/déchargement ;**

– **La position du véhicule ;**

– **La précision GNSS, la date et l'heure de détermination de la position ;**

– **Un marqueur indiquant si la position a été authentifiée ;**

– **Le kilométrage du véhicule.**

306h) La carte de conducteur doit pouvoir stocker 1 624 opérations de chargement/déchargement.

4.5.3.2.21 Saisies du type de chargement (non accessible aux unités embarquées de deuxième génération, version 1)

306i) La carte de conducteur doit permettre le stockage des données suivantes relatives au type de chargement saisi automatiquement par l'UEV à chaque insertion de carte :

– **Le type de chargement saisi (marchandises ou passagers) ;**

– **La date et l'heure de la saisie.**

306j) La carte de conducteur doit pouvoir stocker 336 enregistrements de ce type.

4.5.3.2.22 Configurations de l'UEV (non accessible aux unités embarquées de deuxième génération, version 1)

306k) La carte de conducteur doit pouvoir stocker les paramètres spécifiques du tachygraphe du détenteur de la carte.

306l) La capacité de stockage de la carte de conducteur pour les paramètres spécifiques du tachygraphe du détenteur de la carte doit être de 3 072 octets.

4.5.4 Carte d'atelier

4.5.4.1 Application tachygraphique (accessible aux unités embarquées de première et deuxième générations)

4.5.4.1.1 Identification des applications

307) La carte d'atelier doit permettre le stockage des données suivantes pour l'identification des applications :

– Identification de l'application tachygraphique ;

– Identification du type de carte tachygraphique.

4.5.4.1.2 Clés et certificats

308) La carte d'atelier doit pouvoir stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié ~~à l'appendice~~ **au sous-appendice** 11, partie A.

309) La carte d'atelier doit pouvoir stocker un numéro d'identification personnel (code PIN).

4.5.4.1.3 Identification de la carte

310) La carte d'atelier doit pouvoir stocker les données suivantes pour l'identification de la carte :

– Numéro de la carte ;

– ~~État membre~~ **Partie contractante** qui a délivré la carte, nom de l'autorité de délivrance, date de délivrance ;

– Date de début de validité de la carte et date d'expiration.

4.5.4.1.4 Identification du détenteur de la carte

311) La carte d'atelier doit permettre le stockage des données suivantes pour l'identification du détenteur de la carte :

- Nom de l'atelier ;
- Adresse de l'atelier ;
- Nom du détenteur ;
- Prénom(s) du détenteur ;
- Langue habituelle.

4.5.4.1.5 Téléchargement d'une carte

312) La carte d'atelier doit pouvoir stocker des données relatives au téléchargement des cartes de la même manière qu'une carte de conducteur.

4.5.4.1.6 Données relatives à l'étalonnage et à la remise à l'heure

313) La carte d'atelier doit permettre le stockage des données relatives aux étalonnages et/ou aux remises à l'heure réalisés alors que la carte est insérée dans l'appareil.

314) Chaque enregistrement d'étalonnage doit pouvoir stocker les données suivantes :

- Objet de l'étalonnage (activation, première installation, installation, inspection périodique) ;
- Identification du véhicule ;
- Paramètres mis à jour ou confirmés (w, k, l, taille des pneumatiques, réglage du limiteur de vitesse, compteur kilométrique (valeurs nouvelle et ancienne), date et heure (valeurs nouvelle et ancienne)) ;
- Identification de l'appareil de contrôle (numéro de référence et numéro de série de l'UEV, numéro de série du capteur de mouvement).

315) La carte d'atelier doit pouvoir stocker au moins 88 enregistrements de ce type.

316) La carte d'atelier doit comporter un compteur indiquant le nombre total d'étalonnages réalisés avec la carte.

317) La carte d'atelier doit comporter un compteur indiquant le nombre d'étalonnages réalisés depuis le dernier téléchargement.

4.5.4.1.7 Données relatives aux événements et aux anomalies

318) La carte d'atelier doit pouvoir stocker des données relatives aux événements et aux anomalies de la même manière qu'une carte de conducteur.

319) La carte d'atelier doit permettre le stockage des trois derniers événements de chaque type (soit 18 événements) et des six dernières anomalies de chaque type (soit 12 anomalies).

4.5.4.1.8 Données relatives à l'activité du conducteur

320) La carte d'atelier doit pouvoir stocker des données relatives à l'activité du conducteur de la même manière que la carte de conducteur.

321) La carte d'atelier doit permettre le stockage des données relatives à l'activité du conducteur pendant au moins un jour d'activité moyenne du conducteur.

4.5.4.1.9 Données concernant les véhicules utilisés

322) La carte d'atelier doit pouvoir stocker des données concernant les véhicules utilisés de la même manière que la carte de conducteur.

323) La carte d'atelier doit pouvoir stocker au moins quatre enregistrements de ce type.

4.5.4.1.10 Données concernant le début et/ou la fin des périodes de travail journalières

324) La carte d'atelier doit pouvoir stocker des données relatives au début et/ou à la fin des périodes de travail journalières de la même manière qu'une carte de conducteur.

325) La carte d'atelier doit pouvoir stocker au moins trois paires d'enregistrements de ce type.

4.5.4.1.11 Données de session pour chaque carte

326) La carte d'atelier doit pouvoir stocker des données relatives à une session de carte de la même manière qu'une carte de conducteur.

4.5.4.1.12 Données relatives aux activités de contrôle

327) La carte d'atelier doit pouvoir stocker des données relatives aux activités de contrôle de la même manière qu'une carte de conducteur.

4.5.4.1.13 Données relatives aux conditions particulières

328) La carte d'atelier doit pouvoir stocker des données relatives aux conditions particulières de la même manière qu'une carte de conducteur.

329) La carte d'atelier doit pouvoir stocker au moins deux enregistrements de ce type.

4.5.4.2 Application tachygraphique de deuxième génération (non accessible aux unités embarquées de première génération**, accessible aux unités embarquées de deuxième génération, versions 1 et 2**)

4.5.4.2.1 Identification des applications

330) La carte d'atelier doit permettre le stockage des données suivantes pour l'identification des applications :

- Identification de l'application tachygraphique ;
- Identification du type de carte tachygraphique.

4.5.4.2.1.1 Identification des applications supplémentaires (non accessible aux unités embarquées de deuxième génération, version 1)

330a) La carte d'atelier doit pouvoir stocker des données pour l'identification des applications supplémentaires (applicable uniquement pour la version 2).

4.5.4.2.2 Clés et certificats

331) La carte d'atelier doit pouvoir stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié ~~à l'appendice~~ **au sous-appendice** 11, partie B.

332) La carte d'atelier doit pouvoir stocker un numéro d'identification personnel (code PIN).

4.5.4.2.3 Identification de la carte

333) La carte d'atelier doit pouvoir stocker les données suivantes pour l'identification de la carte :

- Numéro de la carte ;
- ~~État membre~~ **Partie contractante** qui a délivré la carte, nom de l'autorité de délivrance, date de délivrance ;
- Date de début de validité de la carte et date d'expiration.

4.5.4.2.4 Identification du détenteur de la carte

334) La carte d'atelier doit permettre le stockage des données suivantes pour l'identification du détenteur de la carte :

- Nom de l'atelier ;
- Adresse de l'atelier ;
- Nom du détenteur ;
- Prénom(s) du détenteur ;
- Langue habituelle.

4.5.4.2.5 Téléchargement d'une carte

335) La carte d'atelier doit pouvoir stocker des données relatives au téléchargement des cartes de la même manière qu'une carte de conducteur.

4.5.4.2.6 Données relatives à l'étalonnage et à la remise à l'heure

336) La carte d'atelier doit permettre le stockage des données relatives aux étalonnages et/ou aux remises à l'heure réalisés alors que la carte est insérée dans l'appareil.

337) Chaque enregistrement d'étalonnage doit contenir les données suivantes :

- Objet de l'étalonnage (activation, première installation, installation, inspection périodique) ;
- Identification du véhicule ;
- Paramètres mis à jour ou confirmés (w, k, l, taille des pneumatiques, réglage du limiteur de vitesse, compteur kilométrique (valeurs nouvelle et ancienne), date et heure (valeurs nouvelle et ancienne)) ;
- Identification de l'appareil de contrôle (numéro de référence et numéro de série de l'UEV, numéros de série du capteur de mouvement, du dispositif de communication à distance et du dispositif GNSS externe, le cas échéant) ;
- Type et identificateur de tous les scellements en place ;
- Possibilité pour l'UEV d'utiliser les cartes tachygraphiques de première génération (activées ou non).

338) La carte d'atelier doit pouvoir stocker ~~au moins 88~~ **255** enregistrements de ce type.

339) La carte d'atelier doit comporter un compteur indiquant le nombre total d'étalonnages réalisés avec la carte.

340) La carte d'atelier doit comporter un compteur indiquant le nombre d'étalonnages réalisés depuis le dernier téléchargement.

4.5.4.2.7 Données relatives aux événements et aux anomalies

341) La carte d'atelier doit pouvoir stocker des données relatives aux événements et aux anomalies de la même manière qu'une carte de conducteur.

342) La carte d'atelier doit permettre le stockage des trois derniers événements de chaque type (soit 33 événements) et des six dernières anomalies de chaque type (soit 12 anomalies).

4.5.4.2.8 Données relatives à l'activité du conducteur

343) La carte d'atelier doit pouvoir stocker des données relatives à l'activité du conducteur de la même manière que la carte de conducteur.

344) La carte d'atelier doit pouvoir stocker des données concernant l'activité du conducteur pendant ~~au moins~~ un jour **comprenant 240 changements d'activité** ~~d'activité moyenne du conducteur~~.

4.5.4.2.9 Données concernant les véhicules utilisés

345) La carte d'atelier doit pouvoir stocker des données concernant les véhicules utilisés de la même manière que la carte de conducteur.

346) La carte d'atelier doit pouvoir stocker ~~au moins 4~~ **8** enregistrements de ce type.

4.5.4.2.10 Données concernant **les positions et les lieux** ~~le~~ **de** début et/ou ~~la~~ **de** fin des périodes de travail journalières

347) La carte d'atelier doit permettre le stockage des enregistrements de données se rapportant **aux lieux et aux positions** ~~au~~ **de** début et/ou ~~à la~~ **de** fin des périodes de travail journalières de la même manière qu'une carte de conducteur.

348) La carte d'atelier doit pouvoir stocker ~~au moins 3~~ **4** paires d'enregistrements de ce type.

4.5.4.2.11 Données de session pour chaque carte

349) La carte d'atelier doit pouvoir stocker des données relatives à une session de carte de la même manière qu'une carte de conducteur.

4.5.4.2.12 Données relatives aux activités de contrôle

350) La carte d'atelier doit permettre le stockage des données relatives aux activités de contrôle de la même manière qu'une carte de conducteur.

4.5.4.2.13 Données concernant les unités embarquées utilisées

351) La carte d'atelier doit permettre le stockage des données suivantes relatives aux différentes unités embarquées dans lesquelles la carte a été utilisée :

- Date et heure du début de la période d'utilisation du véhicule (c'est-à-dire de la première insertion de la carte dans l'unité embarquée pour cette période) ;
- Fabricant de l'unité embarquée ;
- Type d'unité embarquée ;
- Numéro de version du logiciel de l'unité embarquée.

352) La carte d'atelier doit pouvoir stocker ~~au moins 4~~ **8** enregistrements de ce type.

4.5.4.2.14 Données relatives aux lieux où trois heures de temps de conduite ~~continue~~ **accumulé** sont atteintes

353) La carte d'atelier doit permettre le stockage des données suivantes relatives à la position du véhicule lorsque le temps de conduite ~~continue~~ **accumulé** ~~du conducteur~~ atteint un multiple de trois heures :

- Date et heure auxquelles le temps de conduite ~~continue~~ **accumulé** ~~du détenteur de la carte~~ atteint un multiple de trois heures ;
- Position du véhicule ;
- Précision GNSS, date et heure de détermination de la position ;
- **Kilométrage du véhicule.**

354) La carte d'atelier doit pouvoir stocker ~~au moins 18~~ **24** enregistrements de ce type.

4.5.4.2.15 Données relatives aux conditions particulières

355) La carte d'atelier doit pouvoir stocker des données relatives aux conditions particulières de la même manière qu'une carte de conducteur.

356) La carte d'atelier doit pouvoir stocker ~~au moins 2~~ **4** enregistrements de ce type.

4.5.4.2.16 État d'authentification des positions correspondant aux lieux de début et/ou de fin des périodes de travail journalières (non accessible aux unités embarquées de deuxième génération, version 1)

356a) La carte d'atelier doit permettre le stockage de données supplémentaires se rapportant aux lieux de début et/ou de fin des périodes de travail journalières de la même manière qu'une carte de conducteur.

356b) La mémoire de la carte d'atelier doit pouvoir stocker 4 paires d'enregistrements de ce type.

4.5.4.2.17 État d'authentification des positions correspondant aux lieux où les trois heures de temps de conduite accumulé sont atteintes (non accessible aux unités embarquées de deuxième génération, version 1)

356c) La carte d'atelier doit permettre le stockage de données supplémentaires se rapportant à la position du véhicule correspondant au lieu où le temps de conduite accumulé atteint un multiple de trois heures de la même manière qu'une carte de conducteur.

356d) La carte d'atelier doit pouvoir stocker ~~au moins~~ 24 enregistrements de ce type.

4.5.4.2.18 Passages de frontières (non accessible aux unités embarquées de deuxième génération, version 1)

356e) La carte d'atelier doit permettre le stockage de données concernant les passages de frontières de la même manière qu'une carte de conducteur.

356f) La carte d'atelier doit pouvoir stocker 4 enregistrements de ce type.

4.5.4.2.19 Opérations de chargement/déchargement (non accessible aux unités embarquées de deuxième génération, version 1)

356g) La carte d'atelier doit permettre le stockage de données concernant les opérations de chargement/déchargement de la même manière qu'une carte de conducteur.

356h) La carte d'atelier doit pouvoir stocker 8 opérations de chargement, de déchargement ou de chargement/déchargement simultanés.

4.5.4.2.20 Saisies du type de chargement (non accessible aux unités embarquées de deuxième génération, version 1)

356i) La carte d'atelier doit permettre le stockage de données concernant le type de chargement saisi de la même manière que la carte de conducteur.

356j) La carte d'atelier doit pouvoir stocker 4 enregistrements de ce type.

4.5.4.2.21 Données d'étalonnage supplémentaires (non accessible aux unités embarquées de deuxième génération, version 1)

356k) La carte d'atelier doit pouvoir stocker les données d'étalonnage supplémentaires suivantes (applicable uniquement pour la version 2) :

- **Les anciennes date et heure et le numéro d'identification du véhicule, lesquels doivent être exactement les mêmes que ceux enregistrés dans EF Calibration sous DF Tachograph_G2 ;**
- **Le type de chargement par défaut saisi pendant l'étalonnage ;**
- **Le pays dans lequel l'étalonnage a été effectué, ainsi que la date et l'heure auxquelles la position utilisée pour déterminer ce pays a été fournie par le récepteur GNSS.**

356l) La carte d'atelier doit pouvoir stocker 255 enregistrements de ce type.

4.5.4.2.22 Configurations de l'UEV (non accessible aux unités embarquées de deuxième génération, version 1)

356m) La carte d'atelier doit pouvoir stocker les paramètres spécifiques du tachygraphe du détenteur de la carte.

356n) La capacité de stockage de la carte d'atelier pour les paramètres du tachygraphe correspondant au détenteur de la carte doit être de 3 072 octets.

4.5.5 Carte de contrôleur

4.5.5.1 Application tachygraphique (accessible aux unités embarquées de première et deuxième générations)

4.5.5.1.1 Identification des applications

357) La carte de contrôleur doit permettre le stockage des données suivantes pour l'identification des applications :

- Identification de l'application tachygraphique ;
- Identification du type de carte tachygraphique.

4.5.5.1.2 Clés et certificats

358) La carte de contrôleur doit pouvoir stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié ~~à l'appendice~~ **au sous-appendice** 11, partie A.

4.5.5.1.3 Identification de la carte

359) La carte de contrôleur doit pouvoir stocker les données suivantes pour l'identification de la carte :

- Numéro de la carte ;
- ~~État membre~~ **Partie contractante** qui a délivré la carte, nom de l'autorité de délivrance, date de délivrance ;
- Date de début de validité de la carte et date d'expiration (le cas échéant).

4.5.5.1.4 Identification du détenteur de la carte

360) La carte de contrôleur doit permettre le stockage des données suivantes pour l'identification du détenteur de la carte :

- Nom de l'organisme de contrôle ;
- Adresse de l'organisme de contrôle ;
- Nom du détenteur ;
- Prénom(s) du détenteur ;
- Langue habituelle.

4.5.5.1.5 Données relatives aux activités de contrôle

361) La carte de contrôleur doit permettre le stockage des données suivantes concernant les activités de contrôle :

- Date et heure du contrôle ;
- Type de contrôle (affichage et/ou impression, et/ou téléchargement à partir de l'UEV et/ou de la carte ~~et/ou contrôle de l'étalonnage sur route~~) ;
- Période téléchargée, le cas échéant ;
- Numéro et autorité nationale d'immatriculation du véhicule contrôlé ;

– Numéro de la carte de conducteur contrôlée et ~~État membre~~ **Partie contractante** qui l'a délivrée.

362) La carte de contrôleur doit pouvoir stocker au moins 230 enregistrements de ce type.

4.5.5.2 Application tachygraphique de deuxième génération (non accessible aux unités embarquées de première génération)

4.5.5.2.1 Identification des applications

363) La carte de contrôleur doit permettre le stockage des données suivantes pour l'identification des applications :

– Identification de l'application tachygraphique ;

– Identification du type de carte tachygraphique.

4.5.5.2.1.1 Identification des applications supplémentaires (non accessible aux unités embarquées de deuxième génération, version 1)

363a) La carte de contrôleur doit pouvoir stocker des données pour l'identification des applications supplémentaires (applicable uniquement pour la version 2).

4.5.5.2.2 Clés et certificats

364) La carte de contrôleur doit pouvoir stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié dans ~~l'appendice~~ **le sous-appendice** 11, partie B.

4.5.5.2.3 Identification de la carte

365) La carte de contrôleur doit pouvoir stocker les données suivantes pour l'identification de la carte :

– Numéro de la carte ;

– ~~État membre~~ **Partie contractante** qui a délivré la carte, nom de l'autorité de délivrance, date de délivrance ;

– Date de début de validité de la carte et date d'expiration (le cas échéant).

4.5.5.2.4 Identification du détenteur de la carte

366) La carte de contrôleur doit permettre le stockage des données suivantes pour l'identification du détenteur de la carte :

– Nom de l'organisme de contrôle ;

– Adresse de l'organisme de contrôle ;

– Nom du détenteur ;

– Prénom(s) du détenteur ;

– Langue habituelle.

4.5.5.2.5 Données relatives aux activités de contrôle

367) La carte de contrôleur doit permettre le stockage des données suivantes concernant les activités de contrôle :

– Date et heure du contrôle ;

– Type du contrôle (affichage et/ou impression, et/ou téléchargement à partir de l'UEV et/ou de la carte, et/ou contrôle routier d'étalonnage) ;

– Période téléchargée, le cas échéant ;

– Numéro et autorité nationale d'immatriculation du véhicule contrôlé ;

– Numéro de la carte de conducteur contrôlée et ~~État membre~~ **Partie contractante** qui l'a délivrée.

368) La carte de contrôleur doit pouvoir stocker au moins 230 enregistrements de ce type.

4.5.5.2.6 Configurations de l'UEV (non accessible aux unités embarquées de deuxième génération version 1)

368a) La carte de contrôleur doit pouvoir stocker les paramètres spécifiques du tachygraphe du détenteur de la carte.

268b) La capacité de stockage de la carte de contrôleur pour les paramètres spécifiques du tachygraphe du détenteur de la carte doit être de 3 072 octets.

4.5.6 Carte d'entreprise

4.5.6.1 Application tachygraphique (accessible aux unités embarquées de première et deuxième générations)

4.5.6.1.1 Identification des applications

369) La carte d'entreprise doit permettre le stockage des données suivantes pour l'identification des applications :

– Identification de l'application tachygraphique ;

– Identification du type de carte tachygraphique.

4.5.6.1.2 Clés et certificats

370) La carte d'entreprise doit pouvoir stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié ~~à l'appendice~~ **au sous-appendice** 11, partie A.

4.5.6.1.3 Identification de la carte

371) La carte d'entreprise doit pouvoir stocker les données suivantes pour l'identification de la carte :

– Numéro de la carte ;

– ~~État membre~~ **Partie contractante** qui a délivré la carte, nom de l'autorité de délivrance, date de délivrance ;

– Date de début de validité de la carte et date d'expiration (le cas échéant).

4.5.6.1.4 Identification du détenteur de la carte

372) La carte d'entreprise doit permettre le stockage des données suivantes pour l'identification du détenteur de la carte :

– Nom de l'entreprise ;

– Adresse de l'entreprise.

4.5.6.1.5 Données relatives à l'activité de l'entreprise

373) La carte d'entreprise doit permettre le stockage des données suivantes concernant les activités de l'entreprise :

– Date et heure de l'activité ;

– Type d'activité (verrouillage et/ou déverrouillage de l'UEV, et/ou téléchargement à partir de l'UEV et/ou de la carte) ;

– Période téléchargée (le cas échéant) ;

– Numéro et autorité nationale d'immatriculation du véhicule ;

– Numéro de la carte et ~~État membre~~ **Partie contractante** qui l'a délivrée (en cas de téléchargement à partir de la carte) ;

374) La carte d'entreprise doit pouvoir stocker au moins 230 enregistrements de ce type.

4.5.6.2 Application tachygraphique de deuxième génération (non accessible aux unités embarquées de première génération)

4.5.6.2.1 Identification des applications

375) La carte d'entreprise doit permettre le stockage des données suivantes pour l'identification des applications :

– Identification de l'application tachygraphique ;

– Identification du type de carte tachygraphique.

4.5.6.2.1.1 Identification des applications supplémentaires (non accessible aux unités embarquées de deuxième génération, version 1)

375a) La carte d'entreprise doit pouvoir stocker des données pour l'identification des applications supplémentaires (applicable uniquement pour la version 2).

4.5.6.2.2 Clés et certificats

376) La carte d'entreprise doit pouvoir stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié ~~à l'appendice~~ **au sous-appendice** 11, partie B.

4.5.6.2.3 Identification de la carte

377) La carte d'entreprise doit pouvoir stocker les données suivantes pour l'identification de la carte :

– Numéro de la carte ;

– ~~État membre~~ **Partie contractante** qui a délivré la carte, nom de l'autorité de délivrance, date de délivrance ;

– Date de début de validité de la carte et date d'expiration (le cas échéant).

4.5.6.2.4 Identification du détenteur de la carte

378) La carte d'entreprise doit permettre le stockage des données suivantes pour l'identification du détenteur de la carte :

– Nom de l'entreprise ;

– Adresse de l'entreprise.

4.5.6.2.5 Données relatives à l'activité de l'entreprise

379) La carte d'entreprise doit permettre le stockage des données suivantes concernant les activités de l'entreprise :

– Date et heure de l'activité ;

– Type d'activité (verrouillage et/ou déverrouillage de l'UEV, et/ou téléchargement à partir de l'UEV et/ou de la carte) ;

– Période téléchargée, le cas échéant ;

– Numéro et autorité nationale d'immatriculation du véhicule ;

– Numéro de la carte et ~~État membre~~ **Partie contractante** qui l'a délivrée (en cas de téléchargement à partir de la carte).

380) La carte d'entreprise doit pouvoir stocker au moins 230 enregistrements de ce type.

4.5.6.2.6 Configurations de l'UEV (non accessible aux unités embarquées de deuxième génération, version 1)

380a) La carte d'entreprise doit pouvoir stocker les paramètres spécifiques du tachygraphe du détenteur de la carte.

380b) La capacité de stockage de la carte d'entreprise pour les paramètres spécifiques du tachygraphe du détenteur de la carte doit être de 3 072 octets.

5. Installation de l'appareil de contrôle

5.1 Installation

381) L'appareil de contrôle neuf est livré non activé aux monteurs ou aux constructeurs de véhicules, avec tous les paramètres d'étalonnage figurant sur la liste de la section 3.21, réglés aux valeurs par défaut appropriées et à jour. Lorsqu'aucune valeur particulière ne convient, on aura recours à des séries de points d'interrogation pour les paramètres alphabétiques et à des « 0 » pour les paramètres numériques. La livraison des pièces de l'appareil de contrôle en rapport avec la sécurité peut être restreinte au besoin au cours de la certification de sécurité.

382) Avant son activation, l'appareil de contrôle doit permettre l'accès à la fonction d'étalonnage même s'il n'est pas en mode étalonnage.

383) Avant son activation, l'appareil de contrôle ne doit ni enregistrer ni stocker les données visées **aux exigences 102 à 133** ~~au chapitre 3, points 12.3, 12.9 et 12.12 à 12.15~~ incluse. **Cependant, avant son activation, il peut enregistrer et stocker les tentatives d'atteinte à la sécurité conformément à l'exigence 117, ainsi que les anomalies affectant l'appareil de contrôle conformément à l'exigence 118.**

384) Au cours de l'installation, les constructeurs de véhicule doivent prérégler tous les paramètres connus.

385) Les constructeurs de véhicules ou les monteurs doivent activer l'appareil de contrôle installé au plus tard avant que le véhicule soit utilisé dans le champ d'application ~~du règlement (CE) n° 561/2006~~**du présent Accord**.

386) L'activation de l'appareil de contrôle doit être déclenchée automatiquement par la première insertion d'une carte d'atelier en cours de validité dans l'une ou l'autre des interfaces destinées aux cartes.

387) Les opérations particulières d'appariement nécessaires entre le capteur de mouvement et l'unité embarquée sur le véhicule, le cas échéant, interviennent automatiquement avant ou pendant l'activation.

388) De même, les opérations particulières de couplage nécessaires entre le dispositif GNSS externe et l'unité embarquée sur le véhicule, le cas échéant, interviennent automatiquement avant ou pendant l'activation.

389) Après son activation, l'appareil de contrôle applique pleinement les droits d'accès aux fonctions et aux données.

390) Après son activation, l'appareil de contrôle communique au dispositif de communication à distance les données sécurisées nécessaires aux fins des contrôles routiers ciblés.

391) Les fonctions d'enregistrement et de stockage de l'appareil de contrôle doivent être pleinement opérationnelles après l'activation.

392) L'installation doit être suivie d'un étalonnage. Le premier étalonnage ne comporte pas nécessairement la saisie du numéro d'immatriculation du véhicule (VRN) **et de la Partie contractante d'immatriculation**, s'il**s** ~~n'est~~**ne sont** pas connu**s** de l'atelier agréé qui doit procéder à cet étalonnage. Dans ces circonstances, le propriétaire du véhicule doit pouvoir, uniquement à ce moment, saisir le VRN **et la Partie contractante d'immatriculation** à

l'aide de sa carte d'entreprise avant l'utilisation du véhicule conformément au ~~règlement (CE) n° 561/2006~~ **présent Accord** (par exemple à l'aide de commandes se trouvant dans le menu approprié de l'interface homme-machine de l'unité embarquée)~~[10]~~. Seule l'utilisation d'une carte d'atelier doit permettre la mise à jour ou la confirmation de cette saisie.

393) L'installation d'un dispositif GNSS externe nécessite son couplage avec l'unité embarquée sur le véhicule et la vérification ultérieure des informations de positionnement GNSS.

394) L'appareil de contrôle doit impérativement être positionné dans le véhicule de telle manière que le conducteur ait accès aux fonctions nécessaires depuis son siège.

5.2 Plaquette d'installation

395) Après la vérification de l'appareil de contrôle une fois celui-ci installé, une plaquette d'installation, gravée ou imprimée de façon permanente, bien visible et facilement accessible, doit être fixée sur l'appareil de contrôle. Dans les cas où cela n'est pas possible, la plaquette est apposée sur le pied milieu du véhicule, de manière à être clairement visible. Si le véhicule n'a pas de pied milieu, la plaquette d'installation doit être apposée à proximité de ~~sur l'encadrement de~~ la portière du véhicule ~~du côté conducteur,~~ et être bien visible dans tous les cas.

Après chaque inspection par un atelier ou un monteur agréé, une nouvelle plaquette est fixée à la place de la précédente.

396) La plaquette doit comporter au moins les indications suivantes :

- Le nom, l'adresse ou la raison sociale du monteur ou de l'atelier agréé ;
- Le coefficient caractéristique du véhicule, sous la forme « w = … imp/km » ;
- La constante de l'appareil de contrôle, sous la forme « k = … imp/km » ;
- La circonférence effective des pneumatiques, sous la forme « l = … mm » ;
- La taille des pneumatiques ;
- La date à laquelle le coefficient caractéristique du véhicule et la circonférence effective des pneumatiques ont été mesurés ;
- Le numéro d'identification du véhicule ;
- La présence d'un dispositif GNSS externe (le cas échéant) ;
- Le numéro de série du dispositif GNSS externe (le cas échéant) ;
- Le numéro de série ~~de l'appareil~~ **du dispositif** de communication à distance (le cas échéant) ;
- Le numéro de série de tous les scellements en place ;
- La partie du véhicule où l'adaptateur est installé (le cas échéant) ;
- La partie du véhicule où le capteur de mouvement est installé, s'il n'est pas connecté à la boîte de vitesses ou si un adaptateur n'est pas utilisé ;
- Une description de la couleur du câble entre l'adaptateur et la partie du véhicule qui fournit les impulsions entrantes ;
- Le numéro de série du capteur de mouvement intégré de l'adaptateur ;
- **Le type de chargement par défaut associé au véhicule.**

~~[10] JO L 102 du 11.4.2006, p. 1.~~

397) Une plaquette supplémentaire peut être utilisée uniquement pour les véhicules des catégories M1 et N1, qui sont équipés d'un adaptateur conforme au ~~règlement (CE) n° 68/2009[11]~~**sous-appendice 16**, tel que modifié en dernier lieu, et pour lesquels il n'est pas possible d'inclure toutes les informations nécessaires en vertu de l'exigence 396. Dans ce cas, la plaquette comporte au moins les informations figurant aux quatre derniers tirets de l'exigence 396.

Si cette plaquette supplémentaire est utilisée, elle doit être apposée à côté ou en dessous de la plaquette principale décrite à l'exigence 396, et doit avoir le même niveau de protection. En outre, la plaquette supplémentaire doit aussi comporter le nom, l'adresse ou la raison sociale de l'atelier ou du monteur agréé qui a procédé à l'installation, ainsi que la date d'installation.

5.3 Scellement

398) Les éléments suivants doivent être scellés :

- Toute connexion qui, si elle était interrompue, entraînerait des altérations ou des pertes de données indécelables (cela peut s'appliquer, par exemple, au raccord du capteur de mouvement sur la boîte de vitesses, à l'adaptateur pour les véhicules des catégories M1 et N1, à la connexion GNSS externe ou à l'unité embarquée sur le véhicule) ;
- La plaquette d'installation, sauf si elle est fixée de telle manière qu'elle ne puisse être enlevée sans détruire les indications qu'elle porte.

398a) Les scellements précités doivent être certifiés conformément à la norme EN 16882:2016[12]**.**

399) Les scellements précités peuvent être retirés :

- En cas d'urgence ;
- Afin d'installer, de régler ou de réparer un limiteur de vitesse ou tout autre dispositif contribuant à la sécurité routière, à condition que l'appareil de contrôle continue à fonctionner de manière fiable et correcte, et qu'il soit scellé à nouveau par un atelier ou un monteur agréé (comme prévu au chapitre 6) immédiatement après l'installation du limiteur de vitesse ou de tout autre dispositif contribuant à la sécurité routière, ou dans les sept jours dans les autres cas.

400) À chaque bris de ces scellements, une déclaration écrite indiquant les raisons de cette action doit être rédigée et transmise à l'autorité compétente.

401) Les scellements doivent porter un numéro d'identification, attribué par leur fabricant. Ce numéro doit être unique et distinct de tout autre numéro de scellement attribué par un fabricant de scellements.

Ce numéro d'identification unique se présente ainsi : ~~MM NNNNNN~~ **MMNNNNNNNN**, marqués de façon indélébile, où MM est l'identification unique du fabricant (enregistrée dans une base de données qui sera gérée par la CE), et ~~NNNN~~ **NNNNNNNN**, le code alphanumérique du scellement, unique dans le domaine du fabricant.

402) Les scellements doivent présenter un espace libre où les monteurs, les ateliers ou les constructeurs de véhicules agréés peuvent ajouter une marque particulière ~~conformément à l'article 22, paragraphe 3 du règlement (UE) n° 165/2014~~.

Cette marque ne doit pas couvrir le numéro d'identification du scellement.

~~[11] JO L 21 du 24.1.2009, p. 3.~~

[12] **Conversion en norme ISO prévue sur une période de cinq ans.**

403) Les fabricants de scellements doivent être enregistrés dans une base de données dédiée **lorsqu'ils obtiennent la certification d'un modèle de scellement conformément à la norme EN 16882:2016**, et rendre publics les numéros d'identification de leurs scellements ~~par une procédure établie par la Commission européenne~~.

404) Les ateliers et les constructeurs de véhicules agréés doivent, dans le cadre du ~~règlement (UE) n° 165/2014~~ **présent Accord**, n'utiliser que des scellements **certifiés selon la norme EN 16882:2016** et issus des fabricants de scellements répertoriés dans la base de données mentionnée ci-dessus.

405) Les fabricants de scellements et leurs distributeurs doivent tenir des registres complets pour la traçabilité des scellements vendus en vue d'une utilisation dans le cadre du ~~règlement (UE) n° 165/2014~~ **présent Accord**, et doivent être prêts à les communiquer aux autorités nationales compétentes à chaque fois que cela est nécessaire.

406) Les numéros d'identification uniques des scellements doivent être visibles sur la plaquette d'installation.

6. Contrôles, inspections et réparations

Les exigences concernant les circonstances dans lesquelles les scellements peuvent être retirés~~, comme indiqué à l'article 22, paragraphe 5, du règlement (UE) n° 165/2014,~~ sont définies à la section 5.3 ~~de la~~ **du** présente ~~annexe~~ **appendice**.

6.1 Agrément des monteurs, des ateliers et des constructeurs de véhicules

Les ~~États membres~~ **Parties contractantes** agréent, contrôlent régulièrement et certifient les organismes chargés des tâches suivantes :

- Installation ;
- Contrôle ;
- Inspection ;
- Réparation.

Les cartes d'atelier ne doivent être délivrées qu'aux monteurs et/ou aux ateliers agréés pour l'activation et/ou l'étalonnage d'appareils de contrôle, conformément ~~à la~~ **au** présente ~~annexe~~ **appendice** et, sauf cas dûment motivé :

- Qui ne sont pas éligibles pour une carte d'entreprise ;
- Dont les autres activités professionnelles ne sont pas de nature à compromettre la sécurité globale du système telle que requise par ~~l'appendice~~ **le sous-appendice** 10.

6.2 Vérification ~~d'instruments~~ des composants neufs ou réparés

407) Chaque dispositif, neuf ou réparé, doit être vérifié pour s'assurer de son bon fonctionnement et de la précision de ses relevés et de ses enregistrements, dans les limites fixées aux sections 3.2.1, 3.2.2, 3.2.3 et 3.3 ~~par le scellement prévu au chapitre 5, point 3, et à l'étalonnage~~.

6.3 Inspection de l'installation

408) Lors de son montage sur un véhicule, l'ensemble de l'installation (y compris l'appareil de contrôle) doit respecter les dispositions concernant les tolérances maximales énoncées aux sections 3.2.1, 3.2.2, 3.2.3 et 3.3. **L'installation dans son ensemble doit être scellée comme prévu à la section 5.3 et soumise à un étalonnage.**

6.4 Inspections périodiques

409) Des inspections périodiques des appareils montés sur les véhicules ont lieu après toute réparation, ou après toute modification du coefficient caractéristique du véhicule ou de la circonférence effective des pneumatiques, ou lorsque l'horloge UTC est fausse de plus de ~~20~~ **5** minutes, ou lorsque le numéro d'immatriculation a changé, et au moins une fois tous les deux ans (24 mois).

410) Ces inspections comprennent les vérifications suivantes :

- Fonctionnement correct de l'appareil de contrôle, y compris de la fonction de stockage de données sur les cartes tachygraphiques et de la communication avec les lecteurs de communication à distance ;
- Respect des dispositions des sections 3.2.1 et 3.2.2, concernant les tolérances maximales à l'installation ;
- Respect des dispositions des sections 3.2.3 et 3.3 ;
- Présence de la marque d'homologation sur l'appareil de contrôle ;
- **Fixation de la plaquette d'installation, définie à l'exigence 396, et de la plaque signalétique, définie à l'exigence 225 ;**
- Taille des pneumatiques et circonférence effective des pneumatiques ;
- Absence de dispositifs de manipulation attachés à l'appareil ;
- Placement correct et bon état des scellements, validité de leurs numéros d'identification (référencement du fabricant de scellements dans la base de données de la CE) et correspondance entre leurs numéros d'identification et les marques des plaquettes d'installation (voir exigence 401) ;
- **Stockage de la carte numérique avec l'identificateur de version le plus récent.**

410a) En cas de détection d'une manipulation par les autorités nationales compétentes, le véhicule peut être envoyé vers un atelier agréé pour un nouvel étalonnage de l'appareil de contrôle.

411) S'il est constaté que l'un des événements figurant dans la section 3.9 (détection des événements et/ou des anomalies) est survenu depuis la dernière inspection, et que les fabricants de tachygraphes et/ou les autorités nationales considèrent que cet événement représente un risque pour la sécurité de l'équipement, l'atelier doit :

a) Effectuer une comparaison entre les données d'identification du capteur de mouvement connecté à la boîte de vitesse et celles du capteur de mouvement appariés qui sont enregistrées dans l'unité embarquée ;

b) Vérifier si les informations inscrites sur la plaquette d'installation correspondent à celles enregistrées dans l'unité embarquée ;

c) Vérifier si le numéro de série et le numéro d'homologation du capteur de mouvement, s'ils sont imprimés sur le corps du capteur de mouvement, correspondent aux informations enregistrées dans la mémoire de l'appareil de contrôle ;

d) Comparer les données d'identification inscrites sur la plaque signalétique du dispositif GNSS externe, le cas échéant, à celles stockées dans la mémoire de l'unité embarquée.

412) Les ateliers consignent dans leurs rapports d'inspection toute constatation concernant un bris de scellement ou un dispositif de manipulation. Ils conservent ces rapports pendant au moins deux ans et les mettent à la disposition de l'autorité compétente sur demande.

413) Ces inspections comprennent un étalonnage et un remplacement préventif des scellements dont l'installation s'effectue sous la responsabilité d'ateliers.

6.5 Mesure des erreurs

414) La mesure des erreurs à l'installation et en service doit être effectuée dans les conditions suivantes, qui sont à considérer comme des conditions normales d'essai :

- Véhicule à vide en ordre de marche ;
- Pression des pneumatiques conforme aux instructions du fabricant ;
- Usure des pneumatiques dans les limites autorisées par la législation nationale ;
- Mouvement du véhicule :
- Le véhicule doit avancer, sous l'action de son propre moteur, en ligne droite sur sol plat à une vitesse de 50 ± 5 km/h, et la distance de mesure doit être d'au moins 1 000 m ;
- Pour autant qu'elles soient d'une précision comparable, d'autres méthodes, par exemple l'utilisation d'un banc d'essai adapté, peuvent également être appliquées.

6.6 Réparations

415) Les ateliers doivent pouvoir télécharger des données à partir de l'appareil de contrôle afin de les restituer à l'entreprise de transport appropriée.

416) Les ateliers agréés délivrent aux entreprises de transport un certificat attestant que les données ne peuvent pas être téléchargées lorsqu'un dysfonctionnement de l'appareil de contrôle empêche de télécharger les données stockées, même après réparation par l'atelier concerné. Les ateliers conservent une copie de chaque certificat délivré pendant au moins deux ans.

7. Délivrance des cartes

Les processus mis en place par les ~~États membres~~ **Parties contractantes** pour la délivrance des cartes sont conformes aux exigences ci-après.

417) Le numéro de carte pour la première délivrance d'une carte tachygraphique doit comporter un indice séquentiel (le cas échéant), ainsi qu'un indice de remplacement et un indice de renouvellement fixés à « 0 ».

418) Les numéros de carte de toutes les cartes tachygraphiques non nominatives délivrées au même organisme de contrôle, au même atelier ou à la même entreprise de transport doivent comporter 13 chiffres identiques suivi d'un indice séquentiel distinct.

419) Une carte tachygraphique délivrée en remplacement d'une carte tachygraphique existante doit avoir le même numéro que celle qu'elle remplace, sauf l'indice de remplacement, qui doit être augmenté d'une unité (dans une série 0 à 9, A à Z).

420) Une carte tachygraphique délivrée en remplacement d'une carte tachygraphique existante doit avoir la même date d'expiration que cette dernière.

421) Une carte tachygraphique délivrée en renouvellement d'une carte existante doit porter le même numéro que cette dernière, sauf pour l'indice de remplacement, qui doit être remis à « 0 », et pour l'indice de renouvellement, qui doit être augmenté d'une unité (dans une série de 0 à 9, A à Z).

422) L'échange d'une carte tachygraphique existante, aux fins de la modification de données administratives, doit suivre les règles applicables au renouvellement s'il est effectué à l'intérieur d'un**e** même ~~État membre~~ **Partie contractante**, ou les règles applicables à une première délivrance s'il est effectué par un**e** autre ~~État membre~~ **Partie contractante**.

423) Dans le cas d'une carte d'atelier ou de contrôleur non nominative, la rubrique « nom du détenteur de la carte » doit être complétée par le nom de l'atelier, de l'organisme de contrôle, du monteur ou de l'agent de contrôle selon ce que décident les ~~États membres~~ **Parties contractantes**.

~~Les États membres échangent des données par voie électronique afin d'assurer l'unicité des cartes de conducteur qu'ils délivrent conformément à l'article 31 du règlement (UE) n° 165/2014.~~

424) Réservé.

8. Homologation de l'appareil de contrôle et des cartes tachygraphiques

8.1 Points généraux

Aux fins du présent chapitre, on entend par « appareil de contrôle », l'appareil de contrôle ou ses composants. Aucune homologation n'est exigée pour le(s) câble(s) reliant le capteur de mouvement à l'UEV, le dispositif GNSS **externe** à l'UEV ou le dispositif de communication à distance à l'UEV. Le papier utilisé par l'appareil de contrôle est considéré comme un composant de l'appareil.

Tout fabricant peut demander l'homologation d'**un ou de plusieurs** composant**s** de l'appareil de contrôle **avec tout autre composant**~~type de capteur de mouvement, de dispositif GNSS externe et vice versa~~, à condition que chaque composant soit conforme aux exigences énoncées dans ~~la~~ **le** présent~~e annexe~~ **appendice**. Les fabricants peuvent également demander l'homologation de l'appareil de contrôle.

Les unités embarquées diffèrent au niveau de l'assemblage de leurs composants. Quel que soit l'assemblage des composants, l'antenne externe et, le cas échéant, le répartiteur d'antenne connecté au récepteur GNSS ou au dispositif de communication à distance ne sont pas inclus dans l'homologation de l'unité embarquée.

Néanmoins, les fabricants qui ont obtenu l'homologation d'un appareil de contrôle doivent tenir à jour et publier une liste des antennes et des répartiteurs compatibles avec chaque unité embarquée, dispositif GNSS externe et dispositif externe de communication à distance homologués.

425) Un appareil de contrôle doit être présenté pour homologation avec tous ses composants ainsi que tout dispositif additionnel éventuellement intégré.

426) L'homologation des appareils de contrôle et des cartes tachygraphiques comporte des essais liés à la sécurité, des essais fonctionnels et des essais d'interopérabilité. Les résultats positifs à chacun de ces essais sont attestés par un certificat correspondant.

427) Les autorités d'homologation des ~~États membres~~ **Parties contractantes** n'accorderont pas de certificat d'homologation tant qu'elles ne sont pas en possession pour l'appareil de contrôle ou la carte tachygraphique faisant l'objet de la demande d'homologation :

- D'un certificat de sécurité **(si requis par le présent sous-appendice) ;**
- D'un certificat de fonctionnement ;
- D'un certificat d'interopérabilité **(si requis par le présent sous-appendice).**

428) Toute modification du logiciel ou du matériel, ou des matériaux utilisés dans la fabrication de l'appareil de contrôle doit être notifiée, avant son utilisation, à l'autorité qui a accordé l'homologation. Cette autorité doit confirmer au fabricant l'extension de l'homologation, ou bien elle peut exiger une mise à jour ou une confirmation des certificats de fonctionnement, de sécurité et/ou d'interopérabilité.

429) Les procédures de mise à ~~niveau~~ **jour** *in situ* du logiciel de l'appareil de contrôle doivent être approuvées par l'autorité qui a accordé l'homologation pour l'appareil de contrôle concerné. La mise à ~~niveau~~ **jour** logicielle ne doit ni modifier ni supprimer les données relatives à l'activité du conducteur stockée dans l'appareil de contrôle. Le logiciel ne peut être mis à ~~niveau~~ **jour** que sous la responsabilité du fabricant de l'appareil de contrôle.

430) L'homologation des modifications de logiciels visant à mettre à ~~niveau~~ **jour** un appareil de contrôle préalablement homologué ne peut être refusée si ces modifications ne s'appliquent qu'à des fonctions non spécifiées dans ~~la~~ **le** présent~~e annexe~~ **appendice**. La mise à jour logicielle d'un appareil de contrôle peut exclure l'introduction de nouveaux jeux de caractères si ce n'est pas techniquement faisable.

8.2 Certificat de sécurité

431) Le certificat de sécurité est délivré conformément aux dispositions ~~de l'appendice~~ **du sous-appendice** 10 ~~de la~~ **du** présent~~e annexe~~ **appendice**. Les composants de l'appareil de contrôle qui doivent être certifiés sont : l'unité embarquée sur le véhicule, le capteur de mouvement, le dispositif GNSS externe et les cartes tachygraphiques.

432) Dans le cas exceptionnel et spécifique où les autorités chargées de la certification de sécurité refusent de certifier un nouvel appareil en invoquant l'obsolescence des mécanismes de sécurité, l'homologation continue à être accordée uniquement lorsqu'il n'existe aucune autre solution conforme au ~~règlement~~ **présent Accord**.

433) Dans ~~cette circonstance~~ **ce cas**, ~~l'État membre~~ **la Partie contractante** concerné**e** informe sans retard ~~la Commission européenne~~ **les autres Parties contractantes**, **afin que soit lancée**, dans les douze mois civils qui suivent l'octroi de l'homologation, une procédure visant à garantir que le niveau de sécurité a été ramené à son niveau d'origine.

8.3 Certificat de fonctionnement

434) Chaque candidat à l'homologation doit fournir à l'autorité d'homologation de ~~l'État membre~~ **la Partie contractante** tout le matériel et la documentation que cette autorité juge nécessaires.

435) Les fabricants fournissent les échantillons pertinents de produits en attente d'homologation et la documentation associée requis par les laboratoires désignés pour effectuer les essais fonctionnels, et ce, dans le mois qui suit la demande. L'entité qui fait la demande supporte les coûts qui en résultent. Les laboratoires traitent toutes les informations sensibles sur le plan commercial en respectant la confidentialité.

436) Un certificat de fonctionnement est délivré par le fabricant uniquement après que l'appareil a obtenu des résultats positifs à tous les essais fonctionnels spécifiés ~~à l'appendice~~ **au sous-appendice** 9.

437) L'autorité d'homologation délivre le certificat de fonctionnement. Ce certificat comporte, outre le nom de son bénéficiaire et le nom du modèle, une liste détaillée des essais réalisés et des résultats obtenus.

438) Le certificat de fonctionnement de tout composant d'appareil de contrôle mentionne aussi les numéros d'homologation des autres composants d'appareil de contrôle compatibles homologués qui sont testés en vue d'obtenir cette certification.

439) Le certificat de fonctionnement d'un composant de l'appareil de contrôle doit également indiquer la norme ISO ou CEN en vertu de laquelle l'interface fonctionnelle a été certifiée.

8.4 Certificat d'interopérabilité

440) Les essais d'interopérabilité sont réalisés par un seul et même ~~laboratoire sous l'autorité et la responsabilité de la Commission européenne~~ **organisme compétent**.

441) Le laboratoire enregistre les demandes d'essais d'interopérabilité introduites par les fabricants dans l'ordre chronologique de leur arrivée.

442) Les demandes ne sont officiellement enregistrées que lorsque le laboratoire est en possession :

- De l'ensemble du matériel et des documents nécessaires aux essais d'interopérabilité ;
- Du certificat de sécurité correspondant ;
- Du certificat de fonctionnement correspondant.

La date de l'enregistrement de la demande est notifiée au fabricant.

443) Aucun essai d'interopérabilité ne doit être réalisé par le laboratoire sur un appareil de contrôle ou une carte tachygraphique qui n'a pas **subi avec succès une analyse de vulnérabilité effectuée dans le cadre** ~~de certificat~~ de l'évaluation de la sécurité, ~~et de certificat~~ **de même qu'une évaluation** fonctionnelle, sauf dans les circonstances exceptionnelles décrites dans l'exigence 432.

444) Tout fabricant demandant des essais d'interopérabilité s'engage à laisser au laboratoire chargé des essais l'ensemble du matériel et de la documentation fournis aux fins des essais.

445) Les essais d'interopérabilité sont effectués, conformément aux dispositions ~~à l'appendice~~ **du sous-appendice** 9 ~~de la~~ **du** présent~~e annexe~~ **appendice**, sur tous les types d'appareil de contrôle ou de cartes tachygraphiques :

- Dont l'homologation est en cours de validité ; ou
- Dont l'homologation est en instance et pour lesquels il existe un certificat d'interopérabilité en cours de validité.

446) Les essais d'interopérabilité doivent couvrir toutes les générations d'appareils de contrôle ou de cartes tachygraphiques encore en usage.

447) Le certificat d'interopérabilité doit être délivré par le laboratoire au fabricant uniquement après la réussite de tous les essais d'interopérabilité requis **et après que le fabricant a présenté un certificat de fonctionnement et un certificat de sécurité valables pour le produit, sauf dans les circonstances exceptionnelles décrites à l'exigence 432**.

448) En cas d'échec aux essais d'interopérabilité effectués sur un ou plusieurs appareils de contrôle ou cartes tachygraphiques, le certificat d'interopérabilité n'est pas délivré tant que le fabricant à l'origine de la demande n'a pas apporté les modifications nécessaires et que l'appareil ou la carte n'a pas satisfait à tous les essais d'interopérabilité. Le laboratoire détermine la cause du problème avec l'aide des fabricants concernés, et s'efforce d'assister le fabricant à l'origine de la demande dans la recherche d'une solution technique. Dans les cas où le fabricant a modifié son produit, il lui incombe de s'assurer auprès des autorités compétentes de la validité du certificat de sécurité et du certificat de fonctionnement.

449) Le certificat d'interopérabilité est valable six mois. Il expire à la fin de cette période si le fabricant n'a pas reçu un certificat d'homologation correspondant. Il est transmis par le fabricant à l'autorité d'homologation de ~~l'État membre~~ **la Partie contractante** qui a délivré le certificat de fonctionnement.

450) Tout élément susceptible d'être à l'origine d'une anomalie d'interopérabilité ne doit pas être utilisé pour réaliser des bénéfices ni pour accéder à une position dominante.

8.5 Certificat d'homologation

451) L'autorité d'homologation de ~~l'État membre~~ **la Partie contractante** peut délivrer le certificat d'homologation dès qu'elle est en possession des trois certificats requis.

452) Le certificat d'homologation de tout composant d'appareil de contrôle mentionne aussi les numéros d'homologation des autres composants d'appareil de contrôle interopérables homologués.

453) Une copie du certificat d'homologation doit être transmise par l'autorité d'homologation au laboratoire chargé des essais d'interopérabilité lors de la délivrance de ce certificat au fabricant.

454) Le laboratoire compétent pour les essais d'interopérabilité doit mettre à jour, sur un site Web public qu'il gère, la liste des modèles d'appareil de contrôle ou de cartes tachygraphiques :

- Pour lesquels une demande d'essais d'interopérabilité a été enregistrée ;
- Qui ont reçu un certificat d'interopérabilité (même provisoire) ;
- Qui ont reçu un certificat d'homologation.

~~7.6 Procédure exceptionnelle : les premiers certificats d'interopérabilité pour des unités de contrôle et des cartes tachygraphiques de deuxième génération~~

~~455) Pendant une période de quatre mois après qu'un premier couple appareil de contrôle de deuxième génération/cartes tachygraphiques de deuxième génération (cartes de conducteur, d'atelier, de contrôleur et d'entreprise) a été certifié interopérable, tous les certificats d'interopérabilité délivrés (y compris les premiers) en relation avec des demandes reçues pendant cette période seront considérés comme provisoires.~~

~~456) À l'issue de cette période, si tous les produits concernés sont interopérables, tous les certificats d'interopérabilité deviennent définitifs.~~

~~457) Si des anomalies d'interopérabilité apparaissent au cours de cette période, le laboratoire chargé des essais d'interopérabilité détermine la cause des problèmes observés, avec l'aide de tous les fabricants concernés, et les invite à apporter les modifications nécessaires.~~

~~458) Si, à la fin de cette période, des problèmes d'interopérabilité demeurent, le laboratoire chargé des essais d'interopérabilité détermine, en collaboration avec les fabricants concernés et avec les autorités d'homologation qui ont délivré les certificats de fonctionnement correspondants, les causes des anomalies d'interopérabilité, et définissent les modifications que chaque fabricant concerné doit apporter. La recherche de solutions techniques peut se prolonger pendant un maximum de deux mois, après quoi la Commission, en l'absence de solution commune, et après consultation du laboratoire chargé des essais d'interopérabilité, décide du ou des appareils et des cartes auxquels est délivré un certificat d'interopérabilité définitif, en précisant les raisons de son choix.~~

~~459) Toute demande d'essais d'interopérabilité enregistrée par le laboratoire entre la fin de la période de quatre mois suivant la délivrance du premier certificat d'interopérabilité provisoire et la date de la décision de la Commission visée à l'exigence 455 est repoussée jusqu'à la résolution des problèmes d'interopérabilité initiaux. Ces demandes sont ensuite traitées dans l'ordre de leur enregistrement.~~

APPENDICE

MARQUE ET CERTIFICAT D'HOMOLOGATION

I. MARQUE D'HOMOLOGATION

1. La marque d'homologation est composée :

a) D'un rectangle à l'intérieur duquel est placée la lettre « e », suivie du numéro distinctif ou de la lettre distinctive du pays qui a délivré l'homologation, conformément aux conventions suivantes :

Note : toutes les Parties contractantes doivent figurer dans la liste.

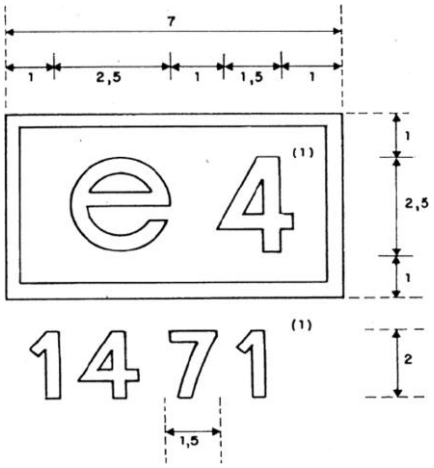
Belgique	6
Bulgarie	34
République tchèque	8
Danemark	18
Allemagne	1
Estonie	29
Irlande	24
Grèce	23
Espagne	9
France	2
Croatie	25
Italie	3
Chypre	CY
Lettonie	32
Lituanie	36
Luxembourg	13
Hongrie	7
Malte	MT
Pays-Bas	4
Autriche	12
Pologne	20
Portugal	21
Roumanie	19
Slovénie	26
Slovaquie	27
Finlande	17
Suède	5

~~a) d'un rectangle à l'intérieur duquel est placée la lettre «e» minuscule suivie d'un numéro distinctif ou d'une lettre distinctive du pays ayant délivré l'homologation, conformément aux conventions suivantes:~~

b) d'un numéro d'homologation correspondant au numéro du certificat d'homologation établi pour le prototype de l'appareil de contrôle, de la feuille d'enregistrement ou ~~correspondant au numéro~~ de la carte tachygraphique, placé dans une position quelconque à proximité du rectangle.

2. La marque d'homologation est apposée sur la plaque signalétique de chaque appareil, sur chaque feuille d'enregistrement et sur chaque carte tachygraphique. Elle doit être indélébile et rester toujours parfaitement lisible.

3. Les dimensions de la marque d'homologation dessinée ci-après(1) sont exprimées en millimètres, ces dimensions constituant des minima. Les rapports entre ces dimensions doivent être respectés.



(1) Ces chiffres sont donnés à titre indicatif uniquement.

II. CERTIFICAT D'HOMOLOGATION DES TACHYGRAPHES ANALOGIQUES

~~Un État membre~~ **Une Partie contractante** qui a procédé à une homologation délivre au demandeur un certificat d'homologation, établi selon le modèle figurant ci-après. Des copies de ce certificat doivent être utilisées pour informer les autres ~~États membres~~ **Parties contractantes** des homologations délivrées ou, le cas échéant, retirées.

CERTIFICAT D'HOMOLOGATION

- Nom de l'administration compétente
- Notification concernant([1]) :
- l'homologation d'un modèle d'appareil de contrôle
- le retrait de l'homologation d'un modèle d'appareil de contrôle
- l'homologation d'un modèle de feuille d'enregistrement
- le retrait de l'homologation d'un modèle de feuille d'enregistrement

N° d'homologation : …….

1. Marque ou appellation commerciale .....
2. Nom du modèle .....
3. Nom du fabricant .....
4. Adresse du fabricant .....
5. Présenté à l'homologation le .....
6. Laboratoire(s) d'essai .....
7. Date et numéro de l'essai ou des essais .....
8. Date de l'homologation .....
9. Date du retrait de l'homologation .....
10. Modèle(s) d'appareil(s) de contrôle sur le(s)quel(s) la feuille est destinée à être utilisée .....
11. Lieu .....
12. Date .....
13. Documents descriptifs ~~annexés~~ **en appendice** .....
14. Remarques (notamment concernant l'emplacement des scellements, le cas échéant .....

(Signature)

[(1)] Rayer les mentions inutiles.

III. CERTIFICAT D'HOMOLOGATION DES TACHYGRAPHES NUMÉRIQUES

~~Un État membre~~ **Une Partie contractante** qui a procédé à une homologation délivre au demandeur un certificat d'homologation, établi selon le modèle figurant ci-après. Des copies de ce certificat doivent être utilisées pour informer les autres ~~États membres~~ **Parties contractantes** des homologations délivrées ou, le cas échéant, retirées.

CERTIFICAT D'HOMOLOGATION DES TACHYGRAPHES NUMÉRIQUES

Nom de l'administration compétente .....

Notification concernant [1] :

□ l'homologation de :

□ le retrait de l'homologation de :

□ modèle d'appareil de contrôle

□ composant d'appareil de contrôle [2]

□ carte de conducteur

□ carte d'atelier

□ carte d'entreprise

□ carte de contrôleur

N° d'homologation : ……..

1. Marque de fabrique ou appellation commerciale .....
2. Nom du modèle .....
3. Nom du fabricant .....
4. Adresse du fabricant .....
5. Présenté à l'homologation ~~de~~ **le** .....
6. Laboratoire(s) .....
7. Date et numéro du rapport du laboratoire .....
8. Date de l'homologation .....
9. Date du retrait de l'homologation .....
10. Modèle(s) d'appareil(s) de contrôle avec le(s)quel(s) le composant est destiné à être utilisé .....
11. Lieu .....
12. Date .....
13. Documents descriptifs ~~annexés~~ **en appendice** .....
14. Remarques (notamment concernant l'emplacement des scellements, le cas échéant)

(Signature)

[1] Cocher les cases pertinentes.

[2] Préciser le composant qui fait l'objet de la notification.

IV. CERTIFICAT D'HOMOLOGATION DES TACHYGRAPHES INTELLIGENTS

~~Un État membre~~ **Une Partie contractante** qui a procédé à une homologation délivre au demandeur un certificat d'homologation, établi selon le modèle figurant ci-après. Des copies de ce certificat doivent être utilisées pour informer les autres ~~États membres~~ **Parties contractantes** des homologations délivrées ou, le cas échéant, retirées.

CERTIFICAT D'HOMOLOGATION DES TACHYGRAPHES INTELLIGENTS

Nom de l'administration compétente .....

Notification concernant [1] :

□ l'homologation de :

□ le retrait de l'homologation de :

□ modèle d'appareil de contrôle

□ composant d'appareil de contrôle[2]

□ carte de conducteur

□ carte d'atelier

□ carte d'entreprise

□ carte de contrôleur

N° d'homologation : ……

1. Marque de fabrique ou appellation commerciale .....
2. Nom du modèle .....
3. Nom du fabricant .....
4. Adresse du fabricant .....
5. Présenté à l'homologation ~~de~~ **le**.....
6. a Laboratoire d'essai pour la certification de fonctionnement .....
   b Laboratoire d'essai pour la certification de sécurité.....
   c Laboratoire d'essai pour la certification d'interopérabilité .....
7. a Date et numéro du certificat de fonctionnement .....
   b Date et numéro du certificat de sécurité .....
   c Date et numéro du certificat d'interopérabilité.....
8. Date de l'homologation .....
9. Date du retrait de l'homologation .....
10. Modèle(s) d'appareil(s) de contrôle avec le(s)quel(s) le composant est destiné à être utilisé .....
11. Lieu .....
12. Date .....
13. Documents descriptifs ~~annexés~~ **en appendice**.....
14. Remarques (notamment concernant l'emplacement des scellements, le cas échéant)

(Signature)

[1] Cocher les cases pertinentes.

[2] Préciser le composant qui fait l'objet de la notification.

~~Appendice~~ Sous-appendice 1

Dictionnaire de données

Table des matières

1. Introduction

Le présent **sous-**appendice spécifie les formats, les éléments et les structures de données utilisés au sein des appareils de contrôle et des cartes tachygraphiques.

1.1 Méthode de définition des types de données

Le présent **sous-**appendice a recours à la notation ASN.1 (*Abstract Syntax Notation One*) pour définir les différents types de données. Cette méthode permet de décrire des données simples et structurées sans nécessiter l'emploi d'une syntaxe de transfert spécifique (règles de codage) qui dépende de l'application et de l'environnement considérés.

Les règles d'affectation des noms de type ASN.1 sont établies conformément à la norme ISO/CEI 8824-1. Il en résulte que :

- Dans la mesure du possible, la signification d'un type de données est implicitement fournie par le nom qui lui est attribué ;
- Si un type de données se compose d'autres types de données, son nom se présente toujours sous la forme d'une seule séquence de caractères alphabétiques commençant par une majuscule, mais des majuscules sont insérées dans le nom pour lui conférer la signification correspondante ;
- De manière générale, les noms des types de données sont en rapport avec le nom des types de données à partir desquels ils sont construits, avec l'équipement au sein duquel les données sont stockées et avec la fonction associée aux données considérées.

Si l'emploi d'un type ASN.1 déjà défini dans le cadre d'une autre norme s'impose avec l'appareil de contrôle, ce type sera défini dans le présent **sous-**appendice.

Afin de permettre l'application de plusieurs types de règles de codage, certains types ASN.1 évoqués dans le présent **sous-**appendice sont limités par des identificateurs de plage de valeurs. Ces identificateurs de plage de valeurs sont définis au paragraphe 3 et au **sous-**appendice 2.

1.2 Références

Dans le présent **sous-**appendice, il est fait référence aux documents suivants :

ISO 639	Code pour la représentation des noms de langue, première édition : 1988.
ISO 3166	Codes pour la représentation des noms de pays et de leurs subdivisions − Partie 1 : codes de pays, 2013.
ISO 3779	Véhicules routiers − Numéro d'identification des véhicules (VIN) − Contenu et structure, 2009.
ISO/CEI 7816-5	Cartes d'identification − Cartes à circuit intégré − Partie 5 : enregistrement des fournisseurs d'application, deuxième édition : 2004.
ISO/CEI 7816-6	Cartes d'identification − Cartes à circuit intégré − Partie 6 : éléments de données intersectoriels pour les échanges, 2004, et rectificatif technique 1: 2006.
ISO/CEI 8824-1	Technologies de l'information − Notation de syntaxe abstraite numéro un (ASN.1) : Spécification de la notation de base, 2008, rectificatif technique1 : 2012 et rectificatif technique 2: 2014.
ISO/CEI 8825-2	Technologies de l'information − Règles de codage ASN.1 : spécification des règles de codage compact (PER), 2008.

ISO/CEI 8859-1	Technologies de l'information − Jeux de caractères graphiques codés sur un seul octet − Partie 1 : alphabet latin nº 1, première édition : 1998.
ISO/CEI 8859-7	Technologies de l'information − Jeux de caractères graphiques codés sur un seul octet − Partie 7 : alphabet latin/grec, 2003.
ISO 16844-3	Véhicules routiers − Systèmes tachygraphes − Interface de capteur de mouvement, 2004, et rectificatif technique 1: 2006.
BSI/ANSSI	Rapport technique TR-03110-3, Mécanismes de sécurité avancés pour les documents de voyage lisibles à la machine et jeton eIDAS − Partie 3 : spécifications communes, version 2.20, 3 février 2015.

2. Définitions des types de données

Quel que soit le type de données considéré parmi ceux qui suivent, la valeur par défaut d'un contenu « inconnu » ou « sans objet » consistera à remplir le champ de l'élément de données concerné avec des octets **Hex** 'FF'**, sauf disposition contraire**.

Tous les types de données servent aux applications de générations 1 et 2, sauf disposition contraire.

Les types de données utilisés exclusivement par les applications de génération 2, version 2, sont spécifiés. Pour les types de données servant aux applications de générations 1 et 2, la taille indiquée dans le présent sous-appendice est celle correspondant aux applications de génération 2. La taille prévue pour les applications de génération 1 est censée être déjà connue du lecteur. Les numéros des exigences de l'appendice 1C liées aux différents types de données concernent à la fois les applications de générations 1 et 2.

Les types de données de carte qui n'ont pas été définis pour les cartes de génération 1 ne sont pas stockés dans l'application de génération 1 des cartes de génération 2. En particulier :

- **Les numéros d'homologation stockés dans l'application de génération 1 des cartes de génération 2 sont réduits aux huit premiers caractères si nécessaire ;**
- **Seule la condition TRAJET EN FERRY/TRAIN (début) d'une condition particulière TRAJET EN FERRY/TRAIN doit être stockée dans l'application de génération 1 des cartes de génération 2.**

2.1 ActivityChangeInfo

Ce type de données permet le codage, en mots de deux octets, d'un état du lecteur à 00 h 00 et/ou d'une situation de conduite à 00 h 00, et/ou de changements d'activité, de situation de conduite et/ou de situation de la carte se rapportant à un conducteur ou un co-conducteur particulier. Ce type de données est lié aux exigences 105, 266, 291, 320, 321, 343 et 344 de ~~l'annexe~~ **l'appendice** 1C.

ActivityChangeInfo ::= OCTET STRING (SIZE(2))

Attribution de valeur − Octet aligné : 'scpaatttttttttt'B (16 bits)

Pour les enregistrements de données (ou d'un état du lecteur) :

's'B Lecteur :

'0'B : CONDUCTEUR

'1'B : CO-CONDUCTEUR

'c'B Situation de conduite :

'0'B : SEUL

‘1’B : ÉQUIPAGE

‘p’B Situation de la carte de conducteur (ou d’atelier) dans le lecteur approprié :

‘0’B : INSÉRÉE, la carte est insérée

‘1’B : NON INSÉRÉE, aucune carte n’est insérée (ou la carte a été retirée)

‘aa’B Activité :

‘00’B : INTERRUPTION/REPOS

‘01’B : DISPONIBILITÉ

‘10’B : TRAVAIL

‘11’B : CONDUITE

‘ttttttttttt’B Heure du changement : nombre de minutes écoulées depuis 00 h 00 le jour considéré.

Pour les enregistrements (et la situation de conduite) sur la carte de conducteur (ou d’atelier) :

‘s’B Lecteur (hors de propos si ‘p’ = 1, sauf remarque ci-après) :

‘0’B : CONDUCTEUR

‘1’B : CO-CONDUCTEUR

‘c’B Situation de conduite (si ‘p’ = 0) ou état d’activité (si ‘p’ = 1) :

‘0’B : SEUL ‘0’B : INCONNU

‘1’B : ÉQUIPAGE ‘1’B : CONNU (= saisie manuelle)

‘p’B Situation de la carte :

‘0’B : INSÉRÉE, la carte est insérée dans un appareil de contrôle

‘1’B : NON INSÉRÉE, aucune carte n’est insérée (ou la carte a été retirée)

‘aa’B Activité (hors de propos si ‘p’ = 1 et ‘c’ = 0, sauf remarque ci-après) :

‘00’B : INTERRUPTION/REPOS

‘01’B : DISPONIBILITÉ

‘10’B : TRAVAIL

‘11’B : CONDUITE

‘ttttttttttt’B Heure du changement : nombre de minutes écoulées depuis 00 h 00 le jour considéré.

Remarque :

En cas de retrait de la carte :

- ‘s’ s’applique et indique le lecteur dont la carte a été extraite ;
- ‘c’ doit être mis à 0 ;
- ‘p’ doit être mis à 1 ;
- ‘aa’ doit coder l’activité en cours sélectionnée à ce moment.

Les bits ‘c’ et ‘aa’ du mot (enregistré sur une carte) peuvent être écrasés à la suite d’une saisie manuelle pour refléter la nouvelle saisie.

2.2 Address

Une adresse.

Address ::= SEQUENCE {

codePage INTEGER (0..255),

address OCTET STRING (SIZE(35))

}

codePage spécifie un jeu de caractères défini au chapitre 4.

address indique une adresse codée à l'aide du jeu de caractères spécifié.

2.3 AESKey

Génération 2 :

Une clé AES d'une longueur de 128, 192 ou 256 bits.

AESKey ::= CHOICE {

aes128Key AES128Key,

aes192Key AES192Key,

aes256Key AES256Key

}

Attribution de valeur : absence d'informations complémentaires.

2.4 AES128Key

Génération 2:

Une clé AES128.

AES128Key ::= SEQUENCE {

length INTEGER(0..255),

aes128Key OCTET STRING (SIZE(16))

}

length indique la longueur de la clé AES128 en octets.

aes128Key désigne une clé AES d'une longueur de 128 bits.

Attribution de valeur : la longueur a une valeur de 16.

2.5 AES192Key

Génération 2 :

Une clé AES192.

AES192Key ::= SEQUENCE {

length INTEGER(0..255),

aes192Key OCTET STRING (SIZE(24))

}

length indique la longueur de la clé AES192 en octets.

aes192Key désigne une clé AES d'une longueur de 192 bits.

Attribution de valeur : la longueur a une valeur de 24.

2.6 AES256Key

Génération 2 :

Une clé AES256.

AES256Key ::= SEQUENCE {

length INTEGER(0..255),

aes256Key OCTET STRING (SIZE(32))

}

length indique la longueur de la clé AES256 en octets.

aes256Key désigne une clé AES d'une longueur de 256 bits.

Attribution de valeur : la longueur a une valeur de 32.

2.7 BCDString

BCDString s'applique à la représentation de données en décimal codé binaire (BCD). Ce type de données permet de représenter un chiffre décimal par un quartet (4 bits). Il est fondé sur le type 'CharacterString' défini dans la norme ISO/CEI 8824-1.

BCDString ::= CHARACTER STRING (WITH COMPONENTS {

identification (WITH COMPONENTS {

fixed PRESENT }) })

BCDString utilise une notation « hstring ». Le chiffre hexadécimal de gauche sera considéré comme le quartet le plus significatif du premier octet. Pour produire un multiple d'octets, il faut insérer à droite le nombre approprié de quartets nuls à partir de la position qu'occupe le quartet de gauche du premier octet.

Chiffres admis : 0, 1, .. 9.

2.8 CalibrationPurpose

Code indiquant la raison de l'enregistrement d'un jeu de paramètres d'étalonnage. Ce type de données est lié aux exigences 097 et 098 de ~~l'annexe~~ **l'appendice** 1B et ~~aux~~ **à l'**exigence~~s~~ 119 de ~~l'annexe~~ **l'appendice** 1C.

CalibrationPurpose ::= OCTET STRING (SIZE(1))

Attribution de valeur :

Génération 1 :

'00'H valeur réservée ;

'01'H activation : enregistrement des paramètres d'étalonnage connus, au moment de l'activation de l'UEV ;

'02'H première installation : premier étalonnage de l'UEV après son activation ;

'03'H installation : premier étalonnage de l'unité embarquée sur le véhicule considéré ;

'04'H inspection périodique.

Génération 2 :

Outre les valeurs prévues pour la génération 1, les valeurs suivantes sont utilisées :

'05'H saisie des numéros d'immatriculation par l'entreprise ;

'06'H remise à l'heure sans étalonnage ;

'07'H à '7F'H réservé pour une utilisation future ;

‘80’H à ‘FF’H propre au fabricant.

2.9 CardActivityDailyRecord

Informations enregistrées sur une carte concernant les activités auxquelles le conducteur s’est livré pendant un jour civil donné. Ce type de données est lié aux exigences 266, 291, 320 et 343 de ~~l’annexe~~ **l’appendice** 1C.

CardActivityDailyRecord :	= SEQUENCE {
activityPreviousRecordLength	INTEGER(0..CardActivityLengthRange),
activityRecordLength	INTEGER(0..CardActivityLengthRange),
activityRecordDate	TimeReal,
activityDailyPresenceCounter	DailyPresenceCounter,
activityDayDistance	Distance,
activityChangeInfo	SET SIZE(1..1440) OF ActivityChangeInfo
}	

activityPreviousRecordLength indique la longueur totale du précédent enregistrement quotidien exprimée en octets. La valeur maximale correspond à la longueur de la chaîne d’octets (OCTET STRING) contenant l’ensemble de ces enregistrements (voir CardActivityLengthRange, ~~appendice~~ **sous-appendice** 2, par. 4). Lorsque cet enregistrement est l’enregistrement quotidien le plus ancien, la valeur d’activityPreviousRecordLength doit être mise à 0.

activityRecordLength indique la longueur totale de cet enregistrement exprimée en octets. La valeur maximale correspond à la longueur de la chaîne d’octets (OCTET STRING) contenant l’ensemble de ces enregistrements.

activityRecordDate indique la date de l’enregistrement.

activityDailyPresenceCounter indique l’état du compteur de présence journalière correspondant à la carte et le jour considérés.

activityDayDistance indique la distance totale parcourue le jour considéré.

activityChangeInfo désigne le jeu de données de type ActivityChangeInfo correspondant au conducteur et au jour considérés. Cette chaîne d’octets ne peut contenir plus de 1 440 valeurs (soit un changement d’activité par minute). Ce jeu comprend toujours l’activityChangeInfo qui code la situation de conduite à 00 h 00.

2.10 CardActivityLengthRange

Nombre d’octets disponibles sur une carte de conducteur ou d’atelier pour le stockage des enregistrements d’activité du conducteur.

CardActivityLengthRange ::= INTEGER(0..2^{16}-1)

Attribution de valeur : voir **sous-**appendice 2.

2.11 CardApprovalNumber

Numéro d’homologation de la carte.

CardApprovalNumber ::= IA5String(SIZE(8))

Attribution de valeur :

le numéro d’homologation doit être indiqué tel qu’il est publié sur le site Web correspondant ~~de la Commission européenne correspondant~~ **du laboratoire compétent pour les essais**

d'interopérabilité, par exemple en incluant les traits d'union. Le numéro d'homologation doit être aligné à gauche.

2.11a CardBorderCrossings

Génération 2, version 2 :

Informations enregistrées sur une carte de conducteur ou d'atelier concernant les passages de frontières du véhicule lorsque celui-ci a franchi la frontière d'un pays (exigences 306f et 356f de l'appendice 1C).

CardBorderCrossings ::= SEQUENCE {

borderCrossingPointerNewestRecord	**INTEGER (0..NoOfBorderCrossingRecords -1),**
cardBorderCrossingRecords	**SET SIZE (NoOfBorderCrossingRecords) OF CardBorderCrossingRecord**

}

borderCrossingPointerNewestRecord désigne l'indice du plus récent enregistrement de passage de frontière sur la carte.

Attribution de valeur : nombre correspondant au numérateur de l'enregistrement de passage de frontière, commençant par une série de '0' pour la première occurrence d'un enregistrement de passage de frontière dans la structure considérée.

cardBorderCrossingRecords désigne le jeu d'enregistrements de passages de frontières.

2.11b CardBorderCrossingRecord

Génération 2, version 2 :

Informations enregistrées sur une carte de conducteur ou d'atelier concernant les passages de frontières du véhicule lorsque celui-ci a franchi la frontière d'un pays (exigences 147b, 306e et 356e de l'appendice 1C).

CardBorderCrossingRecord ::= SEQUENCE {

countryLeft	**NationNumeric,**
countryEntered	**NationNumeric,**
gnssPlaceAuthRecord	**GNSSPlaceAuthRecord,**
vehicleOdometerValue	**OdometerShort**

}

countryLeft désigne le pays que le véhicule a quitté ou indique l'absence d'informations disponibles conformément à l'exigence 147b de l'appendice 1C. La mention « reste du monde » (code NationNumeric 'FF'H) doit être utilisée lorsque l'unité embarquée sur le véhicule n'est pas en mesure de déterminer le pays où se trouve le véhicule (par exemple, ledit pays ne figure pas sur les cartes numériques stockées dans la mémoire).

countryEntered désigne le pays dans lequel le véhicule est entré ou le pays dans lequel le véhicule se trouve au moment de l'insertion de la carte. La mention « reste du monde » (code NationNumeric 'FF'H) doit être utilisée lorsque l'unité embarquée sur le véhicule n'est pas en mesure de déterminer le pays où se trouve le véhicule (par exemple, ledit pays ne figure pas sur les cartes numériques stockées dans la mémoire).

gnssPlaceAuthRecord contient les informations relatives à la position du véhicule lorsque l'unité embarquée a détecté que le véhicule avait franchi la frontière d'un pays, ou la mention « aucune information disponible » conformément à l'exigence 147b de l'appendice 1C, ainsi que l'état d'authentification de cette position.

vehicleOdometerValue est la valeur affichée par le compteur kilométrique lorsque l'unité embarquée a détecté que le véhicule avait franchi la frontière d'un pays, ou la mention « aucune information disponible » conformément à l'exigence 147b de l'appendice 1C.

2.12 CardCertificate

Génération 1 :

Certificat associé à la clé publique d'une carte.

CardCertificate ::= Certificate

2.13 CardChipIdentification

Informations enregistrées sur une carte et se rapportant à l'identification du circuit intégré (IC) de cette carte (exigence 249 de ~~l'annexe~~ **l'appendice** 1C). Le icSerialNumber associé au icManufacturingReferences permet d'identifier de manière unique le circuit de la carte. Le icSerialNumber seul ne permet pas d'identifier le circuit de la carte de manière unique.

CardChipIdentification ::= SEQUENCE {

icSerialNumber	OCTET STRING (SIZE(4)),
icManufacturingReferences	OCTET STRING (SIZE(4))

}

icSerialNumber indique le numéro de série de l'IC.

icManufacturingReferences indique l'identificateur propre au fabricant de l'IC.

2.14 CardConsecutiveIndex

Indice séquentiel de la carte considérée (définition h)).

CardConsecutiveIndex ::= IA5String(SIZE(1))

Attribution de valeur : voir ~~annexe~~ **appendice** 1C, chapitre 7.

Ordre croissant : '0, …, 9, A , …, Z , a, …, z'

2.15 CardControlActivityDataRecord

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant au dernier contrôle auquel le conducteur considéré a été soumis (exigences 274, 299, 327 et 350 de ~~l'annexe~~ **l'appendice** 1C).

CardControlActivityDataRecord ::= SEQUENCE {

controlType	ControlType,
controlTime	TimeReal,
controlCardNumber	FullCardNumber,
controlVehicleRegistration	VehicleRegistrationIdentification,
controlDownloadPeriodBegin	TimeReal,
controlDownloadPeriodEnd	TimeReal }

controlType indique le type de contrôle.

controlTime indique la date et l'heure du contrôle.

controlCardNumber indique le numéro intégral de la carte du contrôleur qui a procédé au contrôle.

controlVehicleRegistration indique le VRN et ~~l'État membre~~ **la Partie contractante** d'immatriculation du véhicule soumis au contrôle considéré.

controlDownloadPeriodBegin et **controlDownloadPeriodEnd** indiquent la période téléchargée, en cas de téléchargement.

2.16 CardCurrentUse

Informations relatives à l'usage effectif de la carte (exigences 273, 298, 326 et 349 de l'~~annexe~~ **l'appendice** 1C).

CardCurrentUse ::= SEQUENCE {

sessionOpenTime TimeReal,

sessionOpenVehicle VehicleRegistrationIdentification

}

sessionOpenTime indique l'heure d'insertion de la carte utilisée dans le cadre de l'activité en cours. Cet élément est mis à zéro lors du retrait de la carte.

sessionOpenVehicle correspond à l'identification du véhicule en cours d'utilisation après insertion de la carte. Cet élément est mis à zéro lors du retrait de la carte.

2.17 CardDriverActivity

Informations enregistrées sur une carte de conducteur ou d'atelier concernant les activités du conducteur (exigences 267, 268, 292, 293, 321 et 344 de ~~l'annexe~~ **l'appendice** 1C).

CardDriverActivity ::= SEQUENCE {

activityPointerOldestDayRecord INTEGER(0.. CardActivityLengthRange-1),

activityPointerNewestRecord INTEGER(0.. CardActivityLengthRange-1),

activityDailyRecords OCTET STRING (SIZE(CardActivityLengthRange))

}

activityPointerOldestDayRecord spécifie le début de l'emplacement en mémoire (nombre d'octets comptés à partir du début de la chaîne) de l'enregistrement quotidien complet le plus ancien que comporte la chaîne activityDailyRecords. La valeur maximale correspond à la longueur de la chaîne.

activityPointerNewestRecord spécifie le début de l'emplacement en mémoire (nombre d'octets comptés à partir du début de la chaîne) de l'enregistrement quotidien le plus récent que comporte la chaîne activityDailyRecords. La valeur maximale correspond à la longueur de la chaîne.

activityDailyRecords indique l'espace disponible pour le stockage de données relatives aux activités du conducteur (structure de données : CardActivityDailyRecord) pour chaque jour civil au cours duquel la carte a été utilisée.

Attribution de valeur : cette chaîne d'octets est périodiquement remplie par de nouveaux enregistrements de type CardActivityDailyRecord. Lors de la première utilisation, l'enregistrement commence au premier octet de la chaîne. Les enregistrements suivants sont ajoutés à la fin du précédent. Lorsque la chaîne est saturée, l'enregistrement se poursuit en reprenant au premier octet de la chaîne, sans tenir compte de la présence d'une discontinuité dans un élément de données. Avant d'introduire de nouvelles données d'activité dans la chaîne (en étendant l'activityDailyRecord existant ou en insérant un nouvel activityDailyRecord), lesquelles se substituent aux données d'activité les plus anciennes, il convient de mettre à jour l'activityPointerOldestDayRecord afin de rendre compte du nouvel

emplacement en mémoire qu'occupe désormais l'enregistrement quotidien complet le plus ancien et de mettre à zéro l'activityPreviousRecordLength de ce nouvel enregistrement quotidien complet le plus ancien.

2.18 CardDrivingLicenceInformation

Informations enregistrées sur une carte de conducteur concernant les données relatives au permis de conduire du détenteur de la carte (exigence 259 et 284 de ~~l'annexe~~ **l'appendice** 1C).

CardDrivingLicenceInformation ::= SEQUENCE {

drivingLicenceIssuingAuthority Name,

drivingLicenceIssuing ~~Nation~~NationNumeric,

drivingLicenceNumber IA5String(SIZE(16))

}

drivingLicenceIssuingAuthority désigne l'autorité responsable de la délivrance du permis de conduire.

drivingLicenceIssuingNation indique la nationalité de l'autorité qui a délivré le permis de conduire.

drivingLicenceNumber indique le numéro du permis de conduire.

2.19 CardEventData

Génération 1 :

Informations enregistrées sur une carte de conducteur ou d'atelier concernant les événements associés au détenteur de la carte (exigences 260~~, 285, 318~~ et ~~341~~ **318** de ~~l'annexe~~ **appendice** 1C).

CardEventData ::= SEQUENCE SIZE(6) OF {

cardEventRecords SET SIZE(NoOfEventsPerType) OF CardEventRecord

}

CardEventData consiste en une séquence de cardEventRecords (à l'exception des enregistrements relatifs aux tentatives d'atteinte à la sécurité, lesquels sont regroupés dans le dernier jeu de données de la séquence) dont l'agencement correspond à celui des EventFaultType classés par ordre croissant.

cardEventRecords désigne un jeu d'enregistrements de données relatives à un type d'événement donné (ou d'une catégorie donnée pour les tentatives d'atteinte à la sécurité).

Génération 2 :

Informations enregistrées sur une carte de conducteur ou d'atelier concernant les événements associés au détenteur de la carte (exigences 285 et 341 de l'appendice 1C).

CardEventData ::= SEQUENCE SIZE(11) OF {

cardEventRecords SET SIZE(NoOfEventsPerType) OF CardEventRecord

}

CardEventData consiste en une séquence de cardEventRecords (à l'exception des enregistrements portant sur les tentatives éventuelles d'atteinte à la sécurité, lesquels sont regroupés dans le dernier jeu de données de la séquence) dont l'agencement correspond à celui des EventFaultType classés par ordre croissant.

cardEventRecords désigne un jeu d'enregistrements de données relatives à un type d'événements donné (ou d'une catégorie donnée pour les tentatives d'atteinte à la sécurité).

2.20 CardEventRecord

Informations enregistrées sur une carte de conducteur ou d'atelier concernant un événement associé au détenteur de la carte (exigences 261, 286, 318 et 341 de l'appendice 1C).

CardEventRecord ::= SEQUENCE {

eventType	EventFaultType,
eventBeginTime	TimeReal,
eventEndTime	TimeReal,
eventVehicleRegistration	VehicleRegistrationIdentification

}

eventType indique le type d'événement.

eventBeginTime indique la date et l'heure du début de l'événement.

eventEndTime indique la date et l'heure de la fin de l'événement.

eventVehicleRegistration indique le VRN et ~~l'État membre~~ **la Partie contractante** d'immatriculation du véhicule dans lequel l'événement considéré s'est produit.

2.21 CardFaultData

Informations enregistrées sur une carte de conducteur ou d'atelier concernant les anomalies associées au détenteur de la carte (exigences 263, 288, 318 et 341 de ~~l'annexe~~ **l'appendice** 1C).

CardEventData ::= SEQUENCE SIZE(2) OF {

cardEventRecords	SET SIZE(NoOfEventsPerType) OF CardEventRecord

}

CardFaultData consiste en une séquence comportant un jeu d'enregistrements d'anomalies affectant l'appareil de contrôle suivi d'un jeu d'enregistrements d'anomalies affectant la ou les cartes utilisée(s).

cardFaultRecords désigne un jeu d'enregistrements relatifs à une catégorie d'anomalies donnée (appareil de contrôle ou carte).

2.22 CardFaultRecord

Informations enregistrées sur une carte de conducteur ou d'atelier concernant une anomalie associée au détenteur de la carte (exigences 264, 289, 318 et 341 de ~~l'annexe~~ **l'appendice** 1C).

CardFaultRecord ::= SEQUENCE {

faultType	EventFaultType,
faultBegin	~~Time~~TimeReal,
faultEndTime	TimeReal,
faultVehicleRegistration	VehicleRegistrationIdentification

}

faultType indique le type d'anomalie.

faultBeginTime indique la date et l'heure du début de l'anomalie.

faultEndTime indique la date et l'heure de la fin de l'anomalie.

faultVehicleRegistration indique le VRN et ~~l'État membre~~ **la Partie contractante** d'immatriculation du véhicule dans lequel l'anomalie considérée s'est produite.

2.23 CardIccIdentification

Informations enregistrées sur une carte et se rapportant à l'identification de son circuit intégré (IC) (exigence 248 de ~~l'annexe~~ **l'appendice** 1C).

CardIccIdentification ::= SEQUENCE {

clockStop	OCTET STRING (SIZE(1)),
cardExtendedSerialNumber	ExtendedSerialNumber,
cardApprovalNumber	CardApprovalNumber,
cardPersonaliserID	ManufacturerCode,
embedderIcAssemblerId	EmbedderIcAssemblerId,
icIdentifier	OCTET STRING (SIZE(2))

}

clockStop désigne le mode Clockstop défini dans ~~l'appendice~~ **le sous-appendice** 2.

cardExtendedSerialNumber indique le numéro de série unique de la carte à circuit intégré précisé par le type de données ExtendedSerialNumber.

cardApprovalNumber indique le numéro d'homologation de la carte.

cardPersonaliserID indique l'ID individuelle de la carte codée sous forme de ManufacturerCode.

embedderIcAssemblerId donne des informations sur l'intégrateur/assembleur du circuit intégré.

icIdentifier indique l'identificateur du circuit intégré de la carte et de son fabricant défini dans la norme ISO/CEI 7816-6.

2.24 CardIdentification

Informations stockées sur une carte et se rapportant à son identification (exigences 255, 280, 310, 333, 359, 365, 371 et 377 de ~~l'annexe~~ **l'appendice** 1C).

CardIdentification ::= SEQUENCE {

cardIssuingMemberState	NationNumeric,
cardNumber	CardNumber,
cardIssuingAuthorityName	Name,
cardIssueDate	TimeReal,
cardValidityBegin	TimeReal,
cardExpiryDate	TimeReal

}

cardIssuingMemberState indique le code de ~~l'État membre~~ **la Partie contractante** qui a délivré la carte.

cardNumber indique le numéro de la carte considérée.

cardIssuingAuthorityName indique le nom de l'autorité qui a délivré la carte considérée.

cardIssueDate indique la date de délivrance de la carte à son détenteur actuel.

cardValidityBegin indique la première date d'entrée en vigueur de la carte.

cardExpiryDate indique la date d'expiration de la carte.

2.24a CardLoadTypeEntries

Génération 2, version 2 :

Informations enregistrées sur une carte de conducteur ou d'atelier concernant les saisies du type de chargement lorsque la carte est insérée dans une unité embarquée (exigences 306j et 356j de l'appendice 1C).

CardLoadTypeEntries ::= SEQUENCE {

loadTypeEntryPointerNewestRecord	**INTEGER(0..NoOfLoadTypeEntryRecords -1),**
cardLoadTypeEntryRecords	**SET SIZE(NoOfLoadTypeEntryRecords) OF CardLoadTypeEntryRecord**

}

loadTypeEntryPointerNewestRecord désigne l'indice du plus récent enregistrement de type de chargement sur la carte.

Attribution de valeur : nombre correspondant au numérateur de l'enregistrement de type de chargement sur la carte, commençant par une série de '0' pour la première occurrence d'un enregistrement de type de chargement dans la structure considérée.

cardLoadTypeEntryRecords désigne le jeu d'enregistrements contenant la date et l'heure de la saisie ainsi que le type de chargement introduit.

2.24b CardLoadTypeEntryRecord

Génération 2, version 2 :

Informations enregistrées sur une carte de conducteur ou d'atelier concernant les changements de type de chargement saisis à l'insertion de la carte dans une unité embarquée (exigences 306i et 356i de l'appendice 1C).

CardLoadTypeEntryRecord ::= SEQUENCE {

timeStamp	**TimeReal,**
loadTypeEntered	**LoadType**

}

timeStamp indique la date et l'heure auxquelles le type de chargement a été saisi.

loadTypeEntered indique le type de chargement introduit.

2.24c CardLoadUnloadOperation

Génération 2, version 2 :

Informations enregistrées sur une carte de conducteur ou d'atelier concernant les opérations de chargement/déchargement du véhicule (exigences 306h et 356h de l'appendice 1C).

CardLoadUnloadOperations ::= SEQUENCE {

loadUnloadPointerNewestRecord	**INTEGER(0..NoOfLoadUnloadRecords -1),**
cardLoadUnloadRecords	**SET SIZE(NoOfLoadUnloadRecords) OF CardLoadUnloadRecord**

}

loadUnloadPointerNewestRecord est l'indice du plus récent enregistrement d'opération de chargement/déchargement sur la carte.

Attribution de valeur : nombre correspondant au numérateur de l'enregistrement de chargement/déchargement, commençant par une série de '0' pour la première occurrence d'un enregistrement de chargement/déchargement dans la structure considérée.

cardLoadUnloadRecords désigne le jeu d'enregistrements contenant l'indication du type d'opération (chargement, déchargement ou chargement/déchargement simultanés), la date et l'heure de saisie de l'opération de chargement/déchargement dans le système, ainsi que les informations relatives à la position et au kilométrage du véhicule.

2.24d CardLoadUnloadRecord

Génération 2, version 2 :

Informations enregistrées sur une carte de conducteur ou d'atelier concernant les opérations de chargement/déchargement du véhicule (exigences 306g et 356g de l'appendice 1C).

CardLoadUnloadRecord ::= SEQUENCE {

timeStamp	**TimeReal,**
operationType	**OperationType,**
gnssPlaceAuthRecord	**GNSSPlaceAuthRecord,**
vehicleOdometerValue	**OdometerShort**

}

timeStamp indique la date et l'heure du début de l'opération de chargement/déchargement.

operationType indique le type d'opération saisi dans le système (chargement, déchargement ou chargement/déchargement simultanés).

gnssPlaceAuthRecord contient les informations relatives à la position du véhicule.

vehicleOdometerValue est la valeur affichée par le compteur kilométrique au début de l'opération de chargement/déchargement.

2.25 CardMACertificate

Génération 2 :

Certificat associé à la clé publique d'une carte et destiné à l'authentification mutuelle avec une UEV. La structure de ce certificat est spécifiée dans ~~l'appendice~~ **le sous-appendice** 11.

CardMACertificate ::= Certificate

2.26 CardNumber

Un numéro de carte (définition g)).

CardNumber ::= CHOICE {

SEQUENCE {

driverIdentification	IA5String(SIZE(14)),
cardReplacementIndex	CardReplacementIndex,

cardRenewalIndex CardRenewalIndex

},

SEQUENCE {

ownerIdentification IA5String(SIZE(13)),

cardConsecutiveIndex CardConsecutiveIndex,

cardReplacementIndex CardReplacementIndex,

cardRenewalIndex CardRenewalIndex

}

}

driverIdentification indique l'identification unique d'un conducteur dans un**e** ~~État membre~~**Partie contractante**.

ownerIdentification indique l'identification unique d'une entreprise, d'un atelier ou d'un organisme de contrôle établis dans un**e** ~~État membre~~**Partie contractante**.

cardConsecutiveIndex est l'indice séquentiel de la carte.

cardReplacementIndex est l'indice de remplacement de la carte.

cardRenewalIndex est l'indice de renouvellement de la carte.

La première séquence de la sélection (CHOICE) permet de coder un numéro de carte de conducteur et la seconde de coder les numéros des cartes d'atelier, de contrôleur et d'entreprise.

2.26a CardPlaceAuthDailyWorkPeriod

Génération 2, version 2 :

Informations enregistrées sur une carte de conducteur ou d'atelier, indiquant l'état d'authentification des lieux de début et/ou de fin des périodes de travail journalières (exigence 306b et 356b de l'appendice 1C).

CardPlaceAuthDailyWorkPeriod ::= SEQUENCE {

placeAuthPointerNewestRecord INTEGER(0 .. NoOfCardPlaceRecords-1),

placeAuthStatusRecords SET SIZE(NoOfCardPlaceRecords) OF PlaceAuthStatusRecord

}

placeAuthPointerNewestRecord est l'indice du plus récent enregistrement d'état d'authentification de lieu.

Attribution de valeur : nombre correspondant au numérateur de l'enregistrement d'état d'authentification de lieu, commençant par une série de '0' pour la première occurrence d'un enregistrement d'état d'authentification de lieu dans la structure considérée.

placeAuthStatusRecords désigne le jeu d'enregistrements contenant l'état d'authentification des lieux saisis dans le système.

2.27 CardPlaceDailyWorkPeriod

Informations enregistrées sur une carte de conducteur ou d'atelier concernant les lieux de début et/ou de fin des périodes de travail journalières (exigences 272, 297, 325 et 348 de ~~l'annexe~~ **l'appendice** 1C).

CardPlaceDailyWorkPeriod ::= SEQUENCE {

placePointerNewestRecord INTEGER(0..NoOfCardPlaceRecords-1),

placeRecords SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord

}

placePointerNewestRecord est l'indice du plus récent enregistrement de lieu mis à jour.

Attribution de valeur : nombre correspondant au numérateur de l'enregistrement de lieu, commençant par une série de '0' pour la première occurrence d'un enregistrement de lieu dans la structure.

placeRecords désigne le jeu d'enregistrements contenant les données relatives aux lieux saisis dans le système.

2.28 CardPrivateKey

Génération 1 :

Clé privée d'une carte.

CardPrivateKey ::= RSAKeyPrivateExponent

2.29 CardPublicKey

Clé publique d'une carte.

CardPublicKey ::= PublicKey

2.30 CardRenewalIndex

Indice de renouvellement d'une carte (définition i)).

CardRenewalIndex ::= IA5String(SIZE(1))

Attribution de valeur : voir chapitre ~~VII~~ **7** ~~de la~~ **du** présent~~e annexe~~ **appendice**.

'0' Première délivrance.

Ordre croissant : '0 , … , 9 , A , … , Z'

2.31 CardReplacementIndex

Indice de remplacement d'une carte (définition j)).

CardReplacementIndex ::= IA5String(SIZE(1))

Attribution de valeur : voir chapitre ~~VII~~**7** ~~de la~~ **du** présent~~e annexe~~ **appendice**.

'0' Carte originale.

Ordre croissant : '0 , … , 9 , A , … , Z'

2.32 CardSignCertificate

Génération 2 :

Certificat associé à la clé publique d'une carte et destiné à la signature. La structure de ce certificat est spécifiée dans ~~l'appendice~~ **le sous-appendice** 11.

CardSignCertificate ::= Certificate

2.33 CardSlotNumber

Code permettant de faire la distinction entre les deux lecteurs de carte d'une unité embarquée.

CardSlotNumber ::= INTEGER {

driverSlot (0),

co-driverSlot (1)

}

Attribution de valeur : absence d'informations complémentaires.

2.34 CardSlotsStatus

Code indiquant le type de carte insérée dans les deux lecteurs de l'unité embarquée.

CardSlotsStatus ::= OCTET STRING (SIZE(1))

Attribution de valeur − Octet aligné : 'ccccdddd'B

'cccc'B identification du type de carte insérée dans le lecteur réservé au co-conducteur ;

'dddd'B identification du type de carte insérée dans le lecteur réservé au conducteur ;

à l'aide des codes d'identification suivants :

'0000'B aucune carte n'est insérée ;

'0001'B une carte de conducteur est insérée ;

'0010'B une carte d'atelier est insérée ;

'0011'B une carte de contrôleur est insérée ;

'0100'B une carte d'entreprise est insérée.

2.35 CardSlotsStatusRecordArray

Génération 2 :

CardSlotsStatus plus les métadonnées servant au protocole de téléchargement.

CardSlotsStatusRecordArray ::= SEQUENCE {

recordType RecordType,

recordSize INTEGER(1..65535),

noOfRecords INTEGER(0..65535),

records SET SIZE(noOfRecords) OF CardSlotsStatus

}

recordType indique le type d'enregistrement (CardSlotsStatus). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type CardSlotsStatus exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne le jeu d'enregistrements de type CardSlotsStatus.

2.36 CardStructureVersion

Code indiquant la version de la structure mise en œuvre au sein d'une carte tachygraphique.

CardStructureVersion ::= OCTET STRING (SIZE(2))

Attribution de valeur : ‘aabb’H :

‘aa’H Indice des modifications apportées à la structure :

‘00’H pour les applications de génération 1

‘01’H pour les applications de génération 2

‘bb’H Indice des modifications relatives à l’utilisation des éléments de données définis pour la structure donné par l’octet le plus significatif :

‘00’H pour ~~cette version d’~~ **les** applications de génération 1

‘00’H pour ~~cette~~ **la** version **1** des applications de génération 2

‘01’H pour la version 2 des applications de génération 2

2.37 CardVehicleRecord

Informations enregistrées sur une carte de conducteur ou d’atelier concernant une période d’utilisation d’un véhicule donné pendant un jour civil déterminé (exigences 269, 294, 322 et 345 de ~~l’annexe~~ **l’appendice** 1C).

Génération 1 :

CardVehicleRecord ::= SEQUENCE {

vehicleOdometerBegin	OdometerShort,
vehicleOdometerEnd	OdometerShort,
vehicleFirstUse	TimeReal,
vehicleLastUse	TimeReal,
vehicleRegistration	VehicleRegistrationIdentification,
vuDataBlockCounter	VuDataBlockCounter

}

vehicleOdometerBegin indique la valeur affichée par le compteur kilométrique du véhicule au début de la période d’utilisation considérée.

vehicleOdometerEnd indique la valeur affichée par le compteur kilométrique du véhicule à la fin de la période d’utilisation considérée.

vehicleFirstUse indique la date et l’heure de début de la période d’utilisation du véhicule.

vehicleLastUse indique la date et l’heure de fin de la période d’utilisation du véhicule.

vehicleRegistration indique le VRN et ~~l’État membre~~ **la Partie contractante** d’immatriculation du véhicule.

vuDataBlockCounter indique la valeur de VuDataBlockCounter lors de la dernière extraction de données pour la période d’utilisation considérée.

Génération 2 :

CardVehicleRecord ::= SEQUENCE {

vehicleOdometerBegin	OdometerShort,
vehicleOdometerEnd	OdometerShort,
vehicleFirstUse	TimeReal,
vehicleLastUse	TimeReal,
vehicleRegistration	VehicleRegistrationIdentification,
vuDataBlockCounter	VuDataBlockCounter,
vehicleIdentificationNumber	VehicleIdentificationNumber

}

L'élément de données suivant est utilisé en plus des éléments composant la structure de génération 1 :

VehicleIdentificationNumber indique le numéro d'identification du véhicule qui correspond au véhicule dans son entier.

2.38 CardVehiclesUsed

Informations enregistrées sur une carte de conducteur ou d'atelier concernant les véhicules utilisés par le détenteur de la carte (exigences 270, 295, 323 et 346 de ~~l'annexe~~ **l'appendice** 1C).

CardVehiclesUsed := SEQUENCE {

vehiclePointerNewestRecord	INTEGER(0..NoOfCardVehicleRecords-1),
cardVehicleRecords	SET SIZE(NoOfCardVehicleRecords) OF CardVehicleRecord

}

vehiclePointerNewestRecord est l'indice du plus récent enregistrement de données relatives à un véhicule mis à jour.

Attribution de valeur : nombre correspondant au numérateur de l'enregistrement de véhicule, commençant par une série de '0' pour la première occurrence d'un enregistrement de véhicule dans la structure considérée.

cardVehicleRecords désigne le jeu d'enregistrements contenant des informations relatives aux véhicules utilisés.

2.39 CardVehicleUnitRecord

Génération 2 :

Informations enregistrées sur une carte de conducteur ou d'atelier concernant une unité embarquée ayant été utilisée (exigences 303 et 351 de ~~l'annexe~~ **l'appendice** 1C).

CardVehicleUnitRecord ::= SEQUENCE {

~~T~~**t**imeStamp	TimeReal,
manufacturerCode	ManufacturerCode,
deviceID	INTEGER(0..255),
vuSoftwareVersion	VuSoftwareVersion

}

timeStamp indique le début de la période d'utilisation de l'unité embarquée sur le véhicule (c'est-à-dire de la première insertion de la carte dans le lecteur approprié de l'unité embarquée pour cette période).

manufacturerCode identifie le fabricant de l'unité embarquée.

deviceID identifie le type d'unité embarquée d'un fabricant. La valeur est propre au fabricant.

vuSoftwareVersion indique le numéro de version du logiciel de l'unité embarquée.

2.40 CardVehicleUnitsUsed

Génération 2 :

Informations enregistrées sur une carte de conducteur ou d'atelier concernant les unités embarquées utilisées par le détenteur de la carte (exigences 30~~46~~ et 352 de l'~~annexe~~**appendice** 1C).

CardVehicleUnitsUsed := SEQUENCE {

vehicleUnitPointerNewestRecord	INTEGER(0..NoOfCardVehicleUnitRecords-1),
cardVehicleUnitRecords	SET SIZE(NoOfCardVehicleUnitRecords) OF CardVehicleUnitRecord

}

vehicleUnitPointerNewestRecord est l'indice du plus récent enregistrement de données relatives à une unité embarquée.

Attribution de valeur : nombre correspondant au numérateur de l'enregistrement d'unité embarquée, commençant par une série de '0' pour la première occurrence d'un enregistrement d'unité embarquée dans la structure considérée.

cardVehicleUnitRecords désigne le jeu d'enregistrements contenant les informations relatives aux unités embarquées utilisées.

2.41 Certificate

Certificat d'une clé publique délivrée par une autorité de certification.

Génération 1 :

Certificate ::= OCTET STRING (SIZE(194))

Attribution de valeur : signature numérique avec récupération partielle du contenu d'un certificat conformément **au** ~~l'appendice~~ **sous-appendice** 11 (Mécanismes de sécurité communs : signature (128 octets) || reste de clé publique (58 octets) || références de l'autorité de certification (8 octets)).

Génération 2 :

Certificate ::= OCTET STRING (SIZE(204..341))

Attribution de valeur : voir **sous-**appendice 11.

2.42 CertificateContent

Génération 1 :

Le contenu (en clair) du certificat d'une clé publique conformément ~~à l'appendice~~ **au sous-appendice** 11 (Mécanismes de sécurité communs).

CertificateContent ::= SEQUENCE {

certificateProfileIdentifier	INTEGER(0..255),
certificationAuthorityReference	KeyIdentifier,
certificateHolderAuthorisation	CertificateHolderAuthorisation,
certificateEndOfValidity	TimeReal,
certificateHolderReference	KeyIdentifier,
publicKey	PublicKey

}

certificateProfileIdentifier indique la version du certificat correspondant.

Attribution de valeur : '01h' pour cette version.

certificationAuthorityReference identifie l'autorité de certification qui a délivré le certificat considéré. Ces données font également référence à la clé publique de cette autorité de certification.

certificateHolderAuthorisation indique les droits du détenteur du certificat.

certificateEndOfValidity indique la date d'expiration administrative du certificat.

certificateHolderReference identifie le détenteur du certificat. Ces données font également référence à sa clé publique.

publicKey indique la clé publique certifiée par ce certificat.

2.43 CertificateHolderAuthorisation

Identification des droits d'un détenteur de certificat.

CertificateHolderAuthorisation ::= SEQUENCE {

tachographApplicationID OCTET STRING(SIZE(6))

equipmentType EquipmentType

}

Génération 1 :

tachographApplicationID est l'identificateur de l'application tachygraphique (AID).

Attribution de valeur : 'FFh' '54h' '41h' '43h' '48h' '4Fh'. L'AID est un identificateur exclusif non homologué, conformément à la norme ISO/CEI 7816-5.

equipmentType indique le type d'équipement visé par le certificat.

Attribution de valeur : en conformité avec le type de données EquipmentType. **0** si le certificat émane de l'un**e** des ~~États membres~~ **Parties contractantes**.

Génération 2 :

tachographApplicationID indique les 6 octets les plus significatifs de l'identificateur d'application pour les cartes tachygraphiques de deuxième génération. La section 6.2 spécifie l'AID correspondant aux applications de carte tachygraphique.

Attribution de valeur : 'FF 53 4D 52 44 54'

equipmentType identifie le type d'équipement spécifié pour la génération 2 et visé par le certificat.

Attribution de valeur : en conformité avec le type de données EquipmentType.

2.44 CertificateRequestID

Code d'identification unique d'une demande de certificat. Il peut également servir d'identificateur de la clé publique d'une unité embarquée sur le véhicule lorsque le numéro de série de l'unité embarquée à laquelle la clé est destinée n'est pas connu au moment de l'établissement du certificat.

CertificateRequestID ::= SEQUENCE{

~~request SerialNumber~~**RrequestSerialNumber** INTEGER(0..2^{32}-1),

requestMonthYear BCDString(SIZE(2)),

crIdentifier OCTET STRING(SIZE(1)),

manufacturerCode ManufacturerCode

}

requestSerialNumber indique le numéro de série de la demande de certificat, propre au fabricant, ainsi que le mois ci-après.

requestMonthYear indique le mois et l'année de la demande de certificat.

Attribution de valeur : codage BCD du mois (deux chiffres) et de l'année (les deux derniers chiffres).

crIdentifier est un identificateur permettant de faire la distinction entre une demande de certificat et un numéro de série étendu.

Attribution de valeur : 'FFh'.

manufacturerCode est le code numérique d'identification du fabricant qui a émis la demande de certificat.

2.45 CertificationAuthorityKID

Identificateur de la clé publique d'une autorité de certification (~~une État membre~~ **Partie contractante** ou ~~l'~~autorité de certification ~~européen~~ **racine**).

CertificationAuthorityKID ::= SEQUENCE{

nationNumeric	NationNumeric,
nationAlpha	NationAlpha,
keySerialNumber	INTEGER(0..255),
additionalInfo	OCTET STRING(SIZE(2)),
caIdentifier	OCTET STRING(SIZE(1))

}

nationNumeric indique le code numérique national de l'autorité de certification.

nationAlpha indique le code alphanumérique national de l'autorité de certification.

keySerialNumber est un numéro de série permettant de faire la distinction entre les différentes clés de l'autorité de certification en cas de modification des clés.

additionalInfo est un champ de deux octets permettant l'introduction de codes supplémentaires (propres à l'autorité de certification).

caIdentifier est un identificateur permettant de faire la distinction entre l'identificateur d'une clé associée à une autorité de certification et d'autres identificateurs de clé.

Attribution de valeur : '01h'.

2.46 CompanyActivityData

Informations enregistrées sur une carte d'entreprise et se rapportant aux activités réalisées avec cette carte (exigence 373 et 379 de ~~l'annexe~~ **l'appendice** 1C).

CompanyActivityData ::= SEQUENCE {

companyPointerNewestRecord	INTEGER(0..NoOfCompanyActivityRecords-1),
companyActivityRecords	SET SIZE(NoOfCompanyActivityRecords) OF
companyActivityRecord	SEQUENCE {
companyActivityType	CompanyActivityType,
companyActivityTime	TimeReal,
cardNumberInformation	FullCardNumber,
vehicleRegistrationInformation	VehicleRegistrationIdentification,

downloadPeriodBegin TimeReal,

downloadPeriodEnd TimeReal

}

}

companyPointerNewestRecord est l'indice du plus récent enregistrement de type companyActivityRecord mis à jour.

Attribution de valeur : nombre correspondant au numérateur de l'enregistrement d'activité d'entreprise, commençant par une série de '0' pour la première occurrence d'un enregistrement d'activité d'entreprise dans la structure considérée.

companyActivityRecords désigne l'ensemble des enregistrements relatifs aux activités de l'entreprise.

companyActivityRecord est la séquence de données relatives à une activité de l'entreprise.

companyActivityType indique le type d'activité réalisée par l'entreprise.

companyActivityTime indique la date et l'heure de l'activité réalisée par l'entreprise.

cardNumberInformation indique, le cas échéant, le numéro de la carte téléchargée et ~~l'État membre~~ **la Partie contractante** qui l'a délivrée.

vehicleRegistrationInformation indique le VRN et ~~l'État membre~~ **la Partie contractante** d'immatriculation du véhicule concerné par le téléchargement, le verrouillage ou le déverrouillage.

downloadPeriodBegin et **downloadPeriodEnd** indiquent la période téléchargée à partir de l'UEV, le cas échéant.

2.47 CompanyActivityType

Code indiquant une activité réalisée par une entreprise à l'aide de sa carte d'entreprise.

CompanyActivityType ::= INTEGER {

card downloading (1),

VU downloading (2),

VU lock-in (3),

VU lock-out (4),

}

2.48 CompanyCardApplicationIdentification

Informations enregistrées sur une carte d'entreprise et se rapportant à l'identification de l'application de la carte (exigences 369 et 375 de ~~l'annexe~~ **l'appendice** 1C).

CompanyCardApplicationIdentification ::= SEQUENCE {

typeOfTachographCardId EquipmentType,

cardStructureVersion CardStructureVersion,

noOfCompanyActivityRecords NoOfCompanyActivityRecords

}

typeOfTachographCardId spécifie le type de la carte utilisée.

cardStructureVersion spécifie la version de la structure mise en œuvre au sein de la carte.

noOfCompanyActivityRecords indique le nombre d'enregistrements d'activité d'entreprise que la carte peut stocker.

2.48a CompanyCardApplicationIdentificationV2

Génération 2, version 2 :

Informations enregistrées sur une carte d'entreprise et se rapportant à l'identification de l'application de la carte (exigence 375a de l'appendice 1C).

CompanyCardApplicationIdentificationV2 ::= SEQUENCE {

lengthOfFollowingData	**LengthOfFollowingData,**
vuConfigurationLengthRange	**VuConfigurationLengthRange**

}

lengthOfFollowingData indique le nombre d'octets consécutifs dans l'enregistrement.

vuConfigurationLengthRange indique le nombre d'octets disponibles sur une carte tachygraphique pour le stockage des configurations de l'UEV.

2.49 CompanyCardHolderIdentification

Informations enregistrées sur une carte d'entreprise et se rapportant à l'identification du détenteur de la carte (exigence 372 et 378 de ~~l'annexe~~ **l'appendice** 1C).

CompanyCardHolderIdentification ::= SEQUENCE {

companyName	Name,
companyAddress	Address,
cardHolderPreferredLanguage	Language

}

companyName indique le nom de l'entreprise détentrice de la carte.

companyAddress indique l'adresse de l'entreprise détentrice de la carte.

cardHolderPreferredLanguage indique la langue de travail habituelle de l'entreprise.

2.50 ControlCardApplicationIdentification

Informations enregistrées sur une carte de contrôleur et se rapportant à l'identification de l'application de la carte (exigences 357 et 363 de ~~l'annexe~~ **l'appendice** 1C).

ControlCardApplicationIdentification ::= SEQUENCE {

typeOfTachographCardId	EquipmentType,
cardStructureVersion	CardStructureVersion,
noOfControlActivityRecords	NoOfControlActivityRecords

}

typeOfTachographCardId spécifie le type de la carte utilisée.

cardStructureVersion spécifie la version de la structure mise en œuvre au sein de la carte.

noOfControlActivityRecords indique le nombre d'enregistrements d'activité d'entreprise que la carte peut stocker.

2.50a ControlCardApplicationIdentificationV2

Génération 2, version 2 :

Informations enregistrées sur une carte de contrôleur et se rapportant à l'identification de l'application de la carte (exigence 363a de l'appendice 1C).

ControlCardApplicationIdentificationV2 ::= SEQUENCE {

lengthOfFollowingData **LengthOfFollowingData,**

vuConfigurationLengthRange **VuConfigurationLengthRange**

}

lengthOfFollowingData indique le nombre d'octets consécutifs dans l'enregistrement.

vuConfigurationLengthRange indique le nombre d'octets disponibles sur une carte tachygraphique pour le stockage des configurations de l'UEV.

2.51 ControlCardControlActivityData

Informations enregistrées sur une carte de contrôleur concernant les activités réalisées avec cette carte (exigences 361 et 367 de ~~l'annexe~~ **l'appendice** 1C).

ControlCardControlActivityData ::= SEQUENCE {

controlPointerNewestRecord	INTEGER(0.. NoOfControlActivityRecords-1),
controlActivityRecords	SET SIZE(NoOfControlActivityRecords) OF
controlActivityRecord	SEQUENCE {
controlType	ControlType,
controlTime	TimeReal,
controlledCardNumber	FullCardNumber,
controlledVehicleRegistration	VehicleRegistrationIdentification,
controlDownloadPeriodBegin	TimeReal,
controlDownloadPeriodEnd	TimeReal

}

}

controlPointerNewestRecord est l'indice du plus récent enregistrement relatif à une activité de contrôle mis à jour.

Attribution de valeur : nombre correspondant au numérateur de l'enregistrement d'activité de contrôle, commençant par une série de '0' pour la première occurrence de l'enregistrement dans la structure considérée.

controlActivityRecords désigne l'ensemble des enregistrements relatifs aux activités de contrôle.

controlActivityRecord est la séquence de données relatives à un contrôle.

controlType indique le type de contrôle.

controlTime indique la date et l'heure du contrôle.

controlledCardNumber indique le numéro de la carte contrôlée et ~~l'État membre~~ **la Partie contractante** qui l'a délivrée.

controlledVehicleRegistration indique le VRN et ~~l'État membre~~ **la Partie contractante** d'immatriculation du véhicule qui a fait l'objet d'un contrôle.

controlDownloadPeriodBegin et **controlDownloadPeriodEnd** indiquent, le cas échéant, la période téléchargée.

2.52 ControlCardHolderIdentification

Informations enregistrées sur une carte de contrôleur et se rapportant à l'identification du détenteur de la carte (exigences 360 et 366~~, annexe~~ **de l'appendice** 1C).

ControlCardHolderIdentification ::= SEQUENCE {

controlBodyName Name,

controlBodyAddress Address,

cardHolderName HolderName,

cardHolderPreferredLanguage Language

}

controlBodyName indique le nom de l'organisme de contrôle dont dépend le détenteur de la carte.

controlBodyAddress indique l'adresse de l'organisme de contrôle dont dépend le détenteur de la carte.

cardHolderName indique les nom et prénom(s) du détenteur de la carte de contrôleur.

cardHolderPreferredLanguage indique la langue habituelle du détenteur de la carte.

2.53 ControlType

Code indiquant les activités menées pendant un contrôle. Ce type de données est lié aux exigences 126, 274, 299, 327 et 350 de ~~l'annexe~~ **l'appendice** 1C.

ControlType ::= OCTET STRING (SIZE(1))

Génération 1 :

Attribution de valeur − Octet aligné : 'cvpdxxxx'B (8 bits)

'c'B téléchargement de la carte :

'0'B : pas de téléchargement de la carte pendant cette activité de contrôle ;

'1'B : téléchargement de la carte pendant cette activité de contrôle.

'v'B téléchargement de l'UEV :

'0'B : pas de téléchargement de l'UEV pendant cette activité de contrôle ;

'1'B : téléchargement de l'UEV pendant cette activité de contrôle.

'p'B impression :

'0'B : pas d'impression pendant cette activité de contrôle ;

'1'B : exécution d'une impression pendant cette activité de contrôle.

'd'B affichage :

'0'B : pas d'affichage de données pendant cette activité de contrôle ;

'1'B : affichage de données pendant cette activité de contrôle.

'xxxx'B inutilisé.

Génération 2 :

Attribution de valeur − Octet aligné : 'cvpdexxx'B (8 bits)

'c'B téléchargement de la carte :

'0'B : pas de téléchargement de la carte pendant cette activité de contrôle ;

'1'B : téléchargement de la carte pendant cette activité de contrôle.

'v'B téléchargement de l'UEV :

'0'B : pas de téléchargement de l'UEV pendant cette activité de contrôle ;

'1'B : téléchargement de l'UEV pendant cette activité de contrôle.

'p'B printing :

‘0’B : pas d’impression pendant cette activité de contrôle ;

‘1’B : exécution d’une impression pendant cette activité de contrôle.

‘d’B affichage :

‘0’B : pas d’affichage de données pendant cette activité de contrôle ;

‘1’B : affichage de données pendant cette activité de contrôle.

‘e’B contrôle routier d’étalonnage :

‘0’B : pas de vérification des paramètres d’étalonnage pendant cette activité de contrôle ;

‘1’B : vérification des paramètres d’étalonnage pendant cette activité de contrôle.

‘xxx’B ~~RFU~~**réservé pour une utilisation future**.

2.54 CurrentDateTime

Date et heure actuelles de l’appareil de contrôle.

CurrentDateTime ::= Temps réel

Attribution de valeur : absence d’informations complémentaires.

2.55 CurrentDateTimeRecordArray

Génération 2 :

La date et l’heure actuelles plus les métadonnées servant au protocole de téléchargement.

CurrentDateTimeRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF CurrentDateTime

}

recordType indique le type d’enregistrement (CurrentDateTime). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type CurrentDateTime exprimée en octets.

noOfRecords indique le nombre d’enregistrements dans le jeu d’enregistrements correspondant.

records désigne un jeu d’enregistrements de date et d’heure.

2.56 DailyPresenceCounter

Compteur enregistré sur une carte de conducteur ou d’atelier et incrémenté d’une unité par jour civil d’insertion de la carte dans le lecteur d’une UEV. Ce type de données est lié aux exigences 266, 299, 320 et 343 de ~~l’annexe~~ **l’appendice** 1C.

DailyPresenceCounter ::= BCDString(SIZE(2))

Attribution de valeur : numérotation consécutive dont la valeur maximale est égale à 9 999 et qui recommence par le numéro 0. Lors de la première entrée en vigueur d’une carte, le compteur est à zéro.

2.57 Datef

Date exprimée dans un format numérique immédiatement imprimable.

Datef ::= SEQUENCE {

year	BCDString(SIZE(2)),
month	BCDString(SIZE(1)),
day	BCDString(SIZE(1))

}

Attribution de valeur :

yyyy	année
mm	mois
dd	jour

‘00000000’H indique explicitement l’absence de date.

2.58 DateOfDayDownloaded

Génération 2 :

La date et l’heure du téléchargement.

DateOfDayDownloaded ::= TimeReal

Attribution de valeur : absence d’informations complémentaires.

2.59 DateOfDayDownloadedRecordArray

Génération 2 :

L’heure et la date du téléchargement plus les métadonnées servant au protocole de téléchargement.

DateofDayDownloadedRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF DateOfDayDownloaded

}

recordType indique le type d’enregistrement (DateOfDayDownloaded). **Attribution de valeur** : voir RecordType.

recordSize indique la taille des enregistrements de type CurrentDateTime exprimée en octets.

noOfRecords indique le nombre d’enregistrements dans le jeu d’enregistrements correspondant.

records désigne le jeu de dates et d’heures associées aux enregistrements relatifs aux téléchargements.

2.60 Distance

Distance parcourue (résultat du calcul de la différence entre deux valeurs affichées par le compteur kilométrique du véhicule considéré).

Distance ::= INTEGER(0..2^{16}-1)

Attribution de valeur : binaire sans signe. Valeur exprimée en km et se situant dans une plage de fonctionnement comprise entre 0 et 9 999 km.

2.60a DownloadInterfaceVersion

Génération 2, version 2 :

Code indiquant la version de l'interface de téléchargement d'une unité embarquée.

DownloadInterfaceVersion ::= OCTET STRING (SIZE(2))

Attribution de valeur : 'aabb'H :

'aa'H '00'H inutilisé ;

'01'H unité embarquée de génération 2 ;

'bb'H '00'H inutilisé ;

'01'H unité embarquée de génération 2, version 2.

2.61 DriverCardApplicationIdentification

Informations enregistrées sur une carte de conducteur et se rapportant à l'identification de l'application de la carte (exigences 253 et 278 de ~~l'annexe~~ **l'appendice** 1C).

Génération 1 :

DriverCardApplicationIdentification ::= SEQUENCE {

typeOfTachographCardId	EquipmentType,
cardStructureVersion	CardStructureVersion,
noOfEventsPerType	NoOfEventsPerType,
noOfFaultsPerType	NoOfFaultsPerType,
activityStructureLength	CardActivityLengthRange,
noOfCardVehicleRecords	NoOfCardVehicleRecords,
noOfCardPlaceRecords	NoOfCardPlaceRecords

}

typeOfTachographCardId spécifie le type de la carte utilisée.

cardStructureVersion spécifie la version de la structure mise en œuvre au sein de la carte.

noOfEventsPerType indique le nombre d'événements que la carte est en mesure d'enregistrer par type d'événement.

noOfFaultsPerType indique le nombre d'anomalies que la carte est en mesure d'enregistrer par type d'anomalie.

activityStructureLength indique le nombre d'octets disponibles pour le stockage d'enregistrements d'activité.

noOfCardVehicleRecords indique le nombre d'enregistrements de véhicule que la carte est en mesure de stocker.

noOfCardPlaceRecords indique le nombre de lieux que la carte est en mesure de stocker.

Génération 2 :

DriverCardApplicationIdentification ::= SEQUENCE {

typeOfTachographCardId	EquipmentType,

cardStructureVersion	CardStructureVersion,
noOfEventsPerType	NoOfEventsPerType,
noOfFaultsPerType	NoOfFaultsPerType,
activityStructureLength	CardActivityLengthRange,
noOfCardVehicleRecords	NoOfCardVehicleRecords,
noOfCardPlaceRecords	NoOfCardPlaceRecords,
~~noOfGNSSCDRecords~~	~~NoOfGNSSCDRecords,~~
noOfGNSSADRecords	**NoOfGNSSADRecords**,
noOfSpecificConditionRecords	NoOfSpecificConditionRecords
noOfCardVehicleUnitRecords	**NoOfCardVehicleUnitRecords**

}

Outre les éléments de données de la structure de génération 1, les éléments de données suivants sont utilisés :

~~noOfGNSSCDRecords~~ **noOfGNSSADRecords** indique le nombre d'enregistrements de temps de conduite ~~continue~~ **accumulé** fourni par le récepteur GNSS que la carte est en mesure de stocker.

noOfSpecificConditionRecords indique le nombre d'enregistrements de conditions particulières que la carte est en mesure de stocker.

noOfCardVehicleUnitRecords indique le nombre d'enregistrements d'unités embarquées utilisées que la carte est en mesure de stocker.

2.61a DriverCardApplicationIdentificationV2

Informations enregistrées sur une carte de conducteur et se rapportant à l'identification de l'application de la carte (exigence 278a de l'appendice 1C).

DriverCardApplicationIdentificationV2 ::= SEQUENCE {

lengthOfFollowingData	**LengthOfFollowingData,**
noOfBorderCrossingRecords	**NoOfBorderCrossingRecords,**
noOfLoadUnloadRecords	**NoOfLoadUnloadRecords,**
noOfLoadTypeEntryRecords	**NoOfLoadTypeEntryRecords,**
vuConfigurationLengthRange	**VuConfigurationLengthRange**

}

lengthOfFollowingData indique le nombre d'octets consécutifs dans l'enregistrement.

noOfBorderCrossingRecords indique le nombre d'enregistrements de passage de frontières que la carte de conducteur est en mesure de stocker.

noOfLoadUnloadRecords indique le nombre d'enregistrements d'opération de chargement/déchargement que la carte de conducteur est en mesure de stocker.

noOfLoadTypeEntryRecords indique le nombre d'enregistrements de type de chargement que la carte de conducteur est en mesure de stocker.

vuConfigurationLengthRange indique le nombre d'octets disponibles sur une carte tachygraphique pour le stockage des configurations de l'UEV.

2.62 DriverCardHolderIdentification

Informations enregistrées sur une carte de conducteur et se rapportant à l'identification du détenteur de la carte (exigences 256 et 281 de ~~l'annexe~~ **l'appendice** 1C).

DriverCardHolderIdentification ::= SEQUENCE {

cardHolderName	HolderName,
cardHolderBirthDate	Datef,
cardHolderPreferredLanguage	Language

}

cardHolderName indique les nom et prénom(s) du détenteur de la carte de conducteur.

cardHolderBirthDate indique la date de naissance du détenteur de la carte de conducteur.

cardHolderPreferredLanguage indique la langue habituelle du détenteur de la carte.

2.63 DSRCSecurityData

Génération 2 :

Pour la définition de ce type de données, se référer au sous-appendice 11.

~~Les informations de texte en clair et le MAC à transmettre via DSRC depuis le tachygraphe vers l'Interrogateur distant (IDis), cf. appendice 11, partie b, chapitre 13~~**63 Réservé** ~~pour des détails complémentaires.~~ **pour une utilisation future**

~~DSRCSecurityData ::= SEQUENCE {~~

~~tagLenthPlainText OCTET STRING(SIZE(2)),~~

~~currentDateTime CurrentDateTime,~~

~~INTEGER (0..224-1),~~

~~vuSerialNumber VuSerialNumber,~~

~~dSRCMKVersionNumber INTEGER(SIZE(1)),~~

~~tagLengthMac OCTET STRING(SIZE(2)),~~

~~mac MAC~~

~~**tagLength** fait partie du codage DER-TLV et doit être défini sur '81 10' (cf. appendice 11, partie B, chapitre 13).~~

~~**currentDateTime** indique la date et l'heure actuelles de l'unité embarquée sur le véhicule.~~

~~**counter** énumère les messages RTM.~~

~~**vuSerialNumber** indique le numéro de série de l'unité embarquée sur le véhicule.~~

~~**dSRCMKVersionNumber** désigne le numéro de version de la clé maîtresse DSRC d'où découlent les clés DSRC propres aux VU.~~

~~**tagLengthMac** désigne la balise et la longueur de l'objet informatif MAC dans le cadre du codage DER-TLV. La balise doit être définie à '8E', la longueur doit coder la longueur du MAC en octets (cf. appendice 11, partie B, chapitre 13).~~

~~**mac** désigne le MAC calculé sur le message RTM (cf. appendice 11, partie B, chapitre 13).~~

2.64 EGFCertificate

Génération 2 :

Certificat associé à la clé publique d'un dispositif GNSS externe destiné à l'authentification mutuelle avec une UEV. La structure de ce certificat est spécifiée dans ~~l'appendice~~ **le sous-appendice** 11.

EGFCertificate ::= Certificate

2.65 EmbedderIcAssemblerId

Informations relatives à l'intégrateur du circuit intégré.

EmbedderIcAssemblerId ::= SEQUENCE{

countryCode	IA5String(SIZE(2)),
moduleEmbedder	BCDString(SIZE(2)),
manufacturerInformation	OCTET STRING(SIZE(1))

}

countryCode est le code à deux lettres du pays où se trouve l'intégrateur du module conformément à la norme ISO 3166.

moduleEmbedder identifie l'intégrateur du module.

manufacturerInformation concerne l'usage interne par le fabricant.

2.66 EntryTypeDailyWorkPeriod

Code permettant de faire la distinction entre les lieux de début et de fin d'une période de travail journalière et les conditions de saisie de ces données.

Génération 1 :

EntryTypeDailyWorkPeriod ::= INTEGER {

Début, temps relatif = heure d'insertion de la carte ou de saisie	(0),
Fin, temps relatif = heure de retrait de la carte ou de saisie	(1),
Début, saisie manuelle du temps relatif (heure de début)	(2),
Fin, saisie manuelle du temps relatif (fin de la période de travail)	(3),
Début, temps relatif adopté par l'UEV	(4),
Fin, temps relatif adopté par l'UEV	(5)

}

Attribution de valeur : conformément à la norme ISO/CEI8824-1.

Génération 2 :

EntryTypeDailyWorkPeriod ::= INTEGER {

Début, temps relatif = heure d'insertion de la carte ou de saisie	(0),
Fin, temps relatif = heure de retrait de la carte ou de saisie	(1),
Début, saisie manuelle du temps relatif (heure de début)	(2),
Fin, saisie manuelle du temps relatif (fin de la période de travail)	(3),
~~Début, temps relatif adopté par l'UEV~~	~~(4),~~
~~Fin, temps relatif adopté par l'UEV~~	~~(5)~~
~~début, temps relatif fondé sur les données GNSS~~	~~(6)~~
~~Fin, temps relatif fondé sur les données GNSS~~	~~(7)~~

}

Attribution de valeur : conformément à la norme ISO/CEI 8824-1.

2.67 EquipmentType

Code permettant à l'application tachygraphique de faire la distinction entre différents types d'équipement.

EquipmentType ::= INTEGER(0..255)

Génération 1 :

--réservé	(0)
--carte de conducteur	(1)
--carte d'atelier	(2)
--carte de contrôleur	(3)
--carte d'entreprise	(4)
--carte de fabricant	(5)
--unité embarquée sur le véhicule	(6)
--capteur de mouvement	(7)
--réservé pour une utilisation future	(8..255)

Attribution de valeur : conformément à la norme ISO/CEI 8824-1.

La valeur 0 est réservée à la désignation ~~d'un État membre ou de l'Europe~~ **d'une Partie contractante ou d'une autorité de certification racine** dans le champ ADCdes certificats.

Génération 2 :

Les mêmes valeurs que pour la génération 1 sont utilisées avec les ajouts suivants :

--dispositif GNSS	(8)
--module de communication à distance	(9)
--module d'interface STI	(10)
--plaque SealRecord	(11) -- peut être utilisé dans SealRecord
--adaptateur M1/N1 SealRecord	(12) -- peut être utilisé dans SealRecord
--autorité de certification racine ~~européenne~~ (ERCA)	(13)
--~~État membre~~ autorité de certification de la Partie contractante (MSCA)	(14)
--connexion GNSS externe	(15) -- peut être utilisé dans SealRecord
--inutilisé	(16) -- utilisé dans SealDataVu
--carte de conducteur (sSign)	**(17) -- à utiliser uniquement dans le champ ADC d'un certificat de signature**
--carte d'atelier (sSign)	**(18) -- à utiliser uniquement dans le champ ADC d'un certificat de signature**
--unité embarquée sur le véhicule (sSign)	**(19) -- à utiliser uniquement dans le champ ADC d'un certificat de signature**

--réservé pour une utilisation future **(20..**255**)**

Remarque **1** : les valeurs associées à la plaque, à l'adaptateur et à la connexion GNSS dans la structure de génération 1 ainsi que les valeurs associées à l'unité embarquée et au capteur de mouvement dans la structure de génération 2 peuvent être utilisées dans SealRecord, le cas échéant.

Remarque 2 : dans le champ ADC (autorisation du détenteur de certificat) d'un certificat de deuxième génération, les valeurs (1), (2) et (6) doivent être interprétées comme désignant le certificat d'authentification mutuelle correspondant à chaque type d'équipement. Pour désigner le certificat de création d'une signature numérique correspondant à chacun de ces types d'équipement, les valeurs (17), (18) ou (19) doivent être utilisées.

2.68 EuropeanPublicKey

Génération 1 :

Clé publique ~~européenne~~ **racine**.

EuropeanPublicKey ::= PublicKey

2.69 EventFaultRecordPurpose

Code expliquant la raison pour laquelle un événement ou une anomalie a été enregistré(e).

EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))

Attribution de valeur :

'00'H	l'un des 10 (derniers) événements ou anomalies les plus récents
'01'H	l'événement le plus long enregistré pour l'un des 10 derniers jours d'occurrence
'02'H	l'un des 5 événements les plus longs survenus au cours des 365 derniers jours,
'03'H	le dernier événement enregistré pour l'un des 10 derniers jours d'occurrence
'04'H	l'événement le plus grave enregistré pour l'un des 10 derniers jours d'occurrence
'05'H	l'un des 5 événements les plus graves survenus au cours des 365 derniers jours
'06'H	le premier événement ou la première anomalie survenu(e) après le dernier étalonnage
'07'H	un événement ou une anomalie en cours
'08'H à '7F'H	réservé pour une utilisation future
'80'H à 'FF'H	propre au fabricant

2.70 EventFaultType

Code caractérisant un événement ou une anomalie.

EventFaultType ::= OCTET STRING (SIZE(1))

Attribution de valeur :

Génération 1 :

'0x'H	événements généraux

‘00’H	absence d’informations complémentaires
‘01’H	insertion d’une carte non valable
‘02’H	conflit de carte
‘03’H	chevauchement temporel
‘04’H	conduite sans carte appropriée
‘05’H	insertion de carte en cours de conduite
‘06’H	clôture incorrecte de la dernière session
‘07’H	excès de vitesse
‘08’H	interruption de l’alimentation électrique
‘09’H	erreur sur les données de mouvement
‘0A’H	conflit concernant le mouvement du véhicule
‘0B’ à ‘0F’H	réservé pour une utilisation future
‘1x’H	tentatives d’atteinte à la sécurité en rapport avec l’UEV
‘10’H	absence d’informations complémentaires
‘11’H	défaut d’authentification du capteur de mouvement
‘12’H	défaut d’authentification d’une carte tachygraphique
‘13’H	remplacement sans autorisation du capteur de mouvement
‘14’H	défaut d’intégrité affectant la saisie de données sur la carte
‘15’H	défaut d’intégrité affectant les données d’utilisateur en mémoire
‘16’H	erreur dans le transfert interne de données
‘17’H	ouverture non autorisée d’un boîtier
‘18’H	sabotage du matériel
‘19’H à ‘1F’H	réservé pour une utilisation future
‘2x’H	tentatives d’atteinte à la sécurité en rapport avec le capteur
‘20’H	absence d’informations complémentaires
‘21’H	échec d’authentification
‘22’H	défaut d’intégrité affectant les données en mémoire
‘23’H	erreur dans le transfert interne de données
‘24’H	ouverture non autorisée d’un boîtier
‘25’H	sabotage du matériel
‘26’H à ‘2F’H	réservé pour une utilisation future
‘3x’H	anomalies de l’appareil de contrôle
‘30’H	absence d’informations complémentaires
‘31’H	anomalie interne de l’UEV
‘32’H	anomalie de l’imprimante
‘33’H	anomalie de l’affichage
‘34’H	anomalie de téléchargement

‘35’H	anomalie du capteur
‘36’H à ‘3F’H	réservé pour une utilisation future
‘4x’H	anomalies de la carte
‘40’H	absence d’informations complémentaires
‘41’H à ‘4F’H	réservé pour une utilisation future
‘50’H à ‘7F’H	réservé pour une utilisation future
‘80’H à ‘FF’H	propre au fabricant

Génération 2**, version 1 :**

~~Les mêmes valeurs que pour la génération 1 servent pour les ajouts suivants :~~

‘**0x’H**	**événements généraux**
‘00’H	**absence d’informations complémentaires**
‘01’H	**insertion d’une carte non valable**
‘02’H	**conflit de carte**
‘03’H	**chevauchement temporel**
‘04’H	**conduite sans carte appropriée**
‘05’H	**insertion d’une carte en cours de conduite**
‘06’H	**clôture incorrecte de la dernière session**
‘07’H	**excès de vitesse**
‘08’H	**interruption de l’alimentation électrique**
‘09’H	**erreur sur les données de mouvement**
‘0A’H	**conflit concernant le mouvement du véhicule**
‘0B’H	conflit temporel (GNSS contre horloge interne de l’UEV)
~~0C à~~ ‘0C’H	**erreur de communication avec le dispositif de communication à distance**
‘0D’H	**absence d’informations de positionnement en provenance du récepteur GNSS**
‘**0E’H**	**erreur de communication avec le dispositif GNSS externe**
‘0F’H	réservé pour une utilisation future
~~‘5x’H GNSS~~ **‘1x’H**	**tentatives d’atteinte à la sécurité liées à l’UEV**
~~50H~~**’10’H**	**absence d’informations complémentaires**
~~‘51’ H~~**’11’H**	**échec d’authentification du capteur de mouvement**
‘12’H	**échec d’authentification d’une carte tachygraphique**
‘13’H	**remplacement sans autorisation du capteur de mouvement**
‘14’H	**défaut d’intégrité affectant la saisie de données sur la carte**
‘15’H	**défaut d’intégrité affectant les données d’utilisateur en mémoire**
‘16’H	~~anomalie du récepteur du dispositif GNSS~~ **erreur dans le transfert** interne **de données**
~~52’H~~	~~anomalie du récepteur du dispositif GNSS externe~~

~~‘53’H~~	~~anomalie de communication du dispositif GNSS externe~~
~~‘54’H~~	~~aucune donnée de positionnement en provenance du dispositif GNSS~~
~~‘55’H~~‘**17’H**	**ouverture non autorisée d’un boîtier**
‘**18’H**	**sabotage du matériel**
‘19’H	détection de manipulation du dispositif GNSS
~~‘56’H ‘~~**1A’H**	**échec d’authentification du dispositif GNSS externe**
‘1B’H	expiration du certificat du dispositif GNSS externe
~~**‘57’H 1C ‘H**~~ à ~~‘5F ‘H~~**1F’H**	réservé pour une utilisation future
~~**‘6x’H**~~ **‘2x’H**	**tentatives d’atteinte à la sécurité liées au capteur**
‘20’H	**absence d’informations complémentaires**
‘21’H	**échec d’authentification**
‘22’H	**défaut d’intégrité affectant les données en mémoire**
‘23’H	**erreur dans le transfert interne de données**
‘24’H	**ouverture non autorisée d’un boîtier**
‘25’H	**sabotage du matériel**
‘26’H à ‘2F’H	**réservé pour une utilisation future**
‘3x’H	**anomalies de l’appareil de contrôle**
‘30’H	**absence d’informations complémentaires**
‘31’H	**anomalie interne de l’UEV**
‘32’H	**anomalie de l’imprimante**
‘33’H	**anomalie de l’affichage**
‘34’H	**anomalie de téléchargement**
‘35’H	**anomalie du capteur**
‘36’H	**récepteur GNSS interne**
‘37’H	**dispositif GNSS externe**
‘38’H	~~anomalie en rapport avec le module~~ **dispositif** de communication à distance
~~‘60’ H~~	~~absence d’informations complémentaires~~
~~‘61’ H~~	~~anomalie du module de communication à distance~~
~~‘62’ H~~	~~anomalie de communication du module de~~ **dispositif de** communication
~~‘63’ H à ‘6F’ H~~	~~réservé pour une utilisation future~~
~~‘7x’ H~~ **‘39’ H**	~~anomalies de l’~~interface STI
~~‘70’ H~~ **3A’H à ‘3F’H**	**réservé pour une utilisation future**
‘4x’H	**anomalies de la carte**
‘40’H	absence d’informations complémentaires
~~‘71’H~~ **‘41F’H à ‘4F’ H**	**réservé pour une utilisation future**
‘50’H à ‘7F’H	réservé pour une utilisation future
‘80’H à ‘FF’H	**propre au fabricant**

Génération 2, version 2 :

‘0x’H	**événements généraux**
‘00’H	**absence d’informations complémentaires**
‘01’H	**insertion d’une carte non valable**
‘02’H	**conflit de carte**
‘03’H	**chevauchement temporel**
‘04’H	**conduite sans carte appropriée**
‘05’H	**insertion d’une carte en cours de conduite**
‘06’H	**clôture incorrecte de la dernière session**
‘07’H	**excès de vitesse**
‘08’H	**interruption de l’alimentation électrique**
‘09’H	**erreur sur les données de mouvement**
‘0A’H	**conflit concernant le mouvement du véhicule**
‘0B’H	**conflit temporel (GNSS contre horloge interne de l’UEV)**
‘0C’H	**erreur de communication avec le dispositif de communication à distance**
‘0D’H	**absence d’informations de positionnement en provenance du récepteur GNSS**
‘0E’H	**erreur de communication avec le dispositif GNSS externe**
‘0F’H	**anomalie du récepteur GNSS**
‘1x’H	**tentatives d’atteinte à la sécurité liées à l’UEV**
‘10’H	**absence d’informations complémentaires**
‘11’H	**défaut d’authentification du capteur de mouvement**
‘12’H	**défaut d’authentification d’une carte tachygraphique**
‘13’H	**remplacement sans autorisation du capteur de mouvement**
‘14’H	**défaut d’intégrité affectant la saisie de données sur la carte**
‘15’H	**défaut d’intégrité affectant les données d’utilisateur en mémoire**
‘16’H	**erreur dans le transfert interne de données**
‘17’H	**ouverture non autorisée d’un boîtier**
‘18’H	**sabotage du matériel**
‘19’H	**détection de manipulation du dispositif GNSS**
‘1A’H	**échec d’authentification du dispositif GNSS externe**
‘1B’H	**expiration du certificat du dispositif GNSS externe**
‘1C’H	**incohérence entre les données de mouvement et les données d’activité du conducteur**
‘1D’H à ‘1F’H	**réservé pour une utilisation future**

‘2x’H	**tentatives d’atteinte à la sécurité liées au capteur**
‘20’H	**absence d’informations complémentaires**
‘21’H	**échec d’authentification**
‘22’H	**défaut d’intégrité affectant les données en mémoire**
‘23’H	**erreur dans le transfert interne de données**
‘24’H	**ouverture non autorisée d’un boîtier**
‘25’H	**sabotage du matériel**
‘26’H à ‘2F’H	**réservé pour une utilisation future**
‘3x’H	**anomalies de l’appareil de contrôle**
‘30’H	**absence d’informations complémentaires**
‘31’H	**anomalie interne de l’UEV**
‘32’H	**anomalie de l’imprimante**
‘33’H	**anomalie de l’affichage**
‘34’H	**anomalie de téléchargement**
‘35’H	**anomalie du capteur**
‘36’H	**récepteur GNSS interne**
‘37’H	**dispositif GNSS externe**
‘38’H	**dispositif de communication à distance**
‘39’H	**interface STI**
‘3A’H	**anomalie interne du capteur**
à ‘3B’H à ‘3F’H	**réservé pour un usage interne**
‘4x’H	**anomalies de la carte**
‘40’H	**absence d’informations complémentaires**
‘41’H à ‘4F’H	**réservé pour une utilisation future**
‘50’H à ‘7F’H	**réservé pour une utilisation future**
‘80’H à ‘FF’H	**propre au fabricant**

2.71 ExtendedSealIdentifier

Génération 2 :

Identificateur de scellement étendu permettant l’identification unique d’un scellement (exigence 401 de ~~l’annexe~~ **l’appendice** 1C).

ExtendedSealIdentifier ::= SEQUENCE{

manufacturerCode **IA5String**~~OCTET STRING~~ (SIZE(2)),

manufacturerCode **IA5String**~~OCTET STRING~~ (SIZE(2))

}

manufacturerCode est le code correspondant au fabricant du scellement. **Attribution de valeur : voir la base de données gérée par les laboratoires compétents pour les essais d’interopérabilité (https://dtc.jrc.ec.europa.eu).**

sealIdentifier est l’identificateur du scellement, unique pour le fabricant. **Attribution de valeur : code alphanumérique, unique dans le domaine du fabricant conformément à la norme ISO 8859-1.**

2.72 ExtendedSerialNumber

Code d'identification unique d'un équipement. Il peut également servir d'identificateur de la clé publique d'un équipement.

Génération 1 :

ExtendedSerialNumber ::= SEQUENCE{

serialNumber	INTEGER(0..2^{32}-1),
monthYear	BCDString(SIZE(2)),
type	OCTET STRING(SIZE(1)),
manufacturerCode	ManufacturerCode

}

serialNumber indique le numéro de série de l'équipement, unique pour le fabricant, ainsi que le type d'équipement, le mois et l'année ci-après.

monthYear indique le mois et l'année de fabrication (ou de l'attribution d'un numéro de série).

Attribution de valeur : codage BCD du mois (deux chiffres) et de l'année (les deux derniers chiffres).

type est un identificateur du type d'équipement utilisé.

Attribution de valeur : propre au fabricant, la valeur 'FFh' étant réservée.

manufacturerCode est le code numérique d'identification d'un fabricant d'équipement homologué.

Génération 2 :

ExtendedSerialNumber ::= SEQUENCE{

serialNumber	INTEGER(0..2^{32}-1),
monthYear	BCDString(SIZE(2)),
type	EquipmentType,
manufacturerCode	ManufacturerCode

}

serialNumber voir génération 1.

monthYear voir génération 1.

type indique le type d'équipement.

monthYear voir génération 1.

2.73 FullCardNumber

Code permettant d'identifier avec certitude une carte tachygraphique.

FullCardNumber ::= SEQUENCE {

cardType	EquipmentType,
cardIssuingMemberState	NationNumeric,
cardNumber	CardNumber

}

cardType indique le type de la carte tachygraphique.

cardIssuingMemberState indique le code de ~~l'État membre~~ **la Partie contractante** qui a délivré la carte considérée.

cardNumber indique le numéro de la carte.

2.74 FullCardNumberAndGeneration

Génération 2 :

Code permettant d'identifier avec certitude une carte tachygraphique et sa génération.

FullCardNumberAndGeneration ::= SEQUENCE {

fullCardNumber	FullCardNumber,
generation	Generation

}

fullCardNumber indique le numéro d'identification de la carte tachygraphique.

generation indique la génération de la carte tachygraphique utilisée.

2.75 Generation

Génération 2 :

Indication de la génération du tachygraphe utilisé.

Generation ::= INTEGER(0..255)

Attribution de valeur :

'00'H	réservé pour une utilisation future
'01'H	Génération 1
'02'H	Génération 2
'03'H .. 'FF'H	réservé pour une utilisation future

2.76 GeoCoordinates

Génération 2 :

Les coordonnées géographiques sont codées sous forme de valeurs entières. Ces valeurs entières sont des multiples du codage ±DDMM.M pour la latitude et du codage ±DDDMM.M pour la longitude. Les codages ±DD et ±DDD indiquent les degrés respectifs et MM.M, les minutes. **La longitude et la latitude d'une position inconnue sont représentées par Hex '7FFFFF' (décimal 8388607).**

GeoCoordinates ::= SEQUENCE {

Latitude	INTEGER(-90000..90001),
longitude	INTEGER(-180000..180001)

}

La **latitude** est codée comme un multiple (facteur 10) de la représentation ±DDMM.M.

La **longitude** est codée comme un multiple (facteur 10) de la représentation ±DDDMM.M.

2.77 GNSSAccuracy

Génération 2 :

Précision des données de position fournies par le récepteur GNSS (définition eee)). La précision est codée sous forme de valeur entière et est un multiple (facteur 10) de la valeur X.Y donnée par la phrase GSA NMEA.

GNSSAccuracy ::= INTEGER(1..100)

~~2.78 GNSSContinuousDriving~~

2.78 GNSSAccumulatedDriving

Génération 2 :

Informations enregistrées sur une carte de conducteur ou d'atelier concernant la position GNSS du véhicule lorsque le temps de conduite accumulé ~~du conducteur~~ atteint un multiple de trois heures (exigences 306 et 354 de ~~l'Annex~~ **l'appendice** 1C).

~~GNSSContinuousDriving~~ **GNSSAccumulatedDriving** := SEQUENCE {

~~gnssCDPointerNewestRecord~~ **gnssADPointerNewestRecord** INTEGER(0..~~NoOfGNSSADRecords~~ **NoOfGNSSADRecords** -1),

~~gnssContinousDrivingRecords~~ **gnssAccumulatedDrivingRecords** SET SIZE(~~NoOfGNSSCDRecords~~ **NoOfGNSSADRecords**) OF ~~GNSScontinousDrivingRecord~~ **GNSSAccumulatedDrivingRecord**

}

~~gnssCDPointerNewestRecord~~**gnssADPointerNewestrecord** est l'indice du plus récent enregistrement du temps de conduite accumulé fourni par le récepteur GNSS ayant été mis à jour.

Attribution de valeur : nombre correspondant au numérateur de l'enregistrement de temps de conduite ~~continue~~ **accumulé** en provenance du récepteur GNSS, commençant par une série de '0' pour la première occurrence d'un enregistrement de temps de conduite dans la structure considérée.

~~gnssContinuousDrivingRecords~~ **gnssAccumulatedDrivingRecords** désigne le jeu d'enregistrements contenant la date et l'heure auxquelles le temps de conduite ~~continue~~ **accumulé** atteint un multiple de trois heures, ainsi que les données relatives à la position du véhicule.

2.79 ~~GNSSContinuousDrivingRecord~~ GNSSAccumulatedDrivingRecord

Génération 2 :

Informations enregistrées sur une carte de conducteur ou d'atelier concernant la position GNSS du véhicule lorsque le temps de conduite ~~continue~~ **accumulé** ~~du conducteur~~ atteint un multiple de trois heures (exigences 305 et 353 de ~~l'Annexe~~ **l'appendice** 1C).

~~GNSSContinousDrivingRecord~~**GNSSAccumulatedDrivingRecord** ::= SEQUENCE {

timeStamp TimeReal,

gnssPlaceRecord GNSSPlaceRecord,

vehicleOdometerValue **OdometerShort**

}

timeStamp indique la date et l'heure auxquelles le temps de conduite ~~continue~~ **accumulé** ~~du détenteur de la carte~~ atteint un multiple de trois heures.

gnssPlaceRecord contient les informations relatives à la position du véhicule.

vehicleOdometerValue indique la valeur affichée par le compteur kilométrique au moment où le temps de conduite accumulé atteint un multiple de trois heures.

2.79a GNSSAuthAccumulatedDriving

Génération 2, version 2 :

Informations enregistrées sur une carte de conducteur ou d'atelier et indiquant l'état d'authentification des positions GNSS du véhicule lorsque le temps de conduite accumulé atteint un multiple de trois heures (exigences 306d et 356d de l'appendice 1C).

GNSSAuthAccumulatedDriving ::= SEQUENCE {

gnssAuthADPointerNewestRecord INTEGER(0..NoOfGNSSADRecords -1),

gnssAuthStatusADRecords SET SIZE (NoOfGNSSADRecords)OF GNSSAuthStatusADRecord

}

gnssAuthADPointerNewestRecord est l'indice du plus récent enregistrement d'état d'authentification des positions GNSS.

Attribution de valeur : nombre correspondant au numérateur de l'enregistrement d'état d'authentification des positions GNSS, commençant par une série de '0' pour la première occurrence d'un enregistrement de ce type dans la structure considérée.

gnssAuthStatusADRecords désigne le jeu d'enregistrements contenant la date et l'heure auxquelles le temps de conduite accumulé atteint un multiple de trois heures, ainsi que l'état d'authentification de la position GNSS.

2.79b GNSSAuthStatusADRecord

Génération 2, version 2 :

Informations enregistrées sur une carte de conducteur ou d'atelier et indiquant l'état d'authentification d'une position GNSS donnée lorsque le temps de conduite accumulé atteint un multiple de trois heures (exigences 306c et 356c de l'appendice 1C). D'autres informations relatives à la position GNSS elle-même sont stockées dans un autre enregistrement (voir 2.79 GNSSAccumulatedDrivingRecord).

GNSSAuthStatusADRecord ::= SEQUENCE {

timeStamp	**TimeReal,**
authenticationStatus	**PositionAuthenticationStatus**

}

timeStamp indique la date et l'heure auxquelles le temps de conduite accumulé atteint un multiple de trois heures (celles-ci sont identiques à la date et à l'heure associées à l'enregistrement GNSSAccumulatedDrivingRecord correspondant).

authenticationStatus indique l'état d'authentification de la position GNSS lorsque le temps de conduite accumulé atteint un multiple de trois heures.

2.79c GNSSPlaceAuthRecord

Génération 2, version 2 :

Informations relatives à la position du véhicule fournie par le récepteur GNSS (exigences 108, 109, 110, 296, 306a, 306c, 306e, 306g, 356a, 356c, 356e et 356g de l'appendice 1C).

GNSSPlaceAuthRecord ::= SEQUENCE {

timeStamp	**TimeReal,**
gnssAccuracy	**GNSSAccuracy,**
geoCoordinates	**GeoCoordinates,**

authenticationStatus **PositionAuthenticationStatus**

}

timeStamp indique la date et l'heure auxquelles la position GNSS du véhicule a été déterminée.

gnssAccuracy indique le degré de précision des données de positionnement GNSS.

geoCoordinates indique l'emplacement enregistré à l'aide du dispositif GNSS.

authenticationStatus indique l'état d'authentification de la position GNSS au moment où celle-ci est déterminée.

2.80 GNSSPlaceRecord

Génération 2 :

Informations relatives à la position GNSS du véhicule (exigences 108, 109, 110, 296, 305, 347 et 353 de ~~l'annexe~~ **l'appendice** 1C).

GNSSPlaceRecord ::= SEQUENCE {

timeStamp	TimeReal,
gnssAccuracy	GNSSAccuracy,
geoCoordinates	GeoCoordinates

}

timeStamp indique la date et l'heure auxquelles la position GNSS du véhicule a été déterminée.

gnssAccuracy indique le degré de précision des données de position fournies par le récepteur GNSS.

geoCoordinates indique l'emplacement enregistré à l'aide du dispositif GNSS.

2.81 HighResOdometer

Valeur affichée par le compteur kilométrique du véhicule, soit la distance totale parcourue par le véhicule pendant son exploitation.

HighResOdometer ::= INTEGER(0..2^{32}-1)

Attribution de valeur : binaire sans signe. Valeur exprimée en 1/200 de km et se situant dans une plage d'exploitation comprise entre 0 et 21 055 406 km.

2.82 HighResTripDistance

Distance parcourue pendant la totalité ou une partie d'un trajet.

HighResTripDistance ::= INTEGER(0..2^{32}-1)

Attribution de valeur : binaire sans signe. Valeur exprimée en 1/200 de km et se situant dans une plage d'exploitation comprise entre 0 et 21 055 406 km.

2.83 HolderName

Nom et prénom(s) d'un détenteur de carte.

HolderName ::= SEQUENCE {

holderSurname	Name
holderFirstNames	Name

}

holderSurname indique le nom du détenteur de la carte. Ce nom ne s'accompagne d'aucun titre.

Attribution de valeur : si la carte considérée n'est pas individuelle, holderSurname contient les mêmes données que companyName, workshopName ou controlBodyName.

holderFirstNames indique le(s) prénom(s) et initiale(s) du détenteur de la carte.

2.84 Réservé pour une utilisation future ~~InternalGNSSReceiver~~

~~Génération 2 :~~

~~Informations définissant si le récepteur GNSS est interne ou externe à l'unité embarquée sur le véhicule. Vrai signifie que le récepteur GNSS est interne à l'UEV. Faux signifie que le récepteur GNSS est externe.~~

~~InternalGNSSReceiver ::= BOOLEAN~~

2.85 K-ConstantOfRecordingEquipment

Constante de l'appareil de contrôle (définition m)).

K-ConstantOfRecordingEquipment ::= INTEGER(0..2^{16}-1)

Attribution de valeur : impulsions par kilomètre dans une plage de fonctionnement comprise entre 0 et 64 255 imp/km.

2.86 KeyIdentifier

Identificateur unique d'une clé publique permettant de la désigner et de la sélectionner, ainsi que d'en identifier le détenteur.

KeyIdentifier ::= CHOICE {

extendedSerialNumber	ExtendedSerialNumber,
certificateRequestID	CertificateRequestID,
certificationAuthorityKID	CertificationAuthorityKID

}

La première option permet de désigner la clé publique d'une unité embarquée**,** ~~ou~~ d'une carte tachygraphique **ou d'un dispositif GNSS externe**.

La deuxième option permet de désigner la clé publique d'une unité embarquée (dans le**s** cas où le numéro de série de l'unité embarquée ne peut pas être connu au moment de l'élaboration du certificat).

La troisième option permet de désigner la clé publique d'un**e** ~~État membre~~ **Partie contractante**.

2.87 KMWCKey

Génération 2 :

Clé AES et la version de clé servant au couplage du capteur de mouvement avec l'UEV qui lui est associée. Pour plus d'informations, voir **sous-**appendice 11.

KMWCKey ::= SEQUENCE {

kMWCKey	AESKey,
keyVersion	INTEGER (SIZE(1))

}

kMWCKey indique la longueur de la clé AES concaténée avec la clé servant au couplage du capteur de mouvement et de l'UEV.

keyVersion désigne la version de la clé AES.

2.88 Language

Code d'identification d'une langue de travail.

Language ::= IA5String(SIZE(2))

Attribution de valeur : code composé de deux lettres minuscules, conformément à la norme ISO 639.

2.89 LastCardDownload

Date et heure du dernier téléchargement d'une carte (à des fins autres que le contrôle) qui sont enregistrées sur une carte de conducteur (exigences 257 et 282 de ~~l'annexe~~ **l'appendice** 1C). La date peut être mise à jour par une UEV ou un lecteur de carte quelconque.

LastCardDownload ::= TimeReal

Attribution de valeur : absence d'informations complémentaires.

2.89a LengthOfFollowingData

Génération 2, version 2 :

Indicateur de longueur pour les enregistrements extensibles.

LengthOfFollowingData ::= INTEGER(0.. 2^{16}-1)

Attribution de valeur : voir sous-appendice 2.

2.90 LinkCertificate

Génération 2 :

Certificat de lien entre les paires de clés de l'autorité de certification racine européenne.

LinkCertificate ::= Certificate

2.90a LoadType

Génération 2, version 2 :

Code d'identification d'un type de chargement.

LoadType ::= INTEGER(0..255)ç

Attribution de valeur :

'00'H	**type de chargement indéfini ;**
'01'H	**marchandises ;**
'02'H	**passagers ;**
'03'H .. 'FF'H	**réservé pour une utilisation future.**

2.91 L-TyreCircumference

Circonférence effective des pneumatiques (définition u)).

L-TyreCircumference ::= INTEGER(0 d'.. 2^{16}-1)

Attribution de valeur : binaire sans signe. Valeur exprimée en 1/8 de mm et se situant dans une plage de fonctionnement comprise entre 0 et 8 031 mm.

2.92 MAC

Génération 2 :

Un total de contrôle cryptographique d'une longueur de 8, 12 ou 16 octets correspondant à des suites cryptographiques spécifiées dans ~~l'appendice~~ **le sous-appendice** 11.

MAC ::= CHOICE {

mac8	OCTET STRING (SIZE(8)),
mac12	OCTET STRING (SIZE(12)),
mac16	OCTET STRING (SIZE(16))

}

2.93 ManualInputFlag

Code permettant de déterminer si un détenteur de carte a saisi manuellement ou non des activités du conducteur à l'insertion de la carte (exigence 081 de ~~l'annexe~~ **l'appendice** 1B et exigence 102 de ~~l'annexe~~ **l'appendice** 1C)

ManualInputFlag ::= INTEGER {

noEntry	(0)
manualEntries	(1)

}

Affectation de valeur : absence d'informations complémentaires.

2.94 ManufacturerCode

Code d'identification d'un fabricant d'équipement homologué.

ManufacturerCode ::= INTEGER(0..255)

Le laboratoire chargé des essais d'interopérabilité publie et tient à jour la liste des codes de fabricant sur son site Web (exigence 454 de ~~l'annexe~~ **l'appendice** 1C).

Les codes de type ManufacturerCodes sont attribués aux concepteurs de tachygraphes à titre provisoire et sur demande auprès du laboratoire chargé des essais d'interopérabilité.

2.95 ManufacturerSpecificEventFaultData

Génération 2 :

Codes d'erreur propres au fabricant qui simplifient l'analyse des erreurs et la maintenance des unités embarquées.

ManufacturerSpecificEventFaultData ::= SEQUENCE {

manufacturerCode	ManufacturerCode,
manufacturerSpecificErrorCode	OCTET STRING(SIZE(3))

}

manufacturerCode est le code d'identification du fabricant de l'unité embarquée sur le véhicule.

manufacturerSpecificErrorCode est un code d'erreur propre au fabricant.

2.96 MemberStateCertificate

Certificat de la clé publique d'un**e** ~~État membre~~ **Partie contractante** délivré par ~~l'organisme~~ **l'autorité** de certification **racine**~~européen~~.

MemberStateCertificate ::= Certificate

2.97 MemberStateCertificateRecordArray

Génération 2 :

Le certificat de ~~l'État membre~~ **la Partie contractante** plus les métadonnées servant au protocole de téléchargement.

MemberStateCertificateRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF MemberStateCertificate

}

recordType indique le type d'enregistrement (MemberStateCertificate). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type MemberStateCertificate exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant. La valeur est fixée à 1, car les certificats peuvent présenter des longueurs variables.

records désigne le jeu de certificats des ~~États membres~~ **Parties contractantes**.

2.98 MemberStatePublicKey

Génération 1 :

Clé publique d'un**e** ~~État membre~~ **Partie contractante**.

MemberStatePublicKey ::= PublicKey

2.99 Name

Un nom.

Name ::= SEQUENCE {

codePage	INTEGER (0..255),
name	OCTET STRING (SIZE(35))

}

codePage spécifie un jeu de caractères défini au chapitre 4.

name indique un nom codé à l'aide du jeu de caractères spécifié.

2.100 NationAlpha

Désignation d'un pays par un code alphabétique conforme aux signes distinctifs apposés sur les véhicules en circulation internationale (Convention de Vienne sur la circulation routière, Nations unies, 1968).

NationAlpha ::= IA5String(SIZE(3))

Les codes NationAlpha et NationNumeric sont consignés sur une liste publiée sur le site Web du laboratoire chargé des essais d'interopérabilité, comme prévu à l'exigence 440 de l'~~annexe~~**appendice** 1C.

2.101 NationNumeric

Code numérique désignant un pays.

NationNumeric ::= INTEGER(0 .. 255)

Attribution de valeur : voir le type de données 2.100 (NationAlpha).

Toute modification ou mise à jour des spécifications relatives aux types de données NationAlpha ou NationNumeric décrites ci-dessus ne peut intervenir qu'après consultation, par le laboratoire désigné, des fabricants d'unités embarquées dotées de tachygraphes numérique et intelligent homologués.

2.101a NoOfBorderCrossingRecords

Génération 2, version 2 :

Nombre d'enregistrements de passage de frontières qu'une carte de conducteur ou d'atelier est en mesure de stocker.

NoOfBorderCrossingRecords ::= INTEGER(0.. 2^{16}-1)

Attribution de valeur : voir sous-appendice 2.

2.102 NoOfCalibrationRecords

Nombre d'enregistrements d'étalonnage qu'une carte d'atelier est en mesure de stocker.

Génération 1 :

NoOfCalibrationRecords ::= INTEGER(0..255)

Attribution de valeur : voir **sous-**appendice 2.

Génération 2 :

NoOfCalibrationRecords ::= INTEGER(0..2^{16}-1)

Attribution de valeur : voir **sous-**appendice 2.

2.103 NoOfCalibrationsSinceDownload

Compteur indiquant le nombre d'étalonnages effectués avec une carte d'atelier depuis son dernier téléchargement (exigences 317 et 340 de ~~l'annexe~~**l'appendice** 1C).

NoOfCalibrationsSinceDownload ::= INTEGER(0..2^{16}-1)

Attribution de valeur : absence d'informations complémentaires.

2.104 NoOfCardPlaceRecords

Nombre d'enregistrements de lieu qu'une carte de conducteur ou d'atelier est en mesure de stocker.

Génération 1 :

NoOfCardPlaceRecords ::= INTEGER(0..255)

Attribution de valeur : voir **sous-**appendice 2.

Génération 2 :

NoOfCardPlaceRecords ::= INTEGER(0..2^{16}-1)

Attribution de valeur : voir **sous-**appendice 2.

2.105 NoOfCardVehicleRecords

Nombre d'enregistrements de véhicules utilisés qu'une carte de conducteur ou d'atelier est en mesure de stocker.

NoOfCardVehicleRecords ::= INTEGER(0.. 2^{16}-1)

Attribution de valeur : voir **sous-**appendice 2.

2.106 NoOfCardVehicleUnitRecords

Génération 2 :

Nombre d'enregistrements d'unités embarquées utilisées qu'une carte de conducteur ou d'atelier est en mesure de stocker.

NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2^{16}-1)

Attribution de valeur : voir **sous-**appendice 2.

2.107 NoOfCompanyActivityRecords

Nombre d'enregistrements d'activité d'entreprise qu'une carte d'entreprise est en mesure de stocker.

NoOfCompanyActivityRecords ::= INTEGER(0.. 2^{16}-1)

Attribution de valeur : voir **sous-**appendice 2.

2.108 NoOfControlActivityRecords

Nombre d'enregistrements d'activité de contrôle qu'une carte de contrôleur est en mesure de stocker.

NoOfControlActivityRecords ::= INTEGER(0.. 2^{16}-1)

Attribution de valeur : voir **sous-**appendice 2.

2.109 NoOfEventsPerType

Nombre d'événements qu'une carte est en mesure de stocker par type d'événement.

NoOfEventsPerType ::= INTEGER(0..255)

Attribution de valeur : voir **sous-**appendice 2.

2.110 NoOfFaultsPerType

Nombre d'anomalies qu'une carte est en mesure de stocker par type d'anomalie.

NoOfFaultsPerType ::= INTEGER(0..255)

Attribution de valeur : voir **sous-**appendice 2.

~~2.111 NoOfGNSSCDRecords~~

2.111 NoOfGNSSADRecords

Génération 2 :

Nombre d'enregistrements du temps de conduite ~~continue~~ **accumulé** en provenance du récepteur GNSS qu'une carte est en mesure de stocker.

~~NoOfGNSSCDRecords~~ **NoOfGNSSADRecords**::= INTEGER(0..2^{16}-1)

Attribution de valeur : voir **sous-**appendice 2.

2.111a NoOfLoadUnloadRecords

Génération 2, version 2 :

Nombre d'enregistrements de chargement/déchargement qu'une carte est en mesure de stocker.

NoOfLoadUnloadRecords ::= INTEGER(0..2^{16}-1)

Attribution de valeur : voir sous-appendice 2.

2.112 NoOfSpecificConditionRecords

Génération 2 :

Nombre d'enregistrements de condition particulière qu'une carte est en mesure de stocker.

NoOfSpecificConditionRecords ::= INTEGER(0..2^{16}-1)

Attribution de valeur : voir **sous-**appendice 2.

2.112a NoOfLoadTypeEntryRecords

Génération 2, version 2 :

Nombre d'enregistrements de type de chargement qu'une carte de conducteur ou d'atelier est en mesure de stocker.

NoOfLoadTypeEntryRecords ::= INTEGER(0..2^{16}-1)

Attribution de valeur : voir sous-appendice 2.

2.113 OdometerShort

Valeur affichée par le compteur kilométrique du véhicule sous une forme abrégée.

OdometerShort ::= INTEGER(0..224-1)

Attribution de valeur : binaire sans signe. Valeur exprimée en km et se situant dans une plage de fonctionnement comprise entre 0 et 9 999 999 km.

2.114 OdometerValueMidnight

Valeur affichée par le compteur kilométrique du véhicule à minuit un jour donné (exigence 090 de ~~l'annexe~~**l'appendice** 1B et exigence 113 de ~~l'annexe~~**l'appendice** 1C).

OdometerValueMidnight ::= OdometerShort

Affectation de valeur : absence d'informations complémentaires.

2.114a OperationType

Génération 2, version 2 :

Code d'identification d'un type d'opération.

OperationType ::= INTEGER(0..255)

Attribution de valeur :

'00'H	**réservé pour une utilisation future ;**
'01'H	**chargement ;**
'02'H	**déchargement ;**
'03'H	**chargement/déchargement simultanés ;**
'04'H .. 'FF'H	**réservé pour une utilisation future.**

2.115 OdometerValueMidnightRecordArray

Génération 2 :

OdometerValueMidnight plus les métadonnées servant au protocole de téléchargement.

OdometerValueMidnightRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF OdometerValueMidnight

}

recordType indique le type d'enregistrement (OdometerValueMidnight).

Attribution de valeur : voir RecordType.

recordSize indique la taille des enregistrements de type OdometerValueMidnight exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne le jeu d'enregistrements de type OdometerValueMidnight.

2.116 OverspeedNumber

Nombre d'événements de type excès de vitesse survenus depuis le dernier contrôle d'excès de vitesse.

OverspeedNumber ::= INTEGER(0..255)

Attribution de valeur : 0 signifie qu'aucun événement de type excès de vitesse n'est survenu depuis le dernier contrôle d'excès de vitesse ; 1 signifie qu'un événement de type excès de vitesse est survenu depuis le dernier contrôle d'excès de vitesse ; …255 signifie que le nombre d'événements de type excès de vitesse enregistrés depuis le dernier contrôle d'excès de vitesse est égal ou supérieur à 255.

2.116a PlaceAuthRecord

Informations relatives à un lieu de début ou de fin d'une période de travail journalière (exigences 108, 271, 296, 324 et 347 de l'appendice 1C).

Génération 2, version 2 :

PlaceAuthRecord ::= SEQUENCE {

entryTime	**TimeReal,**
entryTypeDailyWorkPeriod	**EntryTypeDailyWorkPeriod,**
dailyWorkPeriodCountry	**NationNumeric,**
dailyWorkPeriodRegion	**RegionNumeric,**
vehicleOdometerValue	**OdometerShort,**
entryGNSSPlaceAuthRecord	**GNSSPlaceAuthRecord**

}

entryTime indique la date et l'heure de la saisie des données.

entryTypeDailyWorkPeriod indique le type de saisie.

dailyWorkPeriodCountry indique le pays saisi.

dailyWorkPeriodRegion indique la région saisie.

vehicleOdometerValue indique la valeur affichée par le compteur kilométrique à l'heure où le lieu a été saisi.

entryGNSSPlaceAuthRecord indique le lieu enregistré, l'état d'authentification de la position GNSS et l'heure correspondante.

2.116b PlaceAuthStatusRecord

Génération 2, version 2 :

Informations enregistrées sur une carte de conducteur ou d'atelier, indiquant l'état d'authentification d'un lieu de début ou de fin d'une période de travail journalière (exigences 306a et 356b). D'autres informations concernant le lieu lui-même sont stockées dans un autre enregistrement (voir 2.117 PlaceRecord).

PlaceAuthStatusRecord ::= SEQUENCE {

entryTime	**TimeReal,**
authenticationStatus	**PositionAuthenticationStatus**

}

entryTime indique la date et l'heure de la saisie des données (qui sont identiques à celles associées à l'enregistrement PlaceRecord correspondant).

authenticationStatus indique l'état d'authentification de la position GNSS enregistrée.

2.117 PlaceRecord

Informations relatives à un lieu de début ou de fin d'une période de travail journalière (exigences 108, 271, 296, 324 et 347 de ~~l'annexe~~**l'appendice** 1C).

Génération 1 :

PlaceRecord ::= SEQUENCE {

entryTime	TimeReal,
entryTypeDailyWorkPeriod	EntryTypeDailyWorkPeriod,
dailyWorkPeriodCountry	NationNumeric,
dailyWorkPeriodRegion	RegionNumeric,
vehicleOdometerValue	OdometerShort

}

entryTime indique la date et l'heure de la saisie des données.

entryTypeDailyWorkPeriod indique le type de saisie.

dailyWorkPeriodCountry indique le pays saisi.

dailyWorkPeriodRegion indique la région saisie.

vehicleOdometerValue indique la valeur affichée par le compteur kilométrique à l'heure à laquelle le lieu a été saisi.

Génération 2 :

PlaceRecord ::= SEQUENCE {

entryTime	TimeReal,
entryTypeDailyWorkPeriod	EntryTypeDailyWorkPeriod,
dailyWorkPeriodCountry	NationNumeric,
dailyWorkPeriodRegion	RegionNumeric,
vehicleOdometerValue	OdometerShort,
entryGNSSPlaceRecord	GNSSPlaceRecord

}

L'élément de données suivant est utilisé en plus des éléments composant la structure de génération 1 :

entryGNSSPlaceRecord indique le lieu enregistré et l'heure correspondante.

2.117a PositionAuthenticationStatus

Génération 2, version 2 :

PositionAuthenticationStatus ::= INTEGER(0..255)

Attribution de valeur (voir sous-appendice 12) :

'00'H	**non authentifié (voir sous-appendice 12, exigence GNS_39) ;**
'01'H	**authentifié (voir sous-appendice 12, exigence GNS_39) ;**
'02'H .. 'FF'H	**réservé pour une utilisation future.**

2.118 PreviousVehicleInfo

Informations relatives au véhicule précédemment utilisé par un conducteur enregistrées lors

de l'insertion de la carte dans le lecteur approprié d'une unité embarquée (exigence 081 de ~~l'annexe~~**l'appendice** 1B et exigence 102 de ~~l'annexe~~**l'appendice** 1C).

Génération 1:

PreviousVehicleInfo ::= SEQUENCE {

vehicleRegistrationIdentification	VehicleRegistrationIdentification,
cardWithdrawalTime	TimeReal

}

vehicleRegistrationIdentification indique le VRN et ~~l'État membre~~ **la Partie contractante** d'immatriculation du véhicule.

cardWithdrawalTime indique la date et l'heure de retrait de la carte.

Génération 2:

PreviousVehicleInfo ::= SEQUENCE {

vehicleRegistrationIdentification	VehicleRegistrationIdentification,
cardWithdrawalTime	TimeReal,
vuGeneration	Generation

}

L'élément de données suivant est utilisé en plus des éléments composant la structure de génération 1 :

vuGeneration indique la génération de l'unité embarquée sur le véhicule.

2.119 PublicKey

Génération 1 :

Clé publique RSA.

PublicKey ::= SEQUENCE {

rsaKeyModulus	RSAKeyModulus,
rsaKeyPublicExponent	RSAKeyPublicExponent

}

rsaKeyModulus indique le module de la paire de clés.

rsaKeyPublicExponent indique l'exposant public de la paire de clés.

2.120 RecordType

Génération 2 :

Désignation d'un type d'enregistrement. Ce type de données est utilisé dans les enregistrements de type RecordArrays.

RecordType ::= OCTET STRING(SIZE(1))

Attribution de valeur :

'01'H	ActivityChangeInfo
'02'H	CardSlotsStatus
'03'H	CurrentDateTime
'04'H	MemberStateCertificate
'05'H	OdometerValueMidnight

‘06’H	DateOfDayDownloaded
‘07’H	SensorPaired
‘08’H	Signature
‘09’H	SpecificConditionRecord
‘0A’H	VehicleIdentificationNumber
‘0B’H	VehicleRegistrationNumber
‘0C’H	VuCalibrationRecord
‘0D’H	VuCardIWRecord
‘0E’H	VuCardRecord
‘0F’H	VuCertificate
‘10’H	VuCompanyLocksRecord
‘11’H	VuControlActivityRecord
‘12’H	VuDetailedSpeedBlock
‘13’H	VuDownloadablePeriod
‘14’H	VuDownloadActivityData
‘15’H	VuEventRecord
‘16’H	~~VuGNSSCDRecord,~~**VuGNSSADRecord**
‘17’H	VuITSConsentRecord
‘18’H	VuFaultRecord
‘19’H	VuIdentification
‘1A’H	VuOverSpeedingControlData
‘1B’H	VuOverSpeedingEventRecord
‘1C’H	VuPlaceDailyWorkPeriodRecord
‘1D’H	VuTimeAdjustmentGNSSRecord
‘1E’H	VuTimeAdjustmentRecord
‘1F’H	VuPowerSupplyInterruptionRecord
‘20’H	SensorPairedRecord
‘21’H	SensorExternalGNSSCoupledRecord
‘22’H~~ à ‘7F’H~~	**VuBorderCrossingRecord**~~Réservé pour une utilisation future~~
‘**23**~~80~~’H~~ à ‘FF’H~~	**VuLoadUnloadRecord** ~~propre au fabricant~~
‘24’H	**VehicleRegistrationIdentification**
‘25’H à ‘7F’H	**réservé pour une utilisation future**
‘80’H à ‘FF’H	**propre au fabricant**

2.121 RegionAlpha

Code alphabétique désignant les différentes régions d’un pays déterminé.

RegionAlpha ::= IA5STRING(SIZE(3))

Génération 1 :

Attribution de valeur :

‘‘	aucune donnée disponible

Espagne :

‘AN’	Andalucía
‘AR’	Aragón
‘AST’	Asturias
‘C’	Cantabria
‘CAT’	Cataluña
‘CL’	Castilla-León
‘CM’	Castilla-La-Mancha
‘CV’	Valencia
‘EXT’	Extremadura
‘G’	Galicia
‘IB’	Baleares
‘IC’	Canarias
‘LR’	La Rioja
‘M’	Madrid
‘MU’	Murcia
‘NA’	Navarra
‘PV’	País Vasco

Génération 2 :

Les codes RegionAlpha sont consignés sur une liste publiée sur le site Web du laboratoire chargé des essais d’interopérabilité.

2.122 RegionNumeric

Code numérique désignant les différentes régions d’un pays déterminé.

RegionNumeric ::= OCTET STRING (SIZE(1))

Génération 1:

Attribution de valeur :

‘00’H	aucune information disponible

Espagne :

‘01’H	Andalucía
‘02’H	Aragón
‘03’H	Asturias
‘04’H	Cantabria
‘05’H	Cataluña
‘06’H	Castilla-León
‘07’H	Castilla-La-Mancha
‘08’H	Valencia
‘09’H	Extremadura
‘0A’H	Galicia

‘0B’H	Baleares
‘0C’H	Canarias
‘0D’H	La Rioja
‘0E’H	Madrid
‘0F’H	Murcia
‘10’H	Navarra
‘11’H	País Vasco

Génération 2 :

Les codes RegionNumeric sont consignés sur une liste publiée sur le site Web du laboratoire chargé des essais d’interopérabilité.

2.123 RemoteCommunicationModuleSerialNumber

Génération 2 :

Numéro de série du module de communication à distance.

RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber

2.124 RSAKeyModulus

Génération 1 :

Module d’une paire de clés RSA.

RSAKeyModulus ::= OCTET STRING (SIZE(128))

Attribution de valeur : non spécifié.

2.125 RSAKeyPrivateExponent

Génération 1 :

Exposant privé d’une paire de clés RSA.

RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))

Attribution de valeur : non spécifié.

2.126 RSAKeyPublicExponent

Génération 1 :

Exposant public d’une paire de clés RSA.

RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))

Attribution de valeur : non spécifié.

2.127 RtmData

Génération 2 :

Pour la définition de ce type de données, se référer ~~à l’appendice~~**au sous-appendice** 14.

2.128 SealDataCard

Génération 2 :

Ce type de données sert au stockage, sur une carte, d'informations concernant les scellements associés aux différents composants d'un véhicule. Ce type de données est lié à l'exigence 337 de ~~l'annexe~~**l'appendice** 1C.

SealDataCard ::= SEQUENCE {

noOfSealRecords	INTEGER(1..5),
sealRecords	SET SIZE(noOfSealRecords) OF SealRecord

}

noOfSealRecords indique le nombre d'enregistrements dans sealRecords**.**

sealRecords désigne un jeu d'enregistrements de scellement.

2.129 SealDataVu

Génération 2 :

Ce type de données est destiné au stockage, dans la mémoire d'une unité embarquée, d'informations concernant les scellements associés aux différents composants d'un véhicule.

SealDataVu ::= SEQUENCE SIZE(5) OF {

sealRecords	SealRecord

}

sealRecords désigne un jeu d'enregistrements de scellement. S'il existe moins de cinq scellements disponibles, la valeur d'EquipmentType dans tous les sealRecords inutilisés doit être fixée à ~~16~~**15**, autrement dit « inutilisé ».

2.130 SealRecord

Génération 2 :

Ce type de données permet de stocker les informations relatives à un scellement associé à un composant. Ce type de données est lié à l'exigence 337 de ~~l'annexe~~**l'appendice** 1C.

SealRecord ::= SEQUENCE {

equipmentType	EquipmentType,
extendedSealIdentifier	ExtendedSealIdentifier

}

equipmentType indique le type d'équipement auquel le scellement est associé.

extendedSealIdentifier est l'identificateur du scellement associé à l'équipement concerné.

2.131 SensorApprovalNumber

Numéro d'homologation du capteur.

Génération 1 :

SensorApprovalNumber ::= IA5String(SIZE(8))

Attribution de valeur : non spécifié.

Génération 2 :

SensorApprovalNumber ::= IA5String(SIZE(16))

Attribution de valeur :

Le numéro d'homologation doit être indiqué tel qu'il est publié sur le site Web ~~de la Commission européenne correspondant~~ **géré par le laboratoire compétent pour les essais d'interopérabilité**, par exemple en incluant les traits d'union. Le numéro d'homologation doit être aligné à gauche.

2.132 SensorExternalGNSSApprovalNumber

Génération 2 :

Numéro d'homologation du dispositif GNSS externe.

SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))

Attribution de valeur :

Le numéro d'homologation doit être indiqué tel qu'il est publié sur le site Web ~~de la Commission européenne correspondant~~ **géré par le laboratoire compétent pour les essais d'interopérabilité**, par exemple en incluant les traits d'union. Le numéro d'homologation doit être aligné à gauche.

2.133 SensorExternalGNSSCoupledRecord

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée et se rapportant à l'identification du dispositif GNSS externe couplé avec cette unité embarquée (exigence 100 de ~~l'annexe~~**l'appendice** 1C).

SensorExternalGNSSCoupledRecord ::= SEQUENCE {

sensorSerialNumber	SensorGNSSSerialNumber,
sensorApprovalNumber	SensorExternalGNSSApprovalNumber,
sensorCouplingDate	SensorGNSSCouplingDate

}

sensorSerialNumber indique le numéro de série du dispositif GNSS externe couplé avec l'unité embarquée.

sensorApprovalNumber indique le numéro d'homologation du dispositif GNSS externe considéré.

sensorCouplingDate indique la date du couplage entre ce dispositif GNSS externe et l'unité embarquée.

2.134 SensorExternalGNSSIdentification

Génération 2 :

Informations relatives à l'identification du dispositif GNSS externe (exigence 98 de ~~l'annexe~~ **l'appendice** 1C).

SensorExternalGNSSIdentification ::= SEQUENCE {

sensorSerialNumber	SensorGNSSSerialNumber,
sensorApprovalNumber	SensorExternalGNSSApprovalNumber,
sensorSCIdentifier	SensorExternalGNSSSCIdentifier,
sensorOSIdentifier	SensorExternalGNSSOSIdentifier

}

sensorSerialNumber indique le numéro de série étendu du dispositif GNSS externe.

sensorApprovalNumber indique le numéro d'homologation du dispositif GNSS externe.

sensorSCIdentifier est l'identificateur du composant de sécurité du dispositif GNSS externe.

sensorOSIdentifier est l'identificateur du système d'exploitation du dispositif GNSS externe.

2.135 SensorExternalGNSSInstallation

Génération 2 :

Informations enregistrées dans la mémoire du dispositif GNSS externe concernant l'installation du capteur GNSS externe (exigence 123 de ~~l'annexe~~ **l'appendice** 1C).

SensorExternalGNSSInstallation ::= SEQUENCE {

sensorCouplingDateFirst	SensorGNSSCouplingDate,
firstVuApprovalNumber	VuApprovalNumber,
firstVuSerialNumber	VuSerialNumber,
sensorCouplingDateCurrent	SensorGNSSCouplingDate,
currentVuApprovalNumber	VuApprovalNumber,
currentVUSerialNumber	VuSerialNumber

}

sensorCouplingDateFirst indique la date du premier couplage du dispositif GNSS externe avec une unité embarquée.

firstVuApprovalNumber indique le numéro d'homologation de la première unité embarquée couplée avec le dispositif GNSS externe.

firstVuSerialNumber indique le numéro de série de la première unité embarquée couplée avec le dispositif GNSS externe.

sensorCouplingDateCurrent indique la date du couplage actuel du dispositif GNSS externe avec une unité embarquée.

currentVuApprovalNumber indique le numéro d'homologation de l'unité embarquée actuellement couplée avec le dispositif GNSS externe.

currentVUSerialNumber indique le numéro de série de l'unité embarquée actuellement couplée avec le dispositif GNSS externe.

2.136 SensorExternalGNSSOSIdentifier

Génération 2 :

Identificateur du système d'exploitation du dispositif GNSS externe.

SensorOSIdentifier ::= IA5String(SIZE(2))

Attribution de valeur : propre au fabricant.

2.137 SensorExternalGNSSSCIdentifier

Génération 2 :

Ce type sert, entre autres, à identifier le module cryptographique du dispositif GNSS externe.

Identificateur du composant de sécurité du dispositif GNSS externe.

SensorExternalGNSSSCIdentifier ::= IA5String(SIZE(8))

Attribution de valeur : propre au fabricant.

2.138 SensorGNSSCouplingDate

Génération 2 :

Date d'un couplage du dispositif GNSS externe avec une unité embarquée.

SensorGNSSCouplingDate ::= TimeReal

Attribution de valeur : non spécifié.

2.139 SensorGNSSSerialNumber

Génération 2 :

Ce type sert à stocker le numéro de série du récepteur GNSS, que celui-ci soit situé à l'intérieur ou à l'extérieur de l'UEV.

Numéro de série du récepteur GNSS.

SensorGNSSSerialNumber ::= ExtendedSerialNumber

2.140 SensorIdentification

Informations enregistrées dans la mémoire d'un capteur de mouvement et se rapportant à son identification (exigence 077 de ~~l'annexe~~ **l'appendice** 1B et exigence 95 de ~~l'annexe~~ **l'appendice** 1C).

SensorIdentification ::= SEQUENCE {

sensorSerialNumber	SensorSerialNumber,
sensorApprovalNumber	SensorApprovalNumber,
sensorSCIdentifier	SensorSCIdentifier,
sensorOSIdentifier	SensorOSIdentifier

}

sensorSerialNumber indique le numéro de série étendu du capteur de mouvement (numéro de référence et code du fabricant inclus).

sensorApprovalNumber indique le numéro d'homologation du capteur de mouvement.

sensorSCIdentifier est l'identificateur du composant de sécurité du capteur de mouvement.

sensorOSIdentifier est l'identificateur du système d'exploitation du capteur de mouvement.

2.141 SensorInstallation

Informations enregistrées dans la mémoire d'un capteur de mouvement concernant son installation (exigence 099 de ~~l'annexe~~ **l'appendice** 1B et exigence 122 de ~~l'annexe~~ **l'appendice** 1C).

SensorInstallation ::= SEQUENCE {

sensorPairingDateFirst	SensorPairingDate,
firstVuApprovalNumber	VuApprovalNumber,
firstVuSerialNumber	VuSerialNumber,
sensorPairingDateCurrent	SensorPairingDate,
currentVuApprovalNumber	VuApprovalNumber,

currentVUSerialNumber VuSerialNumber

}

sensorPairingDateFirst indique la date du premier couplage du capteur de mouvement avec une unité embarquée.

firstVuApprovalNumber indique le numéro d'homologation de la première unité embarquée couplée avec le capteur de mouvement.

firstVuSerialNumber indique le numéro de série de la première unité embarquée couplée avec le capteur de mouvement.

sensorPairingDateCurrent indique la date du couplage actuel du capteur de mouvement avec l'unité embarquée.

currentVuApprovalNumber indique le numéro d'homologation de l'unité embarquée actuellement couplée avec le capteur de mouvement.

currentVUSerialNumber indique le numéro de série de l'unité embarquée actuellement couplée avec le capteur de mouvement.

2.142 SensorInstallationSecData

Informations enregistrées sur une carte d'atelier et se rapportant aux données de sécurité nécessaires au couplage des capteurs de mouvement avec des unités embarquées (exigences 308 et 331 de ~~l'annexe~~ **l'appendice** 1C).

Génération 1 :

SensorInstallationSecData ::= TDesSessionKey

Attribution de valeur : conformément à la norme ISO 16844-3.

Génération 2 :

Conformément à la description figurant ~~à l'appendice~~ **au sous-appendice** 11, une carte d'atelier doit mémoriser jusqu'à trois clés pour le couplage du capteur de mouvement avec l'UEV. Il existe différentes versions de ces clés.

SensorInstallationSecData ::= SEQUENCE {

kMWCKey1 KMWCKey,

kMWCKey2 KMWCKey OPTIONAL,

kMWCKey3 KMWCKey OPTIONAL

}

2.143 SensorOSIdentifier

Identificateur du système d'exploitation du capteur de mouvement.

SensorOSIdentifier ::= IA5String(SIZE(2))

Attribution de valeur : propre au fabricant.

2.144 SensorPaired

Génération 1 :

Informations enregistrées dans la mémoire d'une unité embarquée et se rapportant à l'identification du capteur de mouvement couplé avec cette unité embarquée (exigence 079 de ~~l'annexe~~ **l'appendice** 1B).

SensorPaired ::= SEQUENCE {

sensorSerialNumber SensorSerialNumber,

sensorApprovalNumber SensorApprovalNumber,

sensorPairingDateFirst SensorPairingDate

}

sensorSerialNumber indique le numéro de série du capteur de mouvement actuellement couplé avec l'unité embarquée.

sensorApprovalNumber indique le numéro d'homologation du capteur de mouvement actuellement couplé avec l'unité embarquée.

sensorPairingDateFirst indique la date du premier couplage avec une unité embarquée du capteur de mouvement actuellement couplé avec l'unité embarquée sur le véhicule considéré.

2.145 SensorPairedRecord

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée et se rapportant à l'identification du capteur de mouvement couplé avec cette unité embarquée (exigence 97 de ~~l'annexe~~ **l'appendice** 1C).

SensorPairedRecord ::= SEQUENCE {

sensorSerialNumber SensorSerialNumber,

sensorApprovalNumber SensorApprovalNumber,

sensorPairingDate SensorPairingDate

}

sensorSerialNumber indique le numéro de série d'un capteur de mouvement couplé avec l'unité embarquée considérée.

sensorApprovalNumber indique le numéro d'homologation de ce capteur de mouvement.

sensorPairingDate indique une date de couplage de ce capteur de mouvement avec l'unité embarquée considérée.

2.146 SensorPairingDate

Date d'un couplage entre le capteur de mouvement considéré et une unité embarquée sur le véhicule.

SensorPairingDate ::= TimeReal

Attribution de valeur : non spécifié.

2.147 SensorSCIdentifier

Identificateur du composant de sécurité du capteur de mouvement.

SensorSCIdentifier ::= IA5String(SIZE(8))

Attribution de valeur : propre au fabricant du composant.

2.148 SensorSerialNumber

Numéro de série du capteur de mouvement.

SensorSerialNumber ::= ExtendedSerialNumber

2.149 Signature

Une signature numérique.

Génération 1 :

Signature ::= OCTET STRING (SIZE(128))

Attribution de valeur : conformément ~~à l'appendice~~ **au sous-appendice** 11 (Mécanismes de sécurité communs).

Génération 2 :

Signature ::= OCTET STRING (SIZE(64..132))

Attribution de valeur : conformément ~~à l'appendice~~ **au sous-appendice** 11 (Mécanismes de sécurité communs).

2.150 SignatureRecordArray

Génération 2 :

Un jeu de signatures plus les métadonnées servant au protocole de téléchargement.

SignatureRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF Signature

}

recordType indique le type d'enregistrement (Signature). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type Signature exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant. La valeur est fixée à 1, car les signatures peuvent présenter des longueurs variables.

records désigne le jeu de signatures.

2.151 SimilarEventsNumber

Nombre d'événements semblables enregistrés pour un jour donné (exigence 094 de ~~l'annexe~~ **l'appendice** 1B et exigence 117 de ~~l'annexe~~ **l'appendice** 1C).

SimilarEventsNumber ::= INTEGER(0..255)

Attribution de valeur : 0 n'est pas utilisé ; 1 signifie qu'un seul événement de ce type s'est produit et a été enregistré le jour considéré ; 2 signifie que deux événements de ce type se sont produits le jour considéré (un seul d'entre eux a été enregistré) ; …255 signifie que le nombre d'événements de ce type survenus le jour considéré est égal ou supérieur à 255.

2.152 SpecificConditionRecord

Informations enregistrées dans la mémoire d'une carte de conducteur, d'une carte d'atelier ou d'une unité embarquée concernant une condition particulière (exigences 130, 276, 301, 328 et 355 de ~~l'annexe~~ **l'appendice** 1C).

SpecificConditionRecord ::= SEQUENCE {

entryTime	TimeReal,

specificConditionType	SpecificConditionType

}

entryTime indique la date et l'heure de la saisie de ces données.

specificConditionType est le code d'identification d'une condition particulière.

2.153 SpecificConditions

Informations enregistrées dans la mémoire d'une carte de conducteur, d'une carte d'atelier ou d'une unité embarquée concernant une condition particulière (exigences 131, 277, 302, 329 et 356 de ~~l'annexe~~ **l'appendice** 1C).

Generation 2:

SpecificConditions := SEQUENCE {

conditionPointerNewestRecord	INTEGER(0..NoOfSpecificConditionRecords-1),
specificConditionRecords	SET SIZE(NoOfSpecificConditionRecords) OF SpecificConditionRecord

}

conditionPointerNewestRecord est l'indice du plus récent enregistrement de condition particulière mis à jour.

Attribution de valeur : nombre correspondant au numérateur de l'enregistrement de condition particulière, commençant par une série de '0' pour la première occurrence d'un enregistrement de condition particulière dans la structure considérée.

specificConditionRecords désigne le jeu d'enregistrements contenant des informations relatives aux conditions particulières.

2.154 SpecificConditionType

Code d'identification d'une condition particulière donnée (exigences 050b, 105a, 212a et 230a de ~~l'annexe~~ **l'appendice** 1B et exigence~~s~~ 62 de ~~l'annexe~~ **l'appendice** 1C).

SpecificConditionType ::= INTEGER(0..255)

Génération 1 :

Attribution de valeur :

'00'H	réservé pour une utilisation future
'01'H	hors champ (début)
'02'H	hors champ (fin)
'03'H	trajet en ferry/train
'04'H .. 'FF'H	réservé pour une utilisation future

Génération 2 :

Attribution de valeur :

'00'H	réservé pour une utilisation future
'01'H	hors champ (début)
'02'H	hors champ (fin)
'03'H	trajet en ferry/train (début)
'04'H	trajet en ferry/train (fin)
'05'H .. 'FF'H	réservé pour une utilisation future

2.155 Speed

Vitesse du véhicule (en km/h).

Speed ::= INTEGER(0..255)

Attribution de valeur : kilomètres à l'heure dans une plage de fonctionnement comprise entre 0 et 220 km/h.

2.156 SpeedAuthorised

Vitesse maximale autorisée du véhicule (définition hh)).

SpeedAuthorised ::= Speed

2.157 SpeedAverage

Vitesse moyenne mesurée sur une durée définie au préalable (en km/h).

SpeedAverage ::= Speed

2.158 SpeedMax

Vitesse maximale mesurée sur une durée définie au préalable.

SpeedMax ::= Speed

2.158a TachographCardsGen1Suppression

Génération 2, version 2 :

Compatibilité d'une UEV de deuxième génération avec les cartes de conducteur, de contrôleur et d'entreprise de première génération (voir sous-appendice 15, exigence MIG_002).

TachographCardsGen1Suppression ::= INTEGER (0..2^{16}-1)

Attribution de valeur :

'0000'H	**l'UEV est compatible avec les cartes tachygraphiques de génération 1 (valeur par défaut)**
'A5E3'H	**l'UEV n'est pas compatible avec les cartes tachygraphiques de génération 1**

Toutes les autres valeurs inutilisé

2.159 TachographPayload

Génération 2 :

Pour la définition de ce type de données, se référer ~~à l'appendice~~ **au sous-appendice** 14.

2.160 Réservé pour une utilisation future

~~TachographPayloadEncrypted~~

~~Génération 2 :~~

~~La charge du tachygraphe codée en DER-TLV, c'est-à-dire les données codées envoyées dans le message RTM. Concernant le mécanisme de chiffrement, cf. appendice 11 partie B chapitre 13.~~

~~TachographPayloadEncrypted ::= SEQUENCE {~~

~~tag OCTET STRING(SIZE(1)),~~

~~length OCTET STRING(SIZE(1..2)),~~

~~paddingContentIndicatorByte OCTET STRING(SIZE(1)),~~

~~encryptedData OCTET STRING(SIZE(16..192))~~

~~}~~

~~tag fait partie du codage en DER-TLV et doit être défini sur '87 (cf. appendice 11, partie B, chapitre 13).~~

~~length fait partie du codage en DER-TLV et doit coder la longueur de l'octet indicateur de contenu de remplissage suivant ainsi que les données codées.~~

~~paddingContentIndicatorByte doit être défini sur '00'.~~

~~encryptedData désigne la charge de tachygraphe codée comme le précise l'appendice 11, partie B, chapitre 13. La longueur de ces données exprimée en octets doit toujours être un multiple de 16.~~

2.161 TDesSessionKey

Génération 1 :

Clé de session Triple DES.

TDesSessionKey ::= SEQUENCE {

tDesKeyA OCTET STRING (SIZE(8)),

tDesKeyB OCTET STRING (SIZE(8))

}

Attribution de valeur : absence d'informations complémentaires.

2.162 TimeReal

Code associé à une zone combinant date et heure exprimées en secondes à compter de 00 h 00m00s UTC le 1er janvier 1970.

TimeReal{INTEGER:TimeRealRange} ::= INTEGER (0..TimeRealRange)

Attribution de valeur − Octet aligné : nombre de secondes écoulées depuis minuit UTC le 1er janvier 1970.

La date/heure future la plus avancée se situe en l'an 2106.

2.163 TyreSize

Désignation des dimensions des pneumatiques.

TyreSize ::= IA5String(SIZE(15))

Attribution de valeur : conformément ~~à la directive 92/23/CEE du 31.3.1992 (JO L 129, p. 95)~~ **au Règlement ONU nº 54**.

2.164 VehicleIdentificationNumber

Numéro d'identification du véhicule (VIN) correspondant au véhicule dans son entier ; il s'agit habituellement du numéro de série du châssis ou du numéro du cadre.

VehicleIdentificationNumber ::= IA5String(SIZE(17))

Attribution de valeur : conformément à la norme ISO 3779.

2.165 VehicleIdentificationNumberRecordArray

Génération 2 :

Le numéro d'identification du véhicule plus les métadonnées servant au protocole de téléchargement.

VehicleIdentificationNumberRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF VehicleIdentificationNumber

}

recordType indique le type d'enregistrement (VehicleIdentificationNumber). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VehicleIdentificationNumber exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne le jeu de numéros d'identification de véhicule.

2.166 VehicleRegistrationIdentification

Identification d'un véhicule, unique à l'échelle européenne (VRN et ~~État membre~~ **Partie contractante**).

VehicleRegistrationIdentification ::= SEQUENCE {

vehicleRegistrationNation	NationNumeric,
vehicleRegistrationNumber	VehicleRegistrationNumber

}

vehicleRegistrationNation indique le pays d'immatriculation du véhicule.

vehicleRegistrationNumber indique le numéro d'immatriculation du véhicule (VRN).

2.166a VehicleRegistrationIdentificationRecordArray

Génération 2, version 2 :

Identification du véhicule (VehicleRegistrationIdentification) plus les métadonnées servant au protocole de téléchargement.

VehicleRegistrationIdentificationRecordArray ::= SEQUENCE {

recordType	**RecordType,**
recordSize	**INTEGER(1..65535),**
noOfRecords	**INTEGER(0..65535),**
records	**SET SIZE(noOfRecords) OF VehicleRegistrationIdentification**

}

recordType indique le type d'enregistrement (VehicleRegistrationIdentification). Attribution de valeur : voir RecordType.

recordSize indique la taille des enregistrements de type VehicleRegistrationIdentification exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne le jeu d'enregistrements de données d'identification de véhicules.

2.167 VehicleRegistrationNumber

Numéro d'immatriculation du véhicule (VRN). Le numéro d'immatriculation est attribué par l'autorité compétente en matière d'immatriculation des véhicules.

VehicleRegistrationNumber ::= SEQUENCE {

codePage INTEGER (0..255),

vehicleRegNumber OCTET STRING (SIZE(13))

}

codePage spécifie un jeu de caractères défini au chapitre 4.

vehicleRegNumber indique un VRN codé à l'aide du jeu de caractères spécifié.

Attribution de valeur : propre à chaque pays.

2.168 VehicleRegistrationNumberRecordArray

Génération 2**, version 1** :

Le numéro d'immatriculation du véhicule plus les métadonnées servant au protocole de téléchargement.

VehicleRegistrationNumberRecordArray ::= SEQUENCE {

recordType RecordType,

recordSize INTEGER(1..65535),

noOfRecords INTEGER(0..65535),

records SET SIZE(noOfRecords) OF VehicleRegistrationNumber

}

recordType indique le type d'enregistrement (VehicleRegistrationNumber). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VehicleRegistrationNumber exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne le jeu de numéros d'immatriculation de véhicule.

2.169 VuAbility

Génération 2 :

Informations enregistrées dans la mémoire d'une UEV concernant sa compatibilité avec les cartes tachygraphiques de génération 1 (exigence 121 de ~~l'annexe~~ **l'appendice** 1C).

VuAbility ::= OCTET STRING (SIZE(1))

Attribution de valeur − Octet aligné : 'xxxxxxxa'B (8 octets)

Pour la capacité à prendre en charge la génération 1 :

‘a’B compatibilité avec les cartes tachygraphiques de génération 1 :

‘0’ B compatible avec la génération 1

‘1’ B incompatible avec la génération 1

‘xxxxxxx’B réservé pour une utilisation future

2.170 VuActivityDailyData

Génération 1 :

Informations enregistrées dans la mémoire d’une UEV concernant les changements d’activité, de situation de conduite et/ou de situation de carte pour un jour civil donné (exigence 084 de ~~l’annexe~~ **l’appendice** 1B et exigences 105, 106 et 107 de ~~l’annexe~~ **l’appendice** 1C), ainsi que l’état des lecteurs à 00 h 00 ce jour-là.

VuActivityDailyData ::= SEQUENCE {

noOfActivityChanges INTEGER SIZE(0..1440),

activityChangeInfos SET SIZE(noOfActivityChanges) OF ActivityChangeInfo

}

noOfActivityChanges indique le nombre de mots ActivityChangeInfo que comporte le jeu d’enregistrements de type activityChangeInfos.

activityChangeInfos désigne le jeu de mots ActivityChangeInfo enregistrés dans l’UEV pour le jour considéré. Il comprend toujours deux mots ActivityChangeInfo indiquant l’état des deux lecteurs à 00 h 00 ce jour-là.

2.171 VuActivityDailyRecordArray

Génération 2 :

Informations enregistrées dans la mémoire d’une UEV concernant les changements d’activité, de situation de conduite et/ou de situation de carte pour un jour civil donné (exigence 105, 106 et 107 de ~~l’annexe~~ **l’appendice** 1C), ainsi que l’état des lecteurs à 00 h 00 ce jour-là.

VuActivityDailyRecordArray ::= SEQUENCE {

recordType RecordType,

recordSize INTEGER(1..65535),

noOfRecords INTEGER(0..65535),

records SET SIZE(noOfRecords) OF ActivityChangeInfo

}

recordType indique le type d’enregistrement (ActivityChangeInfo). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type ActivityChangeInfo exprimée en octets.

noOfRecords indique le nombre d’enregistrements dans le jeu d’enregistrements correspondant.

records désigne le jeu de mots ActivityChangeInfo enregistrés dans l’UEV pour le jour considéré. Il comprend toujours deux mots ActivityChangeInfo indiquant l’état des deux lecteurs à 00 h 00 ce jour-là.

2.172 VuApprovalNumber

Numéro d'homologation de l'unité embarquée sur le véhicule.

Génération 1 :

VuApprovalNumber ::= IA5String(SIZE(8))

Attribution de valeur : non spécifié.

Génération 2 :

VuApprovalNumber ::= IA5String(SIZE(16))

Attribution de valeur : le numéro d'homologation doit être indiqué tel qu'il est publié sur le site Web ~~de la Commission européenne correspondant~~ **du laboratoire chargé des essais d'interopérabilité**, par exemple en incluant les traits d'union. Le numéro d'homologation doit être aligné à gauche.

2.173 VuCalibrationData

Génération 1 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les étalonnages de l'appareil ~~d'enregistrement~~ **de contrôle** (exigence 098 de ~~l'annexe~~ **l'appendice** 1B).

VuCalibrationData ::= SEQUENCE {

noOfVuCalibrationRecords	INTEGER(0..255),
vuCalibrationRecords	SET SIZE(noOfVuCalibrationRecords) OF VuCalibrationRecord

}

noOfVuCalibrationRecords indique le nombre d'enregistrements que contient le jeu de données vuCalibrationRecords.

vuCalibrationRecords désigne le jeu d'enregistrements d'étalonnage.

2.174 VuCalibrationRecord

Informations enregistrées dans la mémoire d'une unité embarquée concernant un étalonnage particulier de l'appareil ~~d'enregistrement~~ **de contrôle** (exigence 098 de ~~l'annexe~~ **l'appendice** 1B et exigences 119 et 120 de ~~l'annexe~~ **l'appendice** 1C).

Génération 1:

VuCalibrationRecord ::= SEQUENCE {

calibrationPurpose	CalibrationPurpose,
workshopName	Name,
workshopAddress	Address,
workshopCardNumber	FullCardNumber,
workshopCardExpiryDate	TimeReal,
vehicleIdentificationNumber	VehicleIdentificationNumber,
vehicleRegistrationIdentification	VehicleRegistrationIdentification,
wVehicleCharacteristicConstant	W-VehicleCharacteristicConstant,
kConstantOfRecordingEquipment	K-ConstantOfRecordingEquipment,
lTyreCircumference	L-TyreCircumference,
tyreSize	TyreSize,

authorisedSpeed	SpeedAuthorised,
oldOdometerValue	OdometerShort,
newOdometerValue	OdometerShort,
oldTimeValue	TimeReal,
newTimeValue	TimeReal,
nextCalibrationDate	TimeReal

}

calibrationPurpose indique la raison de l'étalonnage.

workshopName, workshopAddress indiquent les nom et adresse de l'atelier.

workshopCardNumber identifie la carte d'atelier utilisée lors de l'étalonnage.

workshopCardExpiryDate indique la date d'expiration de la carte.

vehicleIdentificationNumber indique le VIN.

vehicleRegistrationIdentification contient le VRN et ~~l'État membre~~ **la Partie contractante** d'immatriculation.

wVehicleCharacteristicConstant indique le coefficient caractéristique du véhicule.

kConstantOfRecordingEquipment indique la constante de l'appareil de contrôle.

lTyreCircumference indique la circonférence effective des pneumatiques.

tyreSize désigne la dimension des pneumatiques montés sur le véhicule.

authorisedSpeed indique la vitesse autorisée du véhicule.

oldOdometerValue, **newOdometerValue** indiquent les ancienne et nouvelle valeurs affichées par le compteur kilométrique.

oldTimeValue, newTimeValue indiquent les anciennes et nouvelles dates et heures.

nextCalibrationDate indique la date du prochain étalonnage correspondant au type spécifié dans **CalibrationPurpose** et auquel l'organisme d'inspection agréé doit procéder.

Génération 2**, version 1** :

VuCalibrationRecord ::= SEQUENCE {

calibrationPurpose	CalibrationPurpose,
workshopName	Name,
workshopAddress	Address,
workshopCardNumber	FullCardNumber,
workshopCardExpiryDate	TimeReal,
vehicleIdentificationNumber	VehicleIdentificationNumber,
vehicleRegistrationIdentification	VehicleRegistrationIdentification,
wVehicleCharacteristicConstant	W-VehicleCharacteristicConstant,
kConstantOfRecordingEquipment	K-ConstantOfRecordingEquipment,
lTyreCircumference	L-TyreCircumference,
tyreSize	TyreSize,
authorisedSpeed	SpeedAuthorised,
oldOdometerValue	OdometerShort,
newOdometerValue	OdometerShort,
oldTimeValue	TimeReal,

newTimeValue	TimeReal,
nextCalibrationDate	TimeReal,
sealDataVu	SealDataVu

}

Outre les éléments de données de la structure de génération 1, l'élément de données suivant est utilisé :

sealDataVu fournit des informations sur les scellements apposés sur les différents composants du véhicule.

Génération 2, version 2 :

VuCalibrationRecord ::= SEQUENCE {

calibrationPurpose	**CalibrationPurpose,**
workshopName	**Name,**
workshopAddress	**Address,**
workshopCardNumber	**FullCardNumber,**
workshopCardExpiryDate	**TimeReal,**
vehicleIdentificationNumber	**VehicleIdentificationNumber,**
vehicleRegistrationIdentification	**VehicleRegistrationIdentification,**
wVehicleCharacteristicConstant	**W-VehicleCharacteristicConstant,**
kConstantOfRecordingEquipment	**K-ConstantOfRecordingEquipment,**
lTyreCircumference	**L-TyreCircumference,**
tyreSize	**TyreSize,**
authorisedSpeed	**SpeedAuthorised,**
oldOdometerValue	**OdometerShort,**
newOdometerValue	**OdometerShort,**
oldTimeValue	**TimeReal,**
newTimeValue	**TimeReal,**
nextCalibrationDate	**TimeReal,**
sensorSerialNumber	**SensorSerialNumber,**
sensorGNSSSerialNumber	**SensorGNSSSerialNumber,**
rcmSerialNumber	**RemoteCommunicationModuleSerialNumber,**
sealDataVu	**SealDataVu,**
byDefaultLoadType	**LoadType,**
calibrationCountry	**NationNumeric,**
calibrationCountryTimestamp	**TimeReal**

}

Outre les éléments de données de la structure de génération 1, les éléments suivants sont utilisés :

sensorSerialNumber indique le numéro de série du capteur de mouvement couplé avec l'unité embarquée à la fin de l'étalonnage.

sensorGNSSSerialNumber indique, le cas échéant, le numéro de série du dispositif GNSS externe couplé avec l'unité embarquée à la fin de l'étalonnage.

rcmSerialNumber indique, le cas échéant, le numéro de série du dispositif de communication à distance couplé avec l'unité embarquée à la fin de l'étalonnage.

sealDataVu fournit des informations sur les scellements apposés sur les différents composants du véhicule.

byDefaultLoadType indique le type de chargement par défaut du véhicule (uniquement présent dans la version 2).

calibrationCountry désigne le pays dans lequel l'étalonnage a été effectué.

calibrationCountryTimestamp indique la date et l'heure auxquelles la position utilisée pour déterminer le pays dans lequel l'étalonnage a été effectué a été fournie par le récepteur GNSS.

2.175 VuCalibrationRecordArray

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les étalonnages successifs de l'appareil ~~d'enregistrement~~ **de contrôle** (exigences 119 et 120 de ~~l'annexe~~ **l'appendice** 1C).

VuCalibrationRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF VuCalibrationRecord

}

recordType indique le type d'enregistrement (VuCalibrationRecord). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VuCalibrationRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne le jeu d'enregistrements d'étalonnage.

2.176 VuCardIWData

Génération 1 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les cycles d'insertion et de retrait des cartes de conducteur ou d'atelier (exigence 081 de ~~l'annexe~~ **l'appendice** 1B et exigence 103 de ~~l'annexe~~ **l'appendice** 1C).

VuCardIWData ::= SEQUENCE {

noOfIWRecords	INTEGER(0..2^{16}-1),
vuCardIWRecords	SET SIZE(noOfIWRecords) OF VuCardIWRecord

}

noOfIWRecords indique le nombre d'enregistrements dans le jeu vuCardIWRecords

vuCardIWRecords désigne un jeu d'enregistrements relatifs aux cycles d'insertion et de retrait de cartes.

2.177 VuCardIWRecord

Informations enregistrées dans la mémoire d'une unité embarquée concernant les cycles d'insertion et de retrait d'une carte de conducteur ou d'atelier (exigence 081 de ~~l'annexe~~ **l'appendice** 1B et exigence 102 de ~~l'annexe~~ **l'appendice** 1C).

Génération 1 :

VuCardIWRecord ::= SEQUENCE {

cardHolderName	HolderName,
fullCardNumber	FullCardNumber,
cardExpiryDate	TimeReal,
cardInsertionTime	TimeReal,
vehicleOdometerValueAtInsertion	OdometerShort,
cardSlotNumber	CardSlotNumber,
cardWithdrawalTime	TimeReal,
vehicleOdometerValueAtWithdrawal	OdometerShort,
previousVehicleInfo	PreviousVehicleInfo,
manualInputFlag	ManualInputFlag

}

cardHolderName indique les nom et prénom(s) du détenteur de la carte de conducteur ou d'atelier, tels qu'ils sont enregistrés sur celle-ci.

fullCardNumber indique le type et le numéro de la carte ainsi que ~~l'État membre~~ **la Partie contractante** l'ayant délivrée, tels qu'enregistrés sur celle-ci.

cardExpiryDate indique la date d'expiration de la carte telle qu'enregistrée sur celle-ci.

cardInsertionTime indique la date et l'heure d'insertion de la carte.

vehicleOdometerValueAtInsertion indique la valeur affichée par le compteur kilométrique lors de l'insertion de la carte.

cardSlotNumber indique le lecteur dans lequel la carte est insérée.

cardWithdrawalTime indique la date et l'heure de retrait de la carte.

vehicleOdometerValueAtWithdrawal indique la valeur affichée par le compteur kilométrique lors du retrait de la carte.

previousVehicleInfo contient des informations sur le précédent véhicule utilisé par le conducteur, telles qu'enregistrées sur la carte.

manualInputFlag est un code permettant de savoir si le détenteur de la carte a procédé ou non à la saisie manuelle d'activités du conducteur lors de l'insertion de la carte.

Génération 2:

VuCardIWRecord ::= SEQUENCE {

cardHolderName	HolderName,
fullCardNumberAndGeneration	FullCardNumberAndGeneration,
cardExpiryDate	TimeReal,
cardInsertionTime	TimeReal,
vehicleOdometerValueAtInsertion	OdometerShort,
cardSlotNumber	CardSlotNumber,
cardWithdrawalTime	TimeReal,

vehicleOdometerValueAtWithdrawal	OdometerShort,
previousVehicleInfo	PreviousVehicleInfo,
manualInputFlag	ManualInputFlag

}

Au lieu de fullCardNumber, la structure de données de génération 2 comporte l'élément de données suivant :

fullCardNumberAndGeneration indique le type, le numéro et la génération de la carte ainsi que ~~l'État membre~~ **la Partie contractante** l'ayant délivrée, tels qu'enregistrés sur celle-ci.

2.178 VuCardIWRecordArray

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les cycles d'insertion et de retrait des cartes de conducteur ou d'atelier (exigence 103 de ~~l'annexe~~ **l'appendice** 1C).

VuCardIWRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF VuCardIWRecord

}

recordType indique le type d'enregistrements (VuCardIWRecord). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VuCardIWRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne un jeu d'enregistrements relatifs aux cycles d'insertion et de retrait de cartes.

2.179 VuCardRecord

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée à propos de la carte tachygraphique utilisée (exigence 132 de ~~l'annexe~~ **l'appendice** 1C).

VuCardRecord ::= SEQUENCE {

cardNumberAndGenerationInformation	**FullCardNumberAndGeneration,**
cardExtendedSerialNumber	ExtendedSerialNumber,
~~cardPersonaliserID~~	~~OCTET STRING(SIZE(1)),~~
~~typeofTachographCardID~~	~~EquipmentType,~~
cardStructureVersion	CardStructureVersion,
cardNumber	CardNumber

}

cardNumberAndGenerationInformation indique le numéro intégral ainsi que la génération de la carte utilisée (type de données 2.74).

cardExtendedSerialNumber tel qu'extrait du fichier élémentaire EF_ICC dans le MF de la carte.

~~**cardPersonaliserID** tel qu'extrait du fichier EF_ICC dans le MF de la carte.~~

~~**typeOfTachographCardId** tel qu'extrait du fichier élémentaire EF_Application_Identification dans le fichier spécialisé DF_Tachograph_G2.~~

cardStructureVersion telle qu'extraite du fichier élémentaire EF_Application_Identification sous DF_Tachograph_G2.

cardNumber tel qu'extrait du fichier élémentaire EF_Identification sous DF_Tachograph_G2.

2.180 VuCardRecordArray

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les cartes tachygraphiques utilisées avec celle-ci. Ces informations servent à l'analyse des problèmes de carte affectant l'UEV (exigence 132 de ~~l'annexe~~ **l'appendice** 1C).

VuCardRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF VuCardRecord

}

recordType indique le type d'enregistrement (VuCardRecord). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VuCardRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne un jeu d'enregistrements de cartes tachygraphiques utilisées avec l'UEV considérée.

2.181 VuCertificate

Certificat associé à la clé publique d'une unité embarquée.

VuCertificate ::= Certificate

2.182 VuCertificateRecordArray

Génération 2 :

Le certificat de l'UEV plus les métadonnées servant au protocole de téléchargement.

VuCertificateRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF VuCertificate

}

recordType indique le type d'enregistrement (VuCertificate). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VuCertificate exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant. La valeur doit être fixée à 1, car les certificats peuvent présenter des longueurs variables.

records désigne un jeu de certificats d'UEV.

2.183 VuCompanyLocksData

Génération 1 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les verrouillages d'entreprise (exigence 104 de ~~l'annexe~~ **l'appendice** 1B).

VuCompanyLocksData ::= SEQUENCE {

noOfLocks	INTEGER(0..255),
vuCompanyLocksRecords	SET SIZE(noOfLocks) OF VuCompanyLocksRecord

}

noOfLocks indique le nombre de verrouillages répertoriés dans vuCompanyLocksRecords.

vuCompanyLocksRecords désigne le jeu d'enregistrements de verrouillages d'entreprise.

2.184 VuCompanyLocksRecord

Informations enregistrées dans la mémoire d'une unité embarquée concernant un verrouillage d'entreprise particulier (exigence 104 de ~~l'annexe~~ **l'appendice** 1B et exigence 128 de ~~l'annexe~~ **l'appendice** 1C).

Génération 1 :

VuCompanyLocksRecord ::= SEQUENCE {

lockInTime	TimeReal,
lockOutTime	TimeReal,
companyName	Name
companyAddress	Address,
companyCardNumber	FullCardNumber

}

lockInTime, lockOutTime indiquent les dates et heures du verrouillage et du déverrouillage.

companyName, companyAddress indiquent les nom et adresse de l'entreprise associée au verrouillage.

companyCardNumber désigne la carte utilisée lors du verrouillage.

Génération 2:

VuCompanyLocksRecord ::= SEQUENCE {

lockInTime	TimeReal,
lockOutTime	TimeReal,
companyName	Name,
companyAddress	Address,
companyCardNumberAndGeneration	FullCardNumberAndGeneration

}

Au lieu de companyCardNumber, la structure de données de génération 2 comporte l'élément de données suivant :

companyCardNumberAndGeneration identifie la carte utilisée lors du verrouillage ainsi que sa génération.

2.185 VuCompanyLocksRecordArray

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les verrouillages d'entreprise (exigence 128 de ~~l'annexe~~ **l'appendice** 1C).

VuCompanyLocksRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF VuCompanyLocksRecord

}

recordType indique le type d'enregistrement (VuCompanyLocksRecord). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VuCompanyLocksRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant. Valeur 0..255.

records désigne le jeu d'enregistrements de verrouillages d'entreprise.

2.185a VuConfigurationLengthRange

Génération 2, version 2 :

Nombre d'octets disponibles sur une carte tachygraphique pour le stockage des configurations de l'UEV.

VuConfigurationLengthRange ::= INTEGER(0..2^{16}-1)

Attribution de valeur : voir sous-appendice 2.

2.186 VuControlActivityData

Génération 1 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les contrôles effectués à l'aide de celle-ci (exigence 102 de ~~l'annexe~~ **l'appendice** 1B).

VuControlActivityData ::= SEQUENCE {

noOfControls	INTEGER(0..20),
vuControlActivityRecords	SET SIZE(noOfControls) OF VuControlActivityRecord

}

noOfControls indique le nombre de contrôles répertoriés dans vuControlActivityRecords.

vuControlActivityRecords désigne le jeu d'enregistrements relatifs aux activités de contrôle.

2.187 VuControlActivityRecord

Informations enregistrées dans la mémoire d'une unité embarquée concernant les contrôles effectués à l'aide de celle-ci (exigence 102 de ~~l'annexe~~ **l'appendice** 1B et exigence 126 de ~~l'annexe~~ **l'appendice** 1C).

Génération 1 :

VuControlActivityRecord ::= SEQUENCE {

controlType	ControlType,
controlTime	TimeReal,
controlCardNumber	FullCardNumber,
downloadPeriodBeginTime	TimeReal,
downloadPeriodEndTime	TimeReal

}

controlType indique le type de contrôle.

controlTime indique la date et l'heure du contrôle.

ControlCardNumber identifie la carte de contrôleur utilisée lors du contrôle.

downloadPeriodBeginTime indique l'heure de début de la période téléchargée, en cas de téléchargement.

downloadPeriodEndTime indique l'heure de fin de la période téléchargée, en cas de téléchargement.

Génération 2 :

VuControlActivityRecord ::= SEQUENCE {

controlType	ControlType,
controlTime	TimeReal,
controlCardNumberAndGeneration	FullCardNumberAndGeneration,
downloadPeriodBeginTime	TimeReal,
downloadPeriodEndTime	TimeReal

}

Au lieu de controlCardNumber, la structure de données de génération 2 comporte l'élément de données suivant :

controlCardNumberAndGeneration identifie la carte de contrôleur utilisée lors du contrôle ainsi que sa génération.

2.188 VuControlActivityRecordArray

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les contrôles exécutés à l'aide de celle-ci (exigence 126 de ~~l'annexe~~ **l'appendice** 1C).

VuControlActivityRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF VuControlActivityRecord

}

recordType indique le type d'enregistrement (VuControlActivityRecord). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VuControlActivityRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne le jeu d'enregistrements relatifs aux activités de contrôle de l'UEV.

2.189 VuDataBlockCounter

Compteur enregistré sur une carte et permettant de recenser séquentiellement les cycles d'insertion et de retrait de la carte dans des unités embarquées.

VuDataBlockCounter ::= BCDString(SIZE(2))

Attribution de valeur : numérotation consécutive dont la valeur maximale est égale à 9 999 et qui recommence par le numéro 0.

2.190 VuDetailedSpeedBlock

Informations enregistrées dans la mémoire d'une unité embarquée concernant l'évolution de la vitesse du véhicule pendant une minute au cours de laquelle le véhicule était en mouvement (exigence 093 de ~~l'annexe~~ **l'appendice** 1B et exigence 116 de ~~l'annexe~~ **l'appendice** 1C).

VuDetailedSpeedBlock ::= SEQUENCE {

speedBlockBeginDate	TimeReal,
speedsPerSecond	SEQUENCE SIZE(60) OF Speed

}

speedBlockBeginDate indique la date et l'heure de la première vitesse instantanée que comporte le bloc de données.

speedsPerSecond indique la séquence chronologique des vitesses mesurées toutes les secondes pendant la minute qui a commencé à la speedBlockBeginDate (incluse).

2.191 VuDetailedSpeedBlockRecordArray

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant l'évolution de la vitesse du véhicule.

VuDetailedSpeedBlockRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF VuDetailedSpeedBlock

}

recordType indique le type d'enregistrement (VuDetailedSpeedBlock). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VuDetailedSpeedBlock exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne le jeu de blocs de mesure de la vitesse instantanée.

2.192 VuDetailedSpeedData

Génération 1 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant l'évolution de la vitesse du véhicule.

VuDetailedSpeedData ::= SEQUENCE {

noOfSpeedBlocks	INTEGER(0..2^{16}-1),
vuDetailedSpeedBlocks	SET SIZE(noOfSpeedBlocks) OF VuDetailedSpeedBlock

}

noOfSpeedBlocks indique le nombre de blocs de vitesse que comporte le jeu vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks désigne le jeu de blocs de mesure de la vitesse instantanée.

2.192a VuDigitalMapVersion

Génération 2, version 2 :

Version de la carte numérique stockée dans la mémoire de l'unité embarquée (exigence 133j de l'appendice 1C).

VuDigitalMapVersion ::= IA5String(SIZE(12))

Attribution de valeur : comme spécifié sur le site Web sécurisé prévu à cet effet et mis à disposition par le laboratoire compétent pour les essais d'interopérabilité (exigence 133k de l'appendice 1C).

2.193 VuDownloadablePeriod

Dates la plus ancienne et la plus récente pour lesquelles une unité embarquée détient des données relatives aux activités des conducteurs (exigences 081, 084 ou 087 de ~~l'annexe~~ **l'appendice** 1B et exigences 102, 105 et 108 de ~~l'annexe~~ **l'appendice** 1C).

VuDownloadablePeriod ::= SEQUENCE {

minDownloadableTime	TimeReal
maxDownloadableTime	TimeReal

}

minDownloadableTime indique la date et l'heure associées à l'insertion de carte, à la saisie de lieu ou au changement d'activité le plus ancien enregistré dans la mémoire de l'UEV.

maxDownloadableTime indique la date et l'heure associées au retrait de carte, à la saisie de lieu ou au changement d'activité le plus récent enregistrés dans la mémoire de l'UEV.

2.194 VuDownloadablePeriodRecordArray

Génération 2 :

VUDownloadablePeriod plus les métadonnées servant au protocole de téléchargement.

VuDownloadablePeriodRecordArray ::= SEQUENCE {

recordType RecordType,

recordSize INTEGER(1..65535),

noOfRecords INTEGER(0..65535),

records SET SIZE(noOfRecords) OF VuDownloadablePeriod

}

recordType indique le type d'enregistrement (VuDownloadablePeriod). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VuDownloadablePeriod exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne le jeu d'enregistrements de type VuDownloadablePeriod.

2.195 VuDownloadActivityData

Informations enregistrées dans la mémoire d'une unité embarquée concernant son téléchargement le plus récent (exigence 105 de ~~l'annexe~~ **l'appendice** 1B et exigence 129 de ~~l'annexe~~ **l'appendice** 1C).

Génération 1 :

VuDownloadActivityData ::= SEQUENCE {

downloadingTime TimeReal,

fullCardNumber FullCardNumber,

companyOrWorkshopName Name

}

downloadingTime indique la date et l'heure du téléchargement.

fullCardNumber identifie la carte utilisée pour autoriser le téléchargement.

companyOrWorkshopName indique le nom de l'entreprise ou de l'atelier.

Génération 2 :

VuDownloadActivityData ::= SEQUENCE {

downloadingTime TimeReal,

fullCardNumberAndGeneration FullCardNumberAndGeneration,

companyOrWorkshopName Name

}

Au lieu de fullCardNumber, la structure de données de génération 2 comporte l'élément de données suivant :

fullCardNumberAndGeneration identifie la carte utilisée pour autoriser le téléchargement ainsi que sa génération.

2.196 VuDownloadActivityDataRecordArray

Génération 2 :

Informations relatives au dernier téléchargement de l'UEV (exigence 129 de ~~l'annexe~~ **l'appendice** 1C).

VuDownloadActivityDataRecordArray ::= SEQUENCE {

recordType RecordType,

recordSize INTEGER(1..65535),

noOfRecords INTEGER(0..65535),

records SET SIZE(noOfRecords) OF VuDownloadActivityData

}

recordType indique le type d'enregistrement (VuDownloadActivityData). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VuDownloadActivityData exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne le jeu d'enregistrements de données relatives au téléchargement.

2.197 VuEventData

Génération 1 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant des événements (exigence 094 de ~~l'annexe~~ **l'appendice** 1C, à l'exception des événements de type excès de vitesse).

VuEventData ::= SEQUENCE {

noOfVuEvents INTEGER(0..255),

vuEventRecords SET SIZE(noOfVuEvents) OF VuEventRecord

}

noOfVuEvents indique le nombre d'événements répertoriés dans le jeu vuEventRecords.

vuEventRecords désigne un jeu d'enregistrements d'événements.

2.198 VuEventRecord

Informations enregistrées dans la mémoire d'une unité embarquée concernant un événement particulier (exigence 094 de ~~l'annexe~~ **l'appendice** 1B et exigence 117 de ~~l'annexe~~ **l'appendice** 1C, à l'exception des événements de type excès de vitesse).

Génération 1 :

VuEventRecord ::= SEQUENCE {

eventType EventFaultType,

eventRecordPurpose EventFaultRecordPurpose,

eventBeginTime TimeReal,

eventEndTime TimeReal,

cardNumberDriverSlotBegin FullCardNumber,

cardNumberCodriverSlotBegin FullCardNumber,

cardNumberDriverSlotEnd FullCardNumber,

cardNumberCodriverSlotEnd FullCardNumber,

similarEventsNumber SimilarEventsNumber

}

eventType indique le type d'événement.

eventRecordPurpose indique la raison pour laquelle l'événement considéré a été enregistré.

eventBeginTime indique la date et l'heure du début de l'événement.

eventEndTime indique la date et l'heure de la fin de l'événement.

cardNumberDriverSlotBegin identifie la carte insérée dans le lecteur réservé au conducteur, au début de l'événement.

cardNumberCodriverSlotBegin identifie la carte insérée dans le lecteur réservé au co-conducteur, au début de l'événement.

cardNumberDriverSlotEnd identifie la carte insérée dans le lecteur réservé au conducteur, à la fin de l'événement.

cardNumberCodriverSlotEnd identifie la carte insérée dans le lecteur réservé au co-conducteur, à la fin de l'événement.

similarEventsNumber indique le nombre d'événements semblables survenus le même jour.

Cette séquence est utilisée pour tous les événements, sauf ceux de type excès de vitesse.

Génération 2 :

VuEventRecord ::= SEQUENCE {

eventType	EventFaultType,
eventRecordPurpose	EventFaultRecordPurpose,
eventBeginTime	TimeReal,
eventEndTime	TimeReal,
cardNumberAndGenDriverSlotBegin	FullCardNumberAndGeneration,
cardNumberAndGenCodriverSlotBegin	FullCardNumberAndGeneration,
cardNumberAndGenDriverSlotEnd	FullCardNumberAndGeneration,
cardNumberAndGenCodriverSlotEnd	FullCardNumberAndGeneration,
similarEventsNumber	SimilarEventsNumber,
manufacturerSpecificEventFaultData	ManufacturerSpecificEventFaultData

}

Outre les éléments de données de la structure de génération 1, les éléments de données suivants sont utilisés :

manufacturerSpecificEventFaultData contient des informations complémentaires propres au fabricant concernant l'événement.

Au lieu de cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd et cardNumberCodriverSlotEnd, la structure de données de génération 2 comporte les éléments de données suivants :

cardNumberAndGenDriverSlotBegin identifie la carte insérée dans le lecteur réservé au conducteur ainsi que sa génération, au début de l'événement.

cardNumberAndGenCodriverSlotBegin identifie la carte insérée dans le lecteur réservé au co-conducteur ainsi que sa génération, au début de l'événement.

cardNumberAndGenDriverSlotEnd identifie la carte insérée dans le lecteur réservé au conducteur ainsi que sa génération, à la fin de l'événement.

cardNumberAndGenCodriverSlotEnd identifie la carte insérée dans le lecteur réservé au co-conducteur ainsi que sa génération, à la fin de l'événement.

Si l'événement est un conflit temporel, il convient d'interpréter eventBeginTime et eventEndTime de la manière suivante :

eventBeginTime correspond à la date et à l'heure de l'appareil de contrôle.

eventEndTime correspond à la date et à l'heure fournies par le récepteur GNSS.

2.199 VuEventRecordArray

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les événements (exigence 117 de ~~l'annexe~~ **l'appendice** 1C, à l'exception des événements de type excès de vitesse).

VuEventRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF VuEventRecord

}

recordType indique le type d'enregistrement (VuEventRecord). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VuEventRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne un jeu d'enregistrements d'événements.

2.200 VuFaultData

Génération 1 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les anomalies (exigence 096 de ~~l'annexe~~ **l'appendice** 1B).

VuFaultData ::= SEQUENCE {

noOfVuFaults	INTEGER(0..255),
vuFaultRecords	SET SIZE(noOfVuFaults) OF VuFaultRecord

}

noOfVuFaults indique le nombre d'anomalies répertoriées dans le jeu vuFaultRecords.

vuFaultRecords désigne un jeu d'enregistrements d'anomalies.

2.201 VuFaultRecord

Informations enregistrées dans la mémoire d'une unité embarquée concernant une anomalie particulière (exigence 096 de ~~l'annexe~~ **l'appendice** 1B et exigence 118 de ~~l'annexe~~ **l'appendice** 1C).

Génération 1 :

VuFaultRecord ::= SEQUENCE {

faultType	EventFaultType,
faultRecordPurpose	EventFaultRecordPurpose,
faultBeginTime	TimeReal,
faultEndTime	TimeReal,
cardNumberDriverSlotBegin	FullCardNumber,

cardNumberCodriverSlotBegin FullCardNumber,

cardNumberDriverSlotEnd FullCardNumber,

cardNumberCodriverSlotEnd FullCardNumber

}

faultType indique le type d'anomalie affectant l'appareil de contrôle.

faultRecordPurpose indique la raison pour laquelle l'anomalie considérée a été enregistrée.

faultBeginTime indique la date et l'heure du début de l'anomalie.

faultEndTime indique la date et l'heure de la fin de l'anomalie.

cardNumberDriverSlotBegin identifie la carte insérée dans le lecteur réservé au conducteur, au début de l'anomalie.

cardNumberCodriverSlotBegin identifie la carte insérée dans le lecteur réservé au co-conducteur, au début de l'anomalie.

cardNumberDriverSlotEnd identifie la carte insérée dans le lecteur réservé au conducteur, à la fin de l'anomalie.

cardNumberCodriverSlotEnd identifie la carte insérée dans le lecteur réservé au co-conducteur, à la fin de l'anomalie.

Génération 2 :

VuFaultRecord ::= SEQUENCE {

faultType EventFaultType,

faultRecordPurpose EventFaultRecordPurpose,

faultBeginTime TimeReal,

faultEndTime TimeReal,

cardNumberAndGenDriverSlotBegin FullCardNumberAndGeneration,

cardNumberAndGenCodriverSlotBegin FullCardNumberAndGeneration,

cardNumberAndGenDriverSlotEnd FullCardNumberAndGeneration,

cardNumberAndGenCodriverSlotEnd FullCardNumberAndGeneration,

manufacturerSpecificEventFaultData ManufacturerSpecificEventFaultData

}

L'élément de données suivant est utilisé en plus des éléments composant la structure de génération 1 :

manufacturerSpecificEventFaultData contient des informations complémentaires spécifiques au fabricant concernant l'anomalie.

Au lieu de cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd et cardNumberCodriverSlotEnd, la structure de données de génération 2 comporte les éléments de données suivants :

cardNumberAndGenDriverSlotBegin identifie la carte insérée dans le lecteur réservé au conducteur ainsi que sa génération, au début de l'anomalie.

cardNumberAndGenCodriverSlotBegin identifie la carte insérée dans le lecteur réservé au co-conducteur ainsi que sa génération, au début de l'anomalie.

cardNumberAndGenDriverSlotEnd identifie la carte insérée dans le lecteur réservé au conducteur ainsi que sa génération, à la fin de l'anomalie.

cardNumberAndGenCodriverSlotEnd identifie la carte insérée dans le lecteur réservé au co-conducteur ainsi que sa génération, à la fin de l'anomalie.

2.202 VuFaultRecordArray

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les anomalies (exigence 118 de ~~l'annexe~~ **l'appendice** 1C).

VuFaultRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF VuFaultRecord

}

recordType indique le type d'enregistrement (VuFaultRecord). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VuFaultRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne un jeu d'enregistrements d'anomalies.

2.203 VuGNSSADRecord

Génération 2**, version 1 :**

~~2.203. VuGNSSCDRecord~~

Informations enregistrées dans la mémoire d'une unité embarquée concernant la position GNSS du véhicule lorsque le temps de conduite ~~continue~~ **accumulé** ~~du conducteur~~ atteint un multiple de trois heures (exigences 108 et 110 de ~~l'annexe~~ **l'appendice** 1C).

~~VuGNSSCDRecord~~ **VuGNSSADRecord ::**= SEQUENCE {

timeStamp	TimeReal,
cardNumberAndGenDriverSlot	FullCardNumberAndGeneration,
cardNumberAndGenCodriverSlot	FullCardNumberAndGeneration,
gnssPlaceRecord	GNSSPlaceRecord,
vehicleOdometerValue	**OdometerShort**

}

timeStamp indique la date et l'heure auxquelles le temps de conduite ~~continue~~ **accumulé** ~~du détenteur de la carte~~ atteint un multiple de trois heures.

cardNumberAndGenDriverSlot identifie la carte insérée dans le lecteur réservé au conducteur ainsi que sa génération.

cardNumberAndGenCodriverSlot identifie la carte insérée dans le lecteur réservé au co-conducteur ainsi que sa génération.

gnssPlaceRecord contient les données relatives à la position du véhicule.

vehicleOdometerValue indique la valeur affichée par le compteur kilométrique lorsque le temps de conduite accumulée atteint un multiple de trois heures.

Génération 2, version 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant la position GNSS du véhicule lorsque le temps de conduite accumulé atteint un multiple de trois heures (exigences 108 et 110 de l'appendice 1C).

VuGNSSADRecord ::= SEQUENCE {

timestamp	**TimeReal,**
cardNumberAndGenDriverSlot	**FullCardNumberAndGeneration,**
cardNumberAndGenCodriverSlot	**FullCardNumberAndGeneration,**
gnssPlaceAuthRecord	**GNSSPlaceAuthRecord,**
vehicleOdometerValue	**OdometerShort**

}

Dans la structure de la version 2 de la génération 2, gnssPlaceRecord est remplacé par gnssPlaceAuthRecord, ce dernier contenant également l'état d'authentification de la position GNSS.

2.203a VuBorderCrossingRecord

Génération 2, version 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les passages de frontières du véhicule lorsque celui-ci a franchi la frontière d'un pays (exigence 133a et 133b de l'appendice 1C).

VuBorderCrossingRecord ::= SEQUENCE {

cardNumberAndGenDriverSlot	**FullCardNumberAndGeneration,**
cardNumberAndGenCodriverSlot	**FullCardNumberAndGeneration,**
countryLeft	**NationNumeric,**
countryEntered	**NationNumeric,**
gnssPlaceAuthRecord	**GNSSPlaceAuthRecord,**
vehicleOdometerValue	**OdometerShort**

}

cardNumberAndGenDriverSlot identifie la carte insérée dans le lecteur réservé au conducteur ainsi que sa génération.

cardNumberAndGenCoDriverSlot identifie la carte insérée dans le lecteur réservé au co-conducteur ainsi que sa génération.

countryLeft désigne le pays quitté par le véhicule sur la base de la dernière position disponible avant la détection du franchissement de la frontière. La mention « reste du monde » (code NationNumeric 'FF'H) doit être utilisée lorsque l'unité embarquée sur le véhicule n'est pas en mesure de déterminer le pays où se trouve le véhicule (par exemple, ledit pays ne figure pas sur les cartes numériques stockées dans la mémoire).

countryEntered désigne le pays dans lequel le véhicule est entré. La mention « reste du monde » (code NationNumeric 'FF'H) doit être utilisée lorsque l'unité embarquée sur le véhicule n'est pas en mesure de déterminer le pays où se trouve le véhicule (par exemple, ledit pays ne figure pas sur les cartes numériques stockées dans la mémoire).

gnssPlaceAuthRecord contient les informations relatives à la position du véhicule lorsqu'un passage de frontière est détecté, ainsi que l'état d'authentification de cette position.

vehicleOdometerValue indique la valeur affichée par le compteur kilométrique lorsque l'unité embarquée a détecté que le véhicule avait franchi la frontière d'un pays.

2.203b VuBorderCrossingRecordArray

Génération 2, version 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les passages de frontières du véhicule (exigence 133c de l'appendice 1C).

VuBorderCrossingRecordArray ::= SEQUENCE {

recordType	**RecordType,**
recordSize	**INTEGER(1..65535),**
noOfRecords	**INTEGER(0..65535),**
records	**SET SIZE(noOfRecords) OF VuBorderCrossingRecord**

}

recordType indique le type d'enregistrement (VuBorderCrossingRecord). Attribution de valeur : voir RecordType.

recordSize indique la taille des enregistrements de type VuBorderCrossingRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne un jeu d'enregistrements de passage de frontière.

2.204 VuGNSSADRecordArray

~~2.204 VuGNSSCDRecordArray~~

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant la position GNSS du véhicule lorsque le temps de conduite ~~continue~~ **accumulé** ~~du conducteur~~ atteint un multiple de trois heures (exigences 108 et 110 de ~~l'annexe~~ **l'appendice** 1C).

VuGNSSADRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE (noOfRecords) OF ~~VuGNSSCDRecord~~ **VuGNSSADRecord**}

recordType indique le type d'enregistrement (~~VuGNSSCDRecord~~ **VuGNSSADRecord**).

Attribution de valeur : voir RecordType.

recordSize indique la taille des enregistrements de type ~~VuGNSSCDRecord~~ **VuGNSSADRecord** exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne un jeu d'enregistrements de données GNSS relatives au temps de conduite ~~continue~~ **accumulé**.

2.204a VuGnssMaximalTimeDifference

Génération 2, version 2 :

Différence maximale entre l'heure vraie et l'heure réelle donnée par l'horloge de l'UEV, compte tenu de la dérive temporelle maximale spécifiée à l'exigence 41 de l'appendice 1C, et transmise par l'UEV à un dispositif GNSS externe (voir sous-appendice 12, exigence GNS_3g).

VuGnssMaximalTimeDifference ::= INTEGER(0..65535)

2.205 VuIdentification

Informations enregistrées dans la mémoire d'une unité embarquée et se rapportant à son identification (exigence 075 de ~~l'annexe~~ **l'appendice** 1B et exigences 93 et 121 de ~~l'annexe~~ **l'appendice** 1C).

Génération 1 :

VuIdentification ::= SEQUENCE {

vuManufacturerName	VuManufacturerName,
vuManufacturerAddress	VuManufacturerAddress,
vuPartNumber	VuPartNumber,
vuSerialNumber	VuSerialNumber,
vuSoftwareIdentification	VuSoftwareIdentification,
vuManufacturingDate	VuManufacturingDate,
vuApprovalNumber	VuApprovalNumber

}

vuManufacturerName indique le nom du fabricant de l'unité embarquée.

vuManufacturerAddress indique l'adresse du fabricant de l'unité embarquée.

vuPartNumber indique le numéro de référence de l'unité embarquée.

vuSerialNumber indique le numéro de série de l'unité embarquée.

vuSoftwareIdentification identifie le logiciel mis en œuvre au sein de l'unité embarquée.

vuManufacturingDate indique la date de fabrication de l'unité embarquée.

vuApprovalNumber indique le numéro d'homologation de l'unité embarquée.

Génération 2:

VuIdentification ::= SEQUENCE {

vuManufacturerName	VuManufacturerName,
vuManufacturerAddress	VuManufacturerAddress,
vuPartNumber	VuPartNumber,
vuSerialNumber	VuSerialNumber,
vuSoftwareIdentification	VuSoftwareIdentification,
vuManufacturingDate	VuManufacturingDate,
vuApprovalNumber	VuApprovalNumber,
vuGeneration	Generation,
vuAbility	VuAbility
vuDigitalMapVersion	**VuDigitalMapVersion**

}

Outre les éléments de données de la structure de génération 1, ~~L'~~ **les** élément**s** de données suivant**s** ~~est~~ **sont** utilisé**s** :

vuGeneration indique la génération de l'unité embarquée.

vuAbility donne des informations sur l'éventuelle compatibilité de l'UEV avec les cartes tachygraphiques de génération 1.

vuDigitalMapVersion indique la version de la carte numérique stockée dans la mémoire de l'unité embarquée (présent uniquement dans la version 2).

2.206 VuIdentificationRecordArray

Génération 2 :

VuIdentification plus les métadonnées servant au protocole de téléchargement.

VuIdentificationRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF VuIdentification

}

recordType indique le type d'enregistrements (VuIdentification). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VuIdentification exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne un jeu d'enregistrements de type VuIdentification.

2.207 VuITSConsentRecord

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant le consentement d'un conducteur à l'utilisation des systèmes de transport intelligents.

VuITSConsentRecord ::= SEQUENCE {

cardNumberAndGen	FullCardNumberAndGeneration,
consent	BOOLEAN

}

cardNumberAndGen identifie la carte et sa génération. Il doit s'agir d'une carte de conducteur ou d'atelier.

consent est un code qui indique si le conducteur a consenti à l'utilisation de systèmes de transport intelligents avec le véhicule ou l'unité embarquée considéré(e).

Attribution de valeur :

TRUE	indique que le conducteur a consenti à l'utilisation des systèmes de transport intelligents.
FALSE	indique que conducteur n'a pas consenti à l'utilisation des systèmes de transport intelligents.

2.208 VuITSConsentRecordArray

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant le consentement d'un conducteur à l'utilisation des systèmes de transport intelligents (exigence 200 de ~~l'annexe~~ **l'appendice** 1C).

VuITSConsentRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),

noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF VuITSConsentRecord

}

recordType indique le type d'enregistrements (VuITSConsentRecord). **Attribution de valeur** : voir RecordType.

recordSize indique la taille des enregistrements de type VuITSConsentRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne un jeu d'enregistrements relatifs au consentement à l'utilisation des systèmes de transport intelligents.

2.208a VuLoadUnloadRecord

Génération 2, version 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant une opération de chargement/déchargement saisie dans le système (exigences 133e, 133f et 133g de l'appendice 1C).

VuLoadUnloadRecord ::= SEQUENCE {

timeStamp	**TimeReal,**
operationType	**OperationType,**
cardNumberAndGenDriverSlot	**FullCardNumberAndGeneration,**
cardNumberAndGenCodriverSlot	**FullCardNumberAndGeneration,**
gnssPlaceAuthRecord	**GNSSPlaceAuthRecord,**
vehicleOdometerValue	**OdometerShort**

}

timeStamp indique la date et l'heure auxquelles l'opération de chargement/déchargement a été saisie.

operationType est le type d'opération saisi (chargement, déchargement ou chargement/déchargement simultanés).

cardNumberAndGenDriverSlot identifie la carte insérée dans le lecteur réservé au conducteur ainsi que sa génération.

cardNumberAndGenCoDriverSlot identifie la carte insérée dans le lecteur réservé au co-conducteur ainsi que sa génération.

gnssPlaceAuthRecord contient les informations relatives à la position du véhicule ainsi qu'à l'état d'authentification de cette position.

vehicleOdometerValue désigne le kilométrage lié à l'opération de chargement/ déchargement considérée.

2.208b VuLoadUnloadRecordArray

Génération 2, version 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant une opération de chargement/déchargement saisie dans le système (exigence 133h de l'appendice 1C).

VuLoadUnloadRecordArray ::= SEQUENCE {

recordType **RecordType,**

recordSize **INTEGER(1..65535),**

noOfRecords **INTEGER(0..65535),**

records **SET SIZE(noOfRecords) OF VuLoadUnloadRecord**

}

recordType indique le type d'enregistrement (VuLoadUnloadRecord). Attribution de valeur : voir RecordType.

recordSize indique la taille des enregistrements de type VuLoadUnloadRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne un jeu d'enregistrements d'opération de chargement/déchargement.

2.209 VuManufacturerAddress

Adresse du fabricant de l'unité embarquée sur le véhicule.

VuManufacturerAddress ::= Address

Attribution de valeur : non spécifié.

2.210 VuManufacturerName

Nom du fabricant de l'unité embarquée sur le véhicule.

VuManufacturerName ::= Name

Attribution de valeur : non spécifié.

2.211 VuManufacturingDate

Date de fabrication de l'unité embarquée sur le véhicule.

VuManufacturingDate ::= TimeReal

Attribution de valeur : non spécifié.

2.212 VuOverSpeedingControlData

Informations enregistrées dans la mémoire d'une unité embarquée concernant les événements de type excès de vitesse survenus depuis le dernier contrôle d'excès de vitesse (exigence 095 de ~~l'annexe~~**l'appendice** 1B et exigence 117 de ~~l'annexe~~**l'appendice** 1C).

VuOverSpeedingControlData ::= SEQUENCE {

lastOverspeedControlTime TimeReal,

firstOverspeedSince TimeReal,

numberOfOverspeedSince OverspeedNumber

}

lastOverspeedControlTime indique la date et l'heure du dernier contrôle d'excès de vitesse.

firstOverspeedSince indique la date et l'heure du premier excès de vitesse enregistré depuis ce contrôle d'excès de vitesse.

numberOfOverspeedSince indique le nombre d'événements de type excès de vitesse enregistrés depuis le dernier contrôle d'excès de vitesse.

2.213 VuOverSpeedingControlDataRecordArray

Génération 2 :

VuOverSpeedingControlData plus les métadonnées servant au protocole de téléchargement.

VuOverSpeedingControlDataRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF VuOverSpeedingControlData

}

recordType indique le type d'enregistrement (VuOverSpeedingControlData). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VuOverSpeedingControlData exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne un jeu d'enregistrements de données de contrôle d'excès de vitesse.

2.214 VuOverSpeedingEventData

Génération 1 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les événements de type excès de vitesse (exigence 094 de ~~l'annexe~~ **l'appendice** 1B).

VuOverSpeedingEventData ::= SEQUENCE {

noOfVuOverSpeedingEvents	INTEGER(0..255),
vuOverSpeedingEventRecords	SET SIZE(noOfVuOverSpeedingEvents) OF VuOverSpeedingEventRecord

}

noOfVuOverSpeedingEvents indique le nombre d'événements répertoriés dans le jeu vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords désigne un jeu d'enregistrements d'événements de type excès de vitesse.

2.215 VuOverSpeedingEventRecord

Génération 1 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les événements de type excès de vitesse (exigence 094 de ~~l'annexe~~ **l'appendice** 1B et exigence 117 de ~~l'annexe~~ **l'appendice** 1C).

VuOverSpeedingEventRecord ::= SEQUENCE {

eventType	EventFaultType,
eventRecordPurpose	EventFaultRecordPurpose,
eventBeginTime	TimeReal,
eventEndTime	TimeReal,

maxSpeedValue	SpeedMax,
averageSpeedValue	SpeedAverage,
cardNumberDriverSlotBegin	FullCardNumber,
similarEventsNumber	SimilarEventsNumber

}

eventType indique le type d'événement.

eventRecordPurpose indique la raison pour laquelle l'événement considéré a été enregistré.

eventBeginTime indique la date et l'heure du début de l'événement.

eventEndTime indique la date et l'heure de la fin de l'événement.

maxSpeedValue indique la vitesse maximale mesurée au cours de l'événement.

averageSpeedValue indique la vitesse moyenne arithmétique mesurée au cours de l'événement.

cardNumberDriverSlotBegin identifie la carte insérée dans le lecteur réservé au conducteur, au début de l'événement.

similarEventsNumber indique le nombre d'événements semblables survenus le même jour.

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les événements de type excès de vitesse (exigence 094 de ~~l'annexe~~ **l'appendice** 1B et exigence 117 de ~~l'annexe~~ **l'appendice** 1C).

VuOverSpeedingEventRecord ::= SEQUENCE {

eventType	EventFaultType,
eventRecordPurpose	EventFaultRecordPurpose,
eventBeginTime	TimeReal,
eventEndTime	TimeReal,
maxSpeedValue	SpeedMax,
averageSpeedValue	SpeedAverage,
cardNumberAndGenDriverSlotBegin	FullCardNumberAndGeneration,
similarEventsNumber	SimilarEventsNumber

}

Au lieu de cardNumberDriverSlotBegin, la structure de données de génération 2 comporte l'élément de données suivant :

cardNumberAndGenDriverSlotBegin identifie la carte insérée dans le lecteur réservé au conducteur ainsi que sa génération, au début de l'événement.

2.216 VuOverSpeedingEventRecordArray

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les événements de type excès de vitesse (exigence 117 de ~~l'annexe~~ **l'appendice** 1C).

VuOverSpeedingEventRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),

records	SET SIZE(noOfRecords) OF VuOverSpeedingEventRecord

}

recordType indique le type d'enregistrements (VuOverSpeedingEventRecord). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VuOverSpeedingEventRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne un jeu d'enregistrements d'événements de type excès de vitesse.

2.217 VuPartNumber

Numéro de référence de l'unité embarquée sur le véhicule.

VuPartNumber ::= IA5String(SIZE(16))

Attribution de valeur : propre au fabricant de l'UEV.

2.218 VuPlaceDailyWorkPeriodData

Génération 1 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les lieux de début ou de fin des périodes de travail journalières des conducteurs (exigence 087 de ~~l'annexe~~ **l'appendice** 1B et exigences 108 et 110 de ~~l'annexe~~ **l'appendice** 1C).

VuPlaceDailyWorkPeriodData ::= SEQUENCE {

noOfPlaceRecords	INTEGER(0..255),
vuPlaceDailyWorkPeriodRecords	SET SIZE(noOfPlaceRecords) OF VuPlaceDailyWorkPeriodRecord

}

noOfPlaceRecords indique le nombre d'enregistrements répertoriés dans le jeu vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords désigne un jeu de données relatives aux lieux.

2.219 VuPlaceDailyWorkPeriodRecord

Génération 1 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les lieux de début ou de fin des périodes de travail journalières des conducteurs (exigence 087 de ~~l'annexe~~ **l'appendice** 1B et exigences 108 et 110 de ~~l'annexe~~ **l'appendice** 1C).

VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {

fullCardNumber	FullCardNumber,
placeRecord	PlaceRecord

}

fullCardNumber indique le type et le numéro de la carte du conducteur et ~~l'État membre~~ **la Partie contractante** qui l'a délivrée.

placeRecord contient les informations relatives au lieu saisi dans le système.

Génération 2**, version 1 :**

Informations enregistrées dans la mémoire d'une unité embarquée concernant les lieux de début ou de fin des périodes de travail journalières des conducteurs (exigence 087 de ~~l'annexe~~ **l'appendice** 1B et exigences 108 et 110 de ~~l'annexe~~ **l'appendice** 1C).

VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {

fullCardNumberAndGeneration	FullCardNumberAndGeneration,
placeRecord	PlaceRecord

}

Au lieu de fullCardNumber, la structure de données de génération 2 comporte l'élément de données suivant :

fullCardNumberAndGeneration indique le type**, le numéro et la génération de** la carte, ainsi que ~~l'État membre~~ **la Partie contractante** qui l'a délivrée**, tels qu'enregistrés sur la carte.**

Génération 2, version 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les lieux de début ou de fin des périodes de travail journalières des conducteurs (exigence 087 de l'appendice 1B et exigences 108 et 110 de l'appendice 1C).

VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {

fullCardNumberAndGeneration	**FullCardNumberAndGeneration,**
placeAuthRecord	**PlaceAuthRecord**

}

Au lieu de placeRecord, la structure de données de génération 2, version 2, comporte l'élément de données suivant :

placeAuthRecord contient les informations relatives au lieu saisi, à la position GNSS enregistrée, à l'état d'authentification de cette position et à l'heure à laquelle elle a été déterminée.

2.220 VuPlaceDailyWorkPeriodRecordArray

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les lieux de début ou de fin des périodes de travail journalières des conducteurs (exigences 108 et 110 de ~~l'annexe~~ **l'appendice** 1C).

VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF VuPlaceDailyWorkPeriodRecord

}

recordType indique le type d'enregistrement (VuPlaceDailyWorkPeriodRecord). **Attribution de valeur** : voir RecordType.

recordSize indique la taille de l'enregistrement de type VuPlaceDailyWorkPeriodRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne un jeu d'enregistrements de lieu.

2.221 VuPrivateKey

Génération 1 :

Clé privée d'une unité embarquée sur le véhicule.

VuPrivateKey ::= RSAKeyPrivateExponent

2.222 VuPublicKey

Génération 1 :

Clé publique d'une unité embarquée sur le véhicule.

VuPublicKey ::= PublicKey

2.222a VuRtcTime

Génération 2, version 2 :

Heure de l'horloge RTC de l'UEV, transmise par l'UEV au dispositif GNSS externe (voir sous-appendice 12, exigence GNS_3f).

VuRtcTime ::= TimeReal

2.223 VuSerialNumber

Numéro de série de l'unité embarquée sur le véhicule (exigence 075 de ~~l'annexe~~ **l'appendice** 1B et exigence 93 de ~~l'annexe~~ **l'appendice** 1C).

VuSerialNumber ::= ExtendedSerialNumber

2.224 VuSoftInstallationDate

Date d'installation de la version actuelle du logiciel de l'unité embarquée sur le véhicule.

VuSoftInstallationDate ::= TimeReal

Attribution de valeur : non spécifié.

2.225 VuSoftwareIdentification

Informations enregistrées dans la mémoire d'une unité embarquée concernant le logiciel installé.

VuSoftwareIdentification ::= SEQUENCE {

vuSoftwareVersion VuSoftwareVersion,

vuSoftInstallationDate VuSoftInstallationDate

}

vuSoftwareVersion indique le numéro de version du logiciel de l'unité embarquée sur le véhicule.

vuSoftInstallationDate indique la date d'installation de cette version du logiciel.

2.226 VuSoftwareVersion

Numéro de version du logiciel de l'unité embarquée sur le véhicule.

VuSoftwareVersion ::= IA5String(SIZE(4))

Attribution de valeur : non spécifié.

2.227 VuSpecificConditionData

Génération 1 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant des conditions particulières.

VuSpecificConditionData ::= SEQUENCE {

noOfSpecificConditionRecords	INTEGER(0..2^{16}-1)
specificConditionRecords	SET SIZE (noOfSpecificConditionRecords) OF SpecificConditionRecord

}

noOfSpecificConditionRecords indique le nombre d'enregistrements répertoriés dans le jeu specificConditionRecords.

specificConditionRecords désigne un jeu d'enregistrements relatifs aux conditions particulières.

2.228 VuSpecificConditionRecordArray

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant des conditions particulières (exigence 130 de ~~l'annexe~~ **l'appendice** 1C).

VuSpecificConditionRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF SpecificConditionRecord

}

recordType indique le type d'enregistrement (SpecificConditionRecord). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type SpecificConditionRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne un jeu d'enregistrements de conditions particulières.

2.229 VuTimeAdjustmentData

Génération 1 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les remises à l'heure effectuées hors du cadre d'un étalonnage périodique (exigence 101 de ~~l'annexe~~ **l'appendice** 1B).

VuTimeAdjustmentData ::= SEQUENCE {

noOfVuTimeAdjRecords	INTEGER(0..6),
vuTimeAdjustmentRecords	SET SIZE(noOfVuTimeAdjRecords) OF VuTimeAdjustmentRecord

}

noOfVuTimeAdjRecords indique le nombre d'enregistrements répertoriés dans le jeu vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords désigne un jeu d'enregistrements de données de remise à l'heure.

2.230 Réservé pour une utilisation future

~~2.230 VuTimeAdjustmentGNSSRecord~~

2.231 Réservé pour une utilisation future

2.232 VuTimeAdjustmentRecord

~~Informations enregistrées dans la mémoire d'une unité embarquée sur le véhicule et se rapportant à une remise à l'heure effectuée sur la base des données horaires du GNSS (exigences 124 et 125 de l'annexe 1C).~~

~~VuTimeAdjustmentGNSSRecord ::= SEQUENCE {~~

~~oldTimeValue TimeReal,~~

~~newTimeValue TimeReal~~

~~}~~

~~oldTimeValue, newTimeValue indiquent les anciennes et nouvelles date et heure.~~

~~2.231. VuTimeAdjustmentGNSSRecordArray~~

~~Informations enregistrées dans la mémoire d'une unité embarquée sur le véhicule et se rapportant à une remise à l'heure effectuée sur la base des données horaires du GNSS (exigences 124 et 125 de l'annexe 1C).~~

~~VuTimeAdjustmentGNSSRecordArray SEQUENCE~~

~~recordType RecordType~~

~~recordSize INTEGER(1.65535)~~

~~noOfRecords INTEGER(0.65535)~~

~~records SET SIZE(noOfRecords)OFVuTimeAdjustmentGNSSRecord~~

~~}~~

~~recordType indique le type d'enregistrement (VuTimeAdjustmentGNSSRecord). Attribution de valeur : voir RecordType.~~

~~recordSize indique la taille des VuTimeAdjustmentGNSSRecord exprimée en octets.~~

~~noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.~~

~~records indique un jeu d'enregistrements de remises à l'heure GNSS.~~

Informations enregistrées dans la mémoire d'une unité embarquée concernant une remise à l'heure effectuée hors du cadre d'un étalonnage périodique (exigence 101 de ~~l'annexe~~ **l'appendice** 1B et exigences 124 et 125 de ~~l'annexe~~ **l'appendice** 1C).

Génération 1:

VuTimeAdjustmentRecord ::= SEQUENCE {

oldTimeValue TimeReal,

newTimeValue TimeReal,

workshopName Name,

workshopAddress Address,

workshopCardNumber FullCardNumber

}

oldTimeValue, newTimeValue indiquent les anciennes et nouvelles dates et heures.

workshopName, workshopAddress indiquent les nom et adresse de l'atelier.

workshopCardNumber identifie la carte d'atelier utilisée pour effectuer la remise à l'heure.

Génération 2 :

VuTimeAdjustmentRecord ::= SEQUENCE {

oldTimeValue TimeReal,

newTimeValue TimeReal,

workshopName Name,

workshopAddress Address,

workshopCardNumberAndGeneration FullCardNumberAndGeneration

}

Au lieu de workshopCardNumber, la structure de données de génération 2 comporte l'élément de données suivant :

workshopCardNumberAndGeneration identifie la carte d'atelier utilisée pour effectuer la remise à l'heure ainsi que sa génération.

2.233 VuTimeAdjustmentRecordArray

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les remises à l'heure effectuées hors du cadre d'un étalonnage périodique (exigences 124 et 125 de ~~l'annexe~~ **l'appendice** 1C).

VuTimeAdjustmentRecordArray ::= SEQUENCE {

recordType RecordType,

recordSize INTEGER(1..65535),

noOfRecords INTEGER(0..65535),

records SET SIZE(noOfRecords) OF VuTimeAdjustmentRecord

}

recordType indique le type d'enregistrement (VuTimeAdjustmentRecord). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VuTimeAdjustmentRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records indique un jeu d'enregistrements de données relatives à la remise à l'heure.

2.234 WorkshopCardApplicationIdentification

Informations enregistrées sur une carte d'atelier et se rapportant à l'identification de l'application de la carte (exigences 307 et 330 de ~~l'annexe~~ **de l'appendice** 1C).

Génération 1 :

WorkshopCardApplicationIdentification ::= SEQUENCE {

typeOfTachographCardId	EquipmentType,
cardStructureVersion	CardStructureVersion,
noOfEventsPerType	NoOfEventsPerType,
noOfFaultsPerType	NoOfFaultsPerType,
activityStructureLength	CardActivityLengthRange,
noOfCardVehicleRecords	NoOfCardVehicleRecords,
noOfCardPlaceRecords	NoOfCardPlaceRecords,
noOfCalibrationRecords	NoOfCalibrationRecords

}

typeOfTachographCardId spécifie le type de la carte utilisée.

cardStructureVersion spécifie la version de la structure de données mise en œuvre au sein de la carte.

noOfEventsPerType indique le nombre d'événements que la carte peut enregistrer par type d'événement.

noOfFaultsPerType indique le nombre d'anomalies que la carte peut enregistrer par type d'anomalie.

activityStructureLength indique le nombre d'octets disponibles pour le stockage des données d'activité.

noOfCardVehicleRecords indique le nombre d'enregistrements de véhicule que la carte peut contenir.

noOfCardPlaceRecords indique le nombre de lieux que la carte peut être en mesure de stocker.

noOfCalibrationRecords indique le nombre d'enregistrements de données d'étalonnage que la carte est en mesure de stocker.

Génération 2 :

WorkshopCardApplicationIdentification ::= SEQUENCE {

typeOfTachographCardId	EquipmentType,
cardStructureVersion	CardStructureVersion,
noOfEventsPerType	NoOfEventsPerType,
noOfFaultsPerType	NoOfFaultsPerType,
activityStructureLength	CardActivityLengthRange,
noOfCardVehicleRecords	NoOfCardVehicleRecords,
noOfCardPlaceRecords	NoOfCardPlaceRecords,
noOfCalibrationRecords	NoOfCalibrationRecords,
~~noOfGNSSCDRecords~~	~~NoOfGNSSCDRecords,~~
noOfGNSSADRecords	**NoOfGNSSADRecords,**
noOfSpecificConditionRecords	NoOfSpecificConditionRecords,
noOfCardVehicleUnitRecords	**NoOfCardVehicleUnitRecords**

}

Outre les éléments de données de la structure de génération 1, les éléments de données suivants sont utilisés :

~~noOfGNSSCDRecords~~**noOfGNSSADRecords** indique le nombre d'enregistrements du **temps de** conduite ~~continue~~ **accumulé en provenance du récepteur GNSS** que la carte est en mesure de stocker.

noOfSpecificConditionRecords indique le nombre d'enregistrements de conditions particulières que la carte est en mesure de stocker.

noOfCardVehicleUnitRecords indique le nombre d'enregistrements d'unités embarquées utilisées que la carte est en mesure de stocker.

2.234a WorkshopCardApplicationIdentificationV2

Génération 2, version 2 :

Informations enregistrées sur une carte d'atelier et se rapportant à l'identification de l'application de la carte (exigence 330a de l'appendice 1C).

WorkshopCardApplicationIdentificationV2 ::= SEQUENCE {

lengthOfFollowingData	**LengthOfFollowingData,**
noOfBorderCrossingRecords	**NoOfBorderCrossingRecords,**
noOfLoadUnloadRecords	**NoOfLoadUnloadRecords,**
noOfLoadTypeEntryRecords	**NoOfLoadTypeEntryRecords,**
vuConfigurationLengthRange	**VuConfigurationLengthRange**

}

lengthOfFollowingData indique le nombre d'octets consécutifs dans l'enregistrement.

noOfBorderCrossingRecords indique le nombre d'enregistrements de passage de frontière qu'une carte d'atelier est en mesure de stocker.

noOfLoadUnloadRecords indique le nombre d'enregistrements d'opération de chargement/déchargement qu'une carte d'atelier est en mesure de stocker.

noOfLoadTypeRecords indique le nombre d'enregistrements de type de chargement qu'une carte d'atelier est en mesure de stocker.

vuConfigurationLengthRange indique le nombre d'octets disponibles sur une carte tachygraphique pour le stockage des configurations de l'UEV.

2.234b WorkshopCardCalibrationAddData

Génération 2, version 2 :

Informations enregistrées sur une carte d'atelier concernant les données supplémentaires (par exemple, le type de chargement par défaut) saisies pendant un étalonnage (exigence 356l de l'appendice 1C).

WorkshopCardCalibrationAddData ::= SEQUENCE {

calibrationPointerNewestRecord	**INTEGER(0..NoOfCalibrationRecords -1),**
workshopCardCalibrationAddDataRecords	**SET SIZE(NoOfCalibrationRecords) OF WorkshopCardCalibrationAddDataRecord**

}

calibrationPointerNewestRecord est l'indice du plus récent enregistrement de données supplémentaires d'étalonnage.

Attribution de valeur : nombre correspondant au numérateur de l'enregistrement de données d'étalonnage supplémentaires, commençant par une série de '0' pour la première occurrence d'un enregistrement de données d'étalonnage supplémentaires dans la structure considérée.

workshopCardCalibrationAddDataRecords désigne le jeu d'enregistrements contenant les anciennes date et heure, le numéro d'identification du véhicule et son type de chargement par défaut.

2.234c WorkshopCardCalibrationAddDataRecord

Génération 2, version 2 :

Informations enregistrées sur une carte d'atelier concernant le type de chargement par défaut saisi pendant un étalonnage (exigence 356k de l'appendice 1C).

WorkshopCardCalibrationAddDataRecord ::= SEQUENCE {

oldTimeValue	**TimeReal,**
vehicleIdentificationNumber	**VehicleIdentificationNumber,**
byDefaultLoadType	**LoadType,**
calibrationCountry	**NationNumeric,**
calibrationCountryTimestamp	**TimeReal**

}

oldTimeValue indique les anciennes date et heure contenues dans l'enregistrement de type WorkshopCardCalibrationRecord correspondant.

vehicleIdentificationNumber indique le numéro d'identification du véhicule, qui figure également dans l'enregistrement de type WorkshopCardCalibrationRecord correspondant.

byDefaultLoadType indique le type de chargement par défaut du véhicule (présent uniquement dans la version 2).

calibrationCountry désigne le pays dans lequel l'étalonnage a été effectué.

calibrationCountryTimestamp indique la date et l'heure auxquelles la position utilisée pour déterminer ce pays a été fournie par le récepteur GNSS.

2.235 WorkshopCardCalibrationData

Informations enregistrées sur une carte d'atelier concernant les activités d'atelier réalisées avec cette carte (exigences 314, 316, 337 et 339 de ~~l'annexe~~ **l'appendice** 1C).

WorkshopCardCalibrationData ::= SEQUENCE {

calibrationTotalNumber	INTEGER(0 .. 2^{16}-1),
calibrationPointerNewestRecord	INTEGER(0 .. NoOfCalibrationRecords-1),
calibrationRecords	SET SIZE(NoOfCalibrationRecords) OF WorkshopCardCalibrationRecord

}

calibrationTotalNumber indique le nombre total d'étalonnages effectués avec la carte.

calibrationPointerNewestRecord est l'indice du plus récent enregistrement d'étalonnage mis à jour.

Attribution de valeur : nombre correspondant au numérateur de l'enregistrement d'étalonnage, commençant par une série de '0' pour la première occurrence d'un enregistrement d'étalonnage dans la structure.

calibrationRecords désigne le jeu d'enregistrements contenant des données relatives aux étalonnages et/ou aux remises à l'heure.

2.236 WorkshopCardCalibrationRecord

Informations enregistrées sur une carte d'atelier concernant un étalonnage effectué avec celle-ci (exigences 314 et 337 de ~~l'annexe~~ **l'appendice** 1C).

Génération 1 :

WorkshopCardCalibrationRecord ::= SEQUENCE {

calibrationPurpose	CalibrationPurpose,
vehicleIdentificationNumber	VehicleIdentificationNumber,
vehicleRegistration	VehicleRegistrationIdentification,
wVehicleCharacteristicConstant	W-VehicleCharacteristicConstant,
kConstantOfRecordingEquipment	K-ConstantOfRecordingEquipment,
lTyreCircumference	L-TyreCircumference,
tyreSize	TyreSize,
authorisedSpeed	SpeedAuthorised,
oldOdometerValue	OdometerShort,
newOdometerValue	OdometerShort,
oldTimeValue	TimeReal,
newTimeValue	TimeReal,
nextCalibrationDate	TimeReal,
vuPartNumber	VuPartNumber,
vuSerialNumber	VuSerialNumber,
sensorSerialNumber	SensorSerialNumber

}

calibrationPurpose indique la raison de l'étalonnage.

vehicleIdentificationNumber indique le VIN.

vehicleRegistration contient le VRN et ~~l'État membre~~ **la Partie contractante** d'immatriculation.

wVehicleCharacteristicConstant indique le coefficient caractéristique du véhicule.

kConstantOfRecordingEquipment indique la constante de l'appareil de contrôle.

lTyreCircumference indique la circonférence effective des pneumatiques.

tyreSize est la désignation des dimensions des pneumatiques montés sur le véhicule.

authorisedSpeed indique la vitesse maximale autorisée du véhicule.

oldOdometerValue, **newOdometerValue** indiquent les ancienne et nouvelle valeurs affichées par le compteur kilométrique.

oldTimeValue, newTimeValue indiquent les anciennes et nouvelles dates et heures.

nextCalibrationDate indique la date du prochain étalonnage correspondant au type spécifié dans CalibrationPurpose et auquel l'autorité d'inspection agréée doit procéder.

vuPartNumber, **vuSerialNumber** et **sensorSerialNumber** constituent les éléments de données nécessaires à l'identification de l'appareil ~~d'enregistrement~~ **de contrôle**.

Génération 2:

WorkshopCardCalibrationRecord ::= SEQUENCE {

calibrationPurpose	CalibrationPurpose,
vehicleIdentificationNumber	VehicleIdentificationNumber,
vehicleRegistration	VehicleRegistrationIdentification,
wVehicleCharacteristicConstant	W-VehicleCharacteristicConstant,
kConstantOfRecordingEquipment	K-ConstantOfRecordingEquipment,
lTyreCircumference	L-TyreCircumference,
tyreSize	TyreSize,
authorisedSpeed	SpeedAuthorised,
oldOdometerValue	OdometerShort,
newOdometerValue	OdometerShort,
oldTimeValue	TimeReal,
newTimeValue	TimeReal,
nextCalibrationDate	TimeReal,
vuPartNumber	VuPartNumber,
vuSerialNumber	VuSerialNumber,
sensorSerialNumber	SensorSerialNumber,
sensorGNSSSerialNumber	SensorGNSSSerialNumber,
rcmSerialNumber	RemoteCommunicationModuleSerialNumber,
sealDataCard	SealDataCard

}

Les éléments de données suivants sont utilisés en plus des éléments composant la structure de génération 1 :

sensorGNSSSerialNumber identifie un dispositif GNSS externe.

rcmSerialNumber identifie un module de communication à distance.

sealDataCard donne des informations sur les scellements apposés sur les différents composants du véhicule.

2.237 WorkshopCardHolderIdentification

Informations enregistrées sur une carte d'atelier et se rapportant à l'identification du détenteur de la carte (exigences 311 et 334 de ~~l'annexe~~ **l'appendice** 1C).

WorkshopCardHolderIdentification ::= SEQUENCE {

workshopName	Name,
workshopAddress	Address,
cardHolderName	HolderName,
cardHolderPreferredLanguage	Language

}

workshopName indique le nom de l'atelier du détenteur de la carte.

workshopAddress indique l'adresse de l'atelier du détenteur de la carte.

cardHolderName indique les nom et prénom(s) du détenteur (par exemple, le nom du mécanicien).

cardHolderPreferredLanguage indique la langue habituelle du détenteur de la carte.

2.238 WorkshopCardPIN

Numéro d'identification personnel (PIN) de la carte d'atelier (exigences 309 et 332 de ~~l'annexe~~ **l'appendice** 1C).

WorkshopCardPIN ::= IA5String(SIZE(8))

Attribution de valeur : le PIN connu du détenteur de la carte, complété à droite par une série d'octets 'FF' pouvant aller jusqu'à 8 octets.

2.239 W-VehicleCharacteristicConstant

Coefficient caractéristique du véhicule (définition k)).

W-VehicleCharacteristicConstant ::= INTEGER(0..2^{16}-1))

Attribution de valeur : impulsions par kilomètre dans la plage de fonctionnement 0 à 64 255 imp/km.

2.240 VuPowerSupplyInterruptionRecord

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les événements de type interruption de l'alimentation électrique (exigence 117 de ~~l'annexe~~ **l'appendice** 1C).

VuPowerSupplyInterruptionRecord ::= SEQUENCE {

eventType	EventFaultType,
eventRecordPurpose	EventFaultRecordPurpose,
eventBeginTime	TimeReal,
eventEndTime	TimeReal,
cardNumberAndGenDriverSlotBegin	FullCardNumberAndGeneration,
cardNumberAndGenDriverSlotEnd	FullCardNumberAndGeneration,
cardNumberAndGenCodriverSlotBegin	FullCardNumberAndGeneration,
cardNumberAndGenCodriverSlotEnd	FullCardNumberAndGeneration,
similarEventsNumber	SimilarEventsNumber

}

eventType indique le type d'événement.

eventRecordPurpose indique la raison de l'enregistrement de l'événement considéré.

eventBeginTime indique la date et l'heure du début de l'événement.

eventEndTime indique la date et l'heure de la fin de l'événement.

cardNumberAndGenDriverSlotBegin identifie la carte insérée dans le lecteur réservé au conducteur ainsi que sa génération, au début de l'événement.

cardNumberAndGenDriverSlotEnd identifie la carte insérée dans le lecteur réservé au conducteur ainsi que sa génération, à la fin de l'événement.

cardNumberAndGenCodriverSlotBegin identifie la carte insérée dans le lecteur réservé au co-conducteur ainsi que sa génération, au début de l'événement.

cardNumberAndGenCodriverSlotEnd identifie la carte insérée dans le lecteur réservé au co-conducteur ainsi que sa génération, à la fin de l'événement.

similarEventsNumber indique le nombre d'événements similaires survenus le même jour.

2.241 VuPowerSupplyInterruptionRecordArray

Génération 2 :

Informations enregistrées dans la mémoire d'une unité embarquée concernant les événements de type interruption de l'alimentation électrique (exigence 117 de ~~l'annexe~~ **l'appendice** 1C).

VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF VuPowerSupplyInterruptionRecord

}

recordType indique le type d'enregistrement (VuPowerSupplyInterruptionRecord). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type VuPowerSupplyInterruptionRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne un jeu d'enregistrements d'événements de type interruption de l'alimentation électrique.

2.242 VuSensorExternalGNSSCoupledRecordArray

Génération 2 :

Jeu d'enregistrements de type SensorExternalGNSSCoupledRecord plus les métadonnées servant au protocole de téléchargement.

VuSensorExternalGNSSCoupledRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF SensorExternalGNSSCoupledRecord

}

recordType indique le type d'enregistrements (SensorExternalGNSSCoupledRecord). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type SensorExternalGNSSCoupledRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records désigne un jeu d'enregistrements de données relatives au couplage entre un dispositif GNSS externe et un capteur.

2.243 VuSensorPairedRecordArray

Génération 2 :

Jeu d'enregistrements de type SensorPairedRecord plus les métadonnées servant au protocole de téléchargement.

VuSensorPairedRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	INTEGER(1..65535),
noOfRecords	INTEGER(0..65535),
records	SET SIZE(noOfRecords) OF SensorPairedRecord

}

recordType indique le type d'enregistrement (SensorPairedRecord). **Attribution de valeur :** voir RecordType.

recordSize indique la taille des enregistrements de type SensorPairedRecord exprimée en octets.

noOfRecords indique le nombre d'enregistrements dans le jeu d'enregistrements correspondant.

records indique un jeu d'enregistrements de données relatives au couplage du capteur.

3. Définitions des plages de valeurs et des dimensions

Définition des variables employées dans les définitions du chapitre 2.

TimeRealRange ::= 2^{32}-1

4. Jeux de caractères

Les chaînes IA5 se composent par définition de caractères ASCII aux termes de la norme ISO/CEI 8824-1. Pour améliorer la lisibilité et faciliter la désignation des caractères, l'attribution des valeurs est présentée ci-dessous. En cas de divergence, la norme ISO/CEI 8824-1 l'emporte sur la présente note d'information.

! " # $ % & ‘ ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?

@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _

` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~

D'autres chaînes de caractères (Address, Name, VehicleRegistrationNumber) utilisent en outre les caractères de la plage des caractères décimaux 161 – 255 des jeux de caractères standard codés sur 8 bits suivants, précisés par leur numéro de page de code :	Page de code (décimal)
Jeu de caractères standard	
ISO/CEI 8859-1 Latin-1 Européen occidental	1
ISO/CEI 8859-2 Latin-2 Européen central	2
ISO/CEI 8859-3 Latin-3 Européen du sud	3
ISO/CEI 8859-5 Latin / Cyrillique	5
ISO/CEI 8859-7 Latin / Grec	7
ISO/CEI 8859-9 Latin-5 Turc	9
ISO/CEI 8859-13 Latin-7 Balte	13
ISO/CEI 8859-15 Latin-9	15
ISO/CEI 8859-16 Latin-10 Européen du sud-est	16
KOI8-R Latin / Cyrillique	80
KOI8-U Latin / Cyrillique	85

5. Codage

Si les règles de codage ASN.1 sont appliquées aux différents types de données définis, leur codage doit être conforme à la norme ISO/CEI 8825-2 (variante alignée).

6. Identificateurs d'objet et identificateurs d'application

6.1. Identificateurs d'objet

Les identificateurs d'objet (OID) répertoriés dans le présent chapitre concernent exclusivement les structures de génération 2. Ces OID sont spécifiés dans le rapport technique TR-03110-3 et rappelés ici par souci d'exhaustivité. Ils figurent dans la sous-arborescence bsi-de suivante :

bsi-de OBJECT IDENTIFIER ::= {

itu-t(0) identified-organization(4) etsi(0)

reserved(127) etsi-identified-organization(0) 7

}

Identificateurs de protocole d'authentification destinés aux UEV

id-TA	OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 2}
id-TA-ECDSA	OBJECT IDENTIFIER ::= {id-TA 2}
id-TA-ECDSA-SHA-256	OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}
id-TA-ECDSA-SHA-384	OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}
id-TA-ECDSA-SHA-512	OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}

Exemple : si l'authentification de l'UEV est effectuée à l'aide de SHA-384, l'identificateur d'objet à utiliser est (en notation ASN.1) bsi-de protocols(2) smartcard(2) 2 2 4. La valeur de cet identificateur d'objet en notation par points est 0.4.0.127.0.7.2.2.2.2.4.

	Notation par points	Notation en octets
id-TA-ECDSA-SHA-256	0.4.0.127.0.7.2.2.2.2.3	‘04 00 7F 00 07 02 02 02 02 03’
id-TA-ECDSA-SHA-384	0.4.0.127.0.7.2.2.2.2.4	‘04 00 7F 00 07 02 02 02 02 04’
id-TA-ECDSA-SHA-512	0.4.0.127.0.7.2.2.2.2.5	‘04 00 7F 00 07 02 02 02 02 05’

Identificateurs de protocole d’authentification destinés aux circuits intégrés

id-CA OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 3}

id-CA-ECDH OBJECT IDENTIFIER ::= {id-CA 2}

id-CA-ECDH-AES-CBC-CMAC-128 OBJECT IDENTIFIER ::= {id-CA-ECDH 2}

id-CA-ECDH-AES-CBC-CMAC-192 OBJECT IDENTIFIER ::= {id-CA-ECDH 3}

id-CA-ECDH-AES-CBC-CMAC-256 OBJECT IDENTIFIER ::= {id-CA-ECDH 4}

Exemple : prenons le cas d’une authentification de circuit intégré devant être effectuée à l’aide de l’algorithme ECDH, ce qui entraîne une longueur de clé de session AES de 128 bits. Cette clé de session sera ensuite utilisée dans le mode opératoire CBC pour assurer la confidentialité des données et avec l’algorithme CMAC pour garantir l’authenticité des données. Par conséquent, l’identificateur d’objet à utiliser est (en notation ASN.1) bsi-de protocols(2) smartcard(2) 3 2 2. La valeur de cet identificateur d’objet en notation par points est 0.4.0.127.0.7.2.2.3.2.2.

	Notation par points	Notation en octets
id-CA-ECDH-AES-CBC-CMAC-128	0.4.0.127.0.7.2.2.3.2.2	‘04 00 7F 00 07 02 02 03 02 02’
id-CA-ECDH-AES-CBC-CMAC-192	0.4.0.127.0.7.2.2.3.2.3	‘04 00 7F 00 07 02 02 03 02 03’
id-CA-ECDH-AES-CBC-CMAC-256	0.4.0.127.0.7.2.2.3.2.4	‘04 00 7F 00 07 02 02 03 02 04’

6.2 Identificateurs d’application

Génération 2 :

L’identificateur d’application (AID) pour le dispositif GNSS externe (génération 2) est le suivant : ‘FF 44 54 45 47 4D’. Il s’agit d’un AID exclusif conforme à la norme ISO/CEI 7816-4.

Remarque : les 5 derniers octets codent le DTEGM pour le dispositif GNSS externe des tachygraphes intelligents.

L’identificateur d’application pour les cartes tachygraphiques de deuxième génération est le suivant : ‘FF 53 4D 52 44 54’. Il s’agit d’un AID exclusif conforme à la norme ISO/CEI 7816-4.

~~Appendice~~Sous-appendice 2

Spécification des cartes tachygraphiques

Table des matières

1. Introduction

1.1 Abréviations

Aux fins du présent **sous-**appendice, les abréviations suivantes sont utilisées :

CA	Condition d'accès
AES	Norme de chiffrement avancé (*Advanced Encryption Standard*)
AID	Identificateur d'application (*Application Identifier*)
TJR	Toujours
APDU	Unité de données de protocole d'application (structure d'une commande)
ATR	Réponse à la réinitialisation (*Answer to Reset*)
AUT	Authentifié
C6, C7	Contacts n^{os} 6 et 7 de la carte conformes à la norme ISO/CEI 7816-2
cc	cycle d'horloge (*Clock Cycle*)
ADC	**Autorisation du détenteur de certificat**
VDC	Vérification du détenteur de la carte
CLA	Octet de classe d'une APDU de commande
DSRC	Communication spécialisée à courte portée (*Dedicated Short Range Communication*)
DF	Fichier spécialisé (*Dedicated File*). Un DF peut contenir d'autres fichiers (EF ou DF).
OD	**Objet de données**
ECC	Cryptographie à courbe elliptique *(Elliptic Curve Cryptography)*
EF	Fichier élémentaire *(Elementary File)*
ute	Unité de temps élémentaire
G1	Génération 1
G2	Génération 2
IC	Circuit intégré *(Integrated Circuit)*
ICC	Carte à circuit intégré *(Integrated Circuit Card)*
ID	Identificateur
PIF	Périphérique d'interface
INS	Octet d'instruction d'une APDU de commande
Lc	Longueur des données entrantes pour une APDU de commande
Le	Longueur des données attendues (données sortantes pour une commande)
MF	Fichier maître (*Master File*, DF racine)
MS	Messagerie **sécurisée**
NAD	Adresse du nœud (*Node Address*) utilisée dans le protocole T=1
JMS	Jamais
P1-P2	Octets de paramètre
PIN	Numéro d'identification personnel *(Personal Identification Number)*

PTS	Sélection du protocole de transmission *(Protocol Transmission Selection)*
RESET	**Réinitialisation**
IDFC	Identificateur d'EF court
ME1-ME2	Mots d'état
TS	Caractère initial de l'ATR
V_{pp}	Tension de programmation
UEV	Unité embarquée sur le véhicule *(VU, en anglais)*
XXh	**Valeur** XX en notation hexadécimale
'**XXh**'	Valeur XX en notation hexadécimale
||	Symbole de concaténation 03||04=0304

1.2 Références

Dans le présent **sous-**appendice, il est fait référence aux normes suivantes :

ISO/CEI 7816-2	Cartes d'identification − Cartes à circuit intégré − Partie 2 : Dimensions et emplacements des contacts. ISO/CEI 7816-2:2007.
ISO/CEI 7816-3	Cartes d'identification − Cartes à circuit intégré − Partie 3 : Interface électrique et protocoles de transmission. ISO/CEI 7816-3:2006.
ISO/CEI 7816-4	Cartes d'identification − Cartes à circuit intégré − Partie 4 : Organisation, sécurité et commandes pour les échanges. ISO/CEI 7816-4:2013 et rectificatif technique 1: 2014.
ISO/CEI 7816-6	Cartes d'identification − Cartes à circuit intégré − Partie 6 : Éléments de données intersectoriels pour les échanges. ISO/CEI 7816-6:2004 et rectificatif technique 1: 2006.
ISO/CEI 7816-8	Cartes d'identification − Cartes à circuit intégré − Partie 8 : Commandes pour les opérations de sécurité. ISO/CEI 7816-8:2004.
ISO/CEI 9797-2	Technologies de l'information − Techniques de sécurité − Codes d'authentification de message (MAC) − Partie 2 : Mécanismes utilisant une fonction de hachage dédiée. ISO/CEI 9797-2:2011.

2. Caractéristiques électriques et physiques

TCS_01	Tous les signaux électriques doivent respecter la norme ISO/CEI 7816-3, sauf indication contraire.
TCS_02	L'emplacement et les dimensions des contacts de la carte doivent être conformes à la norme ISO/CEI 7816-2.

2.1 Tension d'alimentation et consommation de courant

TCS_03	La carte doit fonctionner selon les spécifications dans les limites de consommation définies par la norme ISO/CEI 7816-3.
TCS_04	La carte doit fonctionner à Vcc = 3 V (±0,3 V) ou à Vcc = 5 V (±0,5 V).

La sélection de la tension appropriée s'opère conformément à la norme ISO/CEI 7816-3.

2.2 Tension de programmation V_{pp}

TCS_05 La carte ne doit nécessiter l'application d'aucune tension de programmation au niveau de la broche C6. Il est prévu que la broche C6 d'un périphérique d'interface (PIF) ne sera pas connectée. Le contact C6 peut être connecté à la tension d'alimentation V_{cc} de la carte, mais il ne peut pas être raccordé à la masse. Cette tension ne doit donner lieu à aucune interprétation.

2.3 Génération et fréquence d'horloge

TCS_06 La carte doit fonctionner dans une plage de fréquences comprise entre 1 et 5 MHz et peut prendre en charge des fréquences supérieures. Au cours d'une même session de carte, la fréquence d'horloge peut subir des variations de l'ordre de ±2 %. La fréquence d'horloge est générée par l'unité embarquée sur le véhicule (UEV) et non par la carte elle-même. Le coefficient d'utilisation peut varier entre 40 et 60 %.

TCS_07 Il est possible d'arrêter l'horloge externe dans les conditions figurant dans le fichier EF ICC de la carte. Le premier octet du corps du fichier EF ICC programme les conditions d'application du mode Clockstop :

Inférieur	*Supérieur*		
Bit 3	**Bit 2**	**Bit 1**	
0	0	1	Clockstop autorisé, pas de niveau préférentiel
0	1	1	Clockstop autorisé, avec une préférence pour le niveau supérieur
1	0	1	Clockstop autorisé, avec une préférence pour le niveau inférieur
0	0	0	Clockstop interdit
0	1	0	Clockstop autorisé uniquement au niveau supérieur
1	0	0	Clockstop autorisé uniquement au niveau inférieur

Les bits 4 à 8 ne sont pas utilisés.

2.4 Contacts d'entrée/sortie

TCS_08 Le contact d'entrée/sortie C7 permet la réception et l'émission de données en provenance et à destination du PIF. En cours d'exploitation, la carte et le PIF ne peuvent pas fonctionner simultanément en mode émission. Dans l'éventualité où ces deux composants seraient exploités en mode émission, la carte ne courrait cependant aucun risque de détérioration. Lorsque la carte n'émet pas de données, elle passe en mode réception.

2.5 États de la carte

TCS_09 La carte fonctionne selon deux états lorsque la tension d'alimentation requise est appliquée :

État d'exploitation lors de l'exécution de commandes ou en interfaçage avec une unité ~~numérique~~ **embarquée ;**

État de repos dans tous les autres cas de figure ; dans cet état, la carte doit enregistrer toutes les données utiles.

3. Matériel et communication

3.1 Introduction

Les fonctionnalités minimales requises par les cartes tachygraphiques et les UEV pour garantir des conditions d'exploitation et d'interopérabilité satisfaisantes sont décrites dans le présent paragraphe.

Les cartes tachygraphiques sont aussi conformes que possible aux normes ISO/CEI en vigueur (et à la norme ISO/CEI 7816 en particulier). Toutefois, les commandes et les protocoles font l'objet d'une description détaillée afin de préciser certains usages restreints ou d'éventuelles différences. Sauf indication contraire, les commandes spécifiées sont pleinement conformes aux normes mentionnées.

3.2 Protocole de transmission

TCS_10 Le protocole de transmission doit être conforme à la norme ISO/CEI 7816-3 pour T = 0 et T = 1. En particulier, l'UEV doit reconnaître les demandes de prolongation du temps d'attente que lui envoie la carte.

3.2.1 Protocoles

TCS_11 La carte doit prendre en charge les protocoles **T = 0** et **T = 1**. Elle peut en outre prendre en charge d'autres protocoles orientés connexion.

TCS_12 Le protocole **T = 0** est sélectionné par défaut ; par conséquent, le lancement d'une commande **PTS** est nécessaire pour passer au protocole **T = 1**.

TCS_13 Les dispositifs doivent prendre en charge la convention directe que comportent ces deux protocoles ; la convention directe est donc obligatoire pour la carte.

TCS_14 L'ATR doit présenter l'octet **longueur de la zone de données réservée à la carte** au niveau du caractère TA3, avec comme valeur minimale 'F0h' (= 240 octets).

Les restrictions ci-après s'appliquent aux protocoles.

TCS_15 **T = 0**

- Le périphérique d'interface doit prendre en charge une réponse au niveau de l'entrée/sortie après le front montant du signal sur RESET à partir de 400 cc ;
- Le périphérique d'interface doit être à même de lire des caractères séparés par 12 ute ;
- Le périphérique d'interface doit être capable de reconnaître un caractère erroné et sa répétition, même s'ils sont séparés par 13 ute. En cas de détection d'un caractère erroné, le signal d'erreur peut se manifester à l'entrée/sortie dans un délai compris entre 1 et 2 ute. Le dispositif doit supporter un délai d'une ute ;
- Le périphérique d'interface doit accepter une ATR de 33 octets (TS+32) ;
- Si l'ATR présente le caractère TC1, le temps de garde supplémentaire (*Extra Guard Time*) prévu doit être ménagé pour les caractères transmis par le périphérique d'interface, bien que les caractères transmis par la carte puissent encore être séparés par 12 ute. Cette disposition s'applique également au caractère d'accusé de réception (ACK) transmis par la carte après l'émission d'un caractère P3 par le périphérique d'interface ;
- Le périphérique d'interface doit prendre en compte un caractère NUL émis par la carte ;

– Le périphérique d'interface doit accepter le mode complémentaire pour accusé de réception ;

– La commande GET RESPONSE ne peut pas être utilisée en mode chaînage pour obtenir des données dont la longueur pourrait excéder 255 octets.

TCS_16 **T=1**

– Octet NAD : inutilisé (l'octet NAD doit être mis à '00') ;

– Bloc S ABORT : inutilisé ;

– Bloc S erreur d'état Vpp : inutilisé ;

~~– La longueur totale de chaînage associée à une zone de données ne doit pas dépasser 255 octets (pour être garantie par le PIF) ;~~

– Le périphérique d'interface doit indiquer la longueur de la zone de données qui lui est réservée immédiatement après l'ATR : il doit émettre la demande de longueur de la zone de données du bloc S après l'ATR et la carte doit lui renvoyer la longueur correspondante. La longueur recommandée est de 254 octets ;

– La carte ne demandera pas de réajustement de la longueur d'une zone de données.

3.2.2 ATR

TCS_17 Le dispositif procède au contrôle des octets de l'ATR, conformément à la norme ISO/CEI 7816-3. Les caractères historiques de l'ATR ne sont soumis à aucune vérification.

Exemple d'ATR biprotocole de base conforme à la norme ISO/CEI 7816-3

Caractère	*Valeur*	*Remarque*
TS	'3Bh'	Indique une convention directe.
T0	'85h'	TD1 présent : présence de 5 octets historiques.
TD1	'80h'	TD2 présent : utiliser T = 0
TD2	'11h'	TA3 présent : utiliser T = 1
TA3	'XXh' ('F0h' au moins)	Longueur de la zone de données réservée à la carte
TH1à TH5	'XXh'	Caractères historiques
TCK	'XXh'	Caractère de contrôle (OU exclusif)

TCS_18 Après la réponse à la réinitialisation (ATR), le fichier maître (MF) est implicitement sélectionné. Il devient le répertoire en cours.

3.2.3 PTS

TCS_19 Le protocole par défaut est T = 0. Pour sélectionner le protocole T = 1, le dispositif doit envoyer à la carte une commande PTS (également désignée par l'abréviation PPS).

TCS_20 La carte doit prendre en charge les protocoles T = 0 et T = 1 et, par conséquent, la commande PTS de base qui permet la permutation de ces protocoles.

La commande PTS s'utilise, conformément aux dispositions de la norme ISO/CEI 7816-3, pour passer à des débits de transmission supérieurs à celui proposé par défaut par la carte au niveau de l'ATR (octet TA(1)), le cas échéant.

L'emploi de débits supérieurs est facultatif pour la carte.

TCS_21 Si la carte ne prend en charge que le débit de transmission par défaut (ou si le débit sélectionné n'est pas pris en charge), elle doit répondre correctement à la commande PTS en omettant l'octet PPS1, conformément à la norme ISO/CEI 7816-3.

Exemples de commandes PTS de base destinées à la sélection des protocoles

Caractère	*Valeur*	*Remarque*
PPSS	'FFh'	Caractère de lancement.
PPS0	'00h' or '01h'	PPS1 à PPS3 sont absents : '00h' pour sélectionner T0 ; '01h' pour sélectionner T1.
PK	'XXh'	Caractère de contrôle : 'XXh' = 'FFh' si PPS0 = '00h' ; 'XXh' = 'FEh' si PPS0 = '01h'.

3.3 Règles d'accès

TCS_22 Les règles d'accès définissent les conditions de sécurité correspondant à un mode d'accès (une commande). Ces conditions de sécurité doivent être satisfaites pour que la commande soit traitée.

TCS_23 Les conditions de sécurité applicables à la carte tachygraphique se définissent comme suit :

Abréviation	*Signification*
TJR	L'action est toujours possible et peut être exécutée sans restriction. Les APDU de commande et de réponse sont envoyées en texte clair, c'est-à-dire sans messagerie sécurisée.
JMS	L'action n'est jamais possible.
C-CLAIR	L'APDU de commande est envoyée en texte clair, c'est-à-dire sans messagerie sécurisée.
PWD	L'action ne peut être exécutée que si le PIN de la carte d'atelier a été vérifié, c'est-à-dire que l'état de sécurité interne de la carte « PIN_Verified » est défini. La commande doit être envoyée sans messagerie sécurisée.
EXT-AUT-G1	L'action ne peut être exécutée que si la commande EXTERNAL AUTHENTICATE destinée à l'authentification de génération 1 (voir **sous-**appendice 11, partie A) a abouti.
MS-MAC-G1	Les APDU de commande et de réponse doivent être exécutées avec la messagerie sécurisée de génération 1 en mode authentification uniquement (voir **sous-**appendice 11, partie A).
MS-C-MAC-G1	L'APDU de commande doit être exécutée avec la messagerie sécurisée de génération 1 en mode authentification uniquement (voir **sous-**appendice 11, partie A).
MS-R-ENC-G1	L'APDU de réponse doit être exécutée avec la messagerie sécurisée de génération 1 en mode chiffrement (voir **sous-**appendice 11, partie A), c'est-à-dire sans renvoi de code d'authentification de message.
MS-R-ENC-MAC-G1	L'APDU de réponse doit être exécutée avec la messagerie sécurisée de génération 1 en mode chiffrement puis authentification (voir **sous-**appendice 11, partie A).

Abréviation	*Signification*
MS-MAC-G2	Les APDU de commande et de réponse doivent être exécutées avec la messagerie sécurisée de génération 2 en mode authentification uniquement (voir **sous-**appendice 11, partie B).
MS-C-MAC-G2	L'APDU de commande doit être exécutée avec la messagerie sécurisée de génération 2 en mode authentification uniquement (voir **sous-**appendice 11, partie B).
MS-R-ENC-MAC-G2	L'APDU de réponse doit être exécutée avec la messagerie sécurisée de génération 2 en mode chiffrement puis authentification (voir **sous-**appendice 11, partie B).

TCS_24 Ces conditions de sécurité peuvent être associées de la manière suivante :

ET : toutes les conditions de sécurité doivent être remplies ;

OU : au moins l'une des conditions de sécurité doit être remplie.

Les règles d'accès au système de fichiers, à savoir les commandes SELECT, READ BINARY et UPDATE BINARY, sont spécifiées au chapitre 4. Les règles d'accès applicables aux autres commandes sont spécifiées dans les tableaux qui suivent. **Le terme « sans objet » qualifie une commande dont la prise en charge n'est pas obligatoire. Dans ce cas, la commande peut ou non être prise en charge, mais les conditions d'accès ne sont pas définies.**

TCS_25 Dans l'application DF Tachograph_G1, les règles d'accès suivantes sont appliquées :

Commande	**Carte de conducteur**	**Carte d'atelier**	**Carte de contrôleur**	**Carte d'entreprise**
EXTERNAL AUTHENTICATE				
• Pour l'authentification de génération 1	TJR	TJR	TJR	TJR
• Pour l'authentification de génération 2	TJR	PWD	TJR	TJR
INTERNAL AUTHENTICATE	TJR	PWD	TJR	TJR
GENERAL AUTHENTICATE	TJR	TJR	TJR	TJR
GET CHALLENGE	TJR	TJR	TJR	TJR
MSE:SET AT	TJR	TJR	TJR	TJR
MSE:SET DST	TJR	TJR	TJR	TJR
PROCESS DSRC MESSAGE	Sans objet	Sans objet	Sans objet	Sans objet
PSO: COMPUTE DIGITAL SIGNATURE	TJR OU MS-MAC-G2	TJR OU MS-MAC-G2	Sans objet	Sans objet
PSO: HASH	Sans objet	Sans objet	TJR	Sans objet
PERFORM HASH OF FILE	TJR OU MS-MAC-G2	TJR OU MS-MAC-G2	Sans objet	Sans objet
PSO: VERIFY CERTIFICATE	TJR	TJR	TJR	TJR

Commande	Carte de conducteur	Carte d'atelier	Carte de contrôleur	Carte d'entreprise
PSO: VERIFY DIGITAL SIGNATURE	Sans objet	Sans objet	TJR	Sans objet
VERIFY	Sans objet	TJR	Sans objet	Sans objet

TCS_26 Dans l'application DF Tachograph_G2, les règles d'accès suivantes sont appliquées :

Commande	Carte de conducteur	Carte d'atelier	Carte de contrôleur	Carte d'entreprise
EXTERNAL AUTHENTICATE				
• Pour l'authentification de génération 1	Sans objet	Sans objet	Sans objet	Sans objet
• Pour l'authentification de génération 2	TJR	PWD	TJR	TJR
INTERNAL AUTHENTICATE	Sans objet	Sans objet	Sans objet	Sans objet
GENERAL AUTHENTICATE	TJR	TJR	TJR	TJR
GET CHALLENGE	TJR	TJR	TJR	TJR
MSE:SET AT	TJR	TJR	TJR	TJR
MSE:SET DST	TJR	TJR	TJR	TJR
PROCESS DSRC MESSAGE	Sans objet	TJR	TJR	Sans objet
PSO: COMPUTE DIGITAL SIGNATURE	TJR OU MS-MAC-G2	TJR OU MS-MAC-G2	Sans objet	Sans objet
PSO: HASH	Sans objet	Sans objet	TJR	Sans objet
PERFORM HASH OF FILE	TJR OU MS-MAC-G2	TJR OU MS-MAC-G2	Sans objet	Sans objet
PSO: VERIFY CERTIFICATE	TJR	TJR	TJR	TJR
PSO: VERIFY DIGITAL SIGNATURE	Sans objet	Sans objet	TJR	Sans objet
VERIFY	Sans objet	TJR	Sans objet	Sans objet

TCS_27 Dans le MF, les règles d'accès suivantes sont appliquées :

Commande	*Carte de conducteur*	*Carte d'atelier*	*Carte de contrôleur*	*Carte d'entreprise*
EXTERNAL AUTHENTICATE				
• Pour l'authentification de génération 1	Sans objet	Sans objet	Sans objet	Sans objet
• Pour l'authentification de génération 2	TJR	PWD	TJR	TJR
INTERNAL AUTHENTICATE	Sans objet	Sans objet	Sans objet	Sans objet

Commande	*Carte de conducteur*	*Carte d'atelier*	*Carte de contrôleur*	*Carte d'entreprise*
GENERAL AUTHENTICATE	TJR	TJR	TJR	TJR
GET CHALLENGE	TJR	TJR	TJR	TJR
MSE:SET AT	TJR	TJR	TJR	TJR
MSE:SET DST	TJR	TJR	TJR	TJR
PROCESS DSRC MESSAGE	Sans objet	Sans objet	Sans objet	Sans objet
PSO: COMPUTE DIGITAL SIGNATURE	Sans objet	Sans objet	Sans objet	Sans objet
PSO: HASH	Sans objet	Sans objet	Sans objet	Sans objet
PERFORM HASH OF FILE ~~PSO: Hash of File~~	Sans objet	Sans objet	Sans objet	Sans objet
PSO: VERIFY CERTIFICATE	TJR	TJR	TJR	TJR
PSO: VERIFY DIGITAL SIGNATURE	**Sans objet**	**Sans objet**	**Sans objet**	**Sans objet**
VERIFY	Sans objet	TJR	Sans objet	Sans objet

TCS_28 Une carte tachygraphique peut accepter ou non une commande avec un niveau de sécurité supérieur à celui spécifié dans les conditions de sécurité. Par exemple, si la condition de sécurité est TJR (ou C-CLAIR), la carte peut accepter une commande avec messagerie sécurisée (en mode chiffrement et/ou authentification). Si la condition de sécurité impose le recours à une messagerie sécurisée avec le mode authentification, la carte tachygraphique peut accepter une commande avec messagerie sécurisée de même génération en mode chiffrement et authentification.

Remarque : les descriptions des commandes fournissent des informations complémentaires quant à leur prise en charge par les différents types de cartes tachygraphiques et les divers fichiers spécialisés (DF).

3.4 Vue d'ensemble des commandes et des codes d'erreur

Les commandes et la structure des fichiers sont issues de la norme ISO/CEI 7816-4 et sont conformes à ses dispositions.

La présente section décrit les paires d'APDU commande-réponse ci-après. Les variantes de commande prises en charge par les applications de générations 1 et 2 sont spécifiées dans les descriptions des commandes correspondantes.

Commande	*INS*
SELECT	'A4h'
READ BINARY	'B0h', 'B1h'
UPDATE BINARY	'D6h', 'D7h'
GET CHALLENGE	'84h'
VERIFY	'20h'

Commande	*INS*
GET RESPONSE	‘C0h’
PERFORM SECURITY OPERATION	‘2Ah’
- VERIFY CERTIFICATE	
- COMPUTE DIGITAL SIGNATURE	
- VERIFY DIGITAL SIGNATURE	
- HASH	
- PERFORM HASH OF FILE	
- PROCESS DSRC MESSAGE	
INTERNAL AUTHENTICATE	‘88h’
EXTERNAL AUTHENTICATE	‘82h’
MANAGE SECURITY ENVIRONMENT	‘22h’
• SET DIGITAL SIGNATURE TEMPLATE	
• SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	‘86h’

TCS_29 Les mots d’état ME1 et ME2 accompagnent tout message de réponse et indiquent l’état de traitement de la commande correspondante.

ME1	*ME2*	*Signification*
90	00	Traitement normal.
61	XX	Traitement normal. XX = nombre d’octets de réponse disponibles.
62	81	Traitement d’avertissement. Une partie des données renvoyées peut être corrompue.
63	00	Échec d’authentification (avertissement).
63	CX	Informations VDC (PIN) erronées. Compteur de tentatives restantes indiqué par ‘X’.
64	00	Erreur d’exécution − État de la mémoire rémanente inchangé. Erreur d’intégrité.
65	00	Erreur d’exécution − État de la mémoire rémanente modifié.
65	81	Erreur d’exécution − État de la mémoire rémanente modifié – Défaillance de la mémoire.
66	88	Erreur de sécurité : Total de contrôle cryptographique erroné (en cours d’envoi par messagerie sécurisée), ou Certificat erroné (pendant la vérification du certificat), ou Cryptogramme erroné (pendant l’authentification externe), ou Signature erronée (pendant la vérification de la signature).
67	00	Longueur erronée (Lc ou Le erronée).
~~68~~	~~82~~	~~Messagerie sécurisée non prise en charge.~~
68	83	Dernière commande de la chaîne attendue.

ME1	*ME2*	*Signification*
69	00	Commande interdite (pas de réponse disponible en T = 0).
69	82	État de sécurité non satisfait.
69	83	Méthode d'authentification bloquée.
69	85	Conditions d'utilisation non satisfaites.
69	86	Commande non autorisée (pas d'EF actif).
69	87	Absence d'objets de données de messagerie sécurisée attendus.
69	88	Objets de données de messagerie sécurisée incorrects.
6A	80	Paramètres incorrects dans la zone de données.
6A	82	Fichier introuvable.
6A	86	Paramètres P1-P2 erronés.
6A	88	Données désignées introuvables.
6B	00	Paramètres erronés (décalage hors de l'EF).
6C	XX	Longueur erronée ; le ME2 indique la longueur exacte. Aucune zone de données n'est renvoyée.
6D	00	Code d'instruction non pris en charge ou incorrect.
6E	00	Classe non prise en charge.
6F	00	Autres erreurs de contrôle.

D'autres mots d'état définis dans la norme ISO/CEI 7816-4 peuvent être renvoyés, même si leur fonctionnement n'est pas explicitement mentionné dans le présent sous-appendice.

Par exemple, il est possible de renvoyer les mots d'état suivants :

6881 : canal logique non pris en charge ;

6882 : messagerie sécurisée non prise en charge.

TCS_30 Si plus d'une condition d'erreur est satisfaite dans une APDU de commande, la carte peut renvoyer l'un ou l'autre des mots d'état appropriés.

3.5 Descriptions des commandes

Le présent chapitre décrit les commandes obligatoires pour les cartes tachygraphiques.

~~L'appendice~~ **Le sous-appendice** 11 (Mécanismes de sécurité communs pour les tachygraphes de générations 1 et 2) fournit des précisions sur les opérations cryptographiques impliquées.

Toutes les commandes sont décrites indépendamment du protocole employé (T = 0 ou T = 1). Les octets APDU CLA, INS, P1, P2, Lc et Le sont toujours indiqués. Si la commande décrite peut se passer de l'octet Lc ou Le, les cellules longueur, valeur et description associées à ces octets demeurent vides.

TCS_31 Si la présence des deux octets de longueur (Lc et Le) est requise et que le périphérique d'interface emploie le protocole T = 0, la commande décrite doit être scindée en deux parties : le dispositif envoie la commande décrite avec P3=Lc + données, puis il envoie une commande GET RESPONSE (voir **par 3.5.6** ~~Erreur ! Source du renvoi introuvable~~) avec P3=Le.

TCS_32 Si la présence des deux octets de longueur est requise et que Le = 0 (messagerie sécurisée) :

- En cas d'utilisation du protocole T = 1, la carte doit répondre à Le = 0 en envoyant toutes les données de sortie disponibles ;
- En cas d'utilisation du protocole T = 0, le périphérique d'interface doit envoyer la première commande avec P3=Lc + données, et la carte doit répondre (à ce Le = 0 implicite) en envoyant les octets d'état '**61La**', où La correspond au nombre d'octets de réponse disponibles. Ensuite, le dispositif doit générer une commande GET RESPONSE avec P3=La pour procéder à la lecture des données.

TCS_33 Une carte tachygraphique peut, en option, prendre en charge des zones de longueur étendue conformément à la norme ISO/CEI 7816-4. Une carte tachygraphique qui prend en charge des zones de longueur étendue doit :

- Indiquer la prise en charge de la zone de longueur étendue dans l'ATR ;
- Fournir les tailles de tampon pris en charge au moyen des informations de longueur étendue figurant dans l'EF ATR/INFO (voir **TCS_146**) ;
- Indiquer si elle prend en charge les zones de longueur étendue pour T = 1 et/ou T = 0 dans l'EF Extended Length (voir **TCS_147**) ;
- Prendre en charge les zones de longueur étendue pour les applications tachygraphiques de générations 1 et 2.

Remarques :

Toutes les commandes sont spécifiées pour les zones de longueur courte. L'utilisation d'APDU de commande de longueur étendue est décrite en détail dans la norme ISO/CEI 7816-4.

En règle générale, les commandes sont spécifiées pour le mode en clair, c'est-à-dire sans messagerie sécurisée, car la couche de messagerie sécurisée est spécifiée ~~à l'~~ **au sous-**appendice 11. Les règles d'accès à une commande indiquent clairement si la commande prend en charge ou non la messagerie sécurisée et si elle prend en charge la messagerie sécurisée de génération 1 et/ou 2. Certaines variantes de commandes sont décrites avec messagerie sécurisée afin d'illustrer l'utilisation de cette dernière.

TCS_34 L'UEV exécute la totalité du protocole d'authentification mutuelle UEV − carte de génération 2 pour une session, y compris la vérification du certificat (le cas échéant), dans le DF Tachograph, dans le DF Tachograph_G2 ou dans le MF.

3.5.1 SELECT (sélection)

Cette commande est conforme à la norme ISO/CEI 7816-4, mais elle a un usage restreint par comparaison avec la commande analogue définie dans cette norme.

Emploi de la commande SELECT :

- Sélection d'un DF d'application (sélection par nom impérative) ;
- Sélection d'un fichier élémentaire correspondant à l'ID du fichier présenté.

3.5.1.1 Sélection par nom (identificateur d'application)

Cette commande permet de sélectionner un DF d'application enregistré sur la carte.

TCS_35 Cette commande peut être exécutée à partir d'un point quelconque de la structure de fichiers (après l'ATR ou à tout autre moment).

TCS_36 La sélection d'une application réinitialise l'environnement de sécurité actif. Après avoir procédé à la sélection de l'application, plus aucune clé publique active n'est sélectionnée. La condition d'accès EXT-AUT-G1 est également perdue. Si la commande a été exécutée sans messagerie sécurisée, les clés de la session de messagerie sécurisée précédente ne sont plus disponibles.

TCS_37 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Sélection par nom (AID)
P2	1	'0Ch'	Aucune réponse attendue
Lc	1	'NNh'	Nombre d'octets envoyés à la carte (longueur de l'AID) : '06h' pour l'application tachygraphique
#6-#(5+NN)	NN	'XX..XXh'	AID : 'FF 54 41 43 48 4F' pour l'application tachygraphique de génération 1 AID : 'FF 53 4D 52 44 54' pour l'application tachygraphique de génération 2

Le système se passe de réponse à la commande SELECT (Le absent en T = 1 ou pas de réponse requise en T=0).

TCS_38 **Message de réponse (pas de réponse requise)**

Octet	*Longueur*	*Valeur*	*Description*
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- Si le logiciel ne parvient pas à trouver l'application correspondant à l'AID, il renvoie l'état de traitement '**6A82**' ;
- En T = 1, la présence de l'octet Le entraîne le renvoi de l'état '**6700**' ;
- En T = 0, si une réponse est requise après réception de la commande SELECT, le logiciel renvoie l'état '**6900**' ;
- Si l'application sélectionnée est considérée comme altérée (une erreur d'intégrité est détectée dans les attributs du fichier), le logiciel renvoie l'état de traitement '**6400**' ou ~~6581~~'**6500**'.

3.5.1.2 Sélection d'un fichier élémentaire par son identificateur

TCS_39 **Message de commande**

TCS_40 Une carte tachygraphique doit prendre en charge la génération 2 de messagerie sécurisée comme l'indique ~~l'appendice~~ **le sous-appendice** 11, partie B, pour cette variante de commande.

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Sélection d'un EF dans le DF actif

Octet	*Longueur*	*Valeur*	*Description*
P2	1	'0Ch'	Aucune réponse attendue
Lc	1	'02h'	Nombre d'octets envoyés à la carte
#6-#7	2	'XXXXh'	Identificateur de fichier

Le système se passe de réponse à la commande SELECT (Le absent en T = 1 ou pas de réponse requise en T = 0).

TCS_41 Message de réponse (pas de réponse requise)

Octet	*Longueur*	*Valeur*	*Description*
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- Si le logiciel ne parvient pas à trouver le fichier correspondant à l'identificateur de fichier, il renvoie l'état de traitement '**6A82**' ;
- En T = 1, la présence de l'octet Le entraîne le renvoi de l'état '**6700**' ;
- En T = 0, si une réponse est requise après réception de la commande SELECT, le logiciel renvoie l'état '**6900**' ;
- Si le fichier sélectionné est considéré comme altéré (une erreur d'intégrité est détectée dans les attributs du fichier), le logiciel renvoie l'état de traitement '**6400**' ou ~~6581~~'**6500**'.

3.5.2 READ BINARY (lecture des données)

Cette commande est conforme à la norme ISO/CEI 7816-4, mais elle a un usage restreint par rapport à la commande analogue définie dans cette norme.

La commande READ BINARY permet d'extraire les données enregistrées dans un fichier transparent.

La réponse de la carte consiste à renvoyer les données extraites en les encapsulant, le cas échéant, dans une structure de messagerie sécurisée.

3.5.2.1 Commande avec décalage en P1-P2

Cette commande permet au périphérique d'interface de lire les données de l'EF sélectionné sans messagerie sécurisée.

Remarque : cette commande sans messagerie sécurisée permet uniquement de lire un fichier prenant en charge la condition de sécurité TJR en mode lecture.

TCS_42 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	
INS	1	'B0h'	READ BINARY
P1	1	'XXh'	Décalage en octets à compter du début du fichier : octet le plus significatif
P2	1	'XXh'	Décalage en octets à compter du début du fichier : octet le moins significatif
Le	1	'XXh'	Longueur des données attendue. Nombre d'octets à extraire.

Remarque : le bit 8 de P1 doit être mis à 0.

TCS_43 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
#1-#X	X	'XX..XXh'	Données lues
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- Si aucun EF n'est sélectionné, le logiciel renvoie l'état de traitement '**6986**' ;
- Si les conditions de sécurité du fichier sélectionné ne sont pas remplies, la commande est interrompue par '**6982**' ;
- Si le décalage n'est pas compatible avec la taille de l'EF (décalage > taille de l'EF), le logiciel renvoie l'état de traitement '**600**' ;
- Si la volume des données à extraire n'est pas compatible avec la taille de l'EF (décalage + Le > taille de l'EF), le logiciel renvoie l'état de traitement '**6700**' ou '**6Cxx**', où 'xx' indique la longueur exacte ;
- Si une erreur d'intégrité est détectée dans les attributs du fichier, la carte considère le fichier sélectionné comme altéré et irrécupérable, et le logiciel renvoie l'état de traitement '**6400**' ou ~~6581~~'**6500**' ;
- **Si une erreur d'intégrité est détectée dans les données stockées, la carte renvoie les données demandées et le logiciel renvoie l'état de traitement** '**6281**'.

3.5.2.1.1 Commande avec messagerie sécurisée (exemples)

Cette commande permet au périphérique d'interface d'extraire les données de l'EF sélectionné avec messagerie sécurisée afin de vérifier l'intégrité des données reçues et de protéger la confidentialité des données si la condition de sécurité MS-R-ENC-MAC-G1 (génération 1) ou MS-R-ENC-MAC-G2 (génération 2) s'applique.

TCS_44 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'0Ch'	Messagerie sécurisée demandée
INS	1	'B0h'	READ BINARY
P1	1	'XXh'	P1 (décalage en octets à compter du début du fichier) : octet le plus significatif
P2	1	'XXh'	P2 (décalage en octets à compter du début du fichier) : octet le moins significatif
Lc	1	'XXh'	Longueur des données entrantes pour l'envoi par messagerie sécurisée
#6	1	'97h'	T_{LE} : balise spécifiant la longueur attendue
#7	1	'01h'	L_{LE} : longueur de la longueur attendue
#8	1	'NNh'	Spécification de la longueur attendue (Le original) : nombre d'octets à extraire
#9	1	'8Eh'	T_{CC} : balise indiquant le total de contrôle cryptographique
#10	1	'XXh'	L_{CC} : longueur du total de contrôle cryptographique suivante '04h' pour la messagerie sécurisée de génération 1 (voir **sous-**appendice 11, partie A) '08h', '0Ch' ou '10h' selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (voir **sous-**appendice 11, partie B)
#11-#(10+L)	L	'XX..XXh'	Total de contrôle cryptographique
Le	1	'00h'	Conformément à la norme ISO/CEI 7816-4

TCS_45 **Message de réponse si la condition MS-R-ENC-MAC-G1 (génération 1) ou MS-R-ENC-MAC-G2 (génération 2) n'est pas requise et si le format d'entrée de la messagerie sécurisée est correct :**

Octet	*Longueur*	*Valeur*	*Description*
#1	1	'81h'	T_{VC} : balise destinée aux données de valeur en clair
#2	L	'NNh' or	L_{VC} : longueur des données renvoyées (= Le original).
		'81 NNh'	L équivaut à 2 octets si L_{VC} > 127 octets.
#(2+L) - **#(1**+L+NN)	NN	'XX..XXh'	Valeur des données en clair
#(2+L+NN)	1	'99h'	**Balise indiquant l'état de traitement (ME1-ME2) − facultatif pour la messagerie sécurisée de génération 1**
#(3+L+NN)	1	'02h'	**Longueur de l'état de traitement − facultatif pour la messagerie sécurisée de génération 1**
#(4+L+NN) **#(5+L+NN)**	-2	'XX XXh'	**État de traitement de l'APDU de réponse non protégée − facultatif pour la messagerie sécurisée de génération 1**
#(6+L+NN)	1	'8Eh'	T_{CC} : balise indiquant le total de contrôle cryptographique
#(7+L+NN)	1	'XXh'	L_{CC} : longueur du total de contrôle cryptographique suivant '04h' pour la messagerie sécurisée de génération 1 (voir **sous-**appendice 11, partie A) '08h', '0Ch' ou '10h' selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (voir **sous-**appendice 11, partie B)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Total de contrôle cryptographique
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

TCS_46 **Message de réponse si la condition MS-R-ENC-MAC-G1 (génération 1) ou MS-R-ENC-MAC-G2 (génération 2) est requise et si le format d'entrée de la messagerie sécurisée est correct :**

Octet	*Longueur*	*Valeur*	*Description*
#1	1	'87h'	$T_{IR\ CG}$: balise destinée aux données chiffrées (cryptogramme)
#2	L	'MMh' ou '81 MMh'	$L_{IR\ CG}$: longueur des données chiffrées renvoyées (différentes du Le original de la commande en raison du remplissage) L équivaut à 2 octets si $L_{IR\ CG}$ > 127 octets
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Données chiffrées : cryptogramme et indicateur de remplissage
#(2+L+MM)	1	'99h'	Balise indiquant l'état de traitement (ME1-ME2) − facultatif pour la messagerie sécurisée de génération 1
#(3+L+MM)	1	'02h'	Longueur de l'état de traitement − **facultatif pour la messagerie sécurisée de génération 1**
#(4+L+MM) − #(5+L+MM)	2	'XX XXh'	État de traitement de l'APDU de réponse non protégée − **facultatif pour la messagerie sécurisée de génération 1**
#(6+L+MM)	1	'8Eh'	T_{CC} : balise indiquant le total de contrôle cryptographique

Octet	*Longueur*	*Valeur*	*Description*
#(7+L+MM)	1	'XXh'	L_{CC} : longueur du total de contrôle cryptographique suivant '04h' pour la messagerie sécurisée de génération 1 (voir **sous-**appendice 11, partie A) '08h', '0Ch' ou '10h' selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (voir **sous-**appendice 11, partie B)
#(8+L+MM) − #(7+N+L+MM)	N	'XX..XXh'	Total de contrôle cryptographique
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- La commande READ BINARY peut renvoyer les états de traitement normaux énoncés au point **TCS_43** sous la balise '99h' en adoptant la structure de réponse par messagerie sécurisée décrite au point **TCS_59** ;
- **Des erreurs directement liées à la messagerie sécurisée peuvent également survenir. Dans ce cas, le logiciel renvoie simplement l'état de traitement correspondant sans recourir à une structure de messagerie sécurisée :**

TCS_47 **Message de réponse si le format d'entrée de la messagerie sécurisée est incorrect**

Octet	*Longueur*	*Valeur*	*Description*
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- ♦ Si aucune clé de session active n'est disponible, le logiciel renvoie l'état de traitement '**6A88**'. Cet événement se produit si la clé de session n'a pas encore été générée ou si la clé de session est arrivée à expiration (dans ce cas, le périphérique d'interface doit relancer le processus d'authentification mutuelle pour définir une nouvelle clé de session) ;
- ♦ Si certains objets de données attendus (définis ci-avant) font défaut dans la structure de messagerie sécurisée, le logiciel renvoie l'état de traitement '**6987**'. Cette erreur se produit si une balise attendue manque ou si le corps de la commande n'est pas correctement construit ;
- ♦ Si certains objets de données sont incorrects, le logiciel renvoie l'état de traitement '**6988**'. Cette erreur se produit si toutes les balises requises sont présentes, mais que certaines longueurs diffèrent de celles attendues ;
- ♦ Si la vérification du total de contrôle cryptographique échoue, le logiciel renvoie l'état de traitement '**6688**'.

3.5.2.2 Commande avec un identificateur de fichier élémentaire (EF) court

Cette variante de commande permet au périphérique d'interface de sélectionner un EF à l'aide d'un identificateur d'EF court et d'extraire des données de cet EF.

TCS_48 Une carte tachygraphique doit prendre en charge cette variante de commande pour tous les fichiers élémentaires dotés d'un identificateur d'EF court défini. Ces identificateurs d'EF courts sont spécifiés au chapitre 4.

TCS_49 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	
INS	1	'B0h'	READ BINARY

Octet	*Longueur*	*Valeur*	*Description*
P1	1	'XXh'	Le bit 8 est mis à 1. Les bits 7 et 6 sont mis à 00. Les bits 5 - 1 codent l'identificateur d'EF court de l'EF correspondant.
P2	1	'XXh'	Code un décalage de 0 à 255 octets dans l'EF désigné par P1
Le	1	'XXh'	Longueur des données attendue. Nombre d'octets à extraire.

Remarque : les identificateurs d'EF courts utilisés dans l'application tachygraphique de génération 2 sont spécifiés au chapitre 4.

Si P1 code un identificateur d'EF court et que la commande aboutit, l'EF identifié devient l'EF sélectionné (EF actif).

TCS_50 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
#1-#L	L	'XX..XXh'	Données lues
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- Si le logiciel ne parvient pas à trouver le fichier correspondant à l'identificateur d'EF court, il renvoie l'état de traitement **'6A82'** ;
- Si les conditions de sécurité du fichier sélectionné ne sont pas remplies, la commande est interrompue par '**6982**' ;
- Si le décalage n'est pas compatible avec la taille de l'EF (décalage > taille de l'EF), le logiciel renvoie l'état de traitement '**6B00**' ;
- Si le volume des données à extraire n'est pas compatible avec la taille de l'EF (décalage + Le > taille de l'EF), le logiciel renvoie l'état de traitement '**6700**' ou '**6Cxx**', où 'xx' indique la longueur exacte ;
- Si une erreur d'intégrité est détectée dans les attributs du fichier, la carte considère le fichier sélectionné comme altéré et irrécupérable, et le logiciel renvoie l'état de traitement '**6400**' ou ~~6581~~'**6500**' ;
- **Si une erreur d'intégrité est détectée dans les données stockées, la carte renvoie les données demandées et le logiciel renvoie l'état de traitement '6281'.**

3.5.2.3 Commande avec octet d'instruction impair

Cette variante de commande permet au périphérique d'interface d'extraire des données d'un EF de 32 768 octets ou plus.

TCS_51 Une carte tachygraphique prenant en charge des EF de 32 768 octets ou plus doit prendre en charge cette variante de commande pour ces fichiers. Une carte tachygraphique peut ou non prendre en charge cette variante de commande pour les autres EF, à l'exception de l'EF Sensor_Installation_Data **(voir TCS_156 et TCS_160)**.

TCS_52 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	
INS	1	'B1h'	READ BINARY

Octet	*Longueur*	*Valeur*	*Description*
P1	1	‘00h’	EF actif
P2	1	‘00h’	
Lc	1	‘NNh’	Longueur Lc de l’objet de données décalé
#6-#(5+NN)	NN	‘XX..XXh’	Décalage de l’objet de données : Balise ‘54h’ Longueur ‘01h’ ou ‘02h’ Valeur décalage
Le	1	‘XXh’	**Conformément à la norme ISO/CEI 7816-4**

Le périphérique d’interface doit coder la longueur de l’objet de données décalé sur le minimum d’octets possible, c’est-à-dire qu’à l’aide de l’octet de longueur ‘01h’, il doit coder un décalage de 0 à 255 et, à l’aide de l’octet de longueur ‘02h’, un décalage de ‘256’ jusqu’à ’65 535’ octets.

En T = 0, la carte adopte la valeur Le = ‘00h’ si aucune messagerie sécurisée n’est utilisée.

En T = 1, le logiciel renvoie l’état de traitement ‘6700’ si Le = ‘01h’.

TCS_53 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
#1-#L	L	‘XX..XXh’	Les données extraites sont intégrées dans un objet de données discrétionnaire avec une balise ‘53h’
ME	2	‘XXXXh’	Mots d’état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l’état ‘**9000**’ ;
- Si aucun EF n’est sélectionné, le logiciel renvoie l’état de traitement ‘**6986’** ;
- Si les conditions de sécurité du fichier sélectionné ne sont pas remplies, la commande est interrompue par ‘**6982’** ;
- Si le décalage n’est pas compatible avec la taille de l’EF (décalage > taille de l’EF), le logiciel renvoie l’état de traitement ‘**6B00’** ;
- Si le volume des données à extraire n’est pas compatible avec la taille de l’EF (décalage + Le > taille de l’EF) le logiciel renvoie l’état de traitement suivant ‘**6700’** ou ‘**6Cxx**’, où ‘xx’ indique la longueur exacte ;
- Si une erreur d’intégrité est détectée dans les attributs du fichier, la carte considère le fichier sélectionné comme altéré et irrécupérable, et le logiciel renvoie l’état de traitement ‘**6400**’ ou ‘**6500**’ ;
- **Si une erreur d’intégrité est détectée dans les données stockées, la carte renvoie les données demandées et le logiciel renvoie l’état de traitement** ‘**6281**’.

3.5.2.3.1 Commande avec messagerie sécurisée (exemple)

L’exemple suivant illustre l’utilisation de la messagerie sécurisée si la condition de sécurité MS-MAC-G2 s’applique.

TCS_54 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	‘0Ch’	Messagerie sécurisée demandée
INS	1	‘B1h’	READ BINARY
P1	1	‘00h’	EF actif
P2	1	‘00h’	
Lc	1	‘XXh’	Longueur de la zone de données sécurisée
#6	1	‘B3h’	Balise indiquant la valeur des données en clair codées en BER-TLV
#7	1	‘NNh’	L_{VC} : longueur des données transmises
#(8)-#(7+NN)	NN	‘XX..XXh’	Données en clair codées en BER-TLV, c’est-à-dire l’objet de données décalé doté de la balise ‘54’
#(8+NN)	1	‘97h’	T_{LE} : balise spécifiant la longueur attendue
#(9+NN)	1	‘01h’	L_{LE} : longueur de la longueur attendue
#(10+NN)	1	‘XXh’	Spécification de la longueur attendue (Le original) : nombre d’octets à extraire
#(11+NN)	1	‘8Eh’	T_{CC} : balise indiquant le total de contrôle cryptographique
#(12+NN)	1	‘XXh’	L_{CC} : longueur du total de contrôle cryptographique suivant ‘08h’, ‘0Ch’ ou ‘10h’ selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (voir **sous**-appendice 11, partie B)
#(13+NN)-#(12+M+NN)	M	‘XX..XXh’	Total de contrôle cryptographique
Le	1	‘00h’	Conformément à la norme ISO/CEI 7816-4

TCS_55 Message de réponse si la commande aboutit

Octet	*Longueur*	*Valeur*	*Description*
#1	1	‘B3h’	Données en clair codées en BER-TLV
#2	L	‘NNh’ ou ‘81 NNh’	L_{VC} : longueur des données renvoyées (= Le original) L équivaut à 2 octets si L_{VC} > 127 octets
#(2+L)-#(1+L+NN)	NN	‘XX..XXh’	Valeur des données en clair codées en BER-TLV, c’est-à-dire les données extraites intégrées dans un objet de données discrétionnaire doté de la balise ‘53h’
#(2+L+NN)	1	‘99h’	État de traitement de l’APDU de réponse non protégée
#(3+L+NN)	1	‘02h’	Longueur de l’état de traitement
#(4+L+NN)-#(5+L+NN)	2	‘XX XXh’	État de traitement de l’APDU de réponse non protégée

Octet	*Longueur*	*Valeur*	*Description*
#(6+L+NN)	1	'8Eh'	T_{CC} : balise indiquant le total de contrôle cryptographique
#(7+L+NN)	1	'XXh'	L_{CC} : longueur du total de contrôle cryptographique suivant '08h', '0Ch' ou '10h' selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (voir **sous**-appendice 11, partie B)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Total de contrôle cryptographique
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

3.5.3 UPDATE BINARY (actualisation des données)

Cette commande est conforme à la norme ISO/CEI 7816-4, mais elle a un usage restreint par rapport à la commande analogue définie dans cette norme.

Le message de commande UPDATE BINARY lance l'actualisation (effacement + écriture) des bits déjà présents dans un EF avec les bits indiqués dans l'APDU de commande.

3.5.3.1 Commande avec décalage en P1-P2

Cette commande permet au périphérique d'interface d'enregistrer des données dans l'EF sélectionné, sans que la carte vérifie l'intégrité des données reçues.

Remarque : cette commande sans messagerie sécurisée ne peut servir qu'à actualiser un fichier prenant en charge la condition de sécurité TJR en mode actualisation.

TCS_56 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	
INS	1	'D6h'	UPDATE BINARY
P1	1	'XXh'	Décalage en octets à compter du début du fichier : octet le plus significatif
P2	1	'XXh'	Décalage en octets à compter du début du fichier : octet le moins significatif
Lc	1	'NNh'	Longueur Lc des données à actualiser. Nombre d'octets à enregistrer
#6-#(5+NN)	NN	'XX..XXh'	Données à enregistrer

Remarque : le bit 8 de P1 doit être mis à 0.

TCS_57 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- Si aucun EF n'est sélectionné, le logiciel renvoie l'état de traitement '**6986**' ;

- ♦ Si les conditions de sécurité du fichier sélectionné ne sont pas remplies, la commande est interrompue par '**6982**' ;
- ♦ Si le décalage n'est pas compatible avec la taille de l'EF (décalage > taille de l'EF), le logiciel renvoie l'état de traitement '**6B00**' ;
- ♦ Si le volume des données à enregistrer n'est pas compatible avec la taille de l'EF (décalage + Le > taille de l'EF), le logiciel renvoie l'état de traitement '**6700'** ;
- ♦ Si une erreur d'intégrité est détectée dans les attributs du fichier, la carte considère le fichier sélectionné comme altéré et irrécupérable, et le logiciel renvoie l'état de traitement **'6400'** ou **'6500'** ;
- ♦ Si l'enregistrement échoue, le logiciel renvoie l'état de traitement **'6581'**.

3.5.3.1.1 Commande avec messagerie sécurisée (exemples)

Cette commande permet au périphérique d'interface d'enregistrer des données dans l'EF sélectionné, la carte vérifiant l'intégrité des données reçues. Aucune confidentialité n'étant requise, les données ne sont pas chiffrées.

TCS_58 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'0Ch'	Messagerie sécurisée demandée
INS	1	'D6h'	UPDATE BINARY
P1	1	'XXh'	Décalage en octets à compter du début du fichier : octet le plus significatif
P2	1	'XXh'	Décalage en octets à compter du début du fichier : octet le moins significatif
Lc	1	'XXh'	Longueur de la zone de données sécurisée
#6	1	'81h'	T_{VC} : balise indiquant la valeur des données en clair
#7	L	'NNh' ou	L_{VC} : longueur des données transmises
		'81 NNh'	L équivaut à 2 octets si L_{VC} > 127 octets
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Valeur des données en clair (données à enregistrer)
#(7+L+NN)	1	'8Eh'	T_{CC} : balise indiquant le total de contrôle cryptographique
#(8+L+NN)	1	'XXh'	L_{CC} : longueur du total de contrôle cryptographique suivant
			'04h' pour la messagerie sécurisée de génération 1 (voir **sous-**appendice 11, partie A)
			'08h', '0Ch' ou '10h' selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (voir **sous-**appendice 11, partie B)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Total de contrôle cryptographique
Le	1	'00h'	Conformément à la norme ISO/CEI 7816-4

TCS_59 **Message de réponse si le format d'entrée de la messagerie sécurisée est correct**

Octet	*Longueur*	*Valeur*	*Description*
#1	1	'99h'	T_{ME} : balise indiquant les mots d'état (à protéger par CC)
#2	1	'02h'	L_{ME} : longueur des mots d'état renvoyés
#3-#4	2	'XXXXh'	État de traitement de l'APDU de réponse non protégée
#5	1	'8Eh'	T_{CC} : balise indiquant le total de contrôle cryptographique
#6	1	'XXh'	L_{CC} : longueur du total de contrôle cryptographique suivant '04h' pour la messagerie sécurisée de génération 1 (voir **sous-**appendice 11, partie A) '08h', '0Ch' ou '10h' selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (voir **sous-**appendice 11, partie B)
#7-#(6+L)	L	'XX..XXh'	Total de contrôle cryptographique
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

La structure des messages de réponse décrite ci-dessus permet de renvoyer les états de traitement « normaux » définis pour la commande UPDATE BINARY sans messagerie sécurisée **(voir par. 3.5.3.1)**.

Des erreurs directement liées à la messagerie sécurisée peuvent également survenir. Dans ce cas, le logiciel renvoie simplement l'état de traitement correspondant sans recourir à une structure de messagerie sécurisée :

TCS_60 **Message de réponse en cas d'erreur concernant la messagerie sécurisée**

Octet	*Longueur*	*Valeur*	*Description*
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si aucune clé de session active n'est disponible, le logiciel renvoie l'état de traitement **'6A88'** ;
- Si certains objets de données attendus (définis ci-avant) font défaut dans la structure de messagerie sécurisée, le logiciel renvoie l'état de traitement '**6987**'. Cette erreur se produit si une balise attendue manque ou si le corps de la commande n'est pas correctement construit ;
- Si certains objets de données sont incorrects, le logiciel renvoie l'état de traitement '**6988**'. Cette erreur se produit si toutes les balises requises sont présentes, mais que certaines longueurs diffèrent de celles attendues ;
- Si la vérification du total de contrôle cryptographique échoue, le logiciel renvoie l'état de traitement '**6688**'.

3.5.3.2 Commande avec un identificateur de fichier élémentaire (EF) court

Cette variante de commande permet au PIF de sélectionner un EF à l'aide d'un identificateur EF court et d'enregistrer des données à partir de cet EF.

TCS_61 Une carte tachygraphique doit prendre en charge cette variante de commande pour tous les fichiers élémentaires dotés d'un identificateur

d'EF court défini. Ces identificateurs EF courts sont spécifiés au chapitre 4.

TCS_62 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	
INS	1	'D6h'	UPDATE BINARY
P1	1	'XXh'	Le bit 8 est mis à 1. Les bits 7 et 6 sont mis à 00. Les bits 5 - 1 codent l'identificateur d'EF court de l'EF correspondant.
P2	1	'XXh'	Code un décalage de 0 à 255 octets dans l'EF désigné par P1
Lc	1	'NNh'	Longueur Lc des données à actualiser. Nombre d'octets à écrire.
#6-#(5+NN)	NN	'XX..XXh'	Données à enregistrer

TCS_63 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

Remarque : les identificateurs d'EF courts utilisés dans l'application tachygraphique de génération 2 sont spécifiés au chapitre 4.

Si P1 code un identificateur d'EF court et que la commande aboutit, l'EF identifié devient l'EF sélectionné (EF actif).

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- Si le logiciel ne parvient pas à trouver le fichier correspondant à l'identificateur d'EF court, il renvoie l'état de traitement **'6A82'** ;
- Si les conditions de sécurité du fichier sélectionné ne sont pas remplies, la commande est interrompue par '**6982**' ;
- Si le décalage n'est pas compatible avec la taille de l'EF (décalage > taille de l'EF), le logiciel renvoie l'état de traitement '**6B00**' ;
- Si le volume des données à enregistrer n'est pas compatible avec la taille de l'EF (décalage + Le > taille de l'EF), le logiciel renvoie l'état de traitement '**6700**' ;
- Si une erreur d'intégrité est détectée dans les attributs du fichier, la carte considère le fichier sélectionné comme altéré et irrécupérable, et le logiciel renvoie l'état de traitement '**6400**' ou ~~6581~~'**6500**' ;
- Si l'enregistrement échoue, le logiciel renvoie l'état de traitement **'6581'**.

3.5.3.3 Commande avec octet d'instruction impair

Cette variante de commande permet au périphérique d'interface d'enregistrer des données dans un EF de 32 768 octets ou plus.

TCS_64 Une carte tachygraphique prenant en charge des EF de 32 768 octets ou plus doit prendre en charge cette variante de commande pour ces fichiers. Une carte tachygraphique peut ou non prendre en charge cette variante de commande pour les autres EF.

TCS_65 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	‘00h’	
INS	1	‘D7h’	UPDATE BINARY
P1	1	‘00h’	EF actif
P2	1	‘00h’	
Lc	1	‘NNh’	Longueur Lc des données dans la zone de données de la commande
#6-#(5+NN)	NN	‘XX..XXh’	Décalage de l’objet de données doté de la balise ‘54h’ ‖ Objet de données discrétionnaire doté de la balise ‘53h’ qui encapsule les données à enregistrer

LE PIF doit coder la longueur de l’objet de données décalé et de l’objet de données discrétionnaire sur un minimum d’octets, c’est-à-dire qu’à l’aide de l’octet de longueur ‘01h’, le PIF doit coder un décalage/une longueur de 0 à 255 et, à l’aide de l’octet de longueur ‘02h’, un décalage/une longueur de ‘256’ jusqu’à ‘65 535’ octets.

TCS_66 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
ME	2	‘XXXXh’	Mots d’état (ME1, ME2).

- Si la commande aboutit, la carte renvoie l’état ‘**9000**’ ;
- Si aucun EF n’est sélectionné, le logiciel renvoie l’état de traitement ‘**6986**’ ;
- Si les conditions de sécurité du fichier sélectionné ne sont pas remplies, la commande est interrompue par ‘**6982**’ ;
- Si le décalage n’est pas compatible avec la taille de l’EF (décalage > taille de l’EF), le logiciel renvoie l’état de traitement ‘**6B00**’ ;
- Si le volume des données à enregistrer n’est pas compatible avec la taille de l’EF (décalage + Le > taille de l’EF), le logiciel renvoie l’état de traitement ‘**6700’** ;
- Si une erreur d’intégrité est détectée dans les attributs du fichier, la carte considère le fichier sélectionné comme altéré et irrécupérable, et le logiciel renvoie l’état de traitement **‘6400’** ou **‘6500’** ;
- Si l’enregistrement échoue, le logiciel renvoie l’état de traitement **‘6581’**.

3.5.3.3.1 Commande avec messagerie sécurisée (exemple)

L’exemple suivant illustre l’utilisation de la messagerie sécurisée si la condition de sécurité MS-MAC-G2 s’applique.

TCS_67 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	‘0Ch’	Messagerie sécurisée demandée
INS	1	‘D7h’	UPDATE BINARY
P1	1	‘00h’	EF actif
P2	1	‘00h’	

Octet	*Longueur*	*Valeur*	*Description*
Lc	1	‘XXh’	Longueur de la zone de données sécurisée
#6	1	‘B3h’	Balise indiquant la valeur des données en clair codées en BER-TLV
#7	L	‘NNh’ ou	L_{VC} : longueur des données transmises
		‘81 NNh’	L équivaut à 2 octets si L_{VC} > 127 octets.
#(7+L)-#(6+L+NN)	NN	‘XX..XXh’	Données en clair codées en BER-TLV, c’est-à-dire le décalage de l’objet de données doté de la balise ‘54h’ || Objet de données discrétionnaire doté de la balise ‘53h’ qui encapsule les données à enregistrer
#(7+L+NN)	1	‘8Eh’	T_{CC} : balise indiquant le total de contrôle cryptographique
#(8+L+NN)	1	‘XXh’	L_{CC} : longueur du total de contrôle cryptographique suivant
			‘08h’, ‘0Ch’ ou ‘10h’ selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (voir **sous-**appendice 11, partie B)
#(9+L+NN)-#(8+M+L+NN)	M	‘XX..XXh’	Total de contrôle cryptographique
Le	1	‘00h’	Conformément à la norme ISO/CEI 7816-4

TCS_68 Message de réponse si la commande aboutit

Octet	*Longueur*	*Valeur*	*Description*
#1	1	‘99h’	T_{ME} : balise indiquant les mots d’état (à protéger par CC)
#2	1	‘02h’	L_{ME} : longueur des mots d’état renvoyés
#3-#4	2	‘XXXXh’	État de traitement de l’APDU de réponse non protégée
#5	1	‘8Eh’	T_{CC} : balise indiquant le total de contrôle cryptographique
#6	1	‘XXh’	L_{CC} : longueur du total de contrôle cryptographique suivant
			‘08h’, ‘0Ch’ ou ‘10h’ selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (voir **sous-**appendice 11, partie B)
#7-#(6+L)	L	‘XX..XXh’	Total de contrôle cryptographique
ME	2	‘XXXXh’	Mots d’état (ME1, ME2)

3.5.4 GET CHALLENGE (demande de défi)

Cette commande est conforme à la norme ISO/CEI 7816-4, mais elle a un usage restreint par rapport à la commande analogue définie dans cette norme.

La commande GET CHALLENGE demande à la carte de générer un défi (challenge) pour l’appliquer dans le cadre d’une procédure de sécurité consistant à envoyer un cryptogramme ou des données chiffrées à la carte.

TCS_69 Le défi généré par la carte n'est valable que pour la prochaine commande concernée par un défi qui est envoyée à la carte.

TCS_70 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (longueur attendue du défi)

TCS_71 **Message de réponse**

Octet	*Longueur*	*Valeur*	*Description*
#1-#8	8	'XX..XXh'	Défi
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- Si Le est différent de '08h', le logiciel renvoie l'état de traitement '**6700**' ;
- Si les paramètres P1-P2 sont incorrects, le logiciel renvoie l'état de traitement **'6A86'.**

3.5.5 VERIFY (vérification)

Cette commande est conforme à la norme ISO/CEI 7816-4, mais elle a un usage restreint par rapport à la commande analogue définie dans cette norme.

Seule la carte d'atelier doit prendre en charge cette commande.

Les autres types de cartes tachygraphiques peuvent ou non mettre en œuvre cette commande, mais pour ces cartes aucune information VDC de référence n'est définie spécifiquement. Par conséquent, ces cartes ne peuvent pas exécuter cette commande avec succès. Pour les types de cartes tachygraphiques autres que les cartes d'atelier, l'action, c'est-à-dire le renvoi du code d'erreur, sort du champ d'application de la présente spécification, dans le cas où une telle commande est envoyée.

La commande VERIFY lance, au niveau de la carte, la comparaison entre les données VDC (PIN) envoyées et les données VDC de référence enregistrée dans la mémoire de la carte.

TCS_72 Le PIN renseigné par l'utilisateur doit être codé en ASCII et complété à droite par le périphérique d'interface avec une série d'octets 'FFh' jusqu'à atteindre une longueur de 8 octets (voir le type de données WorkshopCardPIN dans le **sous-**appendice 1).

TCS_73 Les applications tachygraphiques de générations 1 et 2 doivent utiliser les mêmes informations VDC de référence.

TCS_74 La carte tachygraphique doit vérifier si la commande est correctement codée. Si la commande n'est pas correctement codée, la carte ne doit pas comparer les valeurs VDC, ni décrémenter le compteur de tentatives VDC restantes, ni réinitialiser l'état de sécurité « PIN_Verified ». Elle doit interrompre la commande. Une commande est correctement codée si les octets CLA, INS, P1, P2, Lc ont les valeurs spécifiées, si Le est absent et si la zone de données de la commande a la longueur adéquate.

TCS_75 Si la commande aboutit, le compteur de tentatives VDC restantes est réinitialisé. La valeur initiale du compteur de tentatives VDC restantes est de 5. Si la commande aboutit, la carte active l'état de sécurité interne « PIN_Verified ». La carte réinitialise cet état de sécurité si la carte est réinitialisée ou si le code VDC transmis dans la commande ne correspond pas au code VDC de référence stocké en mémoire.

Remarque : l'utilisation des mêmes informations VDC de référence et d'un état de sécurité global évite à un employé d'atelier de devoir renseigner à nouveau le PIN après avoir sélectionné un autre DF de l'application tachygraphique.

TCS_76 La carte enregistre l'échec d'une comparaison, c'est-à-dire que le compteur de tentatives VDC restantes doit être décrémenté d'une unité afin de restreindre le nombre de nouvelles tentatives d'utilisation des informations VDC de référence.

TCS_77 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (les informations VDC vérifiées sont implicitement connues)
Lc	1	'08h'	Longueur du code VDC transmis
#6-#13	8	'XX..XXh'	VDC

TCS_78 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- Si les informations VDC de référence sont introuvables, le logiciel renvoie l'état de traitement **'6A88'** ;
- Si les informations VDC sont bloquées (le compteur de tentatives VDC restantes est nul), le logiciel renvoie l'état de traitement **'6983'**. Une fois dans cet état, les informations VDC ne pourront jamais plus être présentées avec succès ;
- Si la comparaison échoue, le compteur de tentatives restantes est décrémenté et le logiciel renvoie l'état **'63CX'** (X > 0 et X correspond au compteur de tentatives VDC restantes).
- Si les informations VDC de référence sont considérées comme altérées, le logiciel renvoie l'état de traitement **'6400'** ou **'6581'**.
- Si Lc est différente de '08h', le logiciel renvoie l'état de traitement '**6700**'.

3.5.6 GET RESPONSE (obtention d'une réponse)

Cette commande est conforme à la norme ISO/CEI 7816-4.

Cette commande (indispensable et exclusivement disponible pour le protocole T = 0) permet d'assurer la transmission de données préparées de la carte au périphérique d'interface (dans le cas où une commande comprendrait les deux octets Lc et Le).

La commande GET RESPONSE doit être émise immédiatement après la commande de préparation des données, sinon celles-ci seront perdues. Après exécution de la commande GET RESPONSE (sauf si l'erreur '**61xx**' ou '**6Cxx**' s'est produite, voir ci-après), les données préparées antérieurement cessent d'être disponibles.

TCS_79 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Nombre d'octets attendus

TCS_80 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
#1-#X	X	'XX..XXh'	Données
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- Si la carte n'a préparé aucune donnée, elle renvoie l'état de traitement **'6900'** ou **'6F00'** ;
- Si l'octet Le dépasse le nombre d'octets disponibles ou si cet octet est nul, le logiciel renvoie l'état de traitement **'6Cxx'**, les caractères 'xx' indiquant le nombre exact d'octets disponibles. Dans ce cas, les données préparées restent disponibles en vue de l'exécution d'une commande GET RESPONSE ultérieure ;
- Si l'octet Le a une valeur non nulle inférieure au nombre d'octets disponibles, la carte procède normalement à l'envoi des données requises et renvoie l'état de traitement **'61xx'**, dans lequel 'xx' indique un nombre d'octets supplémentaires encore disponibles pour l'exécution d'une commande GET RESPONSE ultérieure ;
- Si la commande n'est pas prise en charge (protocole T = 1), la carte renvoie l'état de traitement **'6D00'**.

3.5.7 PSO: VERIFY CERTIFICATE (vérification du certificat)

Cette commande est conforme à la norme ISO/CEI 7816-8, mais elle a un usage restreint par rapport à la commande analogue définie dans cette norme.

La carte utilise la commande VERIFY CERTIFICATE pour obtenir une clé publique provenant de l'extérieur et pour en contrôler la validité.

3.5.7.1 Commande de génération 1 : paire de réponses

TCS_81 Cette variante de commande est uniquement prise en charge par une application tachygraphique de génération 1.

TCS_82 Lorsqu'une commande VERIFY CERTIFICATE aboutit, la clé publique correspondante est stockée en vue d'une utilisation ultérieure dans l'environnement de sécurité. Cette clé doit être explicitement configurée pour être utilisée, dans le cadre de commandes touchant à la sécurité (INTERNAL AUTHENTICATE, EXTERNAL

AUTHENTICATE ou VERIFY CERTIFICATE), par la commande MSE (voir par. ~~3.5.11~~3.5.11) à l'aide de son identificateur de clé.

TCS_83 En tout état de cause, la commande VERIFY CERTIFICATE utilise la clé publique préalablement sélectionnée par la commande MSE pour ouvrir le certificat. Cette clé publique doit être celle ~~d'un État membre ou de l'Europe~~ **d'une Partie contractante ou la clé publique racine**.

TCS_84 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	
INS	1	'2Ah'	Exécution d'une opération de sécurité (PSO)
P1	1	'00h'	P1
P2	1	'AEh'	P2 : données non codées en BER-TLV (concaténation d'éléments de données)
Lc	1	'C2h'	Lc : longueur du certificat (194 octets)
#6-#199	194	'XX..XXh'	Certificat : concaténation d'éléments de données (comme décrit dans ~~l'appendice~~ **le sous-appendice** 11)

TCS_85 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- Si la vérification du certificat échoue, le logiciel renvoie l'état de traitement **'6688'**. Le processus de vérification et de dévoilement du certificat est décrit dans ~~l'appendice~~ **le sous-appendice** 11 pour les générations 1 et 2 ;
- Si aucune clé publique n'est présente dans l'environnement de sécurité, le logiciel renvoie l'état de traitement **'6A88'** ;
- Si la clé publique sélectionnée (et utilisée pour dévoiler le certificat) est considérée comme altérée, le logiciel renvoie l'état de traitement **'6400'** ou **'6581'**.
- Pour la génération 1 uniquement : si la clé publique sélectionnée (et utilisée pour dévoiler le certificat) a un CHA.LSB (CertificateHolderAuthorisation.equipmentType) différent de '00', c'est-à-dire qu'il ne s'agit ni de la clé ~~d'un État membre ni de l'Europe~~**d'une Partie contractante, ni du certificat racine**), le logiciel renvoie l'état de traitement **'6985'**.

3.5.7.2 Commande de génération 2 : paire de réponses

Selon la dimension de la courbe, les certificats ECC peuvent être si longs qu'ils ne peuvent être transmis dans une seule APDU. Dans de tels cas, le chaînage de commandes doit être appliqué, conformément à la norme ISO/CEI 7816-4 et le certificat doit être transmis en deux commandes APDU PSO:VERIFY CERTIFICATE successives.

La structure du certificat et les paramètres de domaine sont définis ~~à l'appendice~~ **au sous-appendice** 11.

TCS_86 La commande peut être exécutée dans le MF ainsi que dans les DF Tachograph et DF Tachograph_G2 (voir également TCS_3~~4~~3).

TCS_87 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	‘X0h’	L’octet CLA indique un chaînage de commandes : ‘00h’ l’unique ou la dernière commande de la chaîne ‘10h’ pas la dernière commande d’une chaîne
INS	1	‘2Ah’	Exécution d’une opération de sécurité (PSO)
P1	1	‘00h’	
P2	1	‘BEh’	Vérification du certificat autodescriptif
Lc	1	‘XXh’	Longueur de la zone de données de la commande (voir **TCS_88** et **TCS_89**)
#6-#5+L	L	‘XX..XXh’	Données codées en DER-TLV : l’objet de données Corps du certificat ECC est le premier objet de données concaténé et l’objet de donnée Signature du certificat ECC est le deuxième objet de données ou une partie de cette concaténation. La balise ‘7F21’ et la longueur correspondante ne doivent pas être transmises. L’ordre de ces objets de données est fixe.

TCS_88 Pour les APDU courtes, les dispositions suivantes s’appliquent : le périphérique d’interface doit utiliser le moins d’APDU possibles pour transmettre les données utiles de la commande et transmettre le maximum d’octets dans la première APDU de commande ~~en fonction de la valeur de l’octet de la carte Dimension de la zone de données, cf. **TCS_14**. Si le PIF a un autre comportement, celui de la carte sort du périmètre~~. **Toutefois, toute valeur de Lc inférieure ou égale à 255 octets doit être prise en charge par la carte.**

TCS_89 Pour les APDU longues, les dispositions suivantes s’appliquent : si le certificat ne s’insère pas dans une seule APDU, la carte doit prendre en charge une chaîne de commandes. Le périphérique d’interface doit utiliser le moins d’APDU possibles pour transmettre les données utiles de la commande et transmettre le maximum d’octets dans la première APDU de commande. **Si un chaînage des commandes est nécessaire, la carte doit prendre en charge toute valeur de Lc inférieure ou égale à la longueur étendue maximale spécifiée.** ~~Si le PIF adopte un autre comportement, celui de la carte sort du périmètre.~~

Remarque : ~~l’appendice~~**le sous-appendice** 11 prévoit que la carte stocke le certificat ou les contenus pertinents du certificat, et actualise son currentAuthenticatedTime.

La structure des messages de réponse et les mots d’état figurent au point **TCS_85**.

TCS_90 Outre les codes d’erreurs énumérés au point 0, la carte peut également renvoyer les codes d’erreur suivants :

- Si la clé publique sélectionnée (et utilisée pour dévoiler le certificat) possède un CHA.LSB (CertificateHolderAuthorisation.equipmentType) qui ne se prête pas à la vérification du certificat comme prévu ~~à l’appendice~~ **au sous-appendice** 11, le logiciel renvoie l’état de traitement ‘**6985**’ ;
- Si le currentAuthenticatedTime de la carte est ultérieur à la date d’expiration du certificat, le logiciel renvoie l’état de traitement ‘**6985**’ ;
- Si la dernière commande de la chaîne est attendue, la carte renvoie ‘**6883**’ ;

- Si des paramètres incorrects sont envoyés dans la zone de données de la commande, la carte renvoie '**6A80**' (code également utilisé dans le cas où les objets de données ne sont pas envoyés dans l'ordre spécifié).

3.5.8 INTERNAL AUTHENTICATE (authentification interne)

Cette commande est conforme à la norme ISO/CEI 7816-4.

TCS_91 Toutes les cartes tachygraphiques doivent prendre en charge cette commande dans le DF Tachograph de génération 1. La commande peut être accessible dans le MF et/ou le DF Tachograph_G2 ou non. Dans ce cas, le logiciel doit interrompre la commande avec un code d'erreur adapté, car la clé privée de la carte (Card.SK) pour le protocole d'authentification de la génération 1 n'est accessible que dans le DF_Tachograph de génération 1.

La commande INTERNAL AUTHENTICATE permet au périphérique d'interface d'authentifier la carte. Le processus d'authentification est décrit ~~à l'appendice~~ **au sous-appendice** 11. Il comprend les instructions suivantes :

TCS_92 La commande INTERNAL AUTHENTICATE utilise la clé privée de la carte (implicitement sélectionnée) pour signer des données d'authentification, y compris K1 (premier élément indiquant la concordance des clés de session) et RND1, et elle utilise la clé publique sélectionnée (au moyen de la dernière commande MSE) pour coder la signature et constituer le jeton d'authentification (pour de plus amples informations, voir **sous-**appendice 11).

TCS_93 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Longueur des données transmises à la carte
#6-#13	8	'XX..XXh'	Défi servant à l'authentification la carte
#14-#21	8	'XX..XXh'	UEV.RDC (voir **sous-**appendice 11)
Le	1	'80h'	Longueur des données attendues en provenance de la carte

TCS_94 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
#1-#128	128	'XX..XXh'	Jeton d'authentification de carte (voir **sous-**appendice 11)
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- Si aucune clé publique n'est présente dans l'environnement de sécurité, le logiciel renvoie l'état de traitement **'6A88'** ;
- Si aucune clé privée n'est présente dans l'environnement de sécurité, le logiciel renvoie l'état de traitement **'6A88'** ;

- Si l'UEV.RDC ne correspond pas à l'identificateur de clé publique actif, le logiciel renvoie l'état de traitement **'6A88'** ;
- Si la clé privée sélectionnée est considérée comme altérée, le logiciel renvoie l'état de traitement **'6400'** ou **'6581'**.

TCS_95 Si la commande INTERNAL AUTHENTICATE aboutit, la clé de session **de génération 1** active, pour autant qu'elle existe, est effacée et cesse d'être disponible. Pour obtenir une nouvelle clé de session **de génération 1**, il convient d'exécuter avec succès la commande EXTERNAL AUTHENTICATE du mécanisme d'authentification de génération 1.

Remarque : pour des informations concernant les clés de session de génération 2, se référer aux points CSM_193 et CSM_195 du sous-appendice 11. Si des clés de session de génération 2 sont générées et que la carte tachygraphique reçoit l'APDU de la commande INTERNAL AUTHENTICATE en clair, la carte interrompt la session de messagerie sécurisée de génération 2 et détruit les clés de sessions correspondantes.

3.5.9 EXTERNAL AUTHENTICATE (authentification externe)

Cette commande est conforme à la norme ISO/CEI 7816-4.

La commande EXTERNAL AUTHENTICATE (authentification externe) permet à la carte d'authentifier le périphérique d'interface. Le processus d'authentification est décrit ~~à l'appendice~~ **au sous-appendice** 11 pour les tachygraphes de générations 1 et 2 (authentification de l'UEV).

TCS_96 La variante de la commande correspondant au mécanisme d'authentification mutuelle de génération 1 est uniquement prise en charge par une application tachygraphique de génération 1.

TCS_97 La variante de la commande destinée à l'authentification mutuelle UEV − carte de génération 2 peut être exécutée dans le MF, le DF Tachograph et le DF Tachograph_G2 (voir TCS_34). **Si la commande EXTERNAL AUTHENTICATE de génération 2 aboutit, la clé de session de génération 1 active, pour autant qu'elle existe, est effacée et cesse d'être disponible.**

Remarque : pour des informations concernant les clés de session de génération 2, se référer aux points CSM_193 et CSM_195 du sous-appendice 11. Si des clés de session de génération 2 sont générées et que la carte tachygraphique reçoit l'APDU de la commande EXTERNAL AUTHENTICATE en clair, la carte interrompt la session de messagerie sécurisée de génération 2 et détruit les clés de session correspondantes.

TCS_98 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Clés et algorithmes implicitement connus
P2	1	'00h'	
Lc	1	'XXh'	Lc (longueur des données transmises à la carte)
#6-#(5+L)	L	'XX..XXh'	Authentification de génération 1 : cryptogramme (voir **sous-**appendice 11, partie A) Authentification de génération 2 : signature générée par le périphérique d'interface (voir **sous-**appendice 11, partie B)

TCS_99 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- Si l'ADC de la clé publique active n'est pas la concaténation de l'identificateur de l'application tachygraphique et d'un type d'équipement d'UEV, le logiciel renvoie un état de traitement **'6F00'** ;
- Si la commande n'est pas immédiatement précédée d'une commande GET CHALLENGE, le logiciel renvoie l'état de traitement **'6985'**.

L'application tachygraphique de génération 1 peut en outre renvoyer les codes d'erreur suivants :

- Si aucune clé publique n'est présente dans l'environnement de sécurité, le logiciel renvoie l'état de traitement **'6A88'** ;
- Si aucune clé privée n'est présente dans l'environnement de sécurité, le logiciel renvoie l'état de traitement **'6A88'** ;
- Si la vérification du cryptogramme échoue, le logiciel renvoie l'état de traitement **'6688'** ;
- Si la clé privée sélectionnée est considérée comme altérée, le logiciel renvoie l'état de traitement **'6400'** ou **'6581'**.

La variante de la commande destinée à l'authentification de génération 2 peut également renvoyer le code d'erreur suivant :

- Si la vérification de la signature échoue, la carte renvoie '**6300**'.

3.5.10 GENERAL AUTHENTICATE (authentification générale)

Cette commande sert au protocole d'authentification du circuit intégré de génération 2 défini ~~à l'appendice~~ **au sous-appendice** 11, partie B, et est conforme à la norme ISO/CEI 7816-4.

TCS_100 La commande peut être exécutée dans le MF, le DF Tachograph et le DF Tachograph_G2 (voir également **TCS_34**).

TCS_101 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	Clés et protocoles implicitement connus
P2	1	'00h'	
Lc	1	'NNh'	Lc : longueur de la zone de données suivante
#6-#(5+L)	L	'7Ch' + L_{7C} + '80h' + L_{80} + 'XX..XXh'	Valeur de la clé publique éphémère et codée en DER-TLV (voir **sous**-appendice 11) L'UEV doit envoyer les objets de données dans cet ordre.
~~**5 + Le + 1**~~	**1**	**'00h'**	**Conformément à ISO/CEI 7816-4**

TCS_102 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
#1-#L	L	'7Ch' + L_{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L_{82} + 'XX..XXh'	Données d'authentification dynamique codées en DER-TLV : jeton 'nonce' et jeton d'authentification (voir **sous-**appendice 11)
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- La carte renvoie '**6A80**' pour indiquer des paramètres incorrects dans la zone de données ;
- La carte renvoie '**6982**' si la commande EXTERNAL AUTHENTICATE échoue.

L'objet de données d'authentification dynamique '7Ch' :

- Doit être présent si l'opération aboutit, c'est-à-dire si les mots d'état sont '**9000**' ;
- Doit être absent en cas d'erreur d'exécution ou de vérification, c'est-à-dire si les mots d'état se situent entre '**6400**' et '**6FFF**' ;
- Peut être absent en cas d'avertissement, c'est-à-dire si les mots d'état se situent entre '**6200**' et '**63FF**'.

3.5.11 MANAGE SECURITY ENVIRONMENT (gestion de l'environnement de sécurité)

Cette commande permet de définir une clé publique à des fins d'authentification.

3.5.11.1 Commande de génération 1 : paire de réponses

Cette commande est conforme à la norme ISO/CEI 7816-4. Son usage est restreint par rapport à la commande analogue définie dans la norme en question.

TCS_103 Cette commande est uniquement prise en charge par une application tachygraphique de génération 1.

TCS_104 La clé désignée dans la zone de données MSE reste la clé publique active jusqu'à la commande MSE correcte suivante, la sélection d'un DF ou la réinitialisation de la carte.

TCS_105 Si la clé mentionnée n'est pas (encore) présente dans la mémoire de la carte, l'environnement de sécurité reste inchangé.

TCS_106 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1 : clé désignée valable pour l'ensemble des opérations cryptographiques
P2	1	'B6h'	P2 (données désignées concernant la signature numérique)
Lc	1	'0Ah'	Lc : longueur de la zone de données suivante
#6	1	'83h'	Balise indiquant une clé publique en cas d'asymétrie
#7	1	'08h'	Longueur de la désignation de la clé (identificateur de clé)

Octet	*Longueur*	*Valeur*	*Description*
#8-#15	8	'XX..XXh'	Identificateur de clé comme spécifié ~~à l'appendice~~ **au sous-appendice** 11

TCS_107 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- Si la clé désignée n'est pas présente dans la mémoire de la carte, le logiciel renvoie l'état de traitement **'6A88'** ;
- S'il manque certains objets de données attendus dans la structure de messagerie sécurisée, le logiciel renvoie l'état de traitement **'6987'**. Cet événement est susceptible de se produire si la balise '83h' fait défaut ;
- Si certains objets de données sont incorrects, le logiciel renvoie l'état de traitement **'6988'**. Cet événement est susceptible de se produire si la longueur de l'identificateur de clé ne correspond pas à '08h' ;
- Si la clé sélectionnée est considérée comme altérée, le logiciel renvoie l'état de traitement **'6400'** ou **'6581'**.

3.5.11.2 Commande de génération 2 : paire de réponses

Pour l'authentification de génération 2, la carte tachygraphique prend en charge les variantes suivantes de la commande MSE:SET qui sont conformes à la norme ISO/CEI 7816-4. Ces variantes de commande ne sont pas adaptées à l'authentification de génération 1.

3.5.11.2.1 MSE:SET AT pour l'authentification d'un circuit intégré

La commande MSE:SET AT ci-après sert à sélectionner les paramètres en vue de l'authentification du circuit intégré effectuée à l'aide d'une commande GENERAL AUTHENTICATE ultérieure.

TCS_108 La commande peut être exécutée dans le MF, le DF Tachograph et leDF Tachograph_G2 (voir TCS_34).

TCS_109 Message de commande MSE:SET AT pour l'authentification d'un circuit intégré

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'41h'	Défini pour l'authentification interne
P2	1	'A4h'	Authentification
Lc	1	'NNh'	Lc : longueur de la zone de données suivante

Octet	*Longueur*	*Valeur*	*Description*
#6-#(5+L)	L	‘80h’ + ‘0Ah’ + ‘XX..XXh’	Référence du mécanisme cryptographique codé en DER-TLV : identificateur d’objet correspondant à l’authentification du circuit (valeur uniquement, balise ‘06h’ absente) Voir **sous-**appendice 1 pour les valeurs attribuées aux identificateurs d’objets ; utiliser la notation en octets. Voir **sous-**appendice 11 pour les instructions relatives à la sélection de l’un de ces identificateurs d’objet

3.5.11.2.2 MSE:SET AT pour l’authentification d’une UEV

La commande MSE:SET AT ci-après sert à sélectionner les paramètres et les clés en vue de l’authentification de l’UEV effectuée à l’aide d’une commande EXTERNAL AUTHENTICATE ultérieure.

TCS_110 La commande peut être exécutée dans le MF, le DF Tachograph et le DF Tachograph_G2 (voir TCS_34).

TCS_111 **Message de commande MSE:SET AT pour l’authentification d’une UEV**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Défini pour l’authentification externe
P2	1	‘A4h’	Authentification
Lc	1	‘NNh’	Lc : longueur de la zone de données suivante
#6-#(5+L)	L	‘80h’ + ‘0Ah’ + ‘XX..XXh’	Référence du mécanisme cryptographique codé en DER-TLV : identificateur d’objet correspondant à l’authentification de l’UEV (valeur uniquement, balise ‘06h’ absente)
			Voir **sous-**appendice 1 pour les valeurs des identificateurs d’objets ; utiliser la notation en octets.
			Voir **sous-**appendice 11 pour les instructions relatives à la sélection de l’un de ces identificateurs d’objet
		‘83h’ + ‘08h’ + ‘XX..XXh’	Référence de la clé publique de l’UEV codée en DER-TLV, c’est-à-dire la référence du détenteur de certificat figurant dans le certificat de la clé publique
		‘91h’ + L_{91} + ‘XX..XXh’	Représentation compressée et codée en DER-TLV de la clé publique éphémère de l’UEV qui servira pendant l’authentification du circuit (voir **sous-**appendice 11)

3.5.11.2.3 MSE:SET DST

La commande MSE:SET DST ci-après sert à définir une clé publique :

- Soit en vue de vérifier une signature fournie dans le cadre d’une commande PSO:VERIFY DIGITAL SIGNATURE ultérieure ;
- Soit en vue de vérifier une signature ou un certificat fourni dans la cadre d’une commande PSO:VERIFY CERTIFICATE ultérieure.

TCS_112 La commande peut être exécutée dans le MF, le DF Tachograph et le DF Tachograph_G2 (voir TCS_33).

TCS_113 Message de commande MSE:SET DST

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Défini pour la vérification
P2	1	‘B6h’	Signature numérique
Lc	1	‘NNh’	Lc : longueur de la zone de données suivante
#6-#(5+L)	L	‘83h’ + ‘08h’ + ‘XX...XXh’	Référence d’une clé publique codée en DER-TLV, c’est-à-dire la référence du détenteur de certificat figurant dans le certificat de la clé publique (voir **sous-**appendice 11)

Pour toutes les versions de la commande, la structure du message de réponse et les mots d’état sont les suivants :

TCS_114 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
ME	2	‘XXXXh’	Mots d’état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l’état ‘**9000**’. Le protocole a été sélectionné et initialisé ;
- **‘6A80’** indique des paramètres incorrects dans la zone de données de la commande ;
- **‘6A88’** indique que les données de référence (par exemple, une clé désignée) ne sont pas disponibles ;
- **Si le currentAuthenticatedTime est ultérieur à la date d’expiration de la clé publique sélectionnée, le logiciel renvoie l’état de traitement ‘6A88’.**

Remarque : dans le cas d’une commande MSE:SET AT destinée à l’authentification d’une UEV, la clé désignée est une clé publique de type UEV_MA. La carte définit la clé publique UEV_MA à utiliser, si celle-ci est disponible dans sa mémoire ; ladite clé correspond à la référence du détenteur de certificat (RDC) indiquée dans la zone de données de la commande (la carte peut identifier les clés publiques UEV_MA au moyen du champ ADC du certificat). Une carte renvoie l’état ‘6A88’ si la clé publique UEV_Sign est la seule disponible ou si aucune clé publique de l’UEV n’est disponible. Voir la définition du champ ADC au sous-appendice 11 et du type de données equipmentType au sous-appendice 1.

De même, si une commande MSE:SET DST renvoyant à un type d’équipement (une UEV ou une carte) est envoyée à une carte de contrôleur, conformément à l’exigence CSM_234, la clé désignée est toujours une clé de type EQT_Sign et doit être utilisée pour vérifier une signature numérique. Conformément à la figure 13 du sous-appendice 11, la carte de contrôleur enregistrera toujours la clé publique EQT_Sign appropriée. Dans certains cas, il est possible que la carte de contrôleur enregistre la clé publique EQT_MA correspondante. La carte de contrôleur doit toujours définir la clé publique EQT_Sign comme étant la clé à utiliser lorsqu’elle reçoit une commande MSE:SET DST.

3.5.12 PSO : HASH (hachage)

Cette commande permet de transférer vers la carte le résultat du calcul de hachage auquel certaines données sont soumises. Cette commande s'emploie lors de la vérification des signatures numériques. La valeur de hachage est enregistrée temporairement en vue d'une commande PSO : VERIFY DIGITAL SIGNATURE ultérieure.

Cette commande est conforme à la norme ISO/CEI 7816-8. Son usage est restreint par rapport à la commande analogue définie dans la norme en question.

Seule la carte de contrôleur doit prendre en charge cette commande dans les DF Tachograph et DF Tachograph_G2.

D'autres types de cartes tachygraphiques peuvent ou non exécuter cette commande. La commande peut être accessible ou non dans le MF.

L'application de la carte de contrôleur de génération 1 prend uniquement en charge SHA-1.

TCS_115 La valeur de hachage enregistrée temporairement doit être supprimée si une nouvelle valeur de hachage est calculée à l'aide de la commande PSO : HASH, si un DF est sélectionné et si la carte tachygraphique est réinitialisée.

TCS_116 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	CLA
INS	1	'2Ah'	Exécution d'une opération de sécurité (PSO)
P1	1	'90h'	Renvoi d'un code de hachage
P2	1	'A0h'	Balise : zone de données contenant les objets de données pertinents pour le hachage
Lc	1	'XXh'	Longueur Lc de la zone de données suivante
#6	1	'90h'	Balise indiquant le code de hachage
#7	1	'XXh'	Longueur L du code de hachage : '14h' dans l'application de génération 1 (voir **sous-**appendice 11, partie A) '20h', '30h' ou '40h' dans l'application de génération 2 (voir **sous-**appendice 11, partie B)
#8-#(7+L)	L	'XX..XXh'	Code de hachage

TCS_117 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- S'il manque certains objets de données attendus (définis ci-avant), le logiciel renvoie l'état de traitement **'6987'**. Cet événement est susceptible de se produire si la balise '90h' fait défaut ;
- Si certains objets de données sont incorrects, le logiciel renvoie l'état de traitement **'6988'**. Cette erreur survient lorsque la balise requise est présente, mais a une longueur différente de '14h' pour SHA-1, '20h' pour SHA-256, '30h' pour SHA-384, '40h' pour SHA-512 (application de génération 2).

3.5.13 PERFORM HASH OF FILE (hachage d'un fichier)

Cette commande n'est pas conforme à la norme ISO/CEI 7816-8. L'octet CLA de cette commande indique donc un usage exclusif de la commande PERFORM SECURITY OPERATION/HASH.

Seules les cartes de conducteur et d'atelier doivent prendre en charge cette commande dans le DF Tachograph et le DF Tachograph_G2.

D'autres types de cartes tachygraphiques peuvent ou non mettre en œuvre cette commande. Si une carte d'entreprise ou de contrôleur met en œuvre cette commande, celle-ci doit être exécutée conformément aux dispositions du présent chapitre.

La commande peut être accessible ou non dans le MF. Le cas échéant, la commande doit être exécutée comme prévu dans le présent chapitre, c'est-à-dire qu'elle ne doit pas permettre le calcul d'une valeur de hachage et doit se terminer par un code d'erreur approprié.

TCS_118 La commande PERFORM HASH OF FILE est utilisée pour hacher la zone de données de l'EF transparent sélectionné.

TCS_119 Une carte tachygraphique doit prendre en charge cette commande uniquement pour les EF figurant au chapitre 0 sous les DF_Tachograph et DF_Tachograph_G2, et en tenant compte de l'exception qui suit. Une carte tachygraphique ne doit pas prendre en charge cette commande pour l'EF Sensor_Installation_Data du DF Tachograph_G2.

TCS_120 Le résultat de l'opération de hachage est enregistré temporairement dans la mémoire de la carte. Il pourra être utilisé par la suite pour obtenir la signature numérique d'un fichier à l'aide de la commande PSO : COMPUTE DIGITAL SIGNATURE.

TCS_121 La valeur de hachage du fichier enregistrée temporairement doit être supprimée si une nouvelle valeur de hachage de fichier est calculée à l'aide de la commande ~~PSO :~~ PERFORM HASH OF FILE, si un DF est sélectionné et si la carte tachygraphique est réinitialisée.

TCS_122 L'application tachygraphique de génération 1 doit prendre en charge SHA-1.

TCS_123 L'application tachygraphique **de génération 2** doit prendre en charge l'algorithme ~~SHA-1 et~~ SHA-2 (**SHA-**256, **SHA-**384 ~~et~~ **ou SHA-**512 ~~bits~~) **désigné par la suite de chiffres prévue au sous-appendice 11, partie B, pour la clé de signature de la carte (Card Sign).**

TCS_124 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'80h'	CLA
INS	1	'2Ah'	Exécution d'une opération de sécurité (PSO)
P1	1	'90h'	Balise : Hash

Octet	*Longueur*	*Valeur*	*Description*
P2	1	~~XXh~~ '00h'	~~P2 : indique l'algorithme à utiliser pour le hachage des données du fichier transparent sélectionné :~~ **Algorithme implicitement connu** **Pour l'application tachygraphique de génération 1 : SHA-1** **Pour l'application tachygraphique de génération 2 : SHA-2 (SHA-256, SHA-384 et ou SHA-512 bits) désigné par la suite de chiffres prévue au sous-appendice 11, partie B, pour la clé de signature de la carte (Card Sign)** ~~'00h' pour SHA-1~~ ~~'01h' pour SHA-256~~ ~~'02h' pour SHA-384~~ ~~'03h' pour SHA-512~~

TCS_125 **Message de réponse**

Octet	*Longueur*	*Valeur*	*Description*
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- Si l'EF actif ne permet pas cette commande (EF Sensor_Installation_Data dans le DF Tachograph_G2), le logiciel renvoie l'état de traitement **'6985'** ;
- Si l'EF sélectionné est considéré comme altéré (une erreur d'intégrité est détectée dans les attributs du fichier ou dans les données enregistrées), le logiciel renvoie l'état de traitement '**6400**' ou **'6581'** ;
- Si le fichier sélectionné n'est pas un fichier transparent ou s'il n'existe aucun EF actif, le logiciel renvoie l'état de traitement '**6986**'.

3.5.14 PSO : COMPUTE DIGITAL SIGNATURE (calcul de la signature numérique)

Cette commande permet de calculer la signature numérique du code de hachage préalablement calculé (voir la commande PERFORM HASH OF FILE au paragraphe ~~3.5.13~~ **5.13**).

Seules les cartes de conducteur et d'atelier doivent prendre en charge cette commande dans le DF Tachograph et le DF Tachograph_G2.

D'autres types de cartes tachygraphiques peuvent ou non mettre en œuvre cette commande~~, mais ne disposent~~. **Dans le cas de l'application tachygraphique de génération 2, seules les cartes de conducteur et** d'atelier disposent d'une ~~d'aucune~~ clé de signature **de génération 2**. ~~Par conséquent, ces~~ **Les autres** cartes **ne parviennent donc pas à** exécuter cette commande avec succès ~~mais~~ **et** l'interrompe par un code d'erreur approprié.

La commande peut être accessible ou non dans le MF. ~~Dans ce cas,~~**Si** la commande **n'est pas accessible dans le MF,** elle doit être interrompue avec un code d'erreur approprié.

Cette commande est conforme à la norme ISO/CEI 7816-8. Son usage est restreint par rapport à la commande analogue définie dans la norme en question.

TCS_126 Cette commande ne doit pas calculer une signature numérique pour un code de hachage préalablement calculé avec la commande PSO : HASH.

TCS_127 La clé privée de la carte permet de calculer la signature numérique et est implicitement connue de la carte.

TCS_128 L'application tachygraphique de génération 1 exécute une signature numérique en recourant à une méthode de remplissage conforme à la norme PKCS1 (pour de plus amples informations, voir **sous-**appendice 11).

TCS_129 L'application tachygraphique de génération 2 calcule une signature numérique basée sur une courbe elliptique (pour de plus amples informations, voir **sous-**appendice 11).

TCS_130 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	CLA
INS	1	'2Ah'	Exécution d'une opération de sécurité (PSO)
P1	1	'9Eh'	Signature numérique à renvoyer
P2	1	'9Ah'	Balise : zone de données contenant les données à signer.
			Comme aucune zone de données n'est incluse, les données sont supposées être déjà présentes sur la carte (hachage du fichier).
Le	1	'NNh'	Longueur de la signature attendue

TCS_131 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
#1-#L	L	'XX..XXh'	Signature correspondant au hachage préalablement calculé
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l'état '**9000**' ;
- Si la clé privée implicitement sélectionnée est considérée comme altérée, le logiciel renvoie l'état de traitement '**6400**' ou **'6581'** ;
- Si le hachage calculé lors d'une exécution antérieure de la commande PERFORM HASH OF FILE n'est pas disponible, le logiciel renvoie l'état de traitement **'6985'**.

3.5.15 PSO : VERIFY DIGITAL SIGNATURE (vérification de la signature numérique)

Cette commande sert à vérifier la signature numérique, fournie comme une entrée, dont la carte connaît le hachage. La carte connaît implicitement l'algorithme de signature.

Cette commande est conforme à la norme ISO/CEI 7816-8. Son usage est restreint par rapport à la commande analogue définie dans la norme en question.

Seule la carte de contrôleur doit prendre en charge cette commande dans le DF Tachograph et le DF Tachograph_G2.

D'autres types de cartes tachygraphiques peuvent ou non exécuter cette commande. La commande peut ou non être accessible dans le MF.

TCS_132 La commande VERIFY DIGITAL SIGNATURE utilise toujours la clé publique sélectionnée par l'intermédiaire de la précédente commande de gestion de l'environnement de sécurité MSE:SET DST et du code de hachage antérieur introduit au moyen d'une commande PSO : HASH.

TCS_133 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Exécution d’une opération de sécurité (PSO)
P1	1	‘00h’	
P2	1	‘A8h’	Balise : zone de données contenant les objets de données utiles pour la vérification
Lc	1	~~83h~~’**XXh**’	Longueur Lc de la zone de données suivante
6	1	‘9Eh’	Balise indiquant une signature numérique
#7-#8	2	~~81 XXh~~ **‘NNh’ ou ‘81NNh’**	Longueur de la signature numérique **(L équivaut à 2 octets si la longueur de la signature numérique est supérieure à 127 octets)** : 128 octets codés conformément ~~à l’appendice~~ **au sous-appendice** 11, partie A, pour l’application tachygraphique de génération 1 Selon la courbe retenue pour l’application tachygraphique de génération 2 (voir **sous-**appendice 11, partie B)
#9-#(8+L)	L	‘XX..XXh’	Contenu de la signature numérique

TCS_134 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
ME	2	‘XXXXh’	Mots d’état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l’état ‘**9000**’ ;
- Si la vérification de la signature échoue, le logiciel renvoie l’état de traitement **‘6688’**. La procédure de vérification est décrite ~~à l’appendice~~**au sous-appendice** 11 ;
- Si aucune clé publique n’est sélectionnée, le logiciel renvoie l’état de traitement **‘6A88’** ;
- S’il manque certains objets de données attendus (définis ci-avant), le logiciel renvoie l’état de traitement **‘6987’**. Cet événement est susceptible de se produire si l’une des balises requises fait défaut ;
- Si aucun code de hachage n’est disponible pour traiter la commande (en raison du traitement d’une commande PSO: HASH antérieure), le logiciel renvoie l’état de traitement **‘6985’**.
- Si certains objets de données sont incorrects, le logiciel renvoie l’état de traitement **‘6988’**. Cette erreur est susceptible de se produire si la longueur de l’un des objets de données requis est incorrecte.
- Si la clé publique sélectionnée est considérée comme altérée, le logiciel renvoie l’état de traitement **‘6400’** ou **‘6581’**.
- **Si la clé publique sélectionnée (et utilisée pour vérifier la signature numérique) possède un CHA.LSB (CertificateHolderAuthorisation.equipmentType) qui ne se prête pas à la vérification du certificat comme prévu au sous-appendice 11, le logiciel renvoie l’état de traitement ‘6985’.**

3.5.16 PROCESS DSRC MESSAGE

Cette commande sert à vérifier l'intégrité et l'authenticité du message DSRC et à déchiffrer les données communiquées par une UEV à une autorité de contrôle ou à un atelier au moyen d'une connexion DSRC. La carte extrait la clé de chiffrement et la clé MAC utilisées pour sécuriser le message DSRC comme décrit ~~à l'appendice~~ **au sous-appendice** 11, partie B, chapitre 13.

Seules les cartes de contrôleur et d'atelier doivent prendre en charge cette commande dans le DF Tachograph_G2.

D'autres types de cartes tachygraphiques peuvent mettre en œuvre cette commande, mais elles ne disposent d'aucune clé maîtresse DSRC. Ces cartes ne peuvent donc pas exécuter cette commande correctement et l'interrompent avec un code d'erreur approprié.

La commande peut être accessible dans le MF et/ou le DF Tachograph ou ne pas l'être. Dans ce second cas, la commande doit être interrompue avec un code d'erreur approprié.

TCS_135 La clé maîtresse DSRC est accessible uniquement dans le DF Tachograph_G2, autrement dit les cartes de contrôleur et d'atelier doivent prendre en charge l'exécution de la commande uniquement dans ce fichier.

TCS_136 La commande doit uniquement déchiffrer les données DSRC et vérifier le total de contrôle cryptographique, mais sans interpréter les données entrantes.

TCS_137 L'ordre des objets de données dans la zone de données de la commande est défini par la présente spécification.

TCS_138 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'80h'	CLA exclusif
INS	1	'2Ah'	Exécution d'une opération de sécurité (PSO)
P1	1	'80h'	Données de la réponse : valeur en clair
P2	1	'B0h'	Données de la commande : valeur en clair codée en BER-TLV et incluant les objets de données de messagerie sécurisée
Lc	1	'NNh'	Longueur Lc de la zone de données suivante
#6-#(5+L)	L	'87h' + L_{87} + 'XX..XXh'	Octet indicateur de contenu de remplissage codé en DER-TLV, suivi des données tachygraphiques utiles codées. Pour l'octet indicateur de contenu de remplissage, il convient d'utiliser la valeur '00h' ('aucune autre information' conformément à la norme ISO/CEI 7816-4:2013, tableau 52). Concernant le mécanisme de chiffrement, voir **sous**-appendice 11, partie B, chapitre 13. Pour l'octet indicateur de contenu de remplissage, les longueurs L_{87} admises sont les multiples de la longueur du bloc AES plus 1, soit entre 17 octets et 193 octets inclus. Remarque : pour l'objet de données de messagerie sécurisée doté de la balise '87h', voir la norme ISO/CEI 7816-4:2013, tableau 49.

Octet	*Longueur*	*Valeur*	*Description*
		‘81h’ + ‘10h’	Modèle de référence pour le contrôle de la confidentialité codé en DER-TLV et intégrant la concaténation des éléments de données suivants (voir ‘DSRCSecurityData’ ~~à l’appendice~~ **au sous-appendice 1** et **sous-**appendice 11, partie B, chap. 13) :
			horodatage sur 4 octets ;
			compteur sur 3 octets ;
			numéro de série de l’UEV sur 8 octets ;
			version de la clé maîtresse DSRC sur 1 octet.
			Remarque : pour l’objet de données de messagerie sécurisée doté de la balise ‘81h’, voir la norme ISO/CEI 7816-4:2013, tableau 49.
		‘8Eh’ + L8E + ‘XX..XXh’	MAC codé en DER-TLV sur le message DSRC. Pour l’algorithme et le calcul des MAC, voir **sous-**appendice 11, partie B, chapitre 13.
			Remarque : pour l’objet de données de messagerie sécurisée doté de la balise ‘8Eh’, voir la norme ISO/CEI 7816-4:2013, tableau 49.
~~5 + Le + 1~~	**1**	**‘00h’**	**Conformément à la norme ISO/CEI 7816-4**

TCS_139 Message de réponse

Octet	*Longueur*	*Valeur*	*Description*
#1-#L	L	‘XX..XXh’	Données absentes (en cas d’erreur) ou déchiffrées (contenu de remplissage supprimé)
ME	2	‘XXXXh’	Mots d’état (ME1, ME2)

- Si la commande aboutit, la carte renvoie l’état ‘**9000**’ ;
- **‘6A80’** indique la présence de paramètres incorrects dans la zone de données de la commande (également utilisé dans le cas où les objets de données ne sont pas envoyés dans l’ordre spécifié) ;
- **‘6A88’** indique que les données désignées, telles que la clé maîtresse DSRC désignée, ne sont pas disponibles ;
- **‘6900’** indique l’échec de la vérification du total de contrôle cryptographique ou du déchiffrement des données ;
- **‘6985’ indique que l’horodatage sur 4 octets figurant dans la zone de données de la commande est antérieur à la cardValidityBegin ou postérieur à la cardExpiryDate.**

4. Structure des cartes tachygraphiques

Le présent chapitre définit les structures de fichiers des cartes tachygraphiques en vue du stockage des données accessibles.

Il n’apporte aucune précision quant aux structures internes qui dépendent du fabricant (en-têtes des fichiers, par exemple). Il n’aborde pas non plus le stockage et le traitement des éléments de données à usage interne tels que EuropeanPublicKey, CardPrivateKey, TDesSessionKey ou WorkshopCardPin.

TCS_140 Une carte tachygraphique de génération 2 doit héberger le fichier maître (MF), ainsi qu'une application tachygraphique de génération 1 et une application tachygraphique de génération 2 de même type (applications de cartes de conducteur, par exemple).

TCS_141 Une carte tachygraphique doit au moins prendre en charge le nombre d'enregistrements spécifiés pour les applications correspondantes et ne doit pas prendre en charge plus d'enregistrements que le nombre maximum d'enregistrements spécifiés pour ces applications.

Les nombres minimum et maximum d'enregistrements sont définis dans le présent chapitre pour les différentes applications. **Dans la version 2 des cartes de conducteur et d'atelier de génération 2, l'application de génération 1 doit prendre en charge le nombre maximum d'enregistrements spécifiés aux points TCS_150 et TCS_158.**

Pour des informations sur les conditions de sécurité définies dans les règles d'accès présentées tout au long du présent chapitre, il convient de consulter la section **3.3**. En règle générale, le mode d'accès « lecture » désigne la commande READ BINARY avec un octet INS pair et, si possible, un octet INS impair, sauf pour l'EF Sensor_Installation_Data de la carte d'atelier (voir **TCS_156 et TCS_160**). Le mode d'accès « actualisation » désigne la commande UPDATE BINARY avec un octet INS pair et, si possible, un octet INS impair, et le mode d'accès « sélection » désigne la commande SELECT.

4.1 Fichier maître (MF)

TCS_142 Après personnalisation, le fichier maître MF doit avoir la structure de fichiers et les règles d'accès aux fichiers permanentes qui suivent :

Remarque : l'identificateur d'EF court (IDFC) est donné sous la forme d'un nombre décimal, par exemple la valeur 30 correspond au nombre binaire 11110.

					Règles d'accès	
Fichier			**ID de fichier**	**IDFC**	**Lecture/Sélection**	**Actualisation**
MF			'3F00h'			
EF	ICC		'0002h'		TJR	JMS
EF	IC		'0005h'		TJR	JMS
EF	DIR		'2F00h'	30	TJR	JMS
EF	ATR/INFO (conditionnel)		'2F01h'	29	TJR	JMS
EF	Extended_Length (conditionnel)		'0006h'	28	TJR	JMS
DF	Tachograph		'0500h'		SC1	
DF	Tachograph_G2				SC1	

Dans le tableau ci-dessus, l'abréviation suivante est utilisée pour désigner la condition de sécurité :

SC1 TJR OU MS-MAC-G2

TCS_143 La structure de tous les EF doit être transparente.

TCS_144 Le fichier maître MF doit présenter la structure de données suivante :

Fichier/Élément de données	*Nombre d'enregistrements*	*Taille (octets)* Min.	Max.	*Valeurs par défaut*
MF		*63*	*184*	
EF ICC		*25*	*25*	
CardIccIdentification		*25*	*25*	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		*8*	*8*	
CardChipIdentification		*8*	*8*	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
EF DIR		*20*	*20*	
Voir TCS_145		*20*	*20*	{00..00}
EF ATR/INFO		*7*	*128*	
Voir TCS_146		*7*	*128*	{00..00}
EF EXTENDED_LENGTH		*3*	*3*	
Voir TCS_147		*3*	*3*	{00..00}
DF Tachograph				
DF Tachograph_G2				

TCS_145 Le fichier élémentaire EF DIR doit contenir les objets de données relatifs à l'application suivants : '61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54'.

TCS_146 Le fichier élémentaire EF ATR/INFO doit être présent si la carte tachygraphique indique dans son ATR qu'elle prend en charge des zones de longueur étendue. Dans ce cas, l'EF ATR/INFO doit contenir les objets de données de longueur étendue (DO'7F66') comme indiqué dans la clause 12.7.1 de la norme ISO/CEI 7816-4:2013.

TCS_147 Le fichier élémentaire EF Extended_Length doit être présent si la carte tachygraphique indique dans son ATR qu'elle prend en charge des zones de longueur étendue. Dans ce cas, l'EF doit contenir l'objet de données '02 01 xx' dont la valeur 'xx' indique si les zones de longueur étendue sont prises en charge pour les protocoles T = 1 et/ou T = 0.

La valeur '01' indique que la zone de longueur étendue est prise en charge pour le protocole T = 1.

La valeur '10' indique que la zone de longueur étendue est prise en charge pour le protocole T = 0.

La valeur '11' indique que la zone de longueur étendue est prise en charge pour les protocoles T = 1 et T = 0.

4.2 Applications des cartes de conducteur

4.2.1 Application de carte de conducteur de génération 1

TCS_148 Après personnalisation, l'application de la carte de conducteur de génération 1 doit avoir la structure de fichiers et les règles d'accès aux fichiers permanentes suivantes :

Fichier			ID de fichier	Règles d'accès		
				Lecture	Sélection	Actualisation
DF	Tachograph		'0500h'		SC1	
EF		Application_Identification	'0501h'	SC2	SC1	JMS
EF		Card_Certificate	'C100h'	SC2	SC1	JMS
EF		CA_Certificate	'C108h'	SC2	SC1	JMS
EF		Identification	'0520h'	SC2	SC1	JMS
EF		Card_Download	'050Eh'	SC2	SC1	SC1
EF		Driving_Licence_Info	'0521h'	SC2	SC1	JMS
EF		Events_Data	'0502h'	SC2	SC1	SC3
EF		Faults_Data	'0503h'	SC2	SC1	SC3
EF		Driver_Activity_Data	'0504h'	SC2	SC1	SC3
EF		Vehicles_Used	'0505h'	SC2	SC1	SC3
EF		Places	'0506h'	SC2	SC1	SC3
EF		Current_Usage	'0507h'	SC2	SC1	SC3
EF		Control_Activity_Data	'0508h'	SC2	SC1	SC3
EF		Specific_Conditions	'0522h'	SC2	SC1	SC3

Dans le tableau ci-dessus, les abréviations suivantes sont utilisées pour désigner les conditions de sécurité :

SC1 TJR OU MS-MAC-G2

SC2 TJR OU MS-MAC-G1 OU MS-MAC-G2

SC3 MS-MAC-G1 OU MS-MAC-G2

TCS_149 La structure de tous les EF doit être transparente.

TCS_150 L'application de la carte de conducteur de génération 1 doit présenter la structure de données suivante :

Fichier/Élément de données	Nombre d'enregistrements	Taille (octets) Min.	Taille (octets) Max.	Valeurs par défaut
DF Tachograph	*11378*	*24926*		
EF Application_Identification	*10*	*10*		
DriverCardApplicationIdentification	*10*	*10*		
typeOfTachographCardId	1	1	{00}	
cardStructureVersion	2	2	{00 00}	
noOfEventsPerType	1	1	{00}	
noOfFaultsPerType	1	1	{00}	
activityStructureLength	2	2	{00 00}	
noOfCardVehicleRecords	2	2	{00 00}	
noOfCardPlaceRecords	1	1	{00}	
EF Card_Certificate	*194*	*194*		
CardCertificate	194	194	{00..00}	

EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{**00**, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	**{00...00}**
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
CardVehiclesUsed		*2606*	*6202*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*2604*	*6200*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}

vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
CardPlaceDailyWorkPeriod		*841*	*1121*	
placePointerNewestRecord		1	1	{00}
placeRecords		*840*	*1120*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
SpecificConditionRecord	56	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_151 Employées pour indiquer les tailles dans le tableau ci-dessus, les valeurs qui suivent correspondent aux nombres d'enregistrements minimum et maximum que doit utiliser la structure de données de la carte de conducteur pour une application de génération 1 :

		Min.	*Max.*
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 octets (28 jours * 93 changements d'activité)	13 776 octets (28 jours * 240 changements d'activité)

4.2.2 Application de la carte de conducteur de génération 2

TCS_152 Après personnalisation, l'application de la carte de conducteur de génération 2 doit avoir la structure de fichiers et les règles d'accès aux fichiers permanentes qui suivent :

Remarques :

- **L'identificateur d'EF court (IDFC) est donné sous la forme d'un nombre décimal, par exemple la valeur 30 correspond au nombre binaire 11110 ;**
- **Les fichiers EF Application_Identification_V2, EF Places_Authentication, EF GNSS_Places_Authentication, EF Border_Crossings, EF Load_Unload_Operations, EF VU_Configuration et EF Load_Type_Entries ne sont présents que dans la version 2 de la carte de conducteur de génération 2 ;**
- **La valeur attribuée à cardStructureVersion dans l'EF Application_Identification est égale à {01 01} pour la version 2 de la carte de conducteur de génération 2, alors qu'elle était égale à {01 00} pour la version 1 de la carte de conducteur de génération 2.**

~~Fichier~~	~~ID de fichier~~	~~IDFC~~	~~Règles d'accès~~ ~~Lecture / Sélection~~	~~Actualisation~~
~~└─DF Tachograph_G2~~			~~SC1~~	
~~├─EF Application_Identification~~	~~'0501h'~~	~~1~~	~~SC1~~	~~JMS~~
~~├─EF CardMA_Certificate~~	~~'C100h'~~	~~2~~	~~SC1~~	~~JMS~~
~~├─EF CardSignCertificate~~	~~'C101h'~~	~~3~~	~~SC1~~	~~JMS~~
~~├─EF CA_Certificate~~	~~'C108h'~~	~~4~~	~~SC1~~	~~JMS~~
~~├─EF Link_Certificate~~	~~'C109h'~~	~~5~~	~~SC1~~	~~JMS~~
~~├─EF Identification~~	~~'0520h'~~	~~6~~	~~SC1~~	~~JMS~~
~~├─EF Card_Download~~	~~'050Eh'~~	~~7~~	~~SC1~~	~~SC1~~
~~├─EF Driving_Licence_Info~~	~~'0521h'~~	~~10~~	~~SC1~~	~~JMS~~
~~├─EF Events_Data~~	~~'0502h'~~	~~12~~	~~SC1~~	~~MS-MAC-G2~~
~~├─EF Faults_Data~~	~~'0503h'~~	~~13~~	~~SC1~~	~~MS-MAC-G2~~
~~├─EF Driver_Activity_Data~~	~~'0504h'~~	~~14~~	~~SC1~~	~~MS-MAC-G2~~
~~├─EF Vehicles_Used~~	~~'0505h'~~	~~15~~	~~SC1~~	~~MS-MAC-G2~~
~~├─EF Places~~	~~'0506h'~~	~~16~~	~~SC1~~	~~MS-MAC-G2~~
~~├─EF Current_Usage~~	~~'0507h'~~	~~17~~	~~SC1~~	~~MS-MAC-G2~~
~~├─EF Control_Activity_Data~~	~~'0508h'~~	~~18~~	~~SC1~~	~~MS-MAC-G2~~
~~├─EF Specific_Conditions~~	~~'0522h'~~	~~19~~	~~SC1~~	~~MS-MAC-G2~~
~~├─EF VehicleUnits_Used~~	~~'0523h'~~	~~20~~	~~SC1~~	~~MS-MAC-G2~~
~~└─EF GNSS_Places~~	~~'0524h'~~	~~21~~	~~SC1~~	~~MS-MAC-G2~~

Fichier	**ID de fichier**	**IDFC**	**Règles d'accès** **Lecture/ Sélection**	**Actualisation**
└─DF Tachograph_G2			**SC1**	
├─EF Application_Identification	**'0501h'**	**1**	**SC1**	**JMS**
├─EF CardMA_Certificate	**'C100h'**	**2**	**SC1**	**JMS**
├─EF CardSignCertificate	**'C101h'**	**3**	**SC1**	**JMS**
├─EF CA_Certificate	**'C108h'**	**4**	**SC1**	**JMS**
├─EF Link_Certificate	**'C109h'**	**5**	**SC1**	**JMS**
├─EF Identification	**'0520h'**	**6**	**SC1**	**JMS**
├─EF Card_Download	**'050Eh'**	**7**	**SC1**	**SC1**
├─EF Driving_Licence_Info	**'0521h'**	**10**	**SC1**	**JMS**
├─EF Events_Data	**'0502h'**	**12**	**SC1**	**MS-MAC-G2**
├─EF Faults_Data	**'0503h'**	**13**	**SC1**	**MS-MAC-G2**
├─EF Driver_Activity_Data	**'0504h'**	**14**	**SC1**	**MS-MAC-G2**
├─EF Vehicles_Used	**'0505h'**	**15**	**SC1**	**MS-MAC-G2**
├─EF Places	**'0506h'**	**16**	**SC1**	**MS-MAC-G2**
├─EF Current_Usage	**'0507h'**	**17**	**SC1**	**MS-MAC-G2**

├─EF Control_Activity_Data	'0508h'	18	SC1	MS-MAC-G2
├─EF Specific_Conditions	'0522h'	19	SC1	MS-MAC-G2
├─EF VehicleUnits_Used	'0523h'	20	SC1	MS-MAC-G2
├─EF GNSS_Places	'0524h'	21	SC1	MS-MAC-G2
├─EF Application_Identification_V2	'0525h'	22	SC1	JMS
├─EF Places_Authentication	'0526h'	23	SC1	MS-MAC-G2
├─EF GNSS_Places_Authentication	'0527h'	24	SC1	MS-MAC-G2
├─EF Border_Crossings	'0528h'	25	SC1	MS-MAC-G2
├─EF Load_Unload_Operations	'0529h'	26	SC1	MS-MAC-G2
├─EF Load_Type_Entries	'0530h'	27	SC1	MS-MAC-G2
└─EF Vu_Configuration	'0540h'	30	SC5/SC1	MS-MAC-G2

Dans le tableau ci-dessus, ~~l'~~ **les** abréviation**s** suivante**s** ~~est~~ **sont** utilisée**s** pour désigner les conditions de sécurité :

SC1 TJR OU MS-MAC-G2

SC5 **Pour la commande READ BINARY avec octet INS pair : MS-C-MAC-G2 ET MS-R-ENC-MAC-G2**

Pour la commande READ BINARY avec octet INS impair (si pris en charge) : JMS

TCS_153 La structure de tous les EF doit être transparente.

TCS_154 L'application de la carte de conducteur de génération 2 doit présenter la structure de données suivante :

Fichier/Élément de données	Nombre d'enregistrements	Taille (octets) Min	Max	Valeurs par défaut
DF Tachograph_G2		98300	98848	
EF Application_Identification		*17*	*17*	
DriverCardApplicationIdentification		*17*	*17*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{01 01}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00 00}
noOfGNSSADRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00 00}
noOfCardVehicleUnitRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMA_Certificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*143*	*143*	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}

Fichier/Élément de données	Nombre d'enregistrements	Taille (octets) Min	Max	Valeurs par défaut
DriverCardHolderIdentification		78	78	
cardHolderName		72	72	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		4	4	
LastCardDownload		4	4	{00..00}
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*3168*	*3168*	
CardEventData		*3168*	*3168*	
cardEventRecords	11	288	288	
CardEventRecord	n1	24	24	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*1152*	*1152*	
CardFaultData		*1152*	*1152*	
cardFaultRecords	2	576	576	
CardFaultRecord	n2	24	24	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*13780*	*13780*	
CardDriverActivity		*13780*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n6	13776	13776	{00..00}
EF Vehicles_Used		*9602*	*9602*	
CardVehiclesUsed		*9602*	*9602*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		9600	9600	
cardVehicleRecord	n3	48	48	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		17	17	{20..20}
EF Places		*2354*	*2354*	
CardPlaceDailyWorkPeriod		*2354*	*2354*	
placePointerNewestRecord		2	2	{00 00}
placeRecords		2352	2352	
PlaceRecord	n4	21	21	

Fichier/Élément de données		Nombre d'enregistrements	Taille (octets) Min	Max	Valeurs par défaut
	entryTime		4	4	{00..00}
	entryTypeDailyWorkPeriod		1	1	{00}
	dailyWorkPeriodCountry		1	1	{00}
	dailyWorkPeriodRegion		1	1	{00}
	vehicleOdometerValue		3	3	{00..00}
	entryGNSSPlaceRecord		11	11	
	timeStamp		4	4	{00..00}
	gnssAccuracy		1	1	{00}
	geoCoordinates		6	6	{00..00}
EF Current_Usage			*19*	*19*	
CardCurrentUse			*19*	*19*	
	sessionOpenTime		4	4	{00..00}
	sessionOpenVehicle				
	vehicleRegistrationNation		1	1	{00}
	vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data			*46*	*46*	
CardControlActivityDataRecord			*46*	*46*	
	controlType		1	1	{00}
	controlTime		4	4	{00..00}
	controlCardNumber				
	cardType		1	1	{00}
	cardIssuingMemberState		1	1	{00}
	cardNumber		16	16	{20..20}
	controlVehicleRegistration				
	vehicleRegistrationNation		1	1	{00}
	vehicleRegistrationNumber		14	14	{00, 20..20}
	controlDownloadPeriodBegin		4	4	{00..00}
	controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions			*562*	*562*	
SpecificConditions			*562*	*562*	
	conditionPointerNewestRecord		2	2	{00 00}
	specificConditionRecords		560	560	
	SpecificConditionRecord	n9	5	5	
	entryTime		4	4	{00..00}
	specificConditionType		1	1	{00}
EF VehicleUnits_Used			*2002*	*2002*	
CardVehicleUnitsUsed			*2002*	*2002*	
	vehicleUnitPointerNewestRecord		2	2	{00 00}
	cardVehicleUnitRecords		2000	2000	
	CardVehicleUnitRecord	n7	10	10	
	timeStamp		4	4	{00..00}
	manufacturerCode		1	1	{00}
	deviceID		1	1	{00}
	vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places			*6050*	*6050*	
GNSSAccumulatedDriving			*6050*	*6050*	
	gnssADPointerNewestRecord		2	2	{00 00}
	gnssAccumulatedDrivingRecords		6048	6048	
	GNSSAccumulatedDrivingRecord	n8	18	18	
	timeStamp		4	4	{00..00}
	gnssPlaceRecord		14	14	
	timeStamp		4	4	{00..00}
	gnssAccuracy		1	1	{00}
	geoCoordinates		6	6	{00..00}
	vehicleOdometerValue		3	3	{00..00}

Fichier/Élément de données	Nombre d'enregistrements	Taille (octets) Min	Max	Valeurs par défaut
EF Application_Identification_V2		10	10	
DriverCardApplicationIdentificationV2		*10*	*10*	
lengthOfFollowingData		2	2	{00 00}
noOfBorderCrossingRecords		2	2	{00 00}
noOfLoadUnloadRecords		2	2	{00 00}
noOfLoadTypeEntryRecords		2	2	{00 00}
VuConfigurationLengthRange		2	2	{00 00}
EF Places_Authentication		*562*	*562*	
CardPlaceAuthDailyWorkPeriod		*562*	*562*	
placeAuthPointerNewestRecord		2	2	{00 00}
placeAuthStatusRecords		560	560	
PlaceAuthStatusRecord	n4	5	5	
entryTime		4	4	{00..00}
authenticationStatus		1	1	{00}
EF GNSS_Places_Authentication		*1682*	*1682*	
GNSSAuthAccumulatedDriving		*1682*	*1682*	
gnssAuthADPointerNewestRecord		2	2	{00 00}
gnssAuthStatusADRecords		1680	1680	
GNSSAuthStatusADRecord	n8	5	5	
timeStamp		4	4	{00..00}
authenticationStatus		1	1	{00}
EF Border_Crossings		*19042*	*19042*	
CardBorderCrossings		*19042*	*19042*	
borderCrossingPointerNewestRecord		2	2	{00 00}
cardBorderCrossingRecords		19040	19040	
CardBorderCrossingRecord	n10	17	17	
countryLeft		1	1	{00}
countryEntered		1	1	{00}
gnssPlaceAuthRecord		12	12	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
authenticationStatus		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Load_Unload_Operations		*32482*	*32482*	
CardLoadUnloadOperations		*32482*	*32482*	
loadUnloadPointerNewestRecord		2	2	{00 00}
cardloadUnloadRecords		32480	32480	
CardLoadUnloadRecord	n11	20	20	
timestamp		4	4	{00}
operationType		1	1	{00..00}
gnssPlaceAuthRecord		12	12	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
authenticationStatus		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Load_Type_Entries		*1682*	*1682*	
CardLoadTypeEntries		*1682*	*1682*	
loadtypeEntryPointerNewestRecord		2	2	{00 00}
cardLoadTypeEntryRecords		1680	1680	
CardLoadTypeEntryRecord	n12	5	5	
timestamp		4	4	{00..00}
loadTypeEntered		1	1	{00}
EF VU_Configuration		*3072*	*3072*	
VuConfigurations	n13	*3072*	*3072*	

TCS_155 Employées pour indiquer les tailles dans le tableau ci-dessus, les valeurs qui suivent correspondent aux nombres d'enregistrements minimum et maximum que doit utiliser la structure de données de la carte de conducteur pour une application de génération 2 :

		Min.	*Max.*
n_1	NoOfEventsPerType	~~6~~**12**	12
n_2	NoOfFaultsPerType	~~12~~**24**	24
n_3	NoOfCardVehicleRecords	~~84~~**200**	200
n_4	NoOfCardPlaceRecords	~~84~~**112**	112
n_6	CardActivityLengthRange	~~5544~~ **13 776** octets (~~28~~ **56** jours * ~~93~~ **117** changements d'activité)	13 776 Bytes (~~28~~ **56** jours * ~~240~~ **117** changements d'activité)
n_7	NoOfCardVehicleUnitRecords	~~84~~**200**	200
n_8	~~NoOfGNSSCDRecords~~ **NoOfGNSSADRecords**	~~252~~**336**	336
n_9	NoOfSpecificConditionRecords	~~56~~**112**	112
n_{10}	**NoOfBorderCrossingRecords**	**1 120**	**1 120**
n_{11}	**NoOfLoadUnloadRecords**	**1 624**	**1 624**
n_{12}	**NoOfLoadTypeEntryRecords**	**336**	**336**
n_{13}	**VuConfigurationLengthRange**	**3 072 octets**	**3 072 octets**

		Règles d'accès		
Fichier	**ID de fichier**	**Lecture**	**Sélection**	**Actualisation**
└ DF Tachograph	'0500h'		SC1	
├ EF Application_Identification	'0501h'	SC2	SC1	JMS
├ EF Card_Certificate	'C100h'	SC2	SC1	JMS
├ EF CA_Certificate	'C108h'	SC2	SC1	JMS
├ EF Identification	'0520h'	SC2	SC1	JMS
├ EF Card_Download	'0509h'	SC2	SC1	**SC1**
├ EF Calibration	'050Ah'	SC2	SC1	SC3
├ EF Sensor_Installation_Data	'050Bh'	**SC4**	SC1	JMS
├ EF Events_Data	'0502h'	SC2	SC1	SC3
├ EF Faults_Data	'0503h'	SC2	SC1	SC3
├ EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├ EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├ EF Places	'0506h'	SC2	SC1	SC3
├ EF Current_Usage	'0507h'	SC2	SC1	SC3
├ EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└ EF Specific_Conditions	'0522h'	SC2	SC1	SC3

4.3 Applications des cartes d'atelier

4.3.1 Application de la carte d'atelier de génération 1

TCS_156 Après personnalisation, l'application de la carte d'atelier de génération 1 doit avoir la structure de fichiers et les règles d'accès aux fichiers permanentes suivantes :

Dans le tableau ci-dessus, les abréviations suivantes sont utilisées pour désigner les conditions de sécurité :

SC1 TJR OU MS-MAC-G2

SC2 TJR OU MS-MAC-G1 OU MS-MAC-G2

SC3 MS-MAC-G1 OU MS-MAC-G2

SC4 Pour la commande READ BINARY avec octet INS pair :

(C-CLAIR ET MS-R-ENC-G1) OU (MS-C-MAC-G1 ET MS-R-ENC-MAC-G1) OU

(MS-C-MAC-G2 ET MS-R-ENC-MAC-G2)

Pour la commande READ BINARY avec octet INS impair (si pris en charge) : JMS

TCS_157 La structure de tous les EF doit être transparente.

TCS_158 L'application de la carte d'atelier de génération 1 doit présenter la structure de données suivante :

Fichier/Élément de données	Nombre d'enregistrements	Taille (octets) Min	Taille (octets) Max	Valeurs par défaut
DF Tachograph		*11055*	*29028*	
EF Application_Identification		*11*	*11*	
WorkshopCardApplicationIdentification		*11*	*11*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	

└NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
└WorkshopCardCalibrationData		*9243*	*26778*	
├calibrationTotalNumber		2	2	{00 00}
├calibrationPointerNewestRecord		1	1	{00}
└nRecords		*9240*	*26775*	
└WorkshopCardCalibrationRecord	n_5	*105*	*105*	
├calibrationPurpose		1	1	{00}
├vehicleIdentificationNumber		17	17	{20..20}
├vehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├wVehicleCharacteristicConstant		2	2	{00 00}
├kConstantOfRecordingEquipment		2	2	{00 00}
├lTyreCircumference		2	2	{00 00}
├tyreSize		15	15	{20..20}
├authorisedSpeed		1	1	{00}
├oldOdometerValue		3	3	{00..00}
├newOdometerValue		3	3	{00..00}
├oldTimeValue		4	4	{00..00}
├newTimeValue		4	4	{00..00}
├ationDate		4	4	{00..00}
├vuPartNumber		16	16	{20..20}
├vuSerialNumber		8	8	{00..00}
└sensorSerialNumber		8	8	{00..00}
EF Sensor_Installation_Data		*16*	*16*	
└SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
└ata		*432*	*432*	
└cardEventRecords	6	*72*	*72*	
└CardEventRecord	n_1	*24*	*24*	
├eventType		1	1	{00}
├eventBeginTime		4	4	{00..00}
├eventEndTime		4	4	{00..00}
├eventVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
└ata		*288*	*288*	
└cardFaultRecords	2	*144*	*144*	
└CardFaultRecord	n_2	*24*	*24*	
├faultType		1	1	{00}
├faultBeginTime		4	4	{00..00}
├faultEndTime		4	4	{00..00}
├faultVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
└CardDriverActivity		*202*	*496*	
├activityPointerOldestDayRecord		2	2	{00 00}
├activityPointerNewestRecord		2	2	{00 00}
└activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
└CardVehiclesUsed		*126*	*250*	
├vehiclePointerNewestRecord		2	2	{00 00}
└cardVehicleRecords		*124*	*248*	
└CardVehicleRecord	n_3	*31*	*31*	
├vehicleOdometerBegin		3	3	{00..00}
├vehicleOdometerEnd		3	3	{00..00}

vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
CardPlaceDailyWorkPeriod		*61*	*81*	
placePointerNewestRecord		1	1	{00}
is		*60*	*80*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*10*	*10*	
SpecificConditionRecord	*2*	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_159 Employées pour indiquer les tailles dans le tableau ci-dessus, les valeurs qui suivent correspondent aux nombres d'enregistrements minimum et maximum que doit utiliser la structure de données de la carte d'atelier pour une application de génération 1 :

		Min.	*Max.*
n_1	NoOfEventsPerType	*3*	*3*
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 octets (1 jour * 93 changements d'activité)	492 octets (1 jour * 240 changements d'activité)

4.3.2 Application de la carte d'atelier de génération 2

TCS_160 Après personnalisation, l'application de la carte d'atelier de génération 2 doit avoir la structure de fichiers et les règles d'accès aux fichiers permanentes qui suivent :

Remarques :

- L'identificateur d'EF court (IDFC) est donné sous la forme d'un nombre décimal, par exemple la valeur 30 correspond au nombre binaire 11110.
- **Les fichiers EF Application_Identification_V2, EF Places_Authentication, EF GNSS_Places_Authentication, EF Border_Crossings, EF Load_Unload_Operations, EF Load_Type_Entries, EF VU_Configuration et EF Calibration_Add_Data ne sont présents que dans la version 2 de la carte d'atelier de génération 2.**
- **La valeur attribuée à cardStructureVersion dans l'EF Application_Identification est égale à {01 01} pour la version 2 de la carte d'atelier de génération 2, alors qu'elle était égale à {01 00} pour la version 1 de la carte d'atelier de génération 2.**

~~Fichier~~	~~ID de fichier~~	~~IDFC~~	~~Règles d'accès~~		
			~~Lecture~~	~~Sélection~~	~~Actualisation~~
~~DF Tachograph_G2~~			~~SC1~~	~~SC1~~	
~~EF Application_Identification~~	~~'0501h'~~	~~1~~	~~SC1~~	~~SC1~~	~~JMS~~
~~EF CardMA_Certificate~~	~~'C100h'~~	~~2~~	~~SC1~~	~~SC1~~	~~JMS~~
~~EF CardSignCertificate~~	~~'C101h'~~	~~3~~	~~SC1~~	~~SC1~~	~~JMS~~
~~EF CA_Certificate~~	~~'C108h'~~	~~4~~	~~SC1~~	~~SC1~~	~~JMS~~
~~EF Link_Certificate~~	~~'C109h'~~	~~5~~	~~SC1~~	~~SC1~~	~~JMS~~
~~EF Identification~~	~~'0520h'~~	~~6~~	~~SC1~~	~~SC1~~	~~JMS~~
~~EF Card_Download~~	~~'0509h'~~	~~7~~	~~SC1~~	~~SC1~~	~~SC1~~
~~EF Calibration~~	~~'050Ah'~~	~~10~~	~~SC1~~	~~SC1~~	~~MS-MAC-G2~~
~~EF Sensor_Installation_Data~~	~~'050Bh'~~	~~11~~	~~SC5~~	~~MS-MAC-G2~~	~~JMS~~
~~EF Events_Data~~	~~'0502h'~~	~~12~~	~~SC1~~	~~SC1~~	~~MS-MAC-G2~~
~~EF Faults_Data~~	~~'0503h'~~	~~13~~	~~SC1~~	~~SC1~~	~~MS-MAC-G2~~
~~EF Driver_Activity_Data~~	~~'0504h'~~	~~14~~	~~SC1~~	~~SC1~~	~~MS-MAC-G2~~
~~EF Vehicles_Used~~	~~'0505h'~~	~~15~~	~~SC1~~	~~SC1~~	~~MS-MAC-G2~~
~~EF Places~~	~~'0506h'~~	~~16~~	~~SC1~~	~~SC1~~	~~MS-MAC-G2~~
~~EF Current_Usage~~	~~'0507h'~~	~~17~~	~~SC1~~	~~SC1~~	~~MS-MAC-G2~~
~~EF Control_Activity_Data~~	~~'0508h'~~	~~18~~	~~SC1~~	~~SC1~~	~~MS-MAC-G2~~
~~EF Specific_Conditions~~	~~'0522h'~~	~~19~~	~~SC1~~	~~SC1~~	~~MS-MAC-G2~~
~~EF VehicleUnits_Used~~	~~'0523h'~~	~~20~~	~~SC1~~	~~SC1~~	~~MS-MAC-G2~~
~~EF GNSS_Places~~	~~'0524h'~~	~~21~~	~~SC1~~	~~SC1~~	~~MS-MAC-G2~~

Fichier	ID de fichier	IDFC	Règles d'accès		
			Lecture	Sélection	Actualisation
DF Tachograph_G2			**SC1**	**SC1**	
EF Application_Identification	**'0501h'**	**1**	**SC1**	**SC1**	**JMS**
EF CardMA_Certificate	**'C100h'**	**2**	**SC1**	**SC1**	**JMS**
EF CardSignCertificate	**'C101h'**	**3**	**SC1**	**SC1**	**JMS**
EF CA_Certificate	**'C108h'**	**4**	**SC1**	**SC1**	**JMS**
EF Link_Certificate	**'C109h'**	**5**	**SC1**	**SC1**	**JMS**
EF Identification	**'0520h'**	**6**	**SC1**	**SC1**	**JMS**
EF Card_Download	**'0509h'**	**7**	**SC1**	**SC1**	**SC1**
EF Calibration	**'050Ah'**	**10**	**SC1**	**SC1**	**MS-MAC-G2**
EF Sensor_Installation_Data	**'050Bh'**	**11**	**SC5**	**MS-MAC-G2**	**JMS**
EF Events_Data	**'0502h'**	**12**	**SC1**	**SC1**	**MS-MAC-G2**
EF Faults_Data	**'0503h'**	**13**	**SC1**	**SC1**	**MS-MAC-G2**

EF Driver_Activity_Data	'0504h'	14	SC1	SC1	MS-MAC-G2
EF Vehicles_Used	'0505h'	15	SC1	SC1	MS-MAC-G2
EF Places	'0506h'	16	SC1	SC1	MS-MAC-G2
EF Current_Usage	'0507h'	17	SC1	SC1	MS-MAC-G2
EF Control_Activity_Data	'0508h'	18	SC1	SC1	MS-MAC-G2
EF Specific_Conditions	'0522h'	19	SC1	SC1	MS-MAC-G2
EF VehicleUnits_Used	'0523h'	20	SC1	SC1	MS-MAC-G2
EF GNSS_Places	'0524h'	21	SC1	SC1	MS-MAC-G2
EF Application_Identification_V2	'0525h'	22	SC1	SC1	JMS
EF Places_Authentication	'0526h'	23	SC1	SC1	MS-MAC-G2
EF GNSS_Places_Authentication	'0527h'	24	SC1	SC1	MS-MAC-G2
EF Border_Crossings	'0528h'	25	SC1	SC1	MS-MAC-G2
EF Load_Unload_Operations	'0529h'	26	SC1	SC1	MS-MAC-G2
EF Load_Type_Entries	'0530h'	27	SC1	SC1	MS-MAC-G2
EF Calibration_Add_Data	'0531h'	28	SC1	SC1	MS-MAC-G2
EF VU_Configuration	'0540h'	30	SC5	SC1	MS-MAC-G2

Dans le tableau ci-dessus, les abréviations suivantes sont utilisées pour désigner les conditions de sécurité :

SC1 TJR OU MS-MAC-G2

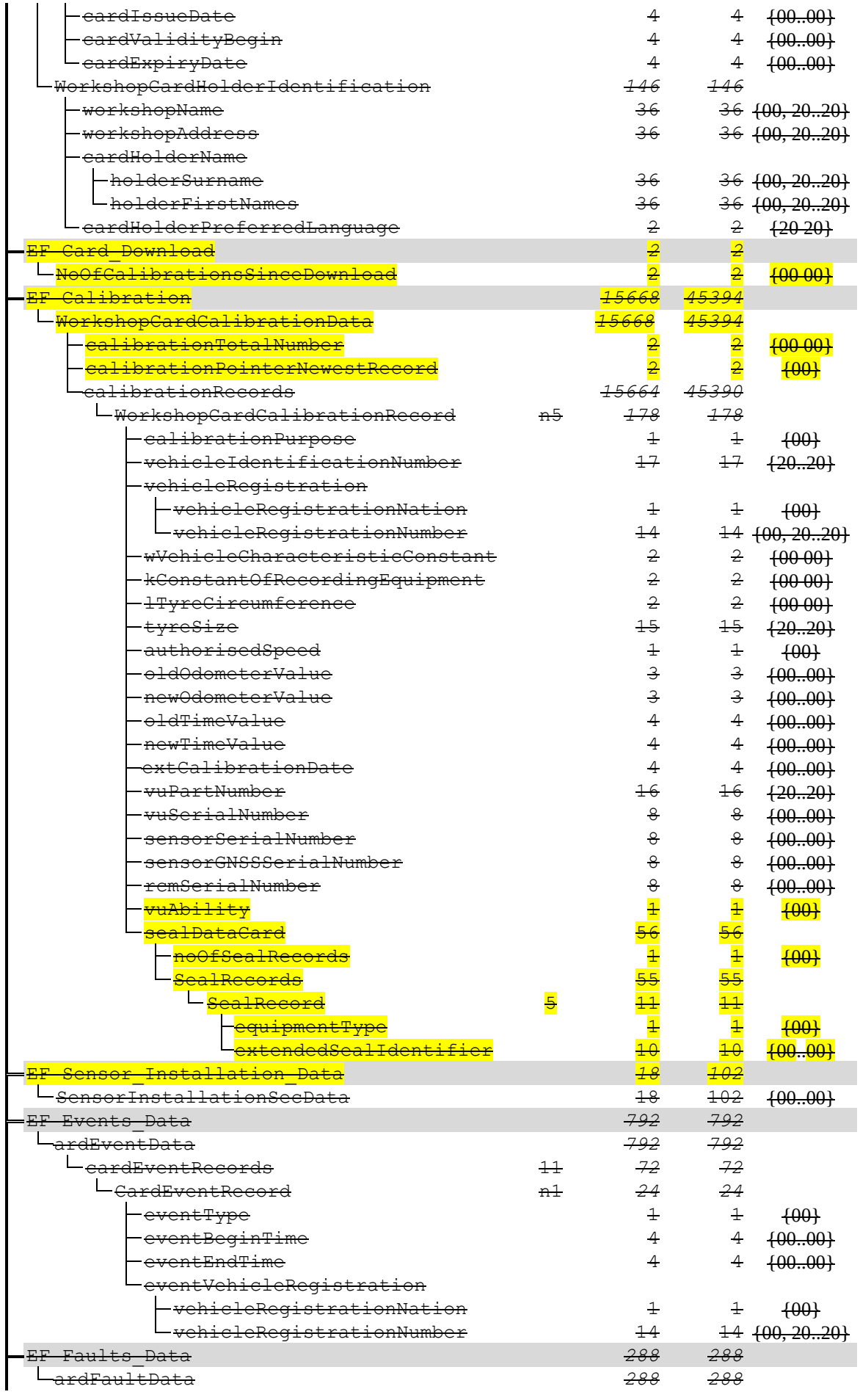
SC5 Pour la commande READ BINARY avec octet INS pair : MS-C-MAC-G2 ET MS-R-ENC-MAC-G2

Pour la commande READ BINARY avec octet INS impair (si pris en charge) : JMS

TCS_161 La structure de tous les EF doit être transparente.

TCS_162 L'application de la carte d'atelier de génération 2 doit présenter la structure de données suivante :

Fichier/Élément de données	Nombre d'enregistrements	Taille (octets) Min	Taille (octets) Max	Valeur par défaut
DF Tachograph_G2		18783	49787	
EF Application_Identification		19	19	
WorkshopCardApplicationIdentification		19	19	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00 00}
noOfCalibrationRecords		2	2	{00 00}
noOfGNSSADRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
noOfCardVehicleUnitRecords		2	2	{00..00}
EF CardMA_Certificate			341	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		204	341	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		204	341	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		204	341	
LinkCertificate		204	341	{00..00}
EF Identification		211	211	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}



cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		146	146	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF_Card_Download		2	2	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF_Calibration		15668	45394	
WorkshopCardCalibrationData		15668	45394	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		15664	45390	
WorkshopCardCalibrationRecord	n5	178	178	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
extCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
sensorGNSSSerialNumber		8	8	{00..00}
remSerialNumber		8	8	{00..00}
vuAbility		1	1	{00}
sealDataCard		56	56	
noOfSealRecords		1	1	{00}
SealRecords		55	55	
SealRecord	5	11	11	
equipmentType		1	1	{00}
extendedSealIdentifier		10	10	{00..00}
EF_Sensor_Installation_Data		18	102	
SensorInstallationSecData		18	102	{00..00}
EF_Events_Data		792	792	
ardEventData		792	792	
cardEventRecords	11	72	72	
CardEventRecord	n1	24	24	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF_Faults_Data		288	288	
ardFaultData		288	288	

└cardFaultRecords	2	144	144	
└CardFaultRecord	n2	24	24	
├faultType		1	1	{00}
├faultBeginTime		4	4	{00..00}
├faultEndTime		4	4	{00..00}
└faultVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		202	496	
└CardDriverActivity		202	496	
├activityPointerOldestDayRecord		2	2	{00 00}
├activityPointerNewestRecord		2	2	{00 00}
└activityDailyRecords	n6	198	492	{00..00}
EF Vehicles_Used		194	386	
└CardVehiclesUsed		194	386	
├vehiclePointerNewestRecord		2	2	{00 00}
└cardVehicleRecords		192	384	
└CardVehicleRecord	n3	48	48	
├vehicleOdometerBegin		3	3	{00..00}
├vehicleOdometerEnd		3	3	{00..00}
├vehicleFirstUse		4	4	{00..00}
├vehicleLastUse		4	4	{00..00}
├vehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├vuDataBlockCounter		2	2	{00 00}
└vehicleIdentificationNumber		17	17	{20..20}
EF Places		128	170	
└CardPlaceDailyWorkPeriod		128	170	
├placePointerNewestRecord		2	2	{00 00}
└placeRecords		126	168	
└PlaceRecord	n4	21	21	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
├vehicleOdometerValue		3	3	{00..00}
└entryGNSSPlaceRecord		11	11	{00..00}
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Current_Usage		19	19	
└CardCurrentUse		19	19	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		46	46	
└CardControlActivityDataRecord		46	46	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}

controlDownloadPeriodEnd		4	4	{00..00}
EF_VehicleUnits_Used		42	42	
CardVehicleUnitsUsed		42	82	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		40	80	
CardVehicleUnitRecord	n7	10	10	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00..00}
deviceID		1	1	{00..00}
vuSoftwareVersion		4	4	{00..00}
EF_GNSS_Places		326	432	
GNSSContinuousDriving		326	434	
gnssADPointerNewestRecord		2	2	{00 00}
gnssAccumulatedDrivingRecords		324	432	
GNSSContinuousDrivingRecord	n8	18	18	
timeStamp		4	4	{00..00}
gnssPlaceRecord		14	14	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}
EF_Specific_Conditions		12	22	
SpecificConditions		12	22	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		10	20	
SpecificConditionRecord	n9	5	5	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}

Fichier/Élément de données	Nombre d'enregis-trements	Taille (octets) Min	Max	Valeurs par défaut
DF Tachograph_G2		**59582**	**60214**	
EF Application_Identification		***19***	***19***	
WorkshopCardApplicationIdentification		***19***	***19***	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{01 01}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00 00}
noOfCalibrationRecords		2	2	{00 00}
noOfGNSSADRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00 00}
noOfCardVehicleUnitRecords		2	2	{00 00}
EF CardMA_Certificate		***204***	***341***	
CardMA_Certificate		204	341	{00..00}
EF CardSignCertificate		***204***	***341***	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		***204***	***341***	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		***204***	***341***	
LinkCertificate		204	341	{00..00}
EF Identification		***211***	***211***	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}

Fichier/Élément de données	Nombre d'enregis-trements	Taille (octets) Min	Max	Valeurs par défaut
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		146	146	
workshopName		36	36	
workshopAddress		36	36	
cardHolderName		72	72	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		2	2	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*45394*	*45394*	
WorkshopCardCalibrationData		*45394*	*45394*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00 00}
calibrationRecords		45390	45390	
WorkshopCardCalibrationRecord	n5	178	178	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
sensorGNSSSerialNumber		8	8	{00..00}
rcmSerialNumber		8	8	{00..00}
vuAbility		1	1	{00}
sealDataCard		56	56	
noOfSealRecords		1	1	{00}
SealRecords		55	55	
SealRecord	5	11	11	
equipmentType		1	1	{00}
extendedSealIdentifier		10	10	{00..00}
EF Sensor_Installation_Data		18	102	
SensorInstallationSecData		18	102	{00..00}
EF Events_Data		*792*	*792*	
CardEventData		*792*	*792*	
cardEventRecords	11	72	72	
CardEventRecord	n1	24	24	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				

Fichier/Élément de données	Nombre d'enregis-trements	Taille (octets) Min	Max	Valeurs par défaut
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	144	144	
CardFaultRecord	n2	24	24	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*496*	*496*	
CardDriverActivity		*496*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n6	492	492	{00..00}
EF Vehicles_Used		*386*	*386*	
CardVehiclesUsed		*386*	*386*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		384	384	
cardVehicleRecord	n3	48	48	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		17	17	{20..20}
EF Places		*170*	*170*	
CardPlaceDailyWorkPeriod		*170*	*170*	
placePointerNewestRecord		2	2	{00 00}
placeRecords		168	168	
PlaceRecord	n4	21	21	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
entryGNSSPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				

Fichier/Élément de données	Nombre d'enregis-trements	Taille (octets) Min	Max	Valeurs par défaut
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF VehicleUnits_Used		*82*	*82*	
CardVehicleUnitsUsed		*82*	*82*	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		80	80	
CardVehicleUnitRecord	n7	10	10	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*434*	*434*	
GNSSAccumulatedDriving		*434*	*434*	
gnssADPointerNewestRecord		2	2	{00 00}
gnssAccumulatedDrivingRecords		432	432	
GNSSAccumulatedDrivingRecord	n8	18	18	
timeStamp		4	4	{00..00}
gnssPlaceRecord		14	14	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}
EF Specific_Conditions		*22*	*22*	
SpecificConditions		*22*	*22*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		20	20	
SpecificConditionRecord	n9	5	5	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF Application_Identification_V2		10	10	
WorkshopCardApplicationIdentificationV2		*10*	*10*	
LengthOfFollowingData		2	2	{00 00}
noOfBorderCrossingRecords		2	2	{00 00}
noOfLoadUnloadRecords		2	2	{00 00}
noOfLoadTypeEntryRecords		2	2	{00 00}
VuConfigurationLengthRange		2	2	{00 00}
EF Places_Authentication		*42*	*42*	
CardPlaceAuthDailyWorkPeriod		*42*	*42*	
placeAuthPointerNewestRecord		2	2	{00 00}
placeAuthStatusRecords		40	40	
PlaceAuthStatusRecord	n4	5	5	
entryTime		4	4	{00..00}
authenticationStatus		1	1	{00}
EF GNSS_Places_Authentication		*122*	*122*	
GNSSAuthAccumulatedDriving		*122*	*122*	
gnssAuthADPointerNewestRecord		2	2	{00 00}
gnssAuthStatusADRecords		120	120	
GNSSAuthStatusADRecord	n8	5	5	
timeStamp		4	4	{00..00}
authenticationStatus		1	1	{00}

Fichier/Élément de données	Nombre d'enregis-trements	Taille (octets) Min	Max	Valeurs par défaut
EF Border_Crossings		*70*	*70*	
CardBorderCrossings		*70*	*70*	
borderCrossingPointerNewestRecord		2	2	{00 00}
cardBorderCrossingRecords		68	68	
CardBorderCrossingRecord	n10	17	17	
countryLeft		1	1	{00}
countryEntered		1	1	{00}
gnssPlaceAuthRecord		12	12	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
authenticationStatus		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Load_Unload_Operations		*162*	*162*	
CardLoadUnloadOperations		*162*	*162*	
loadUnloadPointerNewestRecord		2	2	{00 00}
cardloadUnloadRecords		160	160	
CardLoadUnloadRecord	n11	20	20	
timestamp		4	4	{00}
operationType		1	1	{00..00}
gnssPlaceAuthRecord		12	12	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
authenticationStatus		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Load_Type_Entries		*22*	*22*	
CardLoadTypeEntries		*22*	*22*	
loadtypeEntryPointerNewestRecord		2	2	{00 00}
cardLoadTypeEntryRecords		20	20	
CardLoadTypeEntryRecord	n12	5	5	
timestamp		4	4	{00..00}
loadTypeEntered		1	1	{00}
EF Calibration_Add_Data		*6887*	*6887*	
WorkshopCardCalibrationAddData		*6887*	*6887*	
calibrationPointerNewestRecord		2	2	{00 00}
workshopCardCalibrationAddDataRecords		6885	6885	
WorkshopCardCalibrationAddDataRecord	n5	27	27	
oldTimeValue		4	4	{00..00}
vehicleIdentificationNumber		17	17	{20..20}
byDefaultLoadType		1	1	{00}
calibrationCountry		1	1	{00}
calibrationCountryTimestamp		4	4	{00..00}
EF VU_Configuration		*3072*	*3072*	
VuConfigurations	n13	*3072*	*3072*	

TCS_163 Employées pour indiquer les tailles dans le tableau ci-dessus, les valeurs qui suivent correspondent aux nombres d'enregistrements minimum et maximum que doit utiliser la structure de données de la carte d'atelier pour une application de génération 2 :

		Min.	*Max.*
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6

		Min.	*Max.*
n_3	NoOfCardVehicleRecords	~~**48**~~	8
n_4	NoOfCardPlaceRecords	~~**68**~~	8
n_5	NoOfCalibrationRecords	~~**88**~~**255**	255
n_6	CardActivityLengthRange	~~**198**~~**492** octets (1 jour * ~~**93**~~**240** changements d'activité)	492 octets (1 jour * 240 changements d'activité)
n_7	NoOfCardVehicleUnitRecords	~~**48**~~	8
n_8	~~NoOfGNSSCDRecords~~ **NoOfGNSSADRecords**	~~**18**~~**24**	24
n_9	NoOfSpecificConditionRecords	~~**2**~~**4**	4
n_{10}	**NoOfBorderCrossingRecords**	**4**	**4**
n_{11}	**NoOfLoadUnloadRecords**	**8**	**8**
n_{12}	**NoOfLoadTypeEntryRecords**	**4**	**4**
n_{13}	**VuConfigurationLengthRange**	**3 072 octets**	**3 072 octets**

4.4 Applications des cartes de contrôleur

4.4.1 Application de la carte de contrôleur de génération 1

TCS_164 Après personnalisation, l'application de la carte de contrôleur de génération 1 doit avoir la structure de fichiers et les règles d'accès aux fichiers permanentes suivantes :

		Règles d'accès		
Fichier	**ID de fichier**	**Lecture**	**Sélection**	**Actualisation**
└DF Tachograph	'0500h'			
├EF Application_Identification	'0501h'	SC2	SC1	JMS
├EF Card_Certificate	'C100h'	SC2	SC1	JMS
├EF CA_Certificate	'C108h'	SC2	SC1	JMS
├EF Identification	'0520h'	**SC6**	SC1	JMS
└EF Controller_Activity_Data	'050Ch'	SC2	SC1	SC3

Dans le tableau ci-dessus, les abréviations suivantes sont utilisées pour désigner les conditions de sécurité :

SC1 TJR OU MS-MAC-G2

SC2 TJR OU MS-MAC-G1 OU MS-MAC-G2

SC3 MS-MAC-G1 OU MS-MAC-G2

SC6 EXT-AUT-G1 OU MS-MAC-G1 OU MS-MAC-G2

TCS_165 La structure de tous les EF doit être transparente.

TCS_166 L'application de la carte de contrôleur de génération 1 doit présenter la structure de données suivante :

Fichier/Élément de données	Nombre d'enregis-trements	Taille (octets) Min	Max	
DF Tachograph		*11186*	*24526*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00. 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller Activity Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 Employées pour indiquer les tailles dans le tableau ci-dessus, les valeurs qui suivent correspondent aux nombres d'enregistrements minimum et maximum que doit utiliser la structure de données de la carte de contrôleur pour une application de génération 1 :

		Min.	*Max.*
n_7	NoOfControlActivityRecords	230	520

4.4.2 Application de la carte de contrôleur de génération 2

TCS_168 Après personnalisation, l'application de la carte de contrôleur de génération 2 doit avoir la structure de fichiers et les règles d'accès aux fichiers permanentes qui suivent :

Remarque**s** :

- L'identificateur d'EF court (IDFC) est donné sous la forme d'un nombre décimal, par exemple la valeur 30 correspond au nombre binaire 11110 ;
- **Les fichiers EF Application_Identification_V2 et EF VU_Configuration ne sont présents que dans la version 2 de la carte de contrôleur de génération 2 ;**
- **La valeur attribuée à cardStructureVersion dans l'EF Application_Identification est égale à {01 01} pour la version 2 de la carte de contrôleur de génération 2, alors qu'elle était égale à {01 00} pour la version 1 de la carte de contrôleur de génération 2.**

			Règles d'accès	
Fichier	ID de fichier	IDFC	Lecture/sélection	Actualisation
└DF Tachograph_G2			SC1	
├EF Application_Identification	'0501h'	1	SC1	JMS
├EF CardMA_Certificate	'C100h'	2	SC1	JMS
├EF CA_Certificate	'C108h'	4	SC1	JMS
├EF Link_Certificate	'C109h'	5	SC1	JMS
├EF Identification	'0520h'	6	SC1	JMS
└EF Controller_Activity_Data	'050Ch'	14	SC1	MS-MAC-G2

			Règles d'accès	
Fichier	**ID de fichier**	**IDFC**	**Lecture/sélection**	**Actualisation**
└DF Tachograph_G2			**SC1**	
├EF Application_Identification	**'0501h'**	**1**	**SC1**	**JMS**
├EF CardMA_Certificate	**'C100h'**	**2**	**SC1**	**JMS**
├EF CA_Certificate	**'C108h'**	**4**	**SC1**	**JMS**
├EF Link_Certificate	**'C109h'**	**5**	**SC1**	**JMS**
├EF Identification	**'0520h'**	**6**	**SC1**	**JMS**
├EF Controller_Activity_Data	**'050Ch'**	**14**	**SC1**	**MS-MAC-G2**
├EF Application_Identification_V2	**'0525h'**	**22**	**SC1**	**JMS**
EF VU_Configuration	**'0540h'**	**30**	**SC5/SC1**	**MS-MAC-G2**

Dans le tableau ci-dessus, ~~l'~~**les** abréviation**s** suivante**s** ~~est~~ **sont** utilisée**s** pour désigner les conditions de sécurité :

SC1 TJR OU MS-MAC-G2

SC5 **Pour la commande READ BINARY avec octet INS pair : MS-C-MAC-G2 ET MS-R-ENC-MAC-G2**

Pour la commande READ BINARY avec octet INS impair (si prise en charge) : JMS

TCS_169 La structure de tous les EF doit être transparente.

TCS_170 L'application de la carte de contrôleur de génération 2 doit présenter la structure de données suivante :

Fichier/Élément de données	Nombre d'enregistrements	Taille (octets) Min	Max	
DF Tachograph_G2		11410	25161	
EF Application_Identification		5	5	
ControlCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF CardMA_Certificate		204	341	

└CardMACertificate		204	341	{00..00}
EF CA_Certificate		204	341	
└MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		204	341	
└LinkCertificate		204	341	{00..00}
EF Identification		211	211	
├CardIdentification		65	65	
├cardIssuingMemberState		1	1	{00}
├cardNumber		16	16	{20..20}
├cardIssuingAuthorityName		36	36	{00,
├cardIssueDate		4	4	{00..00}
├cardValidityBegin		4	4	{00..00}
└cardExpiryDate		4	4	{00..00}
└ControlCardHolderIdentification		146	146	
├controlBodyName		36	36	{00,
├controlBodyAddress		36	36	{00,
├cardHolderName				
├holderSurname		36	36	{00,
└holderFirstNames		36	36	{00,
└cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		10582	23922	
└ControlCardControlActivityData		10582	23922	
├controlPointerNewestRecord		2	2	{00 00}
└controlActivityRecords		10580	23920	
└controlActivityRecord	n7	46	46	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlledCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlledVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00,
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}

Fichier/Élément de données	**Nombre d'enregistrements**	**Min**	**Max**	**Valeurs par défaut**
		1448	**2823**	
DF Tachograph_G2		**6**	**7**	
EF Application_Identification		***5***	***5***	
ControlCardApplicationIdentification		***5***	***5***	
typeOfTachographCardId		**1**	**1**	**{00}**
cardStructureVersion		**2**	**2**	**{01 01} V2**
noOfControlActivityRecords		**2**	**2**	**{00 00}**
EF CardMA_Certificate		***204***	***341***	
CardMA_Certificate		**204**	**341**	**{00..00}**
EF CA_Certificate		***204***	***341***	
MemberStateCertificate		**204**	**341**	**{00..00}**
EF Link_Certificate		***204***	***341***	
LinkCertificate		**204**	**341**	**{00..00}**
EF Identification		***211***	***211***	
CardIdentification		**65**	**65**	

cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		146	146	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
		1058	*2392*	
EF Controller_Activity_Data		*2*	*2*	
		1058	*2392*	
ControlCardControlActivityData		*2*	*2*	
controlPointerNewestRecord		2	2	{00 00}
		1058	2392	
controlActivityRecords		0	0	
controlActivityRecord	n7	46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Application_Identification_V2		4	4	
ControlCardApplicationIdentificationV2		*4*	*4*	
lengthOfFollowingData		*2*	*2*	{00 00}
VuConfigurationLengthRange		2	2	{00 00}
EF VuConfiguration		*3072*	*3072*	
VuConfigurations	n13	*3072*	*3072*	

TCS_171 Employées pour indiquer les tailles dans le tableau ci-dessus, les valeurs qui suivent correspondent aux nombres d'enregistrements minimum et maximum que doit utiliser la structure de données de la carte de contrôleur pour une application de génération 2 :

		Min.	*Max.*
n_7	NoOfControlActivityRecords	230	520
n_{13}	**VuConfigurationLengthRange**	**3 072 octets**	**30 72 octets**

4.5 Applications des cartes d'entreprise

4.5.1 Application de la carte d'entreprise de génération 1

TCS_172 Après personnalisation, l'application de la carte d'entreprise de génération 1 doit avoir la structure de fichiers et les règles d'accès aux fichiers permanentes suivantes :

		Règles d'accès		
Fichier	**ID de fichier**	**Lecture**	**Sélection**	**Actualisation**
└DF Tachograph	'0500h'		SC1	
├EF Application Identification	'0501h'	SC2	SC1	JMS
├EF Card_Certificate	'C100h'	SC2	SC1	JMS
├EF CA_Certificate	'C108h'	SC2	SC1	JMS
├EF Identification	'0520h'	**SC6**	SC1	JMS
└EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

Dans le tableau ci-dessus, les abréviations suivantes sont utilisées pour désigner les conditions de sécurité :

SC1 TJR OU MS-MAC-G2

SC2 TJR OU MS-MAC-G1 OU MS-MAC-G2

SC3 MS-MAC-G1 OU MS-MAC-G2

SC6 EXT-AUT-G1 OU MS-MAC-G1 OU MS-MAC-G2

TCS_173 La structure de tous les EF doit être transparente.

TCS_174 L'application de la carte d'entreprise de génération 1 doit présenter la structure de données suivante :

Fichier/Élément de données	Nombre d'enregistrements	Taille (octets) Min	Taille (octets) Max	Valeurs par défaut
DF Tachograph		*11114*	*24454*	
EF Application_Identification		*5*	*5*	
CompanyCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*139*	*139*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00,
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		*74*	*74*	
companyName		36	36	{00,
companyAddress		36	36	{00,
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		*10580*	*23920*	
companyActivityRecord	n_8	*46*	*46*	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00,
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_175 Employées pour indiquer les tailles dans le tableau ci-dessus, les valeurs qui suivent correspondent aux nombres d'enregistrements minimum et maximum que doit utiliser la structure de données de la carte d'entreprise pour une application de génération 1 :

		Min.	*Max.*
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 Application de la carte d'entreprise de génération 2

TCS_176 Après personnalisation, l'application de la carte d'entreprise de génération 2 doit avoir la structure de fichiers et les règles d'accès aux fichiers permanentes qui suivent :

Remarque**s** :

- L'identificateur d'EF court (IDFC) est donné sous la forme d'un nombre décimal, par exemple la valeur 30 correspond au nombre binaire 11110 ;
- **Les fichiers EF Application_Identification_V2 et EF VU_Configuration ne sont présents que dans la version 2 de la carte d'entreprise de génération 2 ;**
- **La valeur attribuée à cardStructureVersion dans l'EF Application_Identification est égale à {01 01} pour la version 2 de la carte d'entreprise de génération 2, alors qu'elle était égale à {01 00} pour la version 1 de la carte d'entreprise de génération 2.**

			~~Règles d'accès~~	
~~Fichier~~	~~ID de fichier~~	~~IDFC~~	~~Lecture/sélection~~	~~Actualisation~~
~~└DF Tachograph_G2~~			~~SC1~~	
~~├EF Application_Identification~~	~~'0501h'~~	~~1~~	~~SC1~~	~~JMS~~
~~├EF CardMA_Certificate~~	~~'C100h'~~	~~2~~	~~SC1~~	~~JMS~~
~~├EF CA_Certificate~~	~~'C108h'~~	~~4~~	~~SC1~~	~~JMS~~
~~├EF Link_Certificate~~	~~'C109h'~~	~~5~~	~~SC1~~	~~JMS~~
~~├EF Identification~~	~~'0520h'~~	~~6~~	~~SC1~~	~~JMS~~
~~└EF Company_Activity_Data~~	~~'050Dh'~~	~~14~~	~~SC1~~	~~MS-MAC-G2~~

			Règles d'accès	
Fichier	**ID de fichier**	**IDFC**	**Lecture/sélection**	**Actualisation**
└DF Tachograph_G2			**SC1**	
├EF Application_Identification	**'0501h'**	**1**	**SC1**	**JMS**
├EF CardMA_Certificate	**'C100h'**	**2**	**SC1**	**JMS**
├EF CA_Certificate	**'C108h'**	**4**	**SC1**	**JMS**
├EF Link_Certificate	**'C109h'**	**5**	**SC1**	**JMS**
├EF Identification	**'0520h'**	**6**	**SC1**	**JMS**
├EF Company_Activity_Data	**'050Dh'**	**14**	**SC1**	**MS-MAC-G2**
├EF Application_Identification_V2	**'0525h'**	**22**	**SC1**	**JMS**
└EF VU_Configuration	**'0540h'**	**30**	**SC5/SC1**	**MS-MAC-G2**

Dans le tableau ci-dessus, ~~l'~~**les** abréviation**s** suivante**s** ~~est~~ **sont** utilisée**s** pour désigner les conditions de sécurité :

SC1 TJR OU MS-MAC-G2

SC5 **Pour la commande READ BINARY avec octet INS pair : MS-C-MAC-G2 ET MS-R-ENC-MAC-G2**

Pour la commande READ BINARY avec octet INS impair (si prise en charge) : JMS

TCS_177 La structure de tous les EF doit être transparente.

TCS_178 L'application de la carte d'entreprise de génération 2 doit présenter la structure de données suivante :

Fichier/Élément de données	Nombre d'enregistrements	Taille (octets) Min	Taille (octets) Max	Valeurs par défaut
DF Tachograph_G2		11338	25089	
EF Application_Identification		5	5	
CompanyCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF CardMA_Certificate		204	341	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		204	341	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		204	341	
LinkCertificate		204	341	{00..00}
EF Identification		139	139	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00,
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		74	74	
companyName		36	36	{00,
companyAddress		36	36	{00,
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		10582	23922	
CompanyActivityData		10582	23922	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		10580	23920	
companyActivityRecord	n_8	46	46	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00,
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

Fichier/Élément de données	Nombre d'enregistrements	Min.	Max.	Valeurs par défaut
DF Tachograph_G2		**14414**	**28165**	
EF Application_Identification		***5***	***5***	
CompanyCardApplicationIdentification		***5***	***5***	
typeOfTachographCardId		**1**	**1**	**{00}**
cardStructureVersion		**2**	**2**	**{01 01} V2**
noOfCompanyActivityRecords		**2**	**2**	**{00 00}**
EF CardMA_Certificate		***204***	***341***	
CardMA_Certificate		**204**	**341**	**{00..00}**

EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*139*	*139*	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		74	74	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		10580	23920	
companyActivityRecord	**n8**	46	46	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}
EF Application_Identification_V2		4	4	
CompanyCardApplicationIdentificationV2		*4*	*4*	
lengthOfFollowingData		*2*	*2*	{00 00}
VuConfigurationLengthRange		2	2	{00 00}
EF VuConfiguration		*3072*	*3072*	
VuConfigurations	**n13**	*3072*	*3072*	

TCS_179 Employées pour indiquer les tailles dans le tableau ci-dessus, les valeurs qui suivent correspondent aux nombres d'enregistrements minimum et maximum que doit utiliser la structure de données de la carte d'entreprise pour une application de génération 2 :

		Min.	*Max.*
n_8	NoOfCompanyActivityRecords	230	520
n_{13}	**VuConfigurationLengthRange**	**3 072 octets**	**3 072 octets**

~~Appendice~~Sous-appendice 3

Pictogrammes

PIC_001 Le tachygraphe peut utiliser les pictogrammes et combinaisons de pictogrammes qui suivent (ou des pictogrammes et combinaisons de pictogrammes suffisamment semblables pour être identifiables sans ambiguïté) :

1. Pictogrammes de base

	Détenteurs	**Actions**	**Modes de fonctionnement**
	Entreprise		Mode entreprise
	Contrôleur	Contrôle	Mode contrôle
	Conducteur	Conduite	Mode opérationnel
	Atelier/laboratoire d'essai	Inspection/étalonnage	Mode étalonnage
	Fabricant		

	Activités	**Durée**
	Disponibilité	Période de disponibilité en cours
	Conduite	Temps de conduite continue
	Repos	Période de repos en cours
	Autres tâches	Période de travail en cours
	Interruption	Temps d'interruption cumulé
	Inconnu	

	Équipements	**Fonctions**
1	Lecteur « conducteur »	
2	Lecteur « co-conducteur »	
	Carte	
	Horloge	
	Écran	Affichage
	Mémoire externe	Téléchargement
	Alimentation électrique	
	Imprimante	Impression
	Capteur	
	Dimensions des pneumatiques	
	Véhicule/unité embarquée sur le véhicule (UEV)	
	Dispositif GNSS	
	Dispositif de détection à distance	
	Interface STI	

	Conditions particulières et saisies manuelles
OUT	Hors champ
	Trajet en ferry/train
	Opération de chargement
	Opération de déchargement
	Opération de chargement/déchargement simultanés
	Type de chargement : passagers
	Type de chargement : marchandises

Type de chargement : indéterminé

Divers

	Événements		Anomalies
	Début de la période de travail journalière		Fin de la période de travail journalière
	Lieu		
	Saisie manuelle des activités du conducteur		
	Sécurité/**données authentifiées/scellements**		
	Vitesse		
	Heure		
	Total/synthèse		
	Carte numérique/passage de frontière		

Qualificatifs

24h	Journalier
	Hebdomadaire
	(Pour) deux semaines
	De ou vers

2. Combinaisons de pictogrammes

Divers

	Lieu de contrôle		
	Lieu de début de la période de travail journalière		Lieu de fin de la période de travail journalière
	Position après 3 heures de temps de conduite accumulé		
	De (heure)		À (heure)
	Du véhicule		
OUT	Hors champ (début)	OUT	Hors champ (fin)

	Position où le véhicule a franchi la frontière entre deux pays
	Position où une opération de chargement a eu lieu
	Position où une opération de déchargement a eu lieu
	Position où une opération de chargement/déchargement simultanés a eu lieu

Cartes

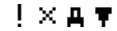
	Carte de conducteur
	Carte d'entreprise
	Carte de contrôleur
	Carte d'atelier
---	Aucune carte

Conduite

	Conduite en équipage
	Temps de conduite hebdomadaire
	Temps de conduite pour deux semaines

Impressions

24h	Tirage papier quotidien des activités du conducteur stockées sur la carte
24h	Tirage papier quotidien des activités du conducteur stockées dans la mémoire de l'UEV
	Tirage papier des événements et anomalies stockés sur la carte


Tirage papier des événements et anomalies stockés dans la mémoire de l'UEV


Tirage papier des données techniques

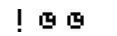

Tirage papier des données relatives aux excès de vitesse


Tirage papier de l'historique des cartes insérées

Événements


Insertion d'une carte non valable


Conflit de carte

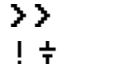

Chevauchement temporel

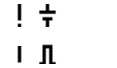

Conduite sans carte appropriée

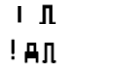

Insertion d'une carte en cours de conduite

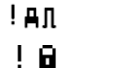

Clôture incorrecte de la dernière session


Excès de vitesse

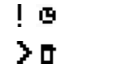

Interruption de l'alimentation électrique

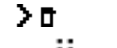

Erreur sur les données de mouvement

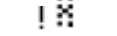

Conflit concernant le mouvement du véhicule


Atteinte à la sécurité


Conflit temporel ou remise à l'heure (en atelier)


Contrôle d'excès de vitesse


Absence de données de positionnement en provenance du récepteur GNSS ou erreur de communication avec le dispositif GNSS externe


Erreur de communication avec le dispositif de communication à distance

Anomalie GNSS

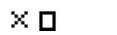
Anomalies

Anomalie de la carte (lecteur « conducteur »)

Anomalie de la carte (lecteur « co-conducteur »)

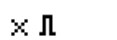

Anomalie de l'affichage


Anomalie de téléchargement


Anomalie de l'imprimante

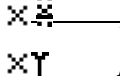

Anomalie du capteur


Anomalie interne de l'UEV


~~Anomalie GNSS~~

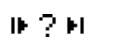

Anomalie de la détection à distance

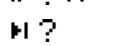
Procédure de saisie manuelle


Même période de travail journalière ?


Fin de la période de travail antérieure ?

Confirmation ou saisie du lieu de fin de la période de travail


Saisie de l'heure de départ


Saisie du lieu de début de la période de travail

Remarque : diverses combinaisons de pictogrammes supplémentaires permettant de former des blocs d'impression ou des identificateurs d'enregistrements sont définies ~~à l'appendice~~ **au sous-appendice** 4.

~~Appendice~~Sous-appendice 4

Tirages papier

Table des matières

1. Généralités

Tout tirage papier se compose d'une succession de blocs de données séquencés, éventuellement associés à un identificateur de bloc.

Un bloc de données contient un ou plusieurs enregistrements, éventuellement associés à un identificateur d'enregistrement.

PRT_001 Si un identificateur de bloc précède immédiatement un identificateur d'enregistrement, ce dernier n'est pas imprimé.

PRT_002 Si un élément de données est inconnu ou ne doit pas être imprimé pour des raisons de droits d'accès aux données, le système imprime des espaces en lieu et place de ces éléments.

PRT_003 Si le contenu d'une ligne complète est inconnu ou ne doit pas nécessairement être imprimé, la ligne correspondante est omise.

PRT_004 Les champs de données numériques sont justifiés à droite au tirage, leur impression s'accompagnant d'espaces de séparation marquant les milliers et les millions, sans comporter de zéros en tête.

PRT_005 Les champs constitués de chaînes de caractères sont justifiés à gauche au tirage et, le cas échéant, complétés d'espaces pour atteindre la longueur élémentaire requise ou tronqués pour la même raison. ~~(~~**Les** noms et adresses **peuvent être imprimés sur deux lignes**~~)~~.

PRT_006 Si la longueur du texte impose un retour à la ligne, la nouvelle ligne imprimée doit commencer par un caractère spécial (un point à mi-hauteur, « • »).

2. Caractéristiques des blocs de données

Dans ce chapitre, les conventions de notation suivantes ont été appliquées :

- Les caractères affichés en gras indiquent le texte en clair à imprimer (au tirage, les caractères sont normaux) ;
- Les caractères normaux indiquent à l'affichage des variables (pictogrammes ou données) qui seront remplacées au tirage par leurs valeurs respectives ;
- Les noms de variable s'accompagnent de tirets bas indiquant la longueur élémentaire disponible pour la variable considérée ;
- Les dates respectent par défaut le format « jj/mm/aaaa » (jour, mois, année). Le format « jj.mm.aaaa » peut également être appliqué ;
- La rubrique « identification de carte » se compose des éléments suivants : le type de carte indiqué par une combinaison de pictogrammes, le code de ~~l'État membre~~ **la Partie contractante** ayant délivré la carte, une barre oblique suivie du numéro de la carte, puis d'un indice de remplacement et d'un indice de renouvellement séparés tous deux de l'élément qui les précède par un espace ;

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Combinaison de pictogrammes		Code de ~~l'~~ ~~État membre~~ **la Partie contractante** de délivrance				14 premiers caractères du numéro de la carte (comprenant, le cas échéant, un indice séquentiel)														Indice de remplacement		Indice de renouvellement

- **Dans un bloc de données, le texte après 'pi=' désigne le pictogramme ou la combinaison de pictogrammes correspondants définis au sous-appendice 3 ;**

- **Lorsqu'il est imprimé après la longitude et la latitude d'une position enregistrée ou après la date et l'heure auxquelles la position a été déterminée, le pictogramme indique que la position a été calculée à partir de messages de navigation authentifiés ;**
- * **données disponibles uniquement dans les tachygraphes de génération 2 (toutes versions confondues) ;**
- ** **données disponibles uniquement dans les tachygraphes de génération 2, version 2.**

PRT_007 Les tirages se composent des blocs et/ou enregistrements de données présentés ci-après. Leur signification et leur format sont les suivants :

Numéro de bloc ou d'enregistrement Signification	Format des données
1 ***Date et heure d'impression du document***	jj/mm/aaaa hh:mm **(UTC)**
2 ***Type de tirage papier*** Identificateur de bloc **Génération et version de l'UEV**** Combinaison de pictogrammes d'impression (voir **sous-**appendice 3), réglage du limiteur de vitesse (impression uniquement en cas d'excès de vitesse)	----------▼---------- **GEN2 v2** Picto xxx **km/h**
3 ***Identification du détenteur de la carte*** Identificateur de bloc. P = pictogramme « détenteur » Nom du détenteur de la carte Prénom(s) du détenteur de la carte (le cas échéant) Identification de la carte Date d'expiration de la carte (le cas échéant) et génération de la carte (GEN1 ou GEN2)* **et version****	----------P---------- P Nom_____ Prénom_____ Identification_carte____ _ jj/mm/aaaa - GEN2 **v2**

Si la carte considérée n'est pas individuelle et ne contient aucun nom de détenteur, le nom de l'entreprise, de l'atelier ou de l'organisme de contrôle concerné est imprimé en lieu et place de celui-ci.

~~* Seul un tachygraphe intelligent peut imprimer la génération de la carte.~~

4 ***Identification du véhicule*** Identificateur de bloc Numéro d'identification du véhicule ~~État membre~~ **Partie contractante** d'immatriculation du véhicule et VRN	----------🚙---------- 🚙 VIN_____ Nat/VRN_____
4a ***Type de chargement par défaut du véhicule**** **pi = pictogramme « type de chargement »****	**pi**
5 ***Identification de l'UEV*** Identificateur de bloc Nom du fabricant de l'UEV Numéro de référence de l'UEV Génération de l'UEV*	----------⊟---------- ⊟ Fabricant_UEV_____ Numéro_pièce_UEV__ GEN2

~~* Seul un tachygraphe intelligent peut imprimer la génération de la carte.~~

6 ***Dernier étalonnage du tachygraphe***

Identificateur de bloc
Nom de l'atelier
Identification de la carte de l'atelier

Date de l'étalonnage

```
----------T-----------
T Nom_______________
Identification_carte____
_
T jj/mm/aaaa
```

7 ***Dernier contrôle (par un contrôleur)***

Identificateur de bloc
Identification de la carte du contrôleur

Date, heure et type de contrôle

```
----------D-----------
Identification_carte____
_
D jj/mm/aaaa hh:mm ppppp
```

Type de contrôle : combinaison composée de cinq pictogrammes au maximum. Le type de contrôle correspond à l'un des pictogrammes suivants (ou à leur combinaison) :

▮ : téléchargement d'une carte ; ↧ téléchargement à partir de l'UEV ; T: impression ; ▯ : affichage ; T : contrôle routier d'étalonnage.

8 ***Activités du conducteur enregistrées sur une carte par ordre chronologique***

Identificateur de bloc
Date de consultation (jour civil dont les données font l'objet du tirage) et compteur de présence journalière de la carte

```
----------⊙----------
    jj/mm/aaaa xxx
```

8a *Condition « hors champ » au début de la journée* (laisser vide si pas de condition « hors champ » ouverte)

```
----------OUT----------
```

8b ***Type de chargement au début de la journée*** (si la carte est insérée dans une UEV ; laisser vide si tel n'est pas le cas), `pi` = pictogramme de type de chargement****

```
----------pi----------
```

8.1 *Période pendant laquelle la carte n'était pas insérée dans un lecteur*

8.1a Identificateur d'enregistrement (début de la période)

8.1b *Période inconnue*. Heure de début, durée

8.1c *Activité saisie manuellement.*
Pictogramme d'activité, heure de début, durée

```
  --------------------
?       hh:mm hhhmm
A       hh:mm hhhmm
```

8.2 *Insertion de la carte dans le lecteur S*

Identificateur d'enregistrement ; S = pictogramme « lecteur »
~~État membre~~ **Partie contractante** d'immatriculation du véhicule et numéro d'immatriculation du véhicule (VRN)
Kilométrage du véhicule à l'insertion de la carte
`pi` = type de chargement du véhicule à l'insertion de la carte**

```
  ---------S---------

 Nat/VRN___________

  x xxx xxx km
pi
```

8.3 *Activité (lors de l'insertion de la carte)*
Pictogramme d'activité, heure de début, durée, situation de l'équipage (pictogramme d'équipage si ÉQUIPAGE, espaces vides si SEUL)

```
A       hh:mm hhhmm ⊙⊙
```

8.3a *Condition particulière*
Heure de saisie, pictogramme (ou combinaison de pictogrammes) associé à une condition particulière

```
        hh:mm ---pppp---
```

8.4 *Retrait de carte*
Kilométrage et distance parcourue depuis la dernière insertion de la carte pour laquelle le kilométrage est connu

```
  x xxx xxx km ; x xxx
km
```

9 ***Activités du conducteur enregistrées sur une UEV par lecteur de carte et par ordre chronologique***

Identificateur de bloc
Date de consultation (jour civil dont les données font l'objet du tirage)
Kilométrages du véhicule à 00 h 00 et à 24 h 00

```
----------⊙----------
      jj/mm/aaaa

x xxx xxx - x xxx xxx km
```

10 ***Activités associées au lecteur S***

Identificateur de bloc

```
----------S----------
```

10a *Condition « hors champ » au début de cette journée*
(laisser vide si pas de condition « hors champ » ouverte)

```
----------OUT----------
```

10.1 *Période pendant laquelle aucune carte n'est insérée dans le lecteur S*

Identificateur d'enregistrement
Aucune carte insérée
Kilométrage au début de la période considérée

```
  ------------------
⊙▪---
  x xxx xxx km
```

10.2 *Insertion de carte*

Identificateur d'enregistrement d'insertion de carte
Nom du conducteur
Prénom du conducteur
Identification de la carte du conducteur
Date d'expiration de la carte (le cas échéant), génération de la carte (GEN1 ou GEN2)* **et version****
~~État membre~~ **Partie contractante** d'immatriculation et numéro d'identification du véhicule précédemment utilisé
Date et heure de retrait de la carte du véhicule précédent
Ligne vierge
Kilométrage affiché au compteur à l'insertion de la carte, saisie manuelle d'un marqueur d'activité du conducteur (M si oui, espace vide si non).
S'il n'y a pas eu d'insertion de carte de conducteur le jour pour lequel le tirage papier est effectué, le kilométrage indiqué au bloc 10.2 est celui correspondant à la dernière insertion de carte disponible avant le jour concerné.

```
  ------------------
⊙ Nom_______________
  Prénom____________
Identification_carte____
  jj/mm/aaaa - GEN2 v2

🚘+Nat/VRN___________

  jj/mm/aaaa hh:mm

  x xxx xxx km          M
```

10.3 *Activité*

Pictogramme d'activité, heure de début, durée, situation de l'équipage (pictogramme d'équipage si ÉQUIPAGE, espace vide si SEUL)

```
A       hh:mm hhhmm ⊙⊙
```

10.3a *Condition particulière*

Heure de saisie, pictogramme (ou combinaison de pictogrammes) associé à une condition particulière

```
        hh:mm ---pppp---
```

10.4 *Retrait de carte ou fin de période « sans carte »*

Kilométrage au retrait de la carte ou à la fin de la période « sans carte » et distance parcourue depuis l'insertion de la carte ou depuis le début de la période « sans carte ».

```
  x xxx xxx km ; x xxx
km
```

~~* Seul un tachygraphe intelligent peut imprimer la génération de la carte.~~

11 *Synthèse quotidienne*

Identificateur de bloc

```
----------Σ----------
```

11.1 ***Synthèse des périodes sans carte dans le lecteur « conducteur » de l'UEV***

Identificateur de bloc

```
1⊙▪---
```

11.2 ***Synthèse des périodes sans carte dans le lecteur « co-conducteur » de l'UEV***

Identificateur de bloc

```
2⊙▪---
```

11.3 ***Synthèse quotidienne des données de l'UEV par conducteur***

Identificateur d'enregistrement
Nom du conducteur
Prénom(s) du conducteur
Identification de la carte du conducteur

```
  ------------------
⊙ Nom_______________
  Prénom____________
Identification_carte____
```

11.4 *Saisie du lieu de début et/ou de fin d'une période de travail journalière*

pi = pictogramme du lieu de départ/d'arrivée, heure, pays, région
lat~~ong~~itude de la position enregistrée*, état d'authentification**
long~~at~~itude de la position enregistrée*, état d'authentification**
Date et heure de détermination de la position*, état d'authentification**
Kilométrage

```
pihh:mm Pays Rég
lat~~on~~ ±DD~~D~~°MM.M'
lon~~at~~ ± DDD°MM.M'
~~hh:mm~~
jj/mm/aaaa hh:mm
  x xxx xxx km
```

11.5 ~~*Saisie du lieu de début et/ou de fin d'une période de travail journalière*~~**Positions du véhicule après 3 heures de temps de conduite accumulé***

pi= position après 3 heures de temps de conduite ~~continue~~**accumulé***, **heure de l'enregistrement de la position***
lat~~ong~~itude de la position enregistrée*, état d'authentification**
long~~at~~itude de la position enregistrée*, état d'authentification**
Date et heure de détermination de la position*, état d'authentification**
Kilométrage*

```
pihh:mm
lat~~on~~ ±DD~~D~~°MM.M'
lon~~at~~ ± DDD°MM.M'
jj/mm/aaaa hh:mm
x xxx xxx km
```

11.5a ***Passage de frontière*****
pi = position du véhicule lorsqu'il a franchi la frontière d'un pays**
Pays de provenance/destination du véhicule**
Latitude de la position enregistrée, état d'authentification****
Longitude de la position enregistrée, état d'authentification****
Date et heure de détermination de la position, état d'authentification****
Kilométrage**

```
pi
Pays + Pays
lat ± DD°MM.M'
lon ±DDD°MM.M'
jj/mm/aaaa hh:mm
  x xxx xxx km
```

11.5b ***Opération de chargement/déchargement*****
pi = position du véhicule pendant l'opération de chargement/déchargement, heure de l'enregistrement de la position**
latitude de la position enregistrée, état d'authentification****
longitude de la position enregistrée, état d'authentification****
Date et heure de détermination de la position**
Kilométrage**

```
pihh:mm
lat ± DD°MM.M'
lon ±DDD°MM.M'
dd/mm/yyyy hh:mm
  x xxx xxx km
```

11.6 *Totaux par activité (extraits d'une carte)*

Durée totale de la période de conduite, distance parcourue
Durée totale des périodes de travail et de disponibilité
Durée totale des périodes de repos et d'activité inconnue
Durée totale des activités de l'équipage

```
  hh**h**mm  x xxx km
  hh**h**mm  hh**h**mm
  hh**h**mm  hh**h**mm
  hh**h**mm
```

11.7 *Totaux par activité (périodes sans carte insérée dans le lecteur « conducteur »)*

Durée totale de la période de conduite, distance parcourue
Durée totale des périodes de travail et de disponibilité
Durée totale de la période de repos

```
  hh**h**mm  x xxx km
  hh**h**mm  hh**h**mm
  hh**h**mm
```

11.8 *Totaux par activité (périodes sans carte insérée dans le lecteur « co-conducteur »)*

```
Durée totale des périodes de travail et de disponibilité   ⚒ hhhmm   ⧈ hhhmm
Durée totale de la période de repos                        ⊢ hhhmm
```

11.9 *Totaux par activité (et par conducteur, les deux lecteurs étant inclus dans le calcul)*

```
Durée totale de la période de conduite, distance parcourue   ⊙ hhhmm   x xxx km
Durée totale des périodes de travail et de disponibilité     ⚒ hhhmm   ⧈ hhhmm
Durée totale de la période de repos                          ⊢ hhhmm
Durée totale des activités de l'équipage                     ⊙⊙ hhhmm
```

Si un tirage quotidien est demandé pour la journée en cours, la synthèse des informations s'effectue à partir des données disponibles à l'heure de l'impression.

12 ***Événements et/ou anomalies enregistrés sur une carte***

12.1 Identificateur de bloc pour les 5 derniers « événements et anomalies » extraits d'une carte

```
----------!×▪----------
```

12.2 Identificateur de bloc pour tous les « événements » enregistrés sur une carte

```
----------!▪----------
```

12.3 Identificateur de bloc pour toutes les « anomalies » enregistrées sur une carte

```
----------×▪----------
```

12.4 *Enregistrement d'événement et/ou d'anomalie*

Identificateur d'enregistrement
Pictogramme d'événement/anomalie, motif de l'enregistrement, date et heure de début
Code d'événement/anomalie supplémentaire (le cas échéant), durée
~~État membre~~ **Partie contractante** d'immatriculation et VRN du véhicule dans lequel l'événement ou l'anomalie est survenu

```
--------------------
Pic (p) jj/mm/aaaa hh:mm

!xx                hhhmm

🚗 Nat/VRN__________
```

13 ***Événements et/ou anomalies enregistrés ou en cours dans une UEV***

13.1 Identificateur de bloc pour les 5 derniers « événements et anomalies » extraits d'une UEV

```
----------!×🚗----------
```

13.2 Identificateur de bloc pour l'ensemble des « événements » enregistrés ou en cours dans une UEV

```
----------!🚗----------
```

13.3 Identificateur de bloc pour l'ensemble des « anomalies » enregistrées ou en cours dans une UEV

```
----------×🚗----------
```

13.4 *Enregistrement d'événement et/ou d'anomalie*

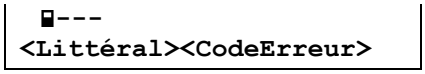
Identificateur d'enregistrement
Pictogramme d'événement/anomalie, motif de l'enregistrement, date et heure de début
Code d'événement/anomalie supplémentaire (le cas échéant), nombre d'événements semblables survenus le même jour, durée
Identification des cartes insérées au début ou à la fin de l'événement ou de l'anomalie (jusqu'à 4 lignes sans répéter aucun numéro de carte)

```
--------------------
Pic (p) jj/mm/aaaa hh:mm

!xx      (xxx)     hhhmm


Identification_carte____
_
Identification_carte____
_
Identification_carte____
_
Identification_carte____
_
```

Cas où aucune carte n'a été insérée
Données spécifiques du fabricant



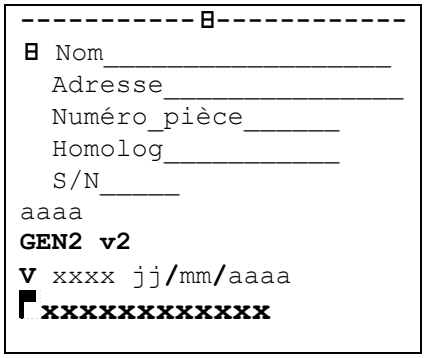
Le motif de l'enregistrement (p) prend la forme d'un code numérique indiquant la raison pour laquelle l'événement ou l'anomalie constaté a été enregistré, et est codé selon l'élément de données EventFaultRecordPurpose.

`Littéral` est un symbole littéral spécifique d'un fabricant de tachygraphe comportant au maximum 12 caractères.

`CodeErreur` est un code d'erreur spécifique d'un fabricant de tachygraphe comportant au maximum 12 caractères.

14 ***Identification de l'UEV***

Identificateur de bloc
Nom du fabricant de l'UEV
Adresse du fabricant de l'UEV
Numéro de référence de l'UEV
Numéro d'homologation de l'UEV
Numéro de série de l'UEV
Année de fabrication de l'UEV
Génération et version de l'UEV**
Version du logiciel de l'UEV et date d'installation
Version de la carte numérique stockée dans la mémoire**

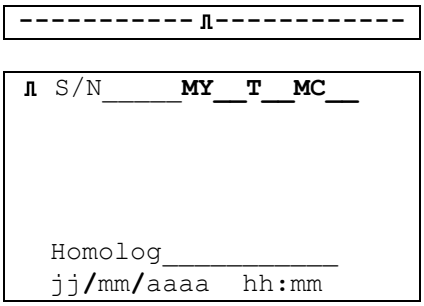


15 ***Identification d'un capteur***

Identificateur de bloc

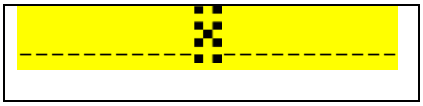
15.1 *Enregistrement de couplage*

Numéro de série du capteur **(S/N = `serialNumber` au format décimal, MY = `monthYear` au format décimal, T = type au format décimal, MC = `manufacturerCode` au format hexadécimal, voir sous-appendice 1, `ExtendedSerialNumber`)**
Numéro d'homologation du capteur
Date de couplage du capteur



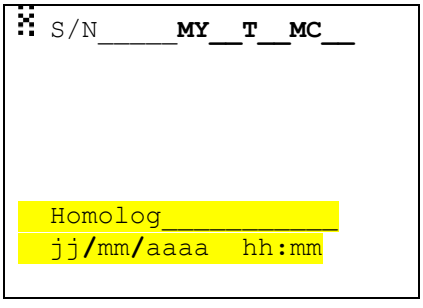
16 ***Identification du dispositif GNSS****

Identificateur de bloc*



16.1 *Enregistrement de couplage**

Numéro de série du dispositif GNSS externe*
(S/N = `serialNumber` au format décimal, MY = `monthYear` au format décimal, T = `type` au format décimal, MC = `manufacturerCode` au format hexadécimal, voir sous-appendice 1, `ExtendedSerialNumber`)
Numéro d'homologation du dispositif GNSS externe*
Date de couplage du dispositif GNSS externe*



~~Le motif d'étalonnage (p) prend la forme d'un code numérique indiquant la raison pour laquelle ces paramètres d'étalonnage ont été enregistrés et codés conformément à l'élément de données CalibrationPurpose.~~

16a ***Identification du dispositif de communication à distance*****
Identificateur de bloc**

```
----------T---------
```

16a.1 ***Numéro de série du dispositif de communication à distance*****
Numéro de série du dispositif de communication à distance (S/N = `serialNumber` au format décimal, MY = `monthYear` au format décimal, T = `type` au format décimal, MC = `manufacturerCode` au format hexadécimal, voir sous-appendice 1, `ExtendedSerialNumber`)**

```
S/N_____ MY____ T____ MC_
```

17 ***Données d'étalonnage***
Identificateur de bloc

```
----------T-----------
```

17.1 *Enregistrement d'étalonnage*
Identificateur d'enregistrement
Atelier ayant procédé à l'étalonnage
Adresse de l'atelier
Identification de la carte de l'atelier

Date d'expiration de la carte de l'atelier
Ligne vierge
Date et heure de l'étalonnage **(`oldTimeValue` dans l'enregistrement)** et motif de l'étalonnage **au format hexadécimal**
VIN
~~État membre~~ **Partie contractante** d'immatriculation du véhicule et VRN
Coefficient caractéristique du véhicule
Constante de ~~l'équipement d'enregistrement~~ **l'appareil de contrôle**
Circonférence effective des pneumatiques
Dimensions des pneumatiques montés
Réglage du limiteur de vitesse
Ancienne et nouvelle valeurs affichées par le compteur kilométrique
pi = type de chargement par défaut du véhicule**
Pays dans lequel l'étalonnage a été effectué, date et heure
Données relatives aux scellements (jusqu'à 5 enregistrements de scellements, 1 ligne par scellement), ET = `equipmentType` au format décimal, MC = `manufacturerCode` en deux caractères**, SI = `sealIdentifier` en huit caractères**, voir sous-appendice 1, `SealRecord`)**

```
  --------------------
T Nom_atelier__________
  Adresse_atelier_____
Identification_carte____
_
  jj/mm/aaaa

T jj/mm/aaaa hh:mm (p)


A VIN________________
  Nat/VRN___________

w xx xxx Imp/km
k xx xxx Imp/km

l xx xxx mm
  TyreSize_______
> xxx  km/h
x xxx xxx - x xxx xxx km

pi
Pays dd/mm/yyyy hh:mm

ET_ MC SI______
```

Le motif d'étalonnage (p) prend la forme d'un code numérique indiquant la raison pour laquelle les paramètres d'étalonnage considérés ont été enregistrés et codés en conformité avec l'élément de données CalibrationPurpose.

18 ***Remise à l'heure***
Identificateur de bloc

```
----------◷-----------
```

18.1 *Enregistrement de la remise à l'heure*
Identificateur d'enregistrement
Anciennes date et heure
Nouvelles date et heure
Atelier ayant procédé à la remise à l'heure
Adresse de l'atelier
Identification de la carte de l'atelier
Date d'expiration de la carte de l'atelier

```
-----------------------
!◷ jj/mm/aaaa  hh:mm
 ◷ jj/mm/aaaa  hh:mm
T Nom_atelier__________
  Adresse_atelier___
Identification_carte____
  jj/mm/aaaa
```

19 ***Événement et anomalie les plus récents enregistrés dans l'UEV***

Identificateur de bloc
Date et heure de l'événement le plus récent
Date et heure de l'anomalie la plus récente

```
----------!×----------
! jj/mm/aaaa  hh:mm
× jj/mm/aaaa  hh:mm
```

20 ***Informations relatives au contrôle d'excès de vitesse***

Identificateur de bloc
Date et heure du dernier CONTRÔLE D'EXCÈS DE VITESSE
Date/heure du premier excès de vitesse et nombre d'événements de cette nature enregistrés depuis lors

```
----------►►----------
►jj/mm/aaaa hh:mm

►►jj/mm/aaaa hh:mm (nnn)
```

21 ***Enregistrement d'excès de vitesse***

21.1 Identificateur de bloc « Premier excès de vitesse survenu après le dernier étalonnage »

```
--------►►T---------
```

21.2 Identificateur de bloc « Les 5 excès de vitesse les plus graves enregistrés au cours des 365 derniers jours »

```
-------►►(365)------
```

21.3 Identificateur de bloc « L'excès de vitesse le plus grave pour chacun des 10 derniers jours d'occurrence »

```
-------►►(10)-------
```

21.4 Identificateur d'enregistrement
Date, heure et durée

Vitesses maximale et moyenne, nombre d'événements semblables survenus le même jour
Nom du conducteur
Prénom(s) du conducteur
Identification de la carte du conducteur

```
  --------------------
►►jj/mm/aaaa hh:mm
hhhmm
  xxx km/h xxx km/h(xxx)

Nom_______________
  Prénom_____________
Identification_carte____
```

21.5 Si un bloc ne contient aucun enregistrement d'excès de vitesse

```
►►---
```

22 ***Informations manuscrites***

Identificateur de bloc

```
------------------------
 .....................
 .....................
 .....................
 .....................
 .....................
```

22.1 Lieu du contrôle
22.2 Signature du contrôleur
22.3 De (heure)
22.4 À (heure)
22.5 Signature du conducteur

« Informations manuscrites » : introduire suffisamment de lignes vierges au-dessus de chaque champ pour pouvoir rédiger les informations requises ou apposer une signature.

23 ***Dernières cartes insérées dans l'UEV****

Identificateur de bloc*

```
-------- ⊟▮◷ --------


----
T <gén> <version> <MC>
Identification de carte
Numéro de série de la
carte
jj/mm/aaaa hh:mm
```

23.1 Carte insérée*
Identificateur d'enregistrement*
Type de carte, génération, version, fabricant*[1]
Identification de la carte*
Numéro de série de la carte*

Date et heure de la dernière insertion de carte*

[1] (le tout sur une seule ligne)
avec
type de carte : pictogramme, un caractère + espace
génération : GEN1 ou GEN2, 4 caractères + espace
version : jusqu'à 10 caractères
MC : code du fabricant, 3 caractères

3. Caractéristiques des tirages papier

Dans ce chapitre, les conventions de notation suivantes ont été appliquées :

N	Impression du bloc ou de l'enregistrement numéro N
N	Impression du bloc ou de l'enregistrement numéro N répété autant de fois que l'exige la situation
X/Y	Impression des blocs ou enregistrements X et/ou Y selon les besoins, et répétition de l'opération autant de fois que l'exige la situation.

3.1 Tirage papier quotidien des activités du conducteur stockées sur une carte

PRT_008 Le tirage quotidien des activités du conducteur stockées sur une carte doit respecter le format suivant :

1	Date et heure d'impression du document
2	Type de document imprimé
3	Identification du contrôleur (en cas d'insertion d'une carte de contrôleur dans l'UEV)
3	Identification du conducteur (extraite de la carte faisant l'objet de l'impression + GEN)
4	Identification du véhicule (à partir duquel le tirage est exécuté)
5	Identification de l'UEV (à partir de laquelle le tirage est exécuté + GEN)
6	Dernier étalonnage de cette UEV
7	Dernier contrôle auquel le conducteur inspecté a été soumis
8	Délimiteur des activités du conducteur
8a	Condition « hors champ » au début de la journée concernée
8b	**Type de chargement au début de la journée concernée (si la carte est insérée dans une UEV)**
8.1a/8.1b/8.1c/8.2/8.3/ 8.3a/8.4	Activités du conducteur par ordre chronologique
11	Délimiteur de synthèse quotidienne
11.4	Lieux saisis, par ordre chronologique
11.5	~~Données du GNSS~~**Positions après 3 heures de temps de conduite accumulé, par ordre chronologique**
11.5a	**Passages de frontières, par ordre chronologique**
11.5b	**Opérations de chargement/déchargement, par ordre chronologique**
11.6	Totaux par activité
12.1	Délimiteur des événements et anomalies extraits d'une carte
12.4	Enregistrements d'événements/anomalies (5 derniers événements ou anomalies enregistrés sur la carte)
13.1	Délimiteur des événements ou anomalies extraits de l'UEV
13.4	Enregistrements d'événements/anomalies (5 derniers événements ou anomalies enregistrés ou en cours dans l'UEV)
22.1	Lieu du contrôle
22.2	Signature du contrôleur
22.5	Signature du conducteur

3.2 Tirage papier quotidien des activités du conducteur stockées dans la mémoire de l'UEV

PRT_009 Le tirage quotidien des activités du conducteur stockées dans la mémoire de l'UEV doit respecter le format suivant :

1	Date et heure d'impression du document
2	Type de document imprimé
3	Identification du détenteur de la carte (pour toutes les cartes insérées dans l'UEV + GEN)
4	Identification du véhicule (à partir duquel le tirage est exécuté)
4a	**Type de chargement par défaut du véhicule**
5	Identification de l'UEV (à partir de laquelle le tirage est exécuté + GEN)
6	Dernier étalonnage de cette UEV
7	Dernier contrôle auquel le tachygraphe a été soumis
9	Délimiteur des activités du conducteur
10	Délimiteur du lecteur conducteur (lecteur 1)
10a	Condition « hors champ » au début de la journée concernée
10.1/10.2/10.3/10.3a/ 10.4	Activités par ordre chronologique (lecteur conducteur)
10	Délimiteur du lecteur co-conducteur (lecteur 2)
10a	Condition « hors champ » au début de la journée concernée
10.1/10.2/10.3/10.3a/ 10.4	Activités par ordre chronologique (lecteur co-conducteur)
11	Délimiteur de synthèse quotidienne
11.1	Synthèse des périodes sans carte dans le lecteur conducteur
11.4	Lieux saisis, par ordre chronologique
11.5	~~Données du GNSS~~ **Positions après 3 heures de temps de conduite accumulé, par ordre chronologique**
11.5a	**Passages de frontières, par ordre chronologique**
11.5b	**Opérations de chargement/déchargement, par ordre chronologique**
11.~~6~~**7**	Totaux par activité
11.2	Synthèse des périodes sans carte dans le lecteur co-conducteur
11.4	Lieux saisis, par ordre chronologique
11.5	~~Données du GNSS~~ **Positions après 3 heures de temps de conduite accumulé, par ordre chronologique**
11.5a	**Passages de frontières, par ordre chronologique**
11.5b	**Opérations de chargement/déchargement, par ordre chronologique**
11.8	Totaux par activité
11.3	Synthèse des activités d'un conducteur, les deux lecteurs étant inclus
11.4	Lieux saisis par ce conducteur, par ordre chronologique
11.5	~~Données du GNSS~~ **Positions du véhicule après 3 heures de temps de conduite accumulé, par ordre chronologique**
11.5a	**Passages de frontières, par ordre chronologique**
11.5b	**Opérations de chargement/déchargement, par ordre chronologique**
11.9	Totaux par activité pour ce conducteur
13.1	Délimiteur d'événements et d'anomalies
13.4	Enregistrements d'événements/anomalies (5 derniers événements ou anomalies enregistrés ou en cours dans l'UEV)
22.1	Lieu du contrôle
22.2	Signature du contrôleur
22.3	De (heure) (espace disponible pour permettre à un conducteur dépourvu de

	carte d'indiquer les périodes qui correspondent à ses prestations)
22.4	À (heure)
22.5	Signature du conducteur

3.3 Tirage papier des événements et des anomalies stockés sur une carte

PRT_010 Le tirage des événements et des anomalies stockés sur une carte doit respecter le format suivant :

1	Date et heure d'impression du document
2	Type de document imprimé
3	Identification du contrôleur (en cas d'insertion d'une carte de contrôle dans l'UEV + GEN)
3	Identification du conducteur (extraite de la carte faisant l'objet de l'impression)
4	Identification du véhicule (à partir duquel le tirage est exécuté)
12.2	Délimiteur des événements
12.4	Enregistrements d'événements (tous les événements enregistrés sur la carte)
12.3	Délimiteur des anomalies
12.4	Enregistrements d'anomalies (toutes les anomalies enregistrées sur la carte)
22.1	Lieu du contrôle
22.2	Signature du contrôleur
22.5	Signature du conducteur

3.4 Tirage papier des événements et des anomalies stockés dans la mémoire de l'UEV

PRT_011 Le tirage des événements et anomalies stockés dans la mémoire de l'UEV doit respecter le format suivant :

1	Date et heure d'impression du document
2	Type de document imprimé
3	Identification du détenteur de la carte (pour toutes les cartes insérées dans l'UEV + GEN)
4	Identification du véhicule (à partir duquel le tirage est exécuté)
13.2	Délimiteur des événements
13.4	Enregistrements d'événements (tous les événements enregistrés ou en cours dans l'UEV)
13.3	Délimiteur des anomalies
13.4	Enregistrements d'anomalies (toutes les anomalies enregistrées ou en cours dans l'UEV)
22.1	Lieu du contrôle
22.2	Signature du contrôleur
22.5	Signature du conducteur

3.5 Tirage papier des données techniques

PRT_012 Le tirage des données techniques doit respecter le format suivant :

1	Date et heure d'impression du document
2	Type de document imprimé

3	Identification du détenteur de la carte (pour toutes les cartes insérées dans l'UEV + GEN)
4	Identification du véhicule (à partir duquel le tirage est exécuté)
14	Identification de l'UEV
15	Identification des capteurs
15.1	Données relatives au couplage des capteurs (toutes les données disponibles, par ordre chronologique)
16	Identification du dispositif GNSS
16.1	Données relatives au couplage du dispositif GNSS externe (toutes les données disponibles, par ordre chronologique)
16a	**Identification du dispositif de communication à distance**
16a.1	**Numéro de série du dispositif de communication à distance**
17	Délimiteur des données d'étalonnage
17.1	Enregistrements d'étalonnage (tous les enregistrements disponibles, par ordre chronologique)
18	Délimiteur de la remise à l'heure
18.1	Enregistrements de données de remise à l'heure (tous les enregistrements disponibles, extraits des enregistrements de données de remise à l'heure et d'étalonnage)
19	Événement et anomalie les plus récents enregistrés dans l'UEV
2	**Type de document imprimé (marque la fin de l'impression)**

3.6 Tirage papier des données relatives aux excès de vitesse

PRT_013 L'impression des données relatives aux excès de vitesse doit respecter le format suivant :

1	Date et heure d'impression du document
2	Type de document imprimé
3	Identification du détenteur de la carte (pour toutes les cartes insérées dans l'UEV + GEN)
4	Identification du véhicule (à partir duquel le tirage est exécuté)
20	Informations relatives aux contrôles d'excès de vitesse
21.1	Identificateur des données d'excès de vitesse
21.4/21.5	Premier excès de vitesse après le dernier étalonnage
21.2	Identificateur des données d'excès de vitesse
21.4/21.5	Les 5 excès de vitesse les plus graves enregistrés au cours des 365 derniers jours
21.3	Identificateur des données d'excès de vitesse
21.4/21.5	L'excès de vitesse le plus grave pour chacun des 10 derniers jours d'occurrence
22.1	Lieu du contrôle
22.2	Signature du contrôleur
22.5	Signature du conducteur

3.7 Tirage papier de l'historique des cartes insérées

PRT_014 Le tirage de l'historique des cartes insérées doit respecter le format suivant :

1	Date et heure d’impression du document
2	Type de document imprimé
3	Identification du détenteur de la carte (pour toutes les cartes insérées dans l’UEV)
23	Carte la plus récente insérée dans l’UEV
23.1	Cartes insérées (jusqu’à 88 enregistrements)
12.3	**Type de document imprimé (marque la fin de l’impression)** ~~Délimiteur des anomalies~~

~~Appendice~~Sous-appendice 5

Affichage

Dans le présent **sous-**appendice, les conventions de présentation suivantes sont appliquées :

- Les caractères **gras** indiquent le texte en clair à afficher (l'affichage demeure en caractères normaux) ;
- Les caractères normaux indiquent des variables (pictogrammes ou données) remplacées à l'affichage par leurs valeurs respectives, à savoir :
- jj mm aaaa : jour, mois, année ;
- hh : heures ;
- mm : minutes ;
- D : pictogramme de durée ;
- EF : combinaison de pictogrammes d'événement ou d'anomalie ;
- O : pictogramme de mode d'exploitation.

DIS_001 Le tachygraphe utilise les formats d'affichage des données suivants :

Données	**Format**
Affichage par défaut	
Heure locale	hh:mm
Mode d'exploitation	O
Informations relatives au conducteur	1 Jhh**h**mm ▮hh**h**mm
Informations relatives au co-conducteur	2 Jhh**h**mm
Condition « hors champ » ouverte	OUT
Affichage d'avertissements	
Dépassement du temps de conduite continue	1 ⊙hh**h**mm ▮hh**h**mm
Événement ou anomalie	EF
Autres affichages	
Date UTC Heure	**UTC** ⊙ jj/mm/aaaa ou **UTC** ⊙ jj.mm.aaaa hh:mm
Temps de conduite continue et temps d'interruption **ac**cumulé du conducteur	1 ⊙hh**h**mm ▮hh**h**mm
Temps de conduite continue et temps d'interruption **ac**cumulé du co-conducteur	2 ⊙hh**h**mm ▮hh**h**mm
Temps de conduite **ac**cumulé du conducteur pour la semaine en cours et pour la semaine précédente	1 ⊙▮ hhh**h**mm
Temps de conduite **ac**cumulé du co-conducteur pour la semaine en cours et la semaine précédente	2 ⊙▮ hhh**h**mm

~~Appendice~~Sous-appendice 6

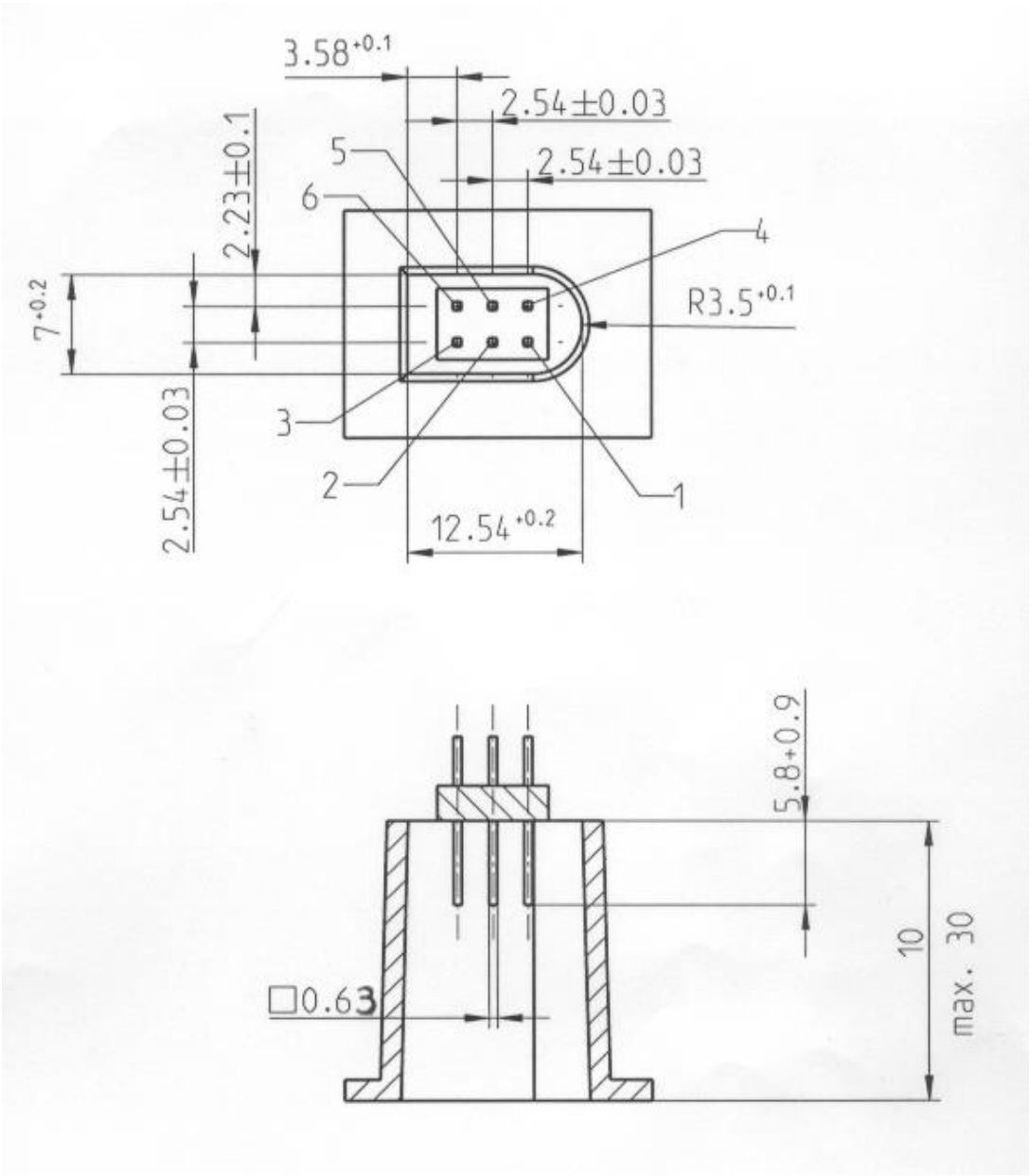
Connecteur frontal pour l'étalonnage et le téléchargement

Table des matières

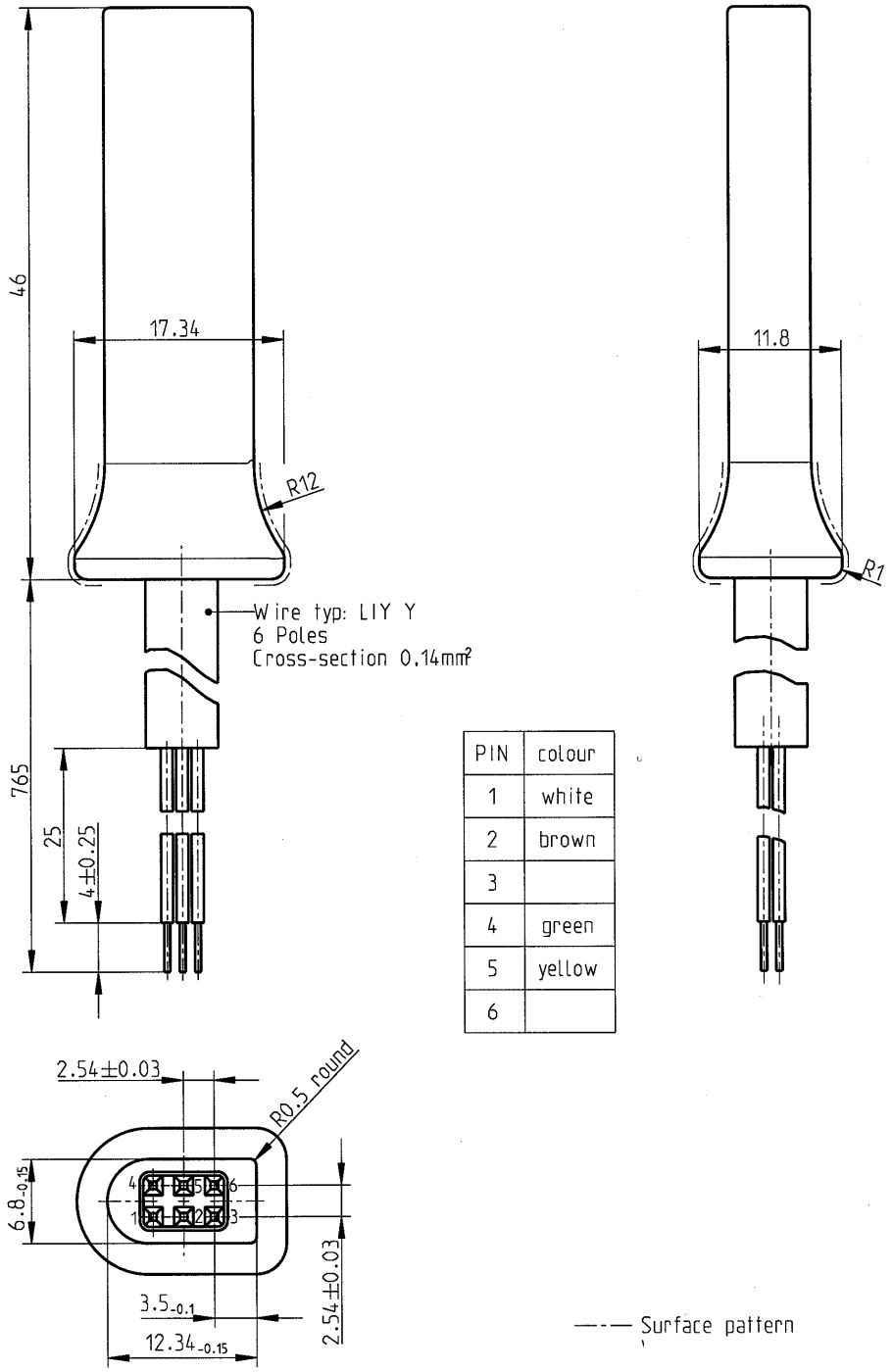
1. Matériel

1.1 Connecteur

INT_001 Le connecteur de téléchargement/d'étalonnage doit se présenter sous la forme d'un connecteur à 6 broches, accessible sur la face avant sans nécessiter la déconnexion d'aucun organe du tachygraphe. Il doit être conforme au schéma suivant (toutes les cotes sont en millimètres) :



Le schéma suivant illustre une fiche d'accouplement à 6 broches classique :



PIN	colour
1	white
2	brown
3	
4	green
5	yellow
6	

1.2 Affectation des contacts

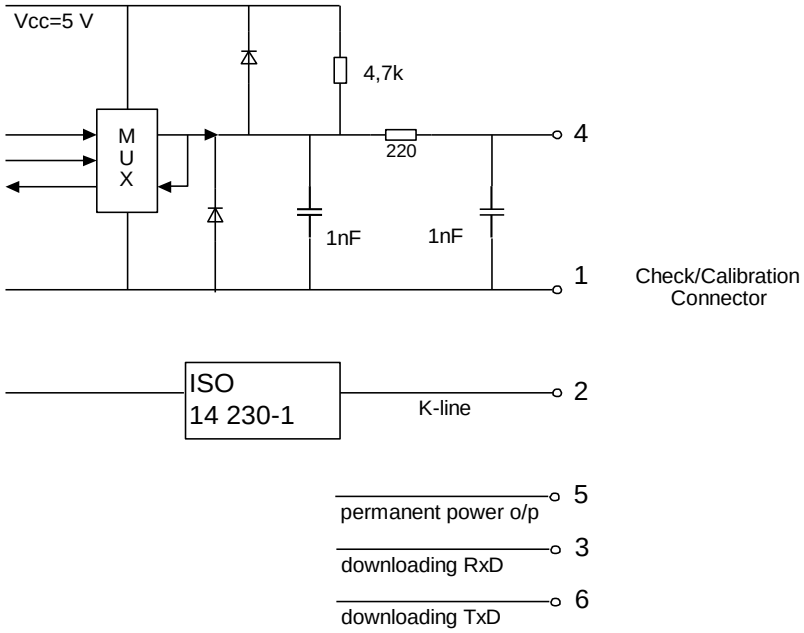
INT_002 L'affectation des contacts doit être conforme au tableau suivant :

Broche	*Description*	*Remarque*
1	Pôle négatif de la batterie	Raccordé à la borne négative de la batterie montée sur le véhicule
2	Communication de données	Ligne K (ISO 14230-1)

Broche	*Description*	*Remarque*
3	RxD − Téléchargement	Entrée de données dans le tachygraphe
4	Signal d'entrée/sortie	Étalonnage
5	Puissance de sortie permanente	La plage de tension doit être identique à celle de l'alimentation électrique du véhicule diminuée de 3 V pour tenir compte de la chute de tension dans les circuits de protection
		Sortie 40 mA
6	TxD − Téléchargement	Extraction de données du tachygraphe

1.3 Schéma fonctionnel

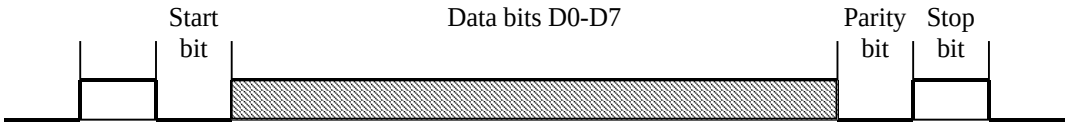
INT_003 Le schéma fonctionnel doit être conforme aux spécifications suivantes :



2. Interface de téléchargement

INT_004 L'interface de téléchargement doit être conforme aux spécifications de la norme RS232.

INT_005 L'interface de téléchargement doit utiliser un bit de départ, huit bits d'information (bit le moins significatif en tête), un bit de parité pair et un bit d'arrêt.



Agencement d'un octet de données

Bit de départ : un bit de niveau logique 0 ;

Bits d'information : transmis avec le bit le moins significatif en tête ;

Bit de parité : parité paire ;

Bit d'arrêt : un bit de niveau logique 1.

En cas de transmission de données numériques composées de plus d'un octet, l'octet le plus significatif est transmis en premier, l'octet le moins significatif en dernier.

INT_006 Les débits de transmission en bauds doivent être réglables dans une plage comprise entre 9 600 et 115 200 bits par seconde. Toute transmission doit s'opérer à la vitesse de transmission la plus élevée possible, le débit initial immédiatement après le début d'une communication étant fixé à 9 600 bits par seconde.

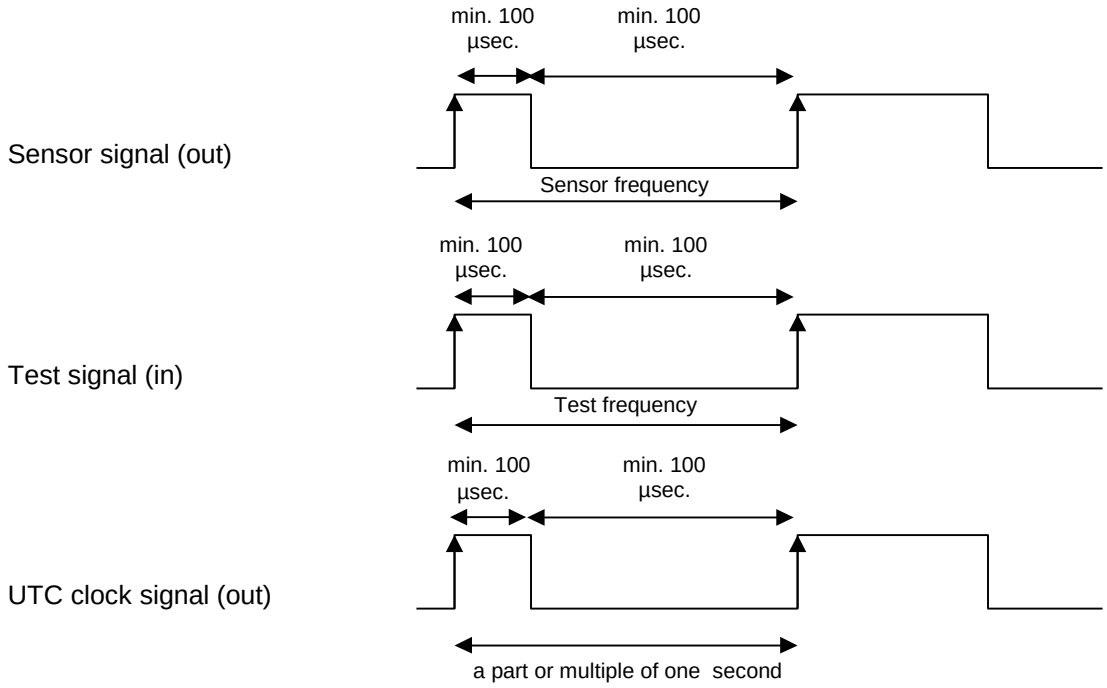
3. Interface d'étalonnage

INT_007 La communication de données doit être conforme aux spécifications de la norme ISO 14230-1 Véhicules routiers − Systèmes de diagnostic − Protocole « Keyword 2000 » − Partie 1 : couche physique, première édition : 1999.

INT_008 Le signal d'entrée/sortie doit être conforme aux spécifications électriques suivantes :

Paramètre	Minimum	Valeur usuelle	Maximum	Remarque
U_{low} (entrée)			1,0 V	I = 750 µA
U_{high} (entrée)	4 V			I = 200 µA
Fréquence			4 kHz	
U_{low} (sortie)			1,0 V	I = 1 mA
U_{high} (sortie)	4 V			I = 1 mA

INT_009 Le signal d'entrée/sortie doit être conforme aux chronogrammes suivants :



~~Appendice~~Sous-appendice 7

Protocoles de téléchargement de données

Table des matières

1. Introduction

Le présent **sous-**appendice traite des procédures qu'il convient d'appliquer pour exécuter les différents types de téléchargement de données vers un support de mémoire externe (SME). Il traite également des protocoles qu'il y a lieu de mettre en œuvre pour assurer un transfert de données correct et garantir la parfaite compatibilité des données téléchargées afin de permettre à tout contrôleur d'inspecter ces données et de vérifier leur authenticité et leur intégrité avant de procéder à leur analyse.

1.1 Champ d'application

Il est possible de télécharger des données vers un support de mémoire externe :

- À partir d'une unité embarquée sur le véhicule (UEV) par l'intermédiaire d'un équipement spécialisé intelligent (ESI) raccordé à celle-ci ;
- À partir d'une carte tachygraphique par l'intermédiaire d'un ESI équipé d'un dispositif de lecture de carte (PIF) ;
- À partir d'une carte tachygraphique par l'intermédiaire d'une unité embarquée sur le véhicule et d'un ESI raccordé à celle-ci.

Afin de permettre la vérification de l'authenticité et de l'intégrité des données téléchargées et sauvegardées sur un SME, ces données s'accompagnent d'une signature conformément ~~à l'appendice~~**au sous-appendice** 11 (Mécanismes de sécurité communs). L'identification de l'équipement source (UEV ou carte) et ses certificats de sécurité (~~État membre~~**Partie contractante** et équipement) sont également téléchargés. Le vérificateur doit être en possession d'une clé publique ~~européenne~~ **racine** sécurisée.

Les données téléchargées à partir d'une UEV sont signées conformément aux dispositions du sous-appendice 11 (Mécanismes de sécurité communs), partie B (Tachygraphe de deuxième génération), sauf lorsque le contrôle du conducteur est effectué par une autorité de contrôle non rattachée à l'UE à l'aide d'une carte de contrôleur de première génération. Dans ce cas, les données sont signées conformément aux dispositions du sous-appendice 11 (Mécanismes de sécurité communs), partie A (Tachygraphe de première génération), comme prévu à l'exigence MIG_015 du sous-appendice 15 (Migration).

Le présent sous-appendice prévoit donc deux types de téléchargement de données à partir de l'UEV :

- **Le téléchargement de données à partir d'une UEV de génération 2, qui fournit la structure de données de génération 2 accompagnée d'une signature conforme aux dispositions du sous-appendice 11 (Mécanismes de sécurité communs), partie B ;**
- **Le téléchargement de données à partir d'une UEV de génération 1, qui fournit la structure de données de génération 1 accompagnée d'une signature conforme aux dispositions du sous-appendice 11 (Mécanismes de sécurité communs), partie A.**

De même, il existe deux types de téléchargement de données à partir des cartes de conducteur de deuxième génération insérées dans les lecteurs d'une UEV, comme spécifié aux paragraphes 3 et 4 du présent sous-appendice.

DDP_001 Les données téléchargées au cours d'une session de téléchargement doivent être stockées dans un seul et même fichier dans le SME.

1.2 Abréviations et notations

Dans le présent **sous-**appendice, les abréviations suivantes sont utilisées :

AID Identificateur d'application (*Application Identifier*)

ATR	Réponse à une réinitialisation (*Answer To Reset*)
CS	Octet de total de contrôle (*Checksum byte*)
DF	Fichier spécialisé (*Dedicated File*)
SD_	Session de diagnostic
EF	Fichier élémentaire (*Elementary File*)
SME	Support de mémoire externe
FID	Identificateur de fichier (*File Identifier*)
FMT	Octet de structure (premier octet de l'en-tête d'un message) *(Format Byte)*
ICC	Carte à circuit intégré *(Integrated Circuit Card)*
ESI	Équipement spécialisé intelligent : équipement servant à télécharger des données vers le SME (par exemple, un PC)
PIF	Périphérique d'interface
KWP	Protocole « Keyword 2000 » (*Keyword Protocol 2000*)
LEN	Octet de longueur (dernier octet de l'en-tête d'un message) (*Length Byte*)
PPS	Sélection des paramètres de protocole (*Protocol Parameter Selection*)
PSO	Exécution d'une opération de sécurité (*Perform Security Operation*)
SID	Identificateur de service (*Service Identifier*)
SRC	Octet source (*Source byte*)
TGT	Octet cible (*Target byte*)
TLV	Structure balise-longueur-valeur (*Tag Length Value*)
PRT	Paramètre de réponse de transfert
PDT	Paramètre de demande de transfert
UEV	Unité embarquée sur le véhicule *(VU, en anglais)*

2. Téléchargement de données à partir de l'UEV

2.1 Procédure de téléchargement

Pour procéder au téléchargement de données à partir de l'UEV, l'opérateur doit exécuter les opérations suivantes :

- Introduire sa carte de tachygraphe dans la fente de l'un des lecteurs de carte de l'UEV (*) ;
- Raccorder l'ESI au connecteur de téléchargement de l'UEV ;
- Établir la liaison entre l'ESI et l'UEV ;
- Sélectionner sur l'ESI les données à télécharger et envoyer la requête à l'UEV ;
- Clôturer la session de téléchargement.

(*) L'insertion de la carte déclenche l'activation des droits d'accès appropriés tant aux données qu'à la fonction de téléchargement. Il est toutefois possible de télécharger des données à partir d'une carte de conducteur insérée dans l'un des lecteurs de l'UEV lorsqu'aucun autre type de carte n'est inséré dans l'autre lecteur.

2.2 Protocole de téléchargement des données

La structure du protocole repose sur une relation maître-esclave, l'ESI jouant le rôle du maître et l'UEV celui de l'unité asservie.

La structure des messages, leur type et leur acheminement sont essentiellement basés sur le protocole « Keyword 2000 » (ISO 14230-2 Véhicules routiers − Systèmes de diagnostic − Protocole « Keyword 2000 » − Partie 2 : couche de liaison de données).

La couche application est principalement basée sur le projet actuel de norme ISO 14229-1 (Véhicules routiers − Systèmes de diagnostic − Partie 1 : services de diagnostic, version 6 du 22 février 2001).

2.2.1 Structure des messages

DDP_002 Tous les messages échangés entre l'ESI et l'UEV se caractérisent par une structure à trois éléments :

- Un en-tête composé d'un octet de structure (FMT), d'un octet cible (TGT), d'un octet source (SRC) et, le cas échéant, d'un octet de longueur (LEN) ;
- Une zone de données composée d'un octet identificateur de service (SID) et d'un nombre variable d'octets de données qui peuvent comprendre un octet optionnel de session de diagnostic (SD_) ou un octet optionnel de paramètre de transfert (PDT ou PRT) ;
- Un total de contrôle composé d'un octet de total de contrôle (CS).

En-tête				Zone de données					Total de contrôle
FMT	TGT	SRC	LEN	SID	DONNÉES	……	…..	…..	CS
4 octets				255 octets max.					1 octet

Les octets TGT et SRC représentent les adresses physiques du destinataire et de l'expéditeur du message. Ils prennent les valeurs Hex F0 pour l'ESI et Hex EE pour l'UEV.

L'octet LEN indique la longueur de la zone de données.

L'octet de total de contrôle correspond à une série de sommes de 8 bits modulo 256 représentant tous les octets du message à l'exclusion du CS lui-même.

Les octets FMT, SID, SD_, PDT et PRT font l'objet d'une description plus loin dans ce document.

DDP_003 Si la longueur des données que le message est censé véhiculer est supérieure à l'espace disponible dans la partie zone de données, l'envoi de ce message prend la forme de plusieurs sous-messages. Chacun de ces sous-messages comporte un en-tête, les mêmes SID et PRT ainsi qu'un compteur de sous-messages de 2 octets indiquant le numéro d'ordre de chaque sous-message au sein du message global. Afin de permettre la détection d'erreurs et l'abandon éventuel d'un échange de données, l'ESI accuse réception de chaque sous-message. L'ESI peut accepter le sous-message, en demander la réémission et demander à l'UEV d'en reprendre ou d'en abandonner la transmission.

DDP_004 Si la zone de données du dernier sous-message contient exactement 255 octets, il est indispensable d'adjoindre à l'ensemble un sous-message final comportant une zone de données vide (à l'exception des octets SID et PRT ainsi que du compteur de sous-messages) pour indiquer la fin du message.

Exemple :

En-tête	SID	PRT	Message	CS
4 octets	Longueur supérieure à 255 octets			

Transmis sous la forme suivante :

En-tête	SID	PRT	00	01	Sous-message 1	CS
4 octets	255 octets					

En-tête	SID	PRT	00	02	Sous-message 2	CS
4 octets	255 octets					

…

En-tête	SID	PRT	xx	yy	Sous-message n	CS
4 octets	Longueur inférieure à 255 octets					

Ou sous la forme :

En-tête	SID	PRT	00	01	Sous-message 1	CS
4 octets	255 octets					

En-tête	SID	PRT	00	02	Sous-message 2	CS
4 octets	255 octets					

…

En-tête	SID	PRT	xx	yy	Sous-message n	CS
4 octets	255 octets					

En-tête	SID	PRT	xx	yy+1	CS
4 octets	4 octets				

2.2.2 Types de message

Le protocole de communication qui s'applique au téléchargement de données entre l'UEV et l'ESI requiert l'échange de 8 types de messages distincts.

La table ci-dessous en présente une synthèse.

Structure du message	En-tête 4 octets max.				Données 255 octets max.			Total de contrôle 1 octet
ESI -> **<- UEV**	FMT	TGT	SRC	LEN	SID	SD_ / PDT	DONNÉES	**CS**
Demande d'établissement de la communication	81	EE	F0		81			E0
Réponse positive à une demande d'établissement de la communication	80	F0	EE	03	C1		EA, 8F	9B
Demande d'ouverture d'une session de diagnostic	80	EE	F0	02	10	81		F1
Réponse positive à une demande d'ouverture de session de diagnostic	80	F0	EE	02	50	81		31
Service de contrôle de liaison								
Vérification du débit en bauds (étape 1)								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	EE
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Réponse positive à une demande de vérification du débit en bauds	80	F0	EE	02	C7		01	28
Débit de transition en bauds (étape 2)	80	EE	F0	03	87		02,03	ED
Demande de téléchargement (upload)	80	EE	F0	0A	35		00,00,00,00, 00,FF,FF, FF,FF	99
Réponse positive à une demande de téléchargement	80	F0	EE	03	75		00,FF	D5
Demande de transfert de données								
Récapitulatif	80	EE	F0	02	36	01		97
Activités	80	EE	F0	06	36	02	Date	**CS**
Événements et anomalies	80	EE	F0	02	36	03		99
Vitesse instantanée	80	EE	F0	02	36	04		9A
Données techniques	80	EE	F0	02	36	05		9B
Téléchargement (download) d'une carte	80	EE	F0	02	36	06	Lecteur	**CS**
Réponse positive à une demande de transfert de données	80	F0	EE	Len	76	**PRT**	Données	**CS**
Demande de fin de transfert	80	EE	F0	01	37			96
Réponse positive à une demande de fin de transfert	80	F0	EE	01	77			D6
Demande d'arrêt de la communication	80	EE	F0	01	82			E1
Réponse positive à une demande d'arrêt de la communication	80	F0	EE	01	C2			21
Accusé de réception d'un sous-message	80	EE	F0	Len	83		Données	**CS**
Réponses négatives								
Téléchargement (général) refusé	80	F0	EE	03	7F	SID dem	10	**CS**
Service incompatible	80	F0	EE	03	7F	SID dem	11	**CS**
Sous-fonction incompatible	80	F0	EE	03	7F	SID dem	12	**CS**
Longueur du message incorrecte	80	F0	EE	03	7F	SID dem	13	**CS**
Conditions non correctes ou erreur affectant la séquence d'interrogation	80	F0	EE	03	7F	SID dem	22	**CS**
Demande excessive	80	F0	EE	03	7F	SID dem	31	**CS**
Téléchargement (upload) refusé	80	F0	EE	03	7F	SID dem	50	**CS**
Réponse en suspens	80	F0	EE	03	7F	SID dem	78	**CS**
Données indisponibles	80	F0	EE	03	7F	SID dem	FA	**CS**

Structure du message	En-tête 4 octets max.				Données 255 octets max.			Total de contrôle 1 octet
ESI -> <- UEV	FMT	TGT	SRC	LEN	SID	SD_/PDT	DONNÉES	CS
Demande d'établissement de la communication	81	EE	F0		81			E0
Réponse positive à une demande d'établissement de la communication	80	F0	EE	03	C1		EA, 8F	9B
Demande d'ouverture d'une session de diagnostic	80	EE	F0	02	10	81		F1
Réponse positive à une demande d'ouverture de session de diagnostic	80	F0	EE	02	50	81		31
Service de contrôle de liaison								
Vérification du débit en bauds (étape 1)								
9 600 Bd	80	EE	F0	04	87	01	01,01	EC
19 200 Bd	80	EE	F0	04	87	01	01,02	ED
38 400 Bd	80	EE	F0	04	87	01	01,03	EE
57 600 Bd	80	EE	F0	04	87	01	01,04	EF
115 200 Bd	80	EE	F0	04	87	01	01,05	F0
Réponse positive à une demande de vérification du débit en bauds	80	F0	EE	02	C7	01		28
Débit de transition en bauds (étape 2)	80	EE	F0	03	87	02	03	ED
Demande de téléchargement (upload)	80	EE	F0	0A	35		00,00,00,00, 00,FF,FF, FF,FF	99
Réponse positive à une demande de téléchargement (upload)	80	F0	EE	03	75		00,FF	D5
Demande de transfert de données								
Version de l'interface de téléchargement	80	EE	F0	02	36	00		96
Récapitulatif	80	EE	F0	02	36	01, 21 ou 31		CS
Activités	80	EE	F0	06	36	02, 22 ou 32	Date	CS
Événements et anomalies	80	EE	F0	02	36	03, 23 ou 33		CS
Vitesse instantanée	80	EE	F0	02	36	04 ou 24		CS
Données techniques	80	EE	F0	02	36	05, 25 ou 35		CS
Téléchargement (download) d'une carte	80	EE	F0	02 ou 03	36	06	Lecteur	CS
Réponse positive à une demande de transfert de données	80	F0	EE	Len	76	PRT	Données	CS
Demande de fin de transfert	80	EE	F0	01	37			96
Réponse positive à une demande de fin de transfert	80	F0	EE	01	77			D6
Demande d'arrêt de la communication	80	EE	F0	01	82			E1
Réponse positive à une demande d'arrêt de la communication	80	F0	EE	01	C2			21
Accusé de réception d'un sous-message	80	EE	F0	Len	83		Données	CS
Réponses négatives								
Téléchargement (général) refusé	80	F0	EE	03	7F	SID dem	10	CS
Service non pris en charge	80	F0	EE	03	7F	SID dem	11	CS
Sous-fonction non prise en charge	80	F0	EE	03	7F	SID dem	12	CS
Longueur du message incorrecte	80	F0	EE	03	7F	SID dem	13	CS
Conditions non correctes ou erreur affectant la séquence d'interrogation	80	F0	EE	03	7F	SID Dem	22	CS
Demande excessive	80	F0	EE	03	7F	SID dem	31	CS
Téléchargement (upload) refusé	80	F0	EE	03	7F	SID dem	50	CS
Réponse en attente	80	F0	EE	03	7F	SID dem	78	CS
Données indisponibles	80	F0	EE	03	7F	SID dem	FA	CS

Remarques :

- SID dem = le SID de la demande correspondante.
- PRT = le PDT de la demande correspondante.
- La présence de cellules noires indique une absence de transmission.
- L'utilisation du terme « upload » (considéré à partir de l'ESI) s'impose pour garantir la compatibilité du système avec la norme ISO 14229. Ce terme possède la même signification que « download » (considéré à partir de l'UEV).
- Cette table ne présente pas de compteur possible de sous-messages de 2 octets.
- Le lecteur désigne le numéro de lecteur, soit « 1 » (carte insérée dans le lecteur réservé au conducteur) soit « 2 » (carte insérée dans le lecteur réservé au co-conducteur).
- Si le lecteur n'est pas précisé, l'UEV sélectionne le lecteur 1 s'il contient une carte et le lecteur 2 uniquement si l'utilisateur le sélectionne.
- **Le PDT 24 est utilisé pour les demandes de téléchargement de données à partir d'une UEV de génération 2, versions 1 et 2.**
- **Les PDT 00, 31, 32, 33 et 35 sont utilisés pour les demandes de téléchargement de données à partir d'une UEV de génération 2, version 2.**
- **Les PDT 21, 22, 23 et 25 sont utilisés pour les demandes de téléchargement de données à partir d'une UEV de génération 2, version 1.**
- **Les PDT 01 à 05 sont utilisés pour les demandes de téléchargement de données à partir d'une UEV de génération 2. Ils peuvent éventuellement être acceptés par une UEV de génération 2, mais uniquement dans le cadre du contrôle des conducteurs effectué par une autorité de contrôle non rattachée à l'UE, à l'aide d'une carte de contrôleur de première génération.**
- **Les PDT 11 à 1F sont réservés aux demandes de téléchargement propres au fabricant.**
- ~~**Les PDT 21 à 25 sont utilisés pour les demandes de téléchargement de données à partir d'une UEV de génération 2 ; les PDT 01 à 05 sont utilisés pour les demandes de téléchargement de données à partir d'une UEV de génération 1, qui ne peuvent être acceptées par une UEV que dans le cadre de contrôles de conducteur effectués par une autorité de contrôle non rattachée à l'UE à l'aide d'une carte de contrôleur de première génération.**~~
- ~~**Les PDT 11 à 19 et 31 à 39 sont réservés aux demandes de téléchargement propres au fabricant.**~~

2.2.2.1 Demande d'établissement de la communication (SID 81)

DDP_005 Ce message est émis par l'ESI pour établir la liaison avec l'UEV. Les communications initiales sont toujours effectuées à 9 600 bauds (jusqu'à ce que ce débit soit modifié au moyen des services de contrôle de liaison appropriés).

2.2.2.2 Réponse positive à une demande d'établissement de la communication (SID C1)

DDP_006 L'UEV émet ce message pour répondre positivement à une demande d'établissement de la communication. Ce message comporte les deux octets clés 'EA' '8F' indiquant que l'unité correspondante prend en charge le protocole concerné, l'en-tête de chaque message incluant les octets cible, source et longueur.

2.2.2.3 Demande d'ouverture d'une session de diagnostic (SID 10)

DDP_007 L'ESI émet un message de demande d'ouverture d'une session de diagnostic afin de solliciter une nouvelle session de diagnostic avec

l'UEV. La sous-fonction « session par défaut » (Hex 81) indique qu'une session de diagnostic standard va être ouverte.

2.2.2.4 Réponse positive à une demande d'ouverture de session de diagnostic (SID 50)

DDP_008 L'UEV émet un message de réponse positive à une demande de diagnostic pour répondre positivement à une demande d'ouverture d'une session de diagnostic.

2.2.2.5 Service de contrôle de liaison (SID 87)

DDP_052 Le service de contrôle de liaison est utilisé par l'ESI pour initier une modification du débit en bauds. Cette opération comporte deux étapes. Dans la première étape, l'ESI propose une modification du débit en bauds, en indiquant le nouveau débit. À la réception d'un message positif de l'UEV, l'ESI envoie la confirmation du changement du débit en bauds à l'UEV (deuxième étape). L'ESI passe alors au nouveau débit en bauds. Après réception de la confirmation, l'UEV passe au nouveau débit en bauds.

2.2.2.6 Réponse positive au contrôle de liaison (SID C7)

DDP_053 La réponse positive au contrôle de liaison est délivrée par l'UEV sur demande de service de contrôle de liaison (première étape). Il convient de noter qu'aucune réponse n'est donnée à la demande de confirmation (deuxième étape).

2.2.2.7 Demande de téléchargement (upload) (SID 35)

DDP_009 L'ESI émet un message de demande de téléchargement pour indiquer à l'UEV qu'une opération de téléchargement est requise. Afin de satisfaire aux exigences de la norme **ISO 14229**, des données sont incluses concernant l'adresse, la taille et les caractéristiques du format des données demandées. Ces informations n'étant pas connues de l'ESI avant le téléchargement, l'adresse de la mémoire est mise à 0, le format est non chiffré et non compressé et la taille de la mémoire est mise au maximum.

2.2.2.8 Réponse positive à une demande de téléchargement (upload) (SID 75)

DDP_010 L'UEV émet un message de réponse positive à une demande de téléchargement pour signifier à l'ESI que l'UEV est prête à télécharger des données. Afin de satisfaire aux exigences de la norme ISO 14229, le message de réponse positive comprend des données indiquant à l'ESI que les messages ultérieurs de réponse positive à une demande de transfert de données comporteront au maximum des octets Hex '00FF'.

2.2.2.9 Demande de transfert de données (SID 36)

DDP_011 L'ESI émet une demande de transfert de données afin de préciser à l'UEV la nature des données à télécharger. Un paramètre de demande de transfert (PDT) d'un octet indique de quel type de transfert il s'agit.

Il existe ~~six~~ **sept** types de transfert de données. **Pour les téléchargements de données à partir de l'UEV, deux valeurs PDT différentes peuvent être utilisées pour chaque type de transfert.**

Type de transfert de données	**Valeur PDT pour le téléchargement de données à partir d'une UEV de génération 1**	**Valeur PDT pour le téléchargement de données à partir d'une UEV de génération 2 version 1**	**Valeur PDT pour le téléchargement de données à partir d'une UEV de génération 2 version 2**
Version de l'interface de téléchargement	**Sans objet**	**Sans objet**	**00**
Récapitulatif	01	21	**31**
Activités associées à une date précise	02	22	**32**
Événements et anomalies	03	23	**33**
Vitesse instantanée	04	24	**24**
Données	05	25	**35**

Type de transfert de données	**Valeur PDT**
Téléchargement de carte	06

DDP_054 Il est obligatoire pour l'ESI de demander un transfert de données de type « récapitulatif » (PDT 01**, 21** ou ~~2~~**3**1) au cours d'une session de téléchargement, car cela seul garantit que les certificats de l'UEV sont enregistrés sur le fichier téléchargé (et permet la vérification de la signature numérique).

Dans le ~~deuxième~~ **troisième** cas de figure (PDT 02**, 22 ou ~~2~~32**), le message de demande de transfert de données comporte l'indication du jour civil (format `TimeReal`) auquel le téléchargement est associé.

2.2.2.10 Réponse positive à une demande de transfert de données (SID 76)

DDP_012 L'UEV émet un message de réponse positive à une demande de transfert de données en réponse à une demande de cette nature. Ce message contient les données requises ainsi qu'un paramètre de réponse à une demande de transfert (PRT) correspondant au PDT de la demande.

DDP_055 Dans le premier cas (PRT 01, **21** ou ~~2~~**3**1), l'UEV enverra des données destinées à aider l'opérateur de l'ESI dans le choix des données qu'il souhaite télécharger. Les informations contenues dans ce message sont les suivantes :

- Certificats de sécurité ;
- Identification du véhicule ;
- Date et heure actuelles de l'UEV ;
- Date la plus ancienne et date la plus récente pour lesquelles le téléchargement est possible (données de l'UEV) ;
- Indications concernant la présence de cartes dans les lecteurs de l'UEV ;
- Téléchargements antérieurs vers une entreprise ;
- Verrouillages d'entreprise ;
- Contrôles précédents.

2.2.2.11 Demande de fin de transfert (SID 37)

DDP_013 L'ESI émet un message de demande de fin de transfert pour informer l'UEV que la session de téléchargement est terminée.

2.2.2.12 Réponse positive à une demande de fin de transfert (SID 77)

DDP_014 L'UEV émet un message de réponse positive à une demande de fin de transfert pour accuser réception de la demande de fin de transfert.

2.2.2.13 Demande d'arrêt de la communication (SID 82)

DDP_015 L'ESI émet un message de demande d'arrêt de la communication pour interrompre la liaison avec l'UEV.

2.2.2.14 Réponse positive à une demande d'arrêt de la communication (SID C2)

DDP_016 L'UEV émet un message de réponse positive à une demande d'arrêt de la communication pour accuser réception de la demande d'arrêt de la communication.

2.2.2.15 Accusé de réception d'un sous-message (SID 83)

DDP_017 L'ESI émet un accusé de réception pour confirmer la réception des différentes parties d'un message transmis sous forme de sous-messages. La zone de données contient le SID transmis par l'UEV ainsi qu'un code de 2 octets qui s'énonce comme suit :

- MsgC + 1 accuse la réception correcte du sous-message numéro MsgC.

Demande d'envoi du sous-message suivant adressée à l'UEV par l'ESI.

- MsgC indique un problème affectant la réception du sous-message numéro MsgC.

Demande de renvoi du sous-message concerné adressée à l'UEV par l'ESI.

- FFFF demande l'interruption du message en cours de transmission.

L'ESI peut recourir à ce code pour mettre un terme à la transmission du message envoyé par l'UEV, et ce, quelle qu'en soit la raison.

Le système permet d'accuser (ou non) réception du dernier sous-message d'un message (octet LEN < 255) en recourant à l'un quelconque de ces codes.

Composée de plusieurs sous-messages, la réponse de l'UEV s'énonce comme suit :

- Réponse positive à une demande de transfert de données (SID 76).

2.2.2.16 Réponses négatives (SID 7F)

DDP_018 L'UEV émet un message de réponse négative en réponse aux messages ci-dessus si elle ne peut pas satisfaire à la demande transmise. Les zones de données du message contiennent le SID de la réponse (7F), le SID de la demande et un code précisant le motif de la réponse négative. Les codes suivants sont d'application :

- 10 téléchargement (général) refusé

L'opération ne peut être exécutée pour une raison qui n'est pas abordée ci-après.

- 11 service non pris en charge

Le SID de la demande n'est pas reconnu par l'UEV.

- 12 sous-fonction non prise en charge

Le SD_ ou le PDT de la demande ne sont pas reconnus par l'UEV ou la transmission des sous-messages est arrivée à son terme.

- 13 longueur du message incorrecte

La longueur du message reçu est incorrecte.

- 22 conditions non correctes ou erreur affectant la séquence de la demande

Le service demandé n'est pas disponible ou la séquence des messages de demande est incorrecte.

- 31 demande excessive

L'enregistrement (zone de données) du paramètre de la demande n'est pas valable.

- 50 téléchargement (upload) refusé

La demande ne peut être exécutée (l'UEV est exploitée dans un mode inapproprié ou elle présente une anomalie interne).

- 78 réponse en attente

L'action demandée ne peut être achevée dans le temps imparti et l'UEV n'est pas prête à accepter une autre demande.

- FA données indisponibles

L'objet d'une demande de transfert de données n'est pas accessible au sein de l'UEV (par exemple, si aucune carte n'est insérée ou si un **téléchargement de données à partir d'une UEV de génération 1 est demandé hors du cadre d'un contrôle de conducteur effectué par une autorité de contrôle non rattachée à l'UE** etc.).

2.2.3 Acheminement des messages

Dans le cadre d'une procédure de téléchargement normale, l'acheminement des messages s'effectue habituellement comme suit :

ESI		**UEV**
Demande d'établissement de la communication	⇨	
	⇦	Réponse positive
Demande d'ouverture d'une session de diagnostic	⇨	
	⇦	Réponse positive
Demande de téléchargement (upload)	⇨	
	⇦	Réponse positive
Demande de récapitulatif de transfert de données	⇨	
	⇦	Réponse positive
Demande de transfert de données #2	⇨	
	⇦	Réponse positive #1
Accusé de réception d'un sous-message #1	⇨	
	⇦	Réponse positive #2
Accusé de réception d'un sous-message #2	⇨	
	⇦	Réponse positive #m
Accusé de réception d'un sous-message #m	⇨	
	⇦	Réponse positive (zone de données <255 octets)
Accusé de réception d'un sous-message (facultatif)	⇨	
…		
Demande de transfert de données #n	⇨	
	⇦	Réponse positive

Demande de fin de transfert	⇨ ⇦	 Réponse positive
Demande d'arrêt de la communication	⇨ ⇦	 Réponse positive

2.2.4 Synchronisation

DDP_019 Dans des conditions d'exploitation normales, les paramètres de synchronisation illustrés dans la figure ci-après sont appliqués :

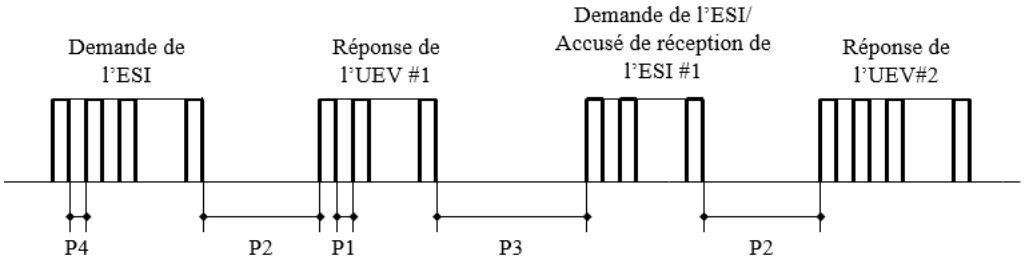


Figure 1 − Acheminement des messages, synchronisation

Où :

P1 = temps entre les octets d'une réponse de l'UEV.

P2 = temps entre la fin d'une demande de l'ESI et le début de la réponse de l'UEV ou entre la fin d'un accusé de réception de l'ESI et le début de la prochaine réponse de l'UEV.

P3 = temps entre la fin d'une réponse de l'UEV et le début d'une nouvelle demande de l'ESI, entre la fin d'une réponse de l'UEV et le début d'un accusé de réception de l'ESI ou entre la fin d'une demande de l'ESI et le début d'une nouvelle demande de l'ESI dans l'éventualité où l'UEV manquerait à répondre.

P4 = temps entre les octets d'une demande de l'ESI.

P5 = valeur étendue de P3 pour le téléchargement de carte.

Le tableau ci-après présente les valeurs que les paramètres de synchronisation sont susceptibles de prendre (jeu étendu de paramètres de synchronisation KWP, utilisés en cas d'adressage physique visant à accroître la vitesse des communications).

Paramètre de synchronisation	Limite inférieure (en ms)	Limite supérieure (en ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	**20 minutes**

(*) Si l'UEV émet une réponse négative contenant un code qui signifie « réception correcte de la demande, réponse en attente », cette valeur est portée à la même limite supérieure que celle de P3.

2.2.5 Traitement des erreurs

Si une erreur survient pendant l'échange de messages, le plan d'acheminement des messages est modifié en fonction de l'équipement qui a détecté l'erreur et du message à l'origine de celle-ci.

Les figures 2 et 3 illustrent les procédures de traitement des erreurs appliquées respectivement à l'UEV et à l'ESI.

2.2.5.1 Phase d'établissement de la communication

DDP_020 Si l'ESI détecte une erreur au cours de la phase d'établissement de la communication, tant au niveau de la synchronisation qu'au niveau du train de bits, il temporise alors pendant une période de P3min avant d'émettre à nouveau la même demande.

DDP_021 Si l'UEV détecte une erreur dans la séquence provenant de l'ESI, elle n'envoie aucune réponse et attend un autre message de demande d'établissement de la communication dans un délai de P3max.

2.2.5.2 Phase de communication

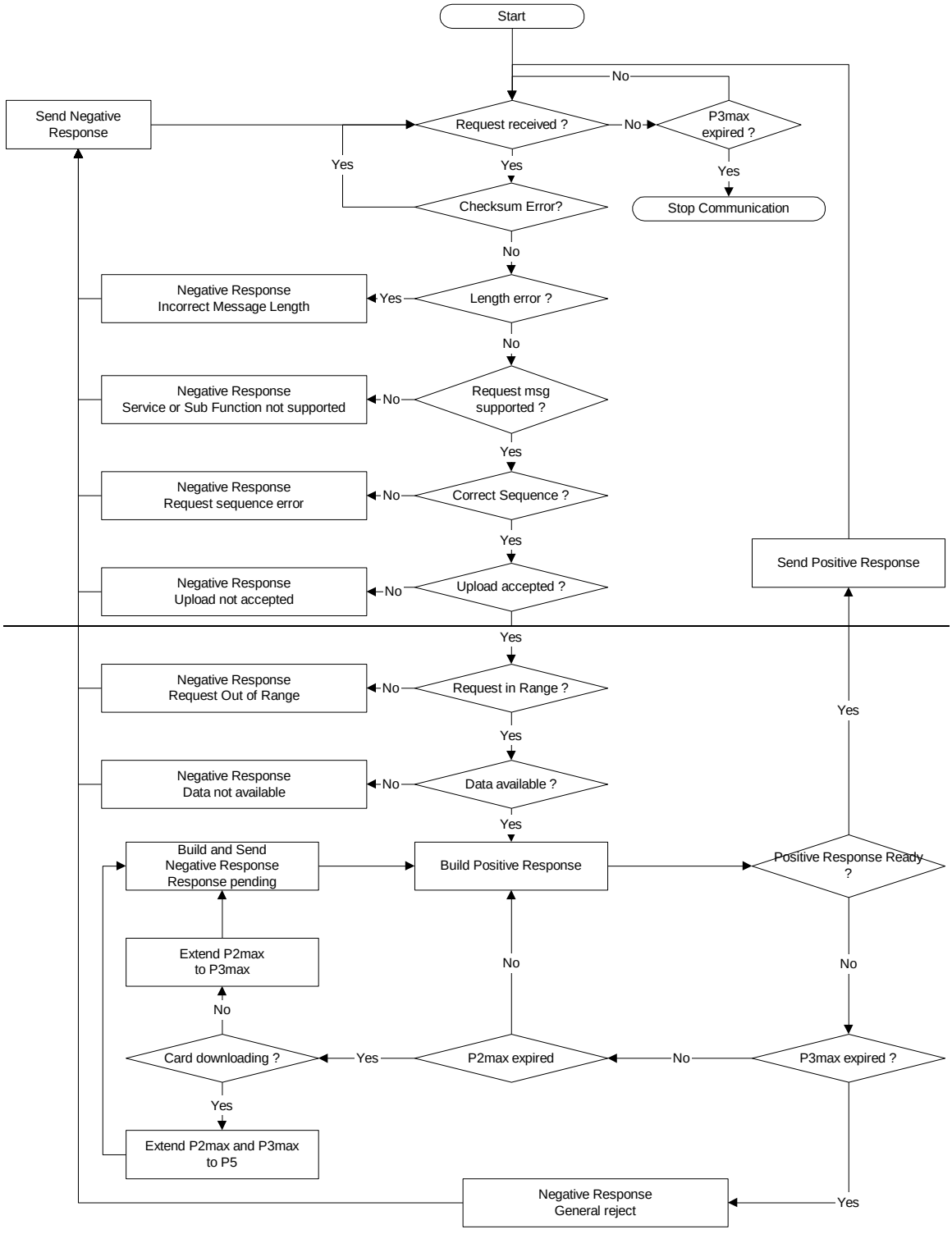
Deux procédures de traitement des erreurs distinctes peuvent être définies :

1. L'UEV détecte une erreur de transmission de l'ESI

DDP_022 L'UEV procède à l'analyse de chaque message reçu afin de déceler toute erreur de synchronisation, de structure des octets (par exemple, des violations affectant les bits de départ et d'arrêt) ou de trame (réception d'un nombre erroné d'octets ou octet de total de contrôle erroné).

DDP_023 Si l'UEV détecte l'une des erreurs susmentionnées, elle n'envoie aucune réponse et ne tient pas compte du message reçu.

DDP_024 L'UEV peut détecter d'autres erreurs dans la structure ou le contenu du message reçu (par exemple, un message incompatible), même si le message satisfait aux critères de longueur et de contrôle. Dans ce cas, l'UEV répond à l'ESI par un message de réponse négatif précisant la nature de l'erreur.


Start
No
Send Negative Response
Request received ?
No
P3max expired ?
Yes
Yes
Yes
Checksum Error?
Stop Communication
No
Negative Response Incorrect Message Length
Yes
Length error ?
No
Negative Response Service or Sub Function not supported
No
Request msg supported ?
Yes
Negative Response Request sequence error
No
Correct Sequence ?
Yes
Send Positive Response
Negative Response Upload not accepted
No
Upload accepted ?
Yes
Negative Response Request Out of Range
No
Request in Range ?
Yes
Yes
Negative Response Data not available
No
Data available ?
Yes
Build and Send Negative Response Response pending
Build Positive Response
Positive Response Ready ?
Extend P2max to P3max
No
No
No
Card downloading ?
Yes
P2max expired
No
P3max expired ?
Yes
Extend P2max and P3max to P5
Negative Response General reject
Yes

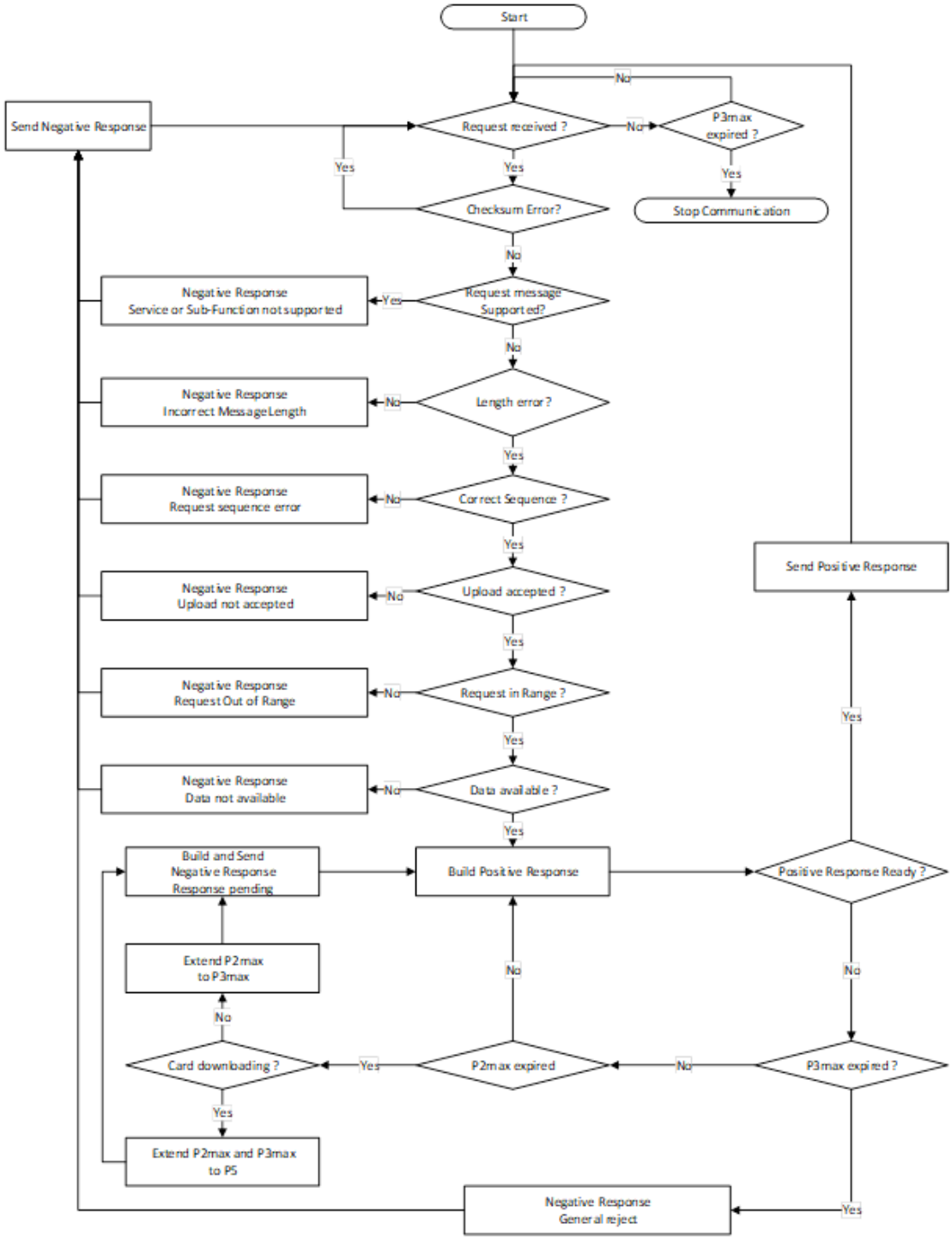


Figure 2 − Traitement des erreurs au niveau de l'UEV

2. L'ESI détecte une erreur de transmission de l'UEV

DDP_025 L'ESI procède à l'analyse de chaque message reçu afin de déceler toute erreur de synchronisation, de structure des octets (par exemple, des violations affectant les bits de départ et d'arrêt) ou de trame (réception d'un nombre erroné d'octets ou octet de total de contrôle erroné).

DDP_026 L'ESI détecte les erreurs de séquence telles que l'incrémentation incorrecte du compteur de sous-messages que comportent les messages successifs reçus.

DDP_027 Si l'ESI détecte une erreur ou si l'UEV ne lui envoie aucune réponse dans un délai de P2max, le message de demande concerné sera renvoyé à trois reprises au maximum à l'unité destinataire. Aux fins de cette détection d'erreurs, tout accusé de réception d'un sous-message sera considéré comme une demande adressée à l'UEV.

DDP_028 L'ESI doit temporiser pendant un laps de temps de P3min avant d'entreprendre toute transmission ; le délai de temporisation se mesure à partir de la dernière occurrence d'un bit d'arrêt relevée après la détection de l'erreur.

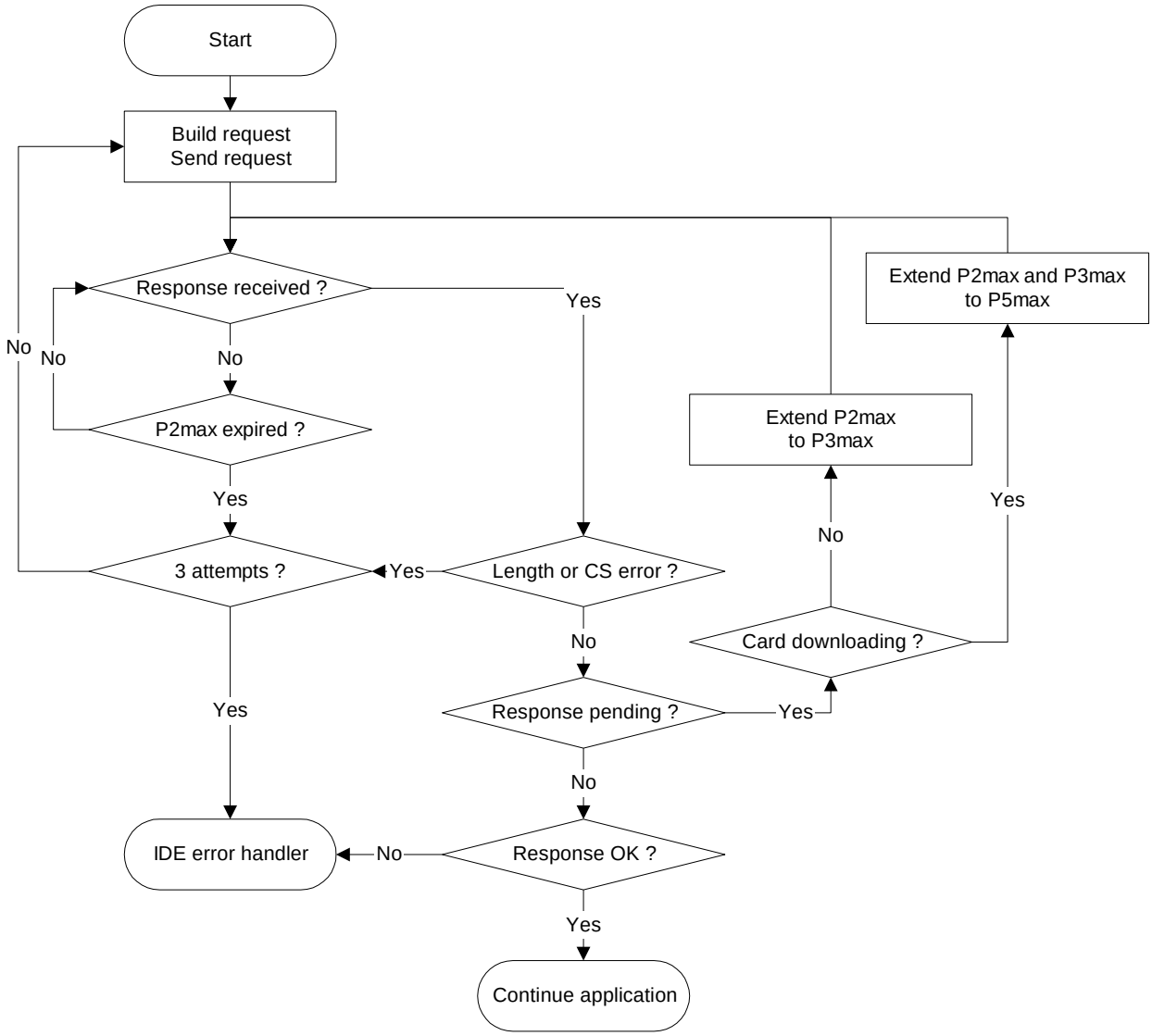


Figure 3 − Traitement des erreurs au niveau de l'ESI

2.2.6 Contenu des messages de réponse

Ce paragraphe précise le contenu des zones de données des différents messages de réponse positive.

Les éléments de données sont définis dans ~~l'appendice~~ **le sous-appendice** 1 (Dictionnaire de données).

Remarque : concernant les téléchargements de génération 2, tous les éléments de données de niveau supérieur sont représentés dans un tableau d'enregistrements, même si celui-ci ne contient qu'un seul enregistrement. Un tableau d'enregistrements commence par un en-tête ; cet en-tête contient le type d'enregistrement, sa taille et le nombre total d'enregistrements.

Les tableaux d'enregistrements sont intitulés « ...RecordArray » (avec en-tête) dans les tableaux ci-après.

2.2.6.1 Réponse positive à une demande de transfert de données relatives à la version de l'interface de téléchargement

DDP_028a **La zone de données du message « Réponse positive à une demande de transfert de données relatives à la version de l'interface de téléchargement » doit contenir les données ci-après dans l'ordre qui suit en fonction des paramètres SID Hex 76 et PRT Hex 00 :**

Structure de données de génération 2, version 2 (PRT Hex 00)

Élément de données	**Commentaire**
`DownloadInterfaceVersion`	**Génération et version de l'UEV : Hex 02,02 pour la génération 2, version 2. Non pris en charge par les UEV de génération 1 et de génération 2, version 1, qui doivent émettre une réponse négative (sous-fonction non prise en charge, voir DDP_018)**

2.2.6.2 Réponse positive à une demande de récapitulatif de transfert de données

DDP_029 La zone de données du message « Réponse positive à une demande de récapitulatif de transfert de données » doit contenir les données ci-après dans l'ordre qui suit, selon les paramètres SID Hex 76 et PRT Hex 01**, 21 ou 31,** ainsi que la séparation et le comptage approprié des sous-messages :

Structure de données de génération 1 (PRT Hex 01)

Élément de données	*Commentaire*
MemberStateCertificate	Certificats de sécurité de l'UEV
VUCertificate	
VehicleIdentificationNumber	Identification du véhicule
VehicleRegistrationIdentification	
CurrentDateTime	Date et heure actuelles de l'UEV
VuDownloadablePeriod	Période téléchargeable
CardSlotsStatus	Type de cartes insérées dans les lecteurs de l'UEV
VuDownloadActivityData	Téléchargement précédent de l'UEV
VuCompanyLocksData	Tous les verrouillages d'entreprise enregistrés. Si cette section est vide, seul l'élément noOfLocks = 0 est envoyé.
VuControlActivityData	Tous les contrôles enregistrés dans l'UEV. Si cette section est vide, seul l'élément noOfControls = 0 est envoyé.
Signature	Signature RSA de toutes les données (à l'exception des certificats) à partir de VehicleIdentificationNumber jusqu'au dernier octet du dernier VuControlActivityData

Structure de données de génération 2, version 1 (PRT Hex 21)

Élément de données	Commentaire
MemberStateCertificateRecordArray	Certificat de ~~l'État membre~~ **la Partie contractante**
VUCertificateRecordArray	Certificat de l'UEV
VehicleIdentificationNumberRecordArray	Identification du véhicule
VehicleRegistrationNumberRecordArray	Numéro d'immatriculation du véhicule
CurrentDateTimeRecordArray	Date et heure actuelles de l'UEV
VuDownloadablePeriodRecordArray	Période téléchargeable
CardSlotsStatusRecordArray	Type de cartes insérées dans les lecteurs de l'UEV
VuDownloadActivityDataRecordArray	Téléchargement précédent de l'UEV
VuCompanyLocksRecordArray	Tous les verrouillages d'entreprise enregistrés. Si cette section est vide, seul l'en-tête noOfRecords = 0 est envoyé.
VuControlActivityRecordArray	Tous les contrôles enregistrés dans l'UEV. Si cette section est vide, seul l'en-tête noOfRecords = 0 est envoyé.
SignatureRecordArray	Signature ECC de toutes les données précédentes à l'exception des certificats

Structure de données de génération 2, version 2 (PRT Hex 31)

Élément de données	Commentaire
MemberStateCertificateRecordArray	Certificat de ~~l'État membre~~ **la Partie contractante**
VUCertificateRecordArray	Certificat de l'UEV
VehicleIdentificationNumberRecordArray	Identification du véhicule
VehicleRegistrationNumberRecordArray	Numéro d'immatriculation du véhicule
CurrentDateTimeRecordArray	Date et heure actuelles de l'UEV
VuDownloadablePeriodRecordArray	Période téléchargeable
CardSlotsStatusRecordArray	Type de cartes insérées dans les lecteurs de l'UEV
VuDownloadActivityDataRecordArray	Téléchargement précédent de l'UEV
VuCompanyLocksRecordArray	Tous les verrouillages d'entreprise enregistrés. Si cette section est vide, seul l'en-tête noOfRecords = 0 est envoyé.
VuControlActivityRecordArray	Tous les contrôles enregistrés dans l'UEV. Si cette section est vide, seul l'en-tête noOfRecords = 0 est envoyé.
SignatureRecordArray	Signature ECC de toutes les données précédentes à l'exception des certificats

2.2.6.~~2~~3 Réponse positive à une demande de transfert de données relatives aux activités

DDP_030 La zone de données du message « Réponse positive à une demande de transfert de données relatives aux activités » doit contenir les données ci-après dans l'ordre qui suit, selon les paramètres SID Hex 76 et PRT Hex 02**, 22** ou ~~2~~**3**2, ainsi que la séparation et le comptage approprié des sous-messages :

Structure de données de génération 1 **(PRT Hex 02)**

Élément de données	*Commentaire*
TimeReal	Date du jour téléchargé
OdometerValueMidnight	Kilométrage à la fin du jour téléchargé
VuCardIWData	Données relatives aux cycles d'insertion et de retrait des cartes. - Si cette section ne contient aucune donnée disponible, seul noOfVuCardIWRecords = 0 est envoyé. - Lorsqu'un enregistrement d'insertion/retrait de carte (VuCardIWRecord) couvre une période débutant avant 00 h 00 (insertion de carte la veille) ou prenant fin après 24 h 00 (retrait de carte le lendemain), il apparaît entièrement sur les deux jours concernés.
VuActivityDailyData	État des lecteurs à 00 h 00 et changements d'activité enregistrés pour la journée téléchargée.
VuPlaceDailyWorkPeriodData	Données relatives aux lieux enregistrés pour le jour téléchargé. Si cette section est vide, seul noOfPlaceRecords = 0 est envoyé.
VuSpecificConditionData	Données relatives aux conditions particulières enregistrées pour le jour téléchargé. Si cette section est vide, seul noOfSpecificConditionRecords = 0 est envoyé.
Signature	Signature RSA pour toutes les données à partir de TimeReal jusqu'au dernier octet du plus récent enregistrement de conditions particulières

Structure de données de génération 2, **version 1 (PRT Hex 22)**

Élément de données	*Commentaire*
DateOfDayDownloadedRecordArray	Date du jour téléchargé
OdometerValueMidnightRecordArray	Kilométrage à la fin du jour téléchargé
VuCardIWRecordArray	Données relatives aux cycles d'insertion et de retrait des cartes. - Si cette section ne contient aucune donnée disponible, l'en-tête noOfRecords = 0 est envoyé. - Lorsqu'un enregistrement d'insertion/retrait de carte (VuCardIWRecord) couvre une période débutant avant 00 h 00 (insertion de carte la veille) ou prenant fin après 24 h 00 (retrait de carte le lendemain), il apparaît entièrement sur les deux jours concernés.
VuActivityDailyRecordArray	État des lecteurs à 00 h 00 et changements d'activité enregistrés pour le jour téléchargé
VuPlaceDailyWorkPeriodRecordArray	Données relatives aux lieux enregistrés pour le jour téléchargé. Si cette section est vide, l'en-tête noOfRecords = 0 est envoyé.
~~VuGNSSCDRecordArray~~ **VuGNSSADRecordArray**	Positions GNSS du véhicule ~~si~~ **lorsque** le temps de conduite ~~continue~~ **accumulé** ~~du conducteur~~ atteint un multiple de trois heures. Si cette section est vide, l'en-tête noOfRecords = 0 est envoyé.

Élément de données	*Commentaire*
VuSpecificConditionRecordArray	Données relatives aux conditions particulières enregistrées pour le jour téléchargé. Si cette section est vide, l'en-tête noOfRecords = 0 est envoyé.
SignatureRecordArray	**Signature ECC de toutes les données précédentes**

Structure de données de génération 2, version 2 (PRT Hex 32)

Élément de données	*Commentaire*
DateOfDayDownloadedRecordArray	**Date du jour téléchargé**
OdometerValueMidnightRecordArray	**Kilométrage à la fin du jour téléchargé**
VuCardIWRecordArray	**Données relatives aux cycles d'insertion et de retrait des cartes.** – **Si cette section ne contient aucune donnée disponible, l'en-tête noOfRecords = 0 est envoyé.** – **Si un enregistrement d'insertion/retrait de carte (VuCardIWRecord) couvre une période débutant avant 00 h 00 (insertion de la carte le jour précédent) ou prenant fin après 24 h 00 (retrait de carte le jour suivant), il apparaît entièrement sur les deux jours concernés.**
VuActivityDailyRecordArray	**État des lecteurs à 00 h 00 et changements d'activité enregistrés pour le jour téléchargé**
VuPlaceDailyWorkPeriodRecordArray	**Données relatives aux lieux enregistrés pour le jour téléchargé. Si cette section est vide, l'en-tête noOfRecords = 0 est envoyé.**
~~**VuGNSSCDRecordArray**~~ **VuGNSSADRecordArray**	**Positions GNSS du véhicule ~~si~~ lorsque le temps de conduite ~~continue~~ accumulé ~~du conducteur~~ atteint un multiple de trois heures. Si cette section est vide, l'en-tête noOfRecords = 0 est envoyé.**
VuSpecificConditionRecordArray	**Données relatives aux conditions particulières enregistrées pour le jour téléchargé. Si cette section est vide, l'en-tête noOfRecords = 0 est envoyé.**
VuBorderCrossingRecordArray	**Passages de frontières enregistrés pour le jour téléchargé. Si cette section est vide, l'en-tête noOfRecords=0 est envoyé.**
VuLoadUnloadRecordArray	**Opérations de chargement/déchargement enregistrées pour le jour téléchargé. Si cette section est vide, l'en-tête noOfRecords=0 est envoyé.**
SignatureRecordArray	**Signature ECC de toutes les données précédentes**

2.2.6.~~3~~4 Réponse positive à une demande de transfert de données relatives aux événements et aux anomalies

DDP_031 La zone de données du message « Réponse positive à une demande de transfert de données relatives aux événements et aux anomalies » doit contenir les données ci-après dans l'ordre qui suit selon les paramètres SID Hex 76 et PRT Hex 03**, 23** ou ~~2~~**3**3, ainsi que la séparation et le comptage approprié des sous-messages :

Structure de données de génération 1 (**PRT Hex 03**)

Élément de données	*Commentaire*
VuFaultData	Toutes les anomalies enregistrées ou en cours au sein de l'UEV. Si cette section est vide, seule l'information noOfVuFaults = 0 est envoyée.
VuEventData	Tous les événements enregistrés ou en cours au sein de l'UEV (à l'exception des excès de vitesse). Si cette section est vide, seule l'information noOfVuEvents = 0 est envoyée.
VuOverSpeedingControlData	Données relatives au dernier contrôle d'excès de vitesse (valeur par défaut en l'absence de données)
VuOverSpeedingEventData	Tous les événements de type excès de vitesse enregistrés dans l'UEV. Si cette section est vide, seule l'information noOfVuOverSpeedingEvents = 0 est envoyée.
VuTimeAdjustmentData	Tous les événements de type remise à l'heure enregistrés dans l'UEV (hors du cadre d'un étalonnage complet). Si cette section est vide, seule l'information noOfVuTimeAdjRecords = 0 est envoyée.
Signature	Signature RSA de toutes les données à partir de noOfVuFaults jusqu'au dernier octet du plus récent enregistrement de remise à l'heure

Structure de données de génération 2, version 1 (PRT Hex 23)

Élément de données	**Commentaire**
VuFaultRecordArray	Toutes les anomalies enregistrées ou en cours au sein de l'UEV. Si cette section est vide, seul l'en-tête noOfRecords = 0 est envoyé.
VuEventRecordArray	Tous les événements enregistrés ou en cours au sein de l'UEV (à l'exception des excès de vitesse). Si cette section est vide, seul l'en-tête noOfRecords = 0 est envoyé.
VuOverSpeedingControlDataRecordArray	Données relatives au dernier contrôle d'excès de vitesse (valeur par défaut en l'absence de données)
VuOverSpeedingEventRecordArray	Tous les événements de type excès de vitesse enregistrés dans l'UEV. Si cette section est vide, seul l'en-tête noOfRecords = 0 est envoyé.
VuTimeAdjustmentRecordArray	Tous les événements de type remise à l'heure enregistrés dans l'UEV (hors du cadre d'un étalonnage complet). Si cette section est vide, seul l'en-tête noOfRecords = 0 est envoyé.
~~VuTimeAdjustmentGNSSRecordArray~~	
SignatureRecordArray	Signature ECC de toutes les données précédentes

Structure de données de génération 2, version 2 (PRT Hex 33)

Élément de données	**Commentaire**
VuFaultRecordArray	Toutes les anomalies enregistrées ou en cours au sein de l'UEV. Si cette section est vide, seul l'en-tête noOfRecords = 0 est envoyé.
VuEventRecordArray	Tous les événements enregistrés ou en cours au sein de l'UEV (à l'exception des excès de vitesse). Si cette section est vide, seul l'en-tête noOfRecords = 0 est envoyé.
VuOverSpeedingControlDataRecordArray	Données relatives au dernier contrôle d'excès de vitesse (valeur par défaut en l'absence de données)
VuOverSpeedingEventRecordArray	Tous les événements de type excès de vitesse enregistrés dans l'UEV. Si cette section est vide, seul l'en-tête noOfRecords = 0 est envoyé.
VuTimeAdjustmentRecordArray	Tous les événements de type remise à l'heure enregistrés dans l'UEV (hors du cadre d'un étalonnage complet). Si cette section est vide, seul l'en-tête noOfRecords = 0 est envoyé.
SignatureRecordArray	Signature ECC de toutes les données précédentes

2.2.6.45 Réponse positive à une demande de transfert de données relatives à la vitesse du véhicule

DDP_032 La zone de données du message « Réponse positive à une demande de transfert de données relatives à la vitesse du véhicule » doit contenir les données ci-après dans l'ordre qui suit, selon les paramètres SID Hex 76 et PRT Hex 02 ou **24**, ainsi que la séparation et le comptage approprié des sous-messages :

Structure de données de génération 1 (**PRT Hex 04**)

Élément de données	*Commentaire*
VuDetailedSpeedData	Toutes les données se rapportant à l'évolution de la vitesse du véhicule enregistrée dans l'UEV pendant une minute au cours de laquelle le véhicule était en mouvement 60 valeurs de vitesse par minute (une par seconde)
Signature	Signature RSA de toutes les données à partir de noOfSpeedBlocks jusqu'au dernier octet du dernier bloc de vitesse

Structure de données de génération 2 (PRT Hex 24)

Élément de données	*Commentaire*
VuDetailedSpeedBlockRecordArray~~Data VuDetailedSpeedBlockRecordArray~~	**Toutes les données se rapportant à l'évolution de la vitesse du véhicule enregistrée dans l'UEV pendant une minute au cours de laquelle le véhicule était en mouvement** **60 valeurs de vitesse par minute (une par seconde)**
SignatureRecordArray	Signature ~~ECC~~**RSAECC** de toutes les données **précédentes**~~précédentes à partir de noOfSpeedBlocks jusqu'au dernier octet du dernier bloc de vitesse~~

2.2.6.~~5~~6

DDP_033 La zone de données du message « Réponse positive à une demande de transfert de données techniques » doit contenir les données ci-après dans l'ordre qui suit, selon les paramètres SID Hex 76 et PRT Hex 05**, 25 ou ~~2~~35**, ainsi que la séparation et le comptage approprié des sous-messages :

Structure de données de génération 1 (**PRT Hex 05**)

Élément de données	*Commentaire*
VuIdentification	
SensorPaired	
VuCalibrationData	Tous les enregistrements d'étalonnage stockés dans la mémoire de l'UEV
Signature	Signature RSA de toutes les données à partir de vuManufacturerName jusqu'au dernier octet du dernier VuCalibrationRecord

Structure de données de génération 2, version 1 (PRT Hex 25)

Élément de données	**Commentaire**
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Tous les couplages du capteur de mouvement enregistrés dans l'UEV
VuSensorExternalGNSSCoupledRecordArray	Tous les couplages du dispositif GNSS externe enregistrés dans l'UEV
VuCalibrationRecordArray	Tous les enregistrements d'étalonnage stockés dans l'UEV
VuCardRecordArray	Toutes les données relatives aux insertions de cartes enregistrées dans l'UEV
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Signature ECC de toutes les données précédentes

Structure de données de génération 2, version 2 (PRT Hex 35)

Élément de données	**Commentaire**
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Tous les appariements de capteur de mouvement enregistrés dans l'UEV
VuSensorExternalGNSSCoupledRecordArray	Tous les couplages de dispositif GNSS externe enregistrés dans l'UEV
VuCalibrationRecordArray	Tous les enregistrements d'étalonnage stockés dans l'UEV
VuCardRecordArray	Toutes les données relatives aux insertions de cartes enregistrées dans l'UEV
VuITSConsentRecordArray	

VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Signature ECC de toutes les données précédentes

2.3 Stockage de fichiers sur un support de mémoire externe

DDP_034 Si une session de téléchargement a comporté une opération de transfert de données à partir de l'UEV, l'ESI doit enregistrer au sein d'un seul et même fichier physique toutes les données reçues de l'UEV pendant cette session de téléchargement dans des messages de réponse positive concernant le transfert de données. La sauvegarde de ces données exclut les en-têtes de message, les compteurs de sous-messages, les sous-messages vides et les totaux de contrôle, mais elle inclut les SID et les PRT (du premier sous-message dans l'éventualité où il y en aurait plus d'un).

3. Protocole de téléchargement des cartes tachygraphiques

3.1 Champ d'application

Ce paragraphe comporte une description du téléchargement direct vers un ESI des données stockées sur une carte tachygraphique. L'ESI n'appartient pas à l'environnement sécurisé ; aucune authentification n'a donc lieu entre la carte et l'ESI.

3.2 Définitions

Session de téléchargement : chaque fois que le système procède à une opération de téléchargement des données enregistrées sur une carte à circuit intégré. Cette session couvre l'ensemble de la procédure, de la réinitialisation de la carte à circuit intégré par un PIF à sa désactivation (retrait de la carte ou réinitialisation suivante).

Fichier de données signé : fichier enregistré sur la carte à circuit intégré. Ce fichier est transféré en clair vers le PIF. Sur la carte à circuit intégré, le fichier est haché et signé ; la signature est transférée vers le PIF.

3.3 Téléchargement d'une carte

DDP_035 Le téléchargement d'une carte tachygraphique comporte les opérations suivantes :

- Téléchargement des informations communes que contient la carte dans les EF (fichiers élémentaires) `ICC` et `IC`. Ces informations à caractère facultatif ne sont pas protégées par une signature numérique.
- **~~(~~Pour les cartes tachygraphiques de première et de deuxième génération~~)~~**
  - **Téléchargement des EF figurant dans le DF Tachograph :**
    - Téléchargement des EF `Card_Certificate` ~~(ou `CardSignCertificate`)~~ et `CA_Certificate`. Ces informations ne sont pas protégées par une signature numérique.

    Il est obligatoire de télécharger ces fichiers pour toute session de téléchargement.

    - Téléchargement des autres EF de données d'application (dans le~~s~~ DF `Tachograph` ~~`et Tachograph_G2 le cas échéant`~~) sauf l'EF `Card_Download`. Ces informations sont protégées par une signature

numérique **conformément aux dispositions du sous-appendice 11 (Mécanismes de sécurité communs), partie A.**

Il est obligatoire de télécharger au moins les EF Application_Identification et **Identification pour toute session de téléchargement.**

- **Lors du téléchargement d'une carte de conducteur, il est également obligatoire de procéder au téléchargement des EF suivants :**

Events_Data,

Faults_Data,

Driver_Activity_Data,

Vehicles_Used,

Places,

Control_Activity_Data,

Specific_Conditions.

- **~~(~~Pour les cartes tachygraphiques de deuxième génération uniquement~~)~~**
  - **Excepté lorsque le téléchargement d'une carte de conducteur insérée dans une UEV est effectué durant le contrôle des conducteurs par une autorité de contrôle non rattachée à l'UE, au moyen d'une carte de contrôleur de première génération, téléchargement des EF figurant dans le DF Tachograph_G2 :**
    - **Téléchargement des EF CardSignCertificate, CA_Certificate et Link_Certificate ~~(le cas échéant)~~. Ces informations ne sont pas protégées par une signature numérique.**

Il est obligatoire de télécharger ces fichiers pour toute session de téléchargement.

- **Téléchargement des autres EF de données d'application (dans le DF Tachygraph_G2) sauf l'EF Card_Download. Ces informations sont protégées par une signature numérique conforme aux dispositions de la partie B du sous-appendice 11 (Mécanismes de sécurité communs).**

Il est obligatoire de télécharger au moins les EF Application_Identification, Application_Identification_V2 (le cas échéant) et Identification pour toute session de téléchargement.

- Lors du téléchargement d'une carte de conducteur, il est également obligatoire de procéder au téléchargement des EF suivants :

Events_Data,

Faults_Data,

Driver_Activity_Data,

Vehicles_Used,

Places,

Control_Activity_Data,

Specific_Conditions,

VehicleUnits_Used,

GNSS_-Places ~~(le cas échéant),~~

Places_Authentication (le cas échéant),

GNSS_Places_Authentication (le cas échéant),

Border_Crossings (le cas échéant),

Load_Unload_Operations (le cas échéant),

Load_Type_Entries (le cas échéant).

- Lors du téléchargement d'une carte de conducteur, il convient de mettre à jour la date du dernier téléchargement (`LastCardDownload`) dans l'EF `Card_Download`**, dans le DF `Tachograph` et, le cas échéant, dans le DF `Tachograph_G2`.**
- Lors du téléchargement d'une carte d'atelier, il convient de réinitialiser le compteur d'étalonnage enregistré dans l'EF `Card_Download` dans le DF `Tachograph` et, le cas échéant, dans le DF `Tachograph_G2`.
- Lors du téléchargement d'une carte d'atelier, l'EF `Sensor_Installation_Data` **dans le DF `Tachograph` et, le cas échéant, dans le `Tachograph_G2`** ne doit pas être téléchargé.

3.3.1 Séquence d'initialisation

DDP_036 L'ESI doit lancer la séquence en procédant comme suit :

Carte	Sens	ESI/PIF	Signification/Remarques
	⇦	Réinitialisation matérielle	
ATR	⇨		

L'utilisateur a l'option de recourir à la sélection des paramètres de protocole (PPS) pour passer à un débit supérieur à condition que la carte à circuit intégré en assure la prise en charge.

3.3.2 Séquence de téléchargement des fichiers de données non signés

DDP_037 La séquence de téléchargement des EF ICC, IC, Card_Certificate (ou CardSignCertificate~~)~~ **pour le DF Tachograph_G2)**, CA_Certificate **et Link_Certificate (pour le DF Tachograph_G2 uniquement)** se présente comme suit :

Carte	Sens	ESI/PIF	Signification/Remarques
	⇦	**SELECT FILE**	Sélection à l'aide de l'identificateur de fichier
OK	⇨		
	⇦	**READ BINARY**	Si le fichier contient plus de données que la mémoire tampon du lecteur ou de la carte ne peut en contenir, la commande doit être réitérée jusqu'à ce que les données aient été extraites dans leur intégralité.
Données OK	⇨	Sauvegarder les données sur le SME	Selon **0** nd avec un identificateur d'EF court. Conformément au paragraphe 3.4 (Format d'archivage des données)

Remarque 1 : avant de sélectionner l'EF Card_Certificate (ou CardSignCertificate), il convient de sélectionner préalablement l'application tachygraphique correspondante (sélection par l'identificateur d'application).

Remarque 2 : la sélection et la lecture d'un fichier sont également réalisables en une étape au moyen de la commande READ BINARY et d'un identificateur d'EF court.

3.3.3 Séquence de téléchargement des fichiers de données signés

DDP_038 Il y a lieu de recourir à la séquence ci-après pour procéder au téléchargement de chacun des fichiers qui suivent accompagnés de leur signature :

Carte	*Sens*	*ESI/PIF*	*Signification/Remarques*
	⇦	**SELECT**	
OK	⇨		
	⇦	**PERFORM HASH OF FILE**	Permet de calculer la valeur de hachage par rapport au contenu du fichier sélectionné en appliquant l'algorithme de hachage prévu ~~à l'appendice~~ **au sous-appendice** 11**, partie A ou B.** Cette commande n'est pas une commande ISO.
Calculer le hachage du fichier et enregistrer temporairement la valeur de hachage retenue			
OK	⇨		
	⇦	**READ BINARY**	Si le fichier contient plus de données que la mémoire tampon du lecteur ou de la carte ne peut en contenir, la commande doit être réitérée jusqu'à ce que les données aient été extraites dans leur intégralité.
Données **OK**	⇨	Sauvegarder les données sur le SME	Selon **0** nd avec un identificateur d'EF court. Conformément au paragraphe 3.4 (Format d'archivage des données)
	⇦	**PSO: COMPUTE DIGITAL SIGNATURE**	
Exécuter une opération de sécurité « calcul de la signature numérique » à l'aide de la valeur de hachage temporairement enregistrée			
Signature **OK**	⇨	Adjonction de données à celles préalablement sauvegardées sur le SME	Selon **0** nd avec un identificateur d'EF court. Conformément au paragraphe 3.4 (Format d'archivage des données)

Remarque : la sélection et la lecture d'un fichier sont également réalisables en une étape au moyen de la commande READ BINARY et d'un identificateur d'EF court. Dans ce cas, l'EF peut être sélectionné et lu avant l'exécution de la commande PERFORM HASH OF FILE.

3.3.4 Séquence de réinitialisation d'un compteur d'étalonnage

DDP_039 La séquence de réinitialisation du compteur NoOfCalibrationsSinceDownload que contient l'EF `Card_Download` d'une carte d'atelier se présente comme suit :

Carte	*Sens*	*ESI/PIF*	*Signification/Remarques*
	⇦	**SELECT FILE** EF Card_Download	Sélection à l'aide de l'identificateur de fichier
OK	⇨		
	⇦	**UPDATE BINARY** NoOfCalibrationsSinceDownload = '00 00'	
Réinitialiser le nombre de téléchargements de la carte			
OK	⇨		

Remarque : la sélection et l'actualisation d'un fichier sont également réalisables en une étape au moyen de la commande UPDATE BINARY et d'un identificateur d'EF court.

3.4 Format de stockage des données

3.4.1 Introduction

DDP_040 Les données téléchargées doivent être enregistrées dans les conditions suivantes :

- L'enregistrement des données doit être transparent. En d'autres termes, l'ordre dans lequel se présentent les octets et les bits constitutifs de ces octets doit être préservé lors de l'opération de stockage exécutée après leur transfert à partir de la carte ;
- Tous les fichiers de la carte téléchargés dans le cadre d'une session de téléchargement doivent être enregistrés au sein d'un seul et même fichier sur le SME.

3.4.2 Format des fichiers

DDP_041 Le format des fichiers se présente comme la concaténation de plusieurs objets codés en TLV.

DDP_042 La balise associée à un EF prend la forme du FID de ce fichier suivi de l'appendice '00'.

DDP_043 La balise associée à la signature d'un EF prend la forme du FID de ce fichier suivi de l'appendice '01'.

DDP_044 La longueur est exprimée par deux octets, dont la valeur détermine le nombre d'octets affectés à la zone valeur. La valeur 'FF FF' dans la zone de longueur est réservée à un usage ultérieur.

DDP_045 Faute de téléchargement, aucune information relative à un fichier déterminé ne sera sauvegardée (pas de balise et pas de longueur zéro).

DDP_046 Toute signature doit être sauvegardée sous forme d'objet TLV immédiatement après l'objet TLV qui contient les données du fichier concerné.

Définition	**Signification**	**Longueur**
FID (2 octets) ||'00'	Balise associée à un EF (FID) **dans le DF `Tachograph` ou aux informations communes que contient la carte**	3 octets
FID (2 octets) ||'01'	Balise associée à la signature d'un EF (FID) **dans le DF `Tachograph`**	3 octets

FID (2 Bytes) || '02'	**Balise associée à un EF (FID) dans le DF Tachograph_G2**	**3 octets**
FID (2 Bytes) || '03'	**Balise associée à la signature d'un EF (FID) dans le DF Tachograph_G2**	**3 octets**
xx xx	Longueur de la zone valeur	2 octets

Exemple de données enregistrées dans un fichier de téléchargement sur un SME :

Balise	Longueur	Valeur
00 02 00	00 1~~1~~	Données de l'EF ICC
C1 00 00	00 C~~2~~	Données de l'EF Card_Certificate
05 05 00	0A 2E	Données de l'EF Vehicles_Used **(dans le DF Tachograph)**
05 05 01	00 80	Signature de l'EF Vehicles_Used **(dans le DF Tachograph)**
05 05 02	**0A 2E**	**Données de l'EF Vehicles_Used dans le DF Tachograph_G2**
05 05 03	**Xx xx**	**Signature de l'EF Vehicles_Used dans le DF Tachograph_G2**

4. Téléchargement d'une carte tachygraphique par l'intermédiaire d'une unité embarquée sur le véhicule

DDP_047 L'UEV doit autoriser le téléchargement du contenu d'une carte de conducteur insérée dans l'un de ses lecteurs vers un ESI connecté.

DDP_048 L'ESI doit envoyer un message « Demande de transfert de données » du type téléchargement de carte à l'UEV pour lancer ce mode de transmission (voir ~~00~~**2.2.2.9**)

DDP_049 Pour les cartes de conducteur de première génération : les données doivent être téléchargées conformément au protocole de téléchargement de données de première génération et doivent avoir la même structure que les données téléchargées à partir d'une UEV de première génération.

Pour les cartes de conducteur de deuxième génération : l'UEV doit procéder au téléchargement de la carte dans son intégralité, fichier par fichier, conformément au protocole de téléchargement de carte défini au paragraphe 0, ainsi qu'à l'envoi à l'ESI de toutes les données extraites de la carte dans le format de fichier TLV approprié (voir -) et encapsulées dans un message « Réponse positive à une demande de transfert de données ».

DDP_050 L'ESI doit extraire les données de la carte intégrées au message « Réponse positive à une demande de transfert de données » (en éliminant tous les en-têtes, SID, PRT, compteurs de sous-messages et totaux de contrôle) et les enregistrer dans un seul et même fichier physique comme décrit au chapitre ~~00~~**0**.

DDP_051 Ensuite, l'UEV doit, s'il y a lieu, procéder à une actualisation des fichiers Control_Activity_Data ou Card_Download sur la carte du conducteur.

~~Appendice~~ Sous-appendice 8

Protocole d'étalonnage

Table des matières

1. Introduction

Le présent **sous-**appendice traite des modalités d'échange des données entre un appareil d'essai et une unité embarquée sur le véhicule par l'intermédiaire de la ligne K. Cette ligne fait partie intégrante de l'interface d'étalonnage décrite ~~à l'appendice~~ **au sous-appendice** 6. Le présent appendice traite aussi du contrôle de la ligne de signalisation d'entrée/sortie au niveau du connecteur d'étalonnage.

L'établissement de communications sur la ligne K est décrit au chapitre **4. Services de communication.**

Le présent **sous-**appendice s'appuie sur le concept de « session de diagnostic » pour déterminer la portée du contrôle de la ligne K dans différentes conditions. La session par défaut est la « StandardDiagnosticSession », où toutes les données que contient une unité embarquée peuvent en être extraites, mais aucune donnée ne peut être enregistrée dans l'unité embarquée.

La sélection de la session de diagnostic fait l'objet d'une description détaillée au chapitre 5.

Le présent **sous-**appendice s'applique aux deux générations d'UEV et de cartes d'atelier, conformément aux exigences d'interopérabilité établies par le présent Règlement.

CPR_001 La session « ECUProgrammingSession » autorise la saisie de données au sein de l'unité embarquée. En cas de saisie de données d'étalonnage, l'unité embarquée doit être exploitée en mode ÉTALONNAGE.

Le transfert de données par l'intermédiaire de la ligne K fait l'objet d'une description détaillée au chapitre 6 (Services de transmission de données). Les structures des données transférées sont décrites en détail au chapitre 8 (Service routineControl (TimeAdjustment)) et au chapitre 9 (Structures des enregistrements de données).

CPR_002 La session « ECUAdjustmentSession » permet de sélectionner le mode d'entrée/sortie de la ligne de signalisation d'entrée/sortie d'étalonnage à l'aide de l'interface de la ligne K. Le contrôle de la ligne de signalisation d'entrée/sortie d'étalonnage est décrit au chapitre 7 (Contrôle des impulsions d'essai − Unité fonctionnelle de contrôle des entrées/sorties).

CPR_003 Tout au long du présent document, l'appareil d'essai possède l'adresse suivante : 'tt'. Bien que certaines adresses d'appareil d'essai soient privilégiées, l'UEV doit réagir correctement à toute adresse d'appareil d'essai. L'adresse physique de l'UEV s'énonce comme suit : 0xEE.

2. Terminologie, définitions et références

Les protocoles, messages et codes d'erreur sont principalement issus d'un projet de norme ISO 14229-1 (Véhicules routiers − Systèmes de diagnostic − Partie 1 : services de diagnostic, version 6 du 22 février 2001).

Un codage en octets et des valeurs hexadécimales sont utilisés pour la définition des identificateurs de service, l'élaboration des demandes et réponses de service et la configuration des paramètres normalisés.

Le terme « appareil d'essai » désigne l'équipement utilisé pour saisir des données de programmation/d'étalonnage dans l'UEV.

Les termes « client » et « serveur » font respectivement référence à l'appareil d'essai et à l'UEV.

Le terme ECU (*Electronic Control Unit*) signifie « unité de commande électronique » et désigne l'UEV.

Références :

ISO 14230-2 Véhicules routiers − Systèmes de diagnostic − Protocole « Keyword 2000 » − Partie 2 : couche liaison de données, première édition : 1999.

~~Véhicules routiers – Diagnostic.~~

3. Vue d'ensemble des services

3.1 Services disponibles

Le tableau qui suit présente une vue d'ensemble des services définis dans le présent document qui seront disponibles dans le tachygraphe.

CPR_004 Le tableau ci-après présente les services disponibles lors d'une session de diagnostic active.

- La **1re colonne** répertorie les services disponibles ;
- La **2e colonne** indique le numéro du chapitre du présent **sous-**appendice qui définit plus précisément le service considéré ;
- La **3e colonne** indique les valeurs attribuées à l'identificateur de service dans les messages de demande de service ;
- La **4e colonne** précise quels sont les services de la « **StandardDiagnosticSession** » (**SD**) qui doivent être mis en œuvre dans l'UEV ;
- La **5e colonne** précise quels sont les services de la « **ECUAdjustmentSession** » (**ECUAS**) qui doivent être mis en œuvre pour permettre un contrôle adéquat de la ligne de signalisation d'entrée/sortie au niveau du connecteur d'étalonnage monté sur la face avant de l'UEV ;
- La **6e colonne** précise quels sont les services de la « **ECUProgrammingSession** » (**ECUPS**) qui doivent être mis en œuvre pour permettre la programmation des paramètres au sein de l'UEV.

			Sessions de diagnostic		
Nom du service de diagnostic	**Chapitre**	**Valeurs attribuées aux identificateurs de service**	**SD**	**ECUAS**	**ECUPS**
StartCommunication	0	81	■	■	■
StopCommunication	0	82	■		
TesterPresent	0	3E	■	■	■
StartDiagnosticSession	0	10	■	■	■
SecurityAccess	**8**	27	■	■	■
ReadDataByIdentifier	0	22	■	■	■
WriteDataByIdentifier	0	2E			■
InputOutputControlByIdentifier	0	2F		■	
RoutineControl	**8**	**31**		■	■

Tableau 1 − Récapitulatif des valeurs attribuées aux identificateurs de service

■ Ce symbole rappelle le caractère obligatoire du service correspondant pendant cette session de diagnostic.

L'absence de symbole indique que l'exécution du service correspondant n'est pas autorisée pendant cette session de diagnostic.

3.2 Codes de réponse

Des codes de réponse sont définis pour chaque service.

4. Services de communication

Certains services sont nécessaires à l'établissement et au maintien des communications. Ils n'apparaissent pas dans la couche application. Les services disponibles sont décrits dans le tableau ci-dessous :

Nom du service	Description
StartCommunication	Le client demande le lancement d'une session de communication avec un ou plusieurs serveurs.
StopCommunication	Le client demande l'arrêt de la session de communication en cours.
TesterPresent	Le client indique au serveur qu'il est encore présent.

Tableau 2 − Services de communication

CPR_005 Le service StartCommunication est utilisé pour établir une communication. L'exécution de tout service suppose l'établissement d'une communication et la sélection de paramètres adaptés au mode de fonctionnement souhaité.

4.1. Service StartCommunication

CPR_006 À la réception d'une primitive d'indication StartCommunication, l'UEV vérifie si l'établissement de la liaison d'intercommunication requise est envisageable dans les présentes conditions. Les conditions d'établissement d'une liaison font l'objet d'une description détaillée dans la norme ISO 14230-2.

CPR_007 Ensuite, l'UEV doit exécuter toutes les actions nécessaires à l'établissement de la liaison d'intercommunication requise et envoyer une primitive de réponse StartCommunication avec les paramètres de réponse positive sélectionnés.

CPR_008 Si une UEV déjà initialisée (et entrée en session de diagnostic) reçoit une nouvelle demande StartCommunication (par exemple, en raison d'une reprise à la suite d'un incident au niveau de l'appareil d'essai), cette demande doit être acceptée et l'UEV réinitialisée.

CPR_009 Si, pour une raison quelconque, l'établissement de la liaison d'intercommunication est impossible, l'UEV doit continuer à fonctionner dans les mêmes conditions qu'immédiatement avant la tentative d'établissement d'une liaison.

CPR_010 Le message de demande d'établissement d'une communication (StartCommunication) doit comporter une adresse physique.

CPR_011 L'initialisation **de l'UEV en vue de la mise en œuvre des services est effectuée selon une méthode d'initialisation rapide qui prévoit :**

- Un temps d'inoccupation préalable à toute activité ;
- La transmission d'une configuration d'initialisation par l'appareil d'essai ;
- L'envoi par l'UEV d'une réponse contenant toutes les informations nécessaires à l'établissement d'une communication.

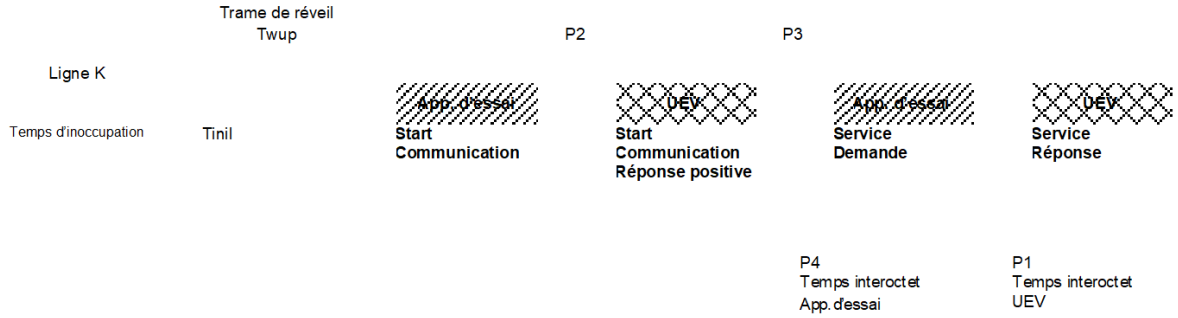
CPR_012 Après initialisation :

- Toutes les valeurs attribuées à l'ensemble des paramètres de communication sont celles définies dans le **tableau 4** en fonction des octets clés ;

- L'UEV attend la première demande en provenance de l'appareil d'essai ;
- L'UEV est exploitée en mode de diagnostic par défaut, c'est-à-dire le mode StandardDiagnosticSession ;
- La ligne de signalisation d'entrée/sortie d'étalonnage est dans son état de fonctionnement par défaut, c'est-à-dire désactivée.

CPR_014 Le débit de transmission de données sur la ligne K est de 10 400 bauds.

CPR_016 L'initialisation rapide est lancée par l'appareil d'essai, lequel émet une trame de réveil (Twup) sur la ligne K. Cette trame débute au terme d'un temps d'inoccupation (Tidle) de la ligne K suivi d'un temps de Tinil. L'appareil d'essai émet le premier bit du service StartCommunication au terme du temps Twup qui suit le premier front descendant.



CPR_017 Les valeurs de synchronisation retenues pour l'initialisation rapide et les communications en général font l'objet d'une description détaillée dans les tableaux ci-après. Pour ce qui est du temps d'inoccupation, il existe plusieurs possibilités :

- Première transmission après la mise en marche, T. inoccup. = 300 ms ;
- Après achèvement du service StopCommunication, T. inoccup. = P3 min. ;
- Après interruption d'une communication pour cause de dépassement du temps imparti (P3 max.), T. inoccup. = 0.

Paramètre		*Valeur minimale*	*Valeur maximale*
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tableau 3 − Valeurs de synchronisation pour l'initialisation rapide

Synchronisation		*Valeurs minimales (ms)*	*Valeurs maximales (ms)*
Paramètre	**Description des paramètres**	**min.**	**max.**
P1	Délai interoctet à respecter dans l'attente d'une réponse de l'UEV	0	20
P2	Laps de temps entre une demande de l'appareil d'essai et une ou deux réponses de l'UEV	25	250
P3	Laps de temps entre la fin des réponses de l'UEV et le début d'une nouvelle demande émise par l'appareil d'essai	55	5 000
P4	Délai interoctet à respecter dans l'attente d'une demande de l'appareil d'essai	5	20

Tableau 4 − Valeurs de synchronisation des communications

CPR_018 La structure des messages transmis dans le cadre d'une initialisation rapide fait l'objet d'une description détaillée dans les tableaux qui suivent.

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	81	FMT
#2	Octet d'adresse de la cible	EE	TGT
#3	Octet d'adresse de la source	tt	SRC
#4	**ID du service Demande StartCommunication**	**81**	**SCR**
#5	Total de contrôle	00-FF	CS

Tableau 5 − Message de demande d'établissement de la communication (StartCommunication)

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LEN
#5	**ID du service Réponse positive à une demande StartCommunication**	**C1**	**SCRPR**
#6	Octet clé 1	EA	KB1
#7	Octet clé 2	8F	KB2
#8	Total de contrôle	00-FF	CS

Tableau 6 − Message de réponse positive à une demande d'établissement de la communication (StartCommunication)

CPR_019 Il n'est pas prévu de réponse négative au message StartCommunication. Faute de message de réponse positive à transmettre, l'UEV n'est pas initialisée, aucune donnée n'est émise et le système demeure en mode de fonctionnement normal.

4.2 Service StopCommunication

4.2.1 Description des messages

Ce service portant sur la couche communication vise à mettre un terme à toute session de communication.

CPR_020 À la réception d'une primitive d'indication StopCommunication, l'UEV doit vérifier si les conditions en vigueur permettent d'interrompre la communication en cours. Si tel est le cas, l'UEV doit exécuter toutes les opérations requises pour mettre un terme à cette communication.

CPR_021 Si une interruption de la communication est possible, l'UEV doit émettre une primitive de réponse StopCommunication en recourant aux paramètres de réponse positive sélectionnés, avant de clore la communication.

CPR_022 Si, pour une raison quelconque, il est impossible d'interrompre la communication concernée, l'UEV doit émettre une primitive de réponse StopCommunication en recourant au paramètre de réponse négative sélectionné.

CPR_023 Si l'UEV détecte un dépassement du délai de temporisation (P3 max.), la communication est interrompue sans s'accompagner d'une primitive de réponse.

4.2.2 Structure des messages

CPR_024 La structure des messages associés aux primitives StopCommunication fait l'objet d'une description détaillée dans les tableaux ci-après.

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	TGT
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	01	LEN
#5	**ID du service Demande StopCommunication**	**82**	**SPR**
#6	Total de contrôle	00-FF	CS

Tableau 7 − Message de demande d'interruption de la communication (StopCommunication)

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure - adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	01	LEN
#5	**ID du service Réponse positive à une demande StopCommunication**	**C2**	**SPRPR**
#6	Total de contrôle	00-FF	CS

Tableau 8 − Message de réponse positive à une demande d'interruption de la communication (StopCommunication)

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LEN
#5	**ID du service Réponse négative**	**7F**	**NR**
#6	**ID du service Demande StopCommunication**	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Total de contrôle	00-FF	CS

Tableau 9 − Message de réponse négative à une demande d'interruption de la communication (StopCommunication)

4.2.3 Définition des paramètres

Ce service ne nécessite la définition d'aucun paramètre.

4.3 Service TesterPresent

4.3.1 Description des messages

Le service TesterPresent est utilisé par l'appareil d'essai pour indiquer au serveur qu'il est encore présent, afin d'empêcher que le serveur ne retourne automatiquement en

fonctionnement normal et n'interrompe, éventuellement, la communication. Ce service, envoyé périodiquement, maintient la session de diagnostic et la communication actives en remettant à zéro le compteur P3 chaque fois qu'une demande est reçue concernant ce service.

4.3.2 Structure des messages

CPR_079 La structure des messages associés aux primitives TesterPresent fait l'objet d'une description détaillée dans les tableaux ci-après.

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	TGT
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	02	LEN
#5	**ID du service Demande TesterPresent**	**3E**	**TP**
#6	Sous-fonction = responseRequired (réponse requise)	01	RESPREQ_Y
	= [yes (oui) no (non)]	02	RESPREQ_NO
#7	Total de contrôle	00-FF	CS

Tableau 10 − Message de demande d'indication de présence de l'appareil d'essai (TesterPresent)

CPR_080 Si la valeur du paramètre responseRequired est « oui », le serveur répondra par le message positif ci-après. Si la valeur du paramètre est « non », le serveur n'envoie pas de réponse.

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	01	LEN
#5	**ID du service Réponse positive à une demande TesterPresent**	**7E**	**TPPR**
#6	Total de contrôle	00-FF	CS

Tableau 11 − Message de réponse positive à une demande d'indication de présence de l'appareil d'essai (TesterPresent)

CPR_081 Le service accepte les codes de réponse négative suivants :

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LEN
#5	**ID du service Réponse négative**	**7F**	**NR**
#6	ID du service TesterPresent Request	3E	TP
#7	responseCode = [SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
	incorrectMessageLength]	13	RC_IML
#8	Total de contrôle	00-FF	CS

Tableau 12 − Message de réponse négative à une demande d'indication de présence de l'appareil d'essai (TesterPresent)

5. Services de gestion

Les services disponibles font l'objet d'une description détaillée dans le tableau ci-dessous :

Nom du service	*Description*
StartDiagnosticSession	Le client demande le lancement d'une session de diagnostic avec une UEV.
SecurityAccess	Le client demande l'accès à certaines fonctions réservées aux utilisateurs autorisés.

Tableau 13 − Services de gestion

5.1 Service StartDiagnosticSession

5.1.1 Description des messages

CPR_025 Le service StartDiagnosticSession permet d'activer différentes sessions de diagnostic au sein du serveur. Une session de diagnostic autorise l'exploitation d'un jeu de services spécifique, conformément aux indications fournies au **tableau 17**. Une session peut donner accès à des services propres au constructeur du véhicule qui ne figurent pas dans le présent document. Les règles de mise en œuvre doivent satisfaire aux exigences suivantes :

- Il doit toujours y avoir exactement une session de diagnostic en cours dans l'UEV ;
- L'UEV doit toujours ouvrir la session standard de diagnostic (StandardDiagnosticSession) lorsqu'elle est mise sous tension. Si aucune autre session de diagnostic n'est ouverte, la session standard de diagnostic doit rester ouverte aussi longtemps que l'UEV est sous tension ;
- Si une session de diagnostic déjà ouverte a été demandée par l'appareil d'essai, l'UEV envoie un message de réponse positive ;
- Lorsque l'appareil d'essai demande une nouvelle session de diagnostic, l'UEV envoie un message de réponse positive à la demande de lancement d'une session de diagnostic avant que la nouvelle session ne s'ouvre dans l'UEV. Si l'UEV n'a pas pu ouvrir la nouvelle session de diagnostic demandée, elle envoie un message de réponse négative à la demande de lancement d'une session de diagnostic et la session en cours se poursuit.

CPR_026 Une session de diagnostic ne peut être lancée qu'à condition qu'une communication ait été préalablement établie entre le client et l'UEV.

CPR_027 Les paramètres de synchronisation définis dans le **tableau 4** deviendront actifs au terme de l'exécution réussie d'un service StartDiagnosticSession, pour autant que le message de demande comporte le paramètre de session de diagnostic « StandardDiagnosticSession » dans l'éventualité où une autre session de diagnostic aurait été précédemment active.

5.1.2 Structure des messages

CPR_028 La structure des messages associés aux primitives StartDiagnosticSession fait l'objet d'une description détaillée dans les tableaux ci-après.

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	TGT
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	02	LEN
#5	**ID du service Demande StartDiagnosticSession**	**10**	**STDS**
#6	Session de diagnostic = [une valeur extraite du **tableau 17**]	xx	SD_…
#7	Total de contrôle	00-FF	CS

Tableau 14 − Message de demande de lancement d'une session de diagnostic (StartDiagnosticSession)

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	02	LEN
#5	**ID du service Réponse positive à une demande StartDiagnosticSession**	**50**	**STDSPR**
#6	Session de diagnostic = [même valeur que l'octet #6 du **tableau 14**]	xx	SD_…
#7	Total de contrôle	00-FF	CS

Tableau 15 − Message de réponse positive à une demande de lancement d'une session de diagnostic (StartDiagnosticSession)

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LEN
#5	**ID du service Réponse négative**	**7F**	**NR**
#6	ID du service Demande StartDiagnosticSession	10	STDS
#7	responseCode =[subFunctionNotSupported[a]	12	RC_SFNS
	incorrectMessageLength[b]	13	RC_IML RC_CNC
	conditionsNotCorrect[c]	22	
#8	Total de contrôle	00-FF	CS

Tableau 16 − Message de réponse négative à une demande de lancement d'une session de diagnostic (StartDiagnosticSession)

[a] La valeur introduite dans l'octet #6 du message de demande n'est pas prise en charge, c'est-à-dire qu'elle ne figure pas dans le tableau 17 ;

[b] La longueur du message est incorrecte ;

[c] Les critères de la demande de lancement d'une session de diagnostic (StartDiagnosticSession) ne sont pas remplis.

5.1.3 Définition des paramètres

CPR_029 Le service StartDiagnosticSession a recours au paramètre ***Session de diagnostic (SD_)*** pour sélectionner le comportement particulier du ou des serveurs. Les sessions de diagnostic suivantes sont précisées dans le présent document :

Hex.	*Description*	*Mnémonique*
81	**StandardDiagnosticSession (session standard de diagnostic)**	**SD**
	Cette session de diagnostic permet d'activer tous les services répertoriés dans le **tableau 1, colonne 4 « SD »**. Ces services autorisent l'extraction de données enregistrées sur un serveur (UEV). Cette session de diagnostic ne devient active qu'après l'initialisation de la communication entre client (appareil d'essai) et serveur (UEV). Cette session de diagnostic peut être écrasée par d'autres sessions de diagnostic spécifiées dans ce chapitre.	
85	**ECUProgrammingSession (session de programmation de l'ECU)**	**ECUPS**
	Cette session de diagnostic permet d'activer tous les services répertoriés dans le **tableau 1**, **colonne 6 « ECUPS ».** Ces services prennent en charge la programmation de la mémoire d'un serveur (UEV). Cette session de diagnostic peut être écrasée par d'autres sessions de diagnostic spécifiées dans ce chapitre.	
87	**ECUAdjustmentSession (session de réglage de l'ECU)**	**ECUAS**
	Cette session de diagnostic permet d'activer tous les services répertoriés dans le **tableau 1, colonne 5 « ECUAS ».** Ces services prennent en charge le contrôle des entrées/sorties d'un serveur (UEV). Cette session de diagnostic peut être écrasée par d'autres sessions de diagnostic spécifiées dans ce chapitre.	

Tableau 17 − Définition des valeurs attribuées au paramètre diagnosticSession

5.2 Service SecurityAccess

L'enregistrement de données d'étalonnage n'est possible que si l'UEV est exploitée en mode ÉTALONNAGE. Outre l'insertion d'une carte d'atelier valide dans le lecteur approprié de l'UEV, il faut entrer le numéro d'identification personnel (PIN) adéquat dans l'UEV pour avoir accès au mode ÉTALONNAGE.

Lorsque l'UEV est en mode ÉTALONNAGE ou CONTRÔLE, il est également possible d'accéder à la ligne d'entrée/sortie d'étalonnage.

Le service SecurityAccess permet d'introduire le PIN et d'indiquer à l'appareil d'essai si l'UEV est exploitée ou non en mode ÉTALONNAGE.

D'autres méthodes peuvent être utilisées pour saisir le PIN.

5.2.1 Description des messages

Le service SecurityAccess consiste en un message « requestSeed » (demande de germe) suivi, le cas échéant, d'un message « sendKey » (demande d'envoi d'une clé). Le service SecurityAccess doit être exécuté après le service StartDiagnosticSession.

CPR_033 L'appareil d'essai doit utiliser le message SecurityAccess « requestSeed » pour vérifier si l'unité embarquée sur le véhicule est prête à accepter un PIN.

CPR_034 Si l'unité embarquée sur le véhicule est déjà en mode ÉTALONNAGE, elle répond à la demande qui lui est adressée par l'envoi d'un « germe » d'une valeur de 0x0000 en utilisant le service Réponse positive à une demande d'accès sécurisé (SecurityAccess).

CPR_035 Si l'unité embarquée sur le véhicule est prête à accepter un PIN en vue d'une opération de vérification au moyen d'une carte d'atelier, elle doit répondre à la demande qui lui est adressée par l'envoi d'un « germe » d'une valeur supérieure à 0x0000 en utilisant le service Réponse positive à une demande d'accès sécurisé (SecurityAccess).

CPR_036 Si l'unité embarquée sur le véhicule n'est pas prête à accepter un PIN émanant de l'appareil d'essai parce que la carte d'atelier insérée dans le lecteur n'est pas valable, que ce dernier n'en contient aucune ou que l'unité embarquée sur le véhicule attend la transmission du PIN requis par une autre méthode, elle doit répondre à la demande qui lui est adressée par l'envoi d'une Réponse négative accompagnée d'un code de réponse conditionsNotCorrectOrRequestSequenceError (conditions non correctes ou erreur affectant la séquence de la demande).

CPR_037 En définitive, l'appareil d'essai devra recourir au message SecurityAccess « sendKey » pour transmettre un PIN à l'unité embarquée sur le véhicule. Pour ménager le temps nécessaire à l'exécution du processus d'authentification de la carte, l'UEV devra recourir au code de réponse négative requestCorrectlyReceived-ResponsePending (demande bien reçue-réponse en attente) afin de prolonger le délai de réponse. Le délai de réponse ne devra cependant pas dépasser 5 minutes. Dès que le service demandé est exécuté, l'UEV envoie un message de réponse positive ou négative avec un code de réponse différent du code précité. Le code de réponse négative requestCorrectlyReceived-ResponsePending peut être répété par l'UEV jusqu'à ce que le service demandé soit exécuté et le message de réponse finale envoyé.

CPR_038 L'unité embarquée sur le véhicule ne doit répondre à cette demande en utilisant le service Réponse positive à une demande d'accès sécurisé (SecurityAccess) qu'en mode ÉTALONNAGE.

CPR_039 Dans les cas énumérés ci-après, l'unité embarquée sur le véhicule doit répondre à cette demande par une réponse négative accompagnée de l'un des codes de réponse suivants :

- subFunctionNot supported : format non valable du paramètre de la sous-fonction (accessType) ;
- conditionsNotCorrectOrRequestSequenceError : UEV pas prête à accepter la saisie d'un PIN ;
- invalidKey : PIN non valable sans dépassement du nombre de tentatives de vérification de ce numéro ;
- exceededNumberOfAttempts : PIN non valable et dépassement du nombre de tentatives de vérification de ce numéro ;
- generalReject : PIN correct, mais échec de l'authentification mutuelle avec la carte d'atelier utilisée.

5.2.2 Structure des messages − SecurityAccess − requestSeed

CPR_040 La structure des messages associés aux primitives SecurityAccess « requestSeed » fait l'objet d'une description détaillée dans les tableaux ci-après.

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	TGT
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	02	LEN
#5	**ID du service Demande SecurityAccess**	**27**	**SA**
#6	accessType − requestSeed	7D	AT_RSD
#7	Total de contrôle	00-FF	CS

Tableau 18 − Message de demande d'accès sécurisé de type « requestSeed »

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	04	LEN
#5	**ID du service Réponse positive à une demande SecurityAccess**	**67**	**SAPR**
#6	accessType − requestSeed	7D	AT_RSD
#7	Seed High (germe supérieur)	00-FF	SEEDH
#8	Seed Low (germe inférieur)	00-FF	SEEDL
#9	Total de contrôle	00-FF	CS

Tableau 19 − Message de réponse positive à une demande d'accès sécurisé (SecurityAccess) de type « requestSeed »

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LEN
#5	**ID du service Réponse négative**	**7F**	**NR**
#6	ID du service Demande SecurityAccess	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
#8	Total de contrôle	00-FF	CS

Tableau 20 − Message de réponse négative à une demande d'accès sécurisé (SecurityAccess)

5.2.3 Structure des messages − SecurityAccess − sendKey

CPR_041 La structure des messages associés aux primitives SecurityAccess « sendKey » fait l'objet d'une description détaillée dans les tableaux ci-après.

Octet #	**Nom du paramètre**	**Valeur hex.**	**Mnémonique**
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	TGT
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	m+2	LEN
#5	**ID du service Demande SecurityAccess**	**27**	**SA**

#6	accessType – sendKey	7E	AT_SK
#7 à #m+6	Clé #1 (supérieure)	xx	KEY
	…	…	
	Clé #m (inférieure, la valeur de m doit être comprise entre 4 et 8 inclus)	xx	
#m+7	Total de contrôle	00-FF	CS

Tableau 21 − Message de demande d'accès sécurisé (SecurityAccess) de type « sendKey »

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	02	LEN
#5	**ID du service Réponse positive à une demande SecurityAccess**	**67**	**SAPR**
#6	accessType − sendKey	7E	AT_SK
#7	Total de contrôle	00-FF	CS

Tableau 22 − Message de réponse positive à une demande d'accès sécurisé (SecurityAccess) de type « sendKey »

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LEN
#5	**ID du service Réponse négative**	**7F**	**NR**
#6	ID du service Demande SecurityAccess	27	SA
#7	responseCode = [generalReject	10	RC_GR
	subFunctionNotSupported	12	RC_SFNS
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	invalidKey	35	RC_IK
	exceededNumberOfAttempts	36	RC_ENA
	requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
#8	Total de contrôle	00-FF	CS

Tableau 23 − Message de réponse négative à une demande d'accès sécurisé (SecurityAccess)

6. Services de transmission de données

Les services disponibles font l'objet d'une description détaillée dans le tableau ci-dessous :

Nom du service	*Description*
ReadDataByIdentifier	Le client demande la transmission de la valeur actuelle d'un enregistrement accessible au moyen d'un identificateur d'enregistrement (recordDataIdentifier).
WriteDataByIdentifier	Le client demande l'écriture de données dans un enregistrement accessible au moyen d'un identificateur d'enregistrement (recordDataIdentifier).

Tableau 24 − Services de transmission de données

6.1 Service ReadDataByIdentifier

6.1.1 Description des messages

CPR_050 Le service ReadDataByIdentifier est utilisé par le client pour demander l'extraction de valeurs enregistrées sur un serveur. Les données sont identifiées au moyen d'un identificateur (recordDataIdentifier). Il incombe au fabricant de l'UEV de veiller à ce que les conditions d'exploitation normale du serveur soient réunies lors de l'exécution de ce service.

6.1.2 Structure des messages

CPR_051 La structure des messages associés aux primitives ReadDataByIdentifier fait l'objet d'une description détaillée dans les tableaux ci-après.

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	TGT
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	03	LEN
#5	**ID du service Demande ReadDataByIdentifier**	**22**	**RDBI**
#6 à #7	recordDataIdentifier = [une valeur extraite du **tableau 28**]	xxxx	RDI_…
#8	Total de contrôle	00-FF	CS

Tableau 25 − Message de demande d'extraction de données par identificateur (ReadDataByIdentifier)

Octet #	*Nom du paramètre*		*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique		80	FMT
#2	Octet d'adresse de la cible		tt	TGT
#3	Octet d'adresse de la source		EE	SRC
#4	Octet de longueur supplémentaire		m+3	LEN
#5	**ID du service Réponse positive à une demande ReadDataByIdentifier**		**62**	**RDBIPR**
#6 à #7	recordDataIdentifier = [même valeur que les octets #6 et #7 du **tableau 25**]		xxxx	RDI_...
#8 à #m+7	dataRecord[] =	[donnée#1	xx	DREC_DATA1
		:	**:**	:
		donnée#m]	xx	DREC_DATAm
#m+8	Total de contrôle		00-FF	CS

Tableau 26 − Message de réponse positive à une demande d'extraction de données par identificateur (ReadDataByIdentifier)

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LEN
#5	**ID du service Réponse négative**	**7F**	**NR**
#6	ID du service Demande ReadDataByIdentifier	22	RDBI

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#7	responseCode = [requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect]	22	RC_CNC
#8	Total de contrôle	00-FF	CS

Tableau 27 − Message de réponse négative à une demande d'extraction de données par identificateur (ReadDataByIdentifier)

6.1.3 Définition des paramètres

CPR_052 Le paramètre ***recordDataIdentifier (RDI_)*** dans le message de demande ReadDataByIdentifier identifie un enregistrement de données.

CPR_053 Les valeurs des identificateurs d'enregistrement (recordDataIdentifier) définies dans le présent document figurent dans le tableau ci-après.

Ce tableau se compose de ~~quatre~~ **cinq** colonnes et de plusieurs lignes.

- La **1re colonne (Hex.)** indique la « valeur hexadécimale » affectée à l'identificateur d'enregistrement spécifié dans la 3e colonne ;
- **La 2e colonne (Élément de donnée)** indique l'élément de donnée ~~de l'Appendice~~ **du sous-appendice** 1 sur lequel est fondé l'identificateur d'enregistrement (un transcodage est parfois nécessaire) ;
- La **3e colonne (Description)** indique le nom de l'identificateur d'enregistrement correspondant ;
- La **4e colonne (Droits d'accès) précise les droits d'accès à cet** identificateur d'enregistrement ;
- **La 5e colonne (Mnémonique)** indique le mnémonique associé à cet identificateur d'enregistrement.

Valeur hex.	*Élément de données*	*Nom de l'identificateur d'enregistrement (voir la structure présentée à la section 8.2)*	***Droits d'accès (lecture/écriture)***	*Mnémonique*
F90B	CurrentDateTime	TimeDate	**L/E**	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicleDistance	**L/E**	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	**L/E**	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	**L/E**	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	**L/E**	RDI_WVCF
F921	TyreSize	TyreSize	**L/E**	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	**L/E**	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	**L/E**	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	**L/E**	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	**L/E**	RDI_VRN
F190	VehicleIdentificationNumber	VIN	**L/E**	RDI__VIN
F9D0	**SensorSerialNumber**	**MotionSensorSerialNumber**	**L**	**RDI_SSN**
F9D1	**RemoteCommunicationModuleSerialNumber**	**RemoteCommunicationFacilitySerialNumber**	**L**	**RDI_RCSN**
F9D2	**SensorGNSSSerialNumber**	**ExternalGNSSFacilitySerialNumber**	**L**	**RDI_GSSN**

Valeur hex.	*Élément de données*	*Nom de l'identificateur d'enregistrement (voir la structure présentée à la section 8.2)*	***Droits d'accès (lecture/écriture)***	*Mnémonique*
F9D3	**SealDataVu**	**SmartTachographSealsSerialNumber**	**L/E**	**RDI_SDV**
F9D4	**VuSerialNumber**	**VuSerialNumber**	**L**	**RDI_VSN**
F9D5	**ByDefaultLoadType**	**ByDefaultLoadType**	**L/E**	**RDI_BDLT**
F9D6	**TachographCardsGen1Suppression**	**TachographCardsGen1Suppression**	**L/E**	**RDI_TCG1S**
F9D7	**VehiclePosition**	**VehiclePosition**	**L**	**RDI_VP**
F9D8	**LastCalibrationCountry**	**CalibrationCountry**	**L**	**RDI_CC**

Tableau 28 − Définition des valeurs attribuées aux identificateurs d'enregistrements (recordDataIdentifier)

CPR_054 Le paramètre ***dataRecord (DREC_)*** est utilisé dans le message de Réponse positive à une demande ReadDataByIdentifier pour fournir au client (appareil d'essai) la valeur de l'enregistrement de données désigné par l'identificateur d'enregistrement. Les structures de données sont spécifiées au chapitre 8. D'autres enregistrements de données (dataRecords), telles que les entrées, les sorties et les données internes propres à l'UEV, peuvent être obtenus au choix de l'utilisateur, mais ils ne sont pas définis dans le présent document.

6.2 Service WriteDataByIdentifier

6.2.1 Description des messages

CPR_056 Le client a recours au service WriteDataByIdentifier pour enregistrer de nouvelles valeurs dans les enregistrements de données présents sur un serveur. Les données sont identifiées par identificateur d'enregistrements (recordDataIdentifier). Il incombe au fabricant de l'UEV de veiller à ce que les conditions d'exploitation normale du serveur soient réunies lors de l'exécution de ce service. Pour procéder à l'actualisation des paramètres répertoriés au tableau 28, il faut que l'UEV soit en mode ÉTALONNAGE.

6.2.2 Structure des messages

CPR_057 La structure des messages associés aux primitives WriteDataByIdentifier fait l'objet d'une description détaillée dans les tableaux ci-après.

Octet #	*Nom du paramètre*		*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique		80	FMT
#2	Octet d'adresse de la cible		EE	TGT
#3	Octet d'adresse de la source		tt	SRC
#4	Octet de longueur supplémentaire		m+3	LEN
#5	**ID du service Demande WriteDataByIdentifier**		**2E**	**WDBI**
#6 à #7	recordDataIdentifier = [une valeur extraite du **tableau 28**]		xxxx	RDI_…
#8 à m+7	dataRecord[] =	[donnée#1	xx	DREC_DATA1
		:	**:**	:
		donnée#m]	xx	DREC_DATAm
#m+8	Total de contrôle		00-FF	CS

Tableau 29 − Message de demande d'écriture de données par identificateur (WriteDataByIdentifier)

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LEN
#5	**ID du service Réponse positive à une demande WriteDataByIdentifier**	**6E**	**WDBIPR**
#6 à #7	recordDataIdentifier = [même valeur que les octets #6 et #7 du tableau 29]	xxxx	RDI_...
#8	Total de contrôle	00-FF	CS

Tableau 30 − Message de réponse positive à une demande d'écriture de données par identificateur (WriteDataByIdentifier)

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LEN
#5	**ID du service Réponse négative**	**7F**	**NR**
#6	ID du service Demande WriteDataByIdentifier	2E	WDBI
#7	responseCode= [requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML RC_CNC
	conditionsNotCorrect]	22	
#8	Total de contrôle	00-FF	CS

Tableau 31 − Message de réponse négative à une demande d'écriture de données par identificateur (WriteDataByIdentifier)

6.2.3 Définition des paramètres

Le paramètre ***recordDataIdentifier (RDI_)*** est défini au **tableau 28**.

Le paramètre ***dataRecord (DREC_)*** est utilisé dans le message de demande WriteDataByIdentifier afin de fournir au serveur (UEV) les valeurs de l'enregistrement de données désigné par l'identificateur d'enregistrement (recordDataIdentifier). Les structures de données sont indiquées au chapitre **8**.

7. Contrôle des impulsions d'essai − Unité fonctionnelle de contrôle des entrées/sorties

Les services disponibles font l'objet d'une description détaillée dans le tableau ci-dessous :

Nom du service	*Description*
InputOutputControlByIdentifier	Le client demande le contrôle d'une entrée/sortie propre au serveur.

Tableau 32 − Unité fonctionnelle de contrôle des entrées/sorties

7.1 Service InputOutputControlByIdentifier

7.1.1 Description des messages

La connexion établie par l'intermédiaire du connecteur frontal permet de contrôler ou de surveiller les impulsions d'essai au moyen d'un testeur prévu à cet effet.

CPR_058 Il est possible de configurer la ligne d'entrée/sortie du signal par l'envoi d'une commande sur la ligne K et en recourant au service InputOutputControlByIdentifier pour sélectionner la fonction d'entrée ou de sortie requise pour la ligne considérée. Les états disponibles sur la ligne sont les suivants :

- Désactivé ;
- speedSignalInput, où la ligne d'entrée/sortie du signal est utilisée pour l'entrée d'un signal de vitesse (signal d'essai) en remplacement du signal de vitesse provenant du détecteur de mouvement ; cette fonction n'est pas disponible en mode CONTRÔLE ;
- realTimeSpeedSignalOutputSensor, où la ligne d'entrée/sortie du signal est utilisée pour la sortie du signal de vitesse du détecteur de mouvement ;
- RTCOutput, où la ligne d'entrée/sortie du signal est utilisée pour la sortie du signal de l'horloge UTC ; cette fonction n'est pas disponible en mode CONTRÔLE.

CPR_059 Pour pouvoir configurer l'état de la ligne, il faut que l'unité embarquée sur le véhicule ait entamé une session de réglage et qu'elle soit exploitée en mode ÉTALONNAGE ou CONTRÔLE. Lorsque l'UEV est en mode ÉTALONNAGE, les quatre états de la ligne peuvent être sélectionnés (désactivé, speedSignalInput, realTimeSpeedSignalOutputSensor et RTCOutput). Lorsque l'UEV est en mode CONTRÔLE, seuls deux états peuvent être sélectionnés (désactivé et realTimeSpeedOutputSensor). Lorsque l'opérateur décide de sortir du mode ÉTALONNAGE ou CONTRÔLE, l'unité embarquée sur le véhicule doit s'assurer que la ligne d'entrée/sortie du signal d'étalonnage est revenue à son état de désactivation (par défaut).

CPR_060 En cas de réception d'impulsions de vitesse sur la ligne d'entrée du signal de vitesse instantanée de l'UEV alors que la ligne d'entrée/sortie du signal est exploitée en mode entrée, cette dernière passera en mode sortie ou sera ramenée à son état de désactivation.

CPR_061 La séquence des opérations est la suivante :

- Établissement d'une liaison d'intercommunication au moyen du service StartCommunication ;
- Lancement d'une session de réglage au moyen du service StartDiagnosticSession et passage en mode ÉTALONNAGE ou CONTRÔLE (l'ordre d'exécution de ces deux opérations est sans importance) ;
- Modification de l'état de la ligne de sortie au moyen du service InputOutputControlByIdentifier.

7.1.2 Structure des messages

CPR_062 La structure des messages associés aux primitives InputOutputControlByIdentifier fait l'objet d'une description détaillée dans les tableaux ci-après.

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	TGT
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	xx	LEN
#5	**ID du service Demande InputOutputControlByIdentifier**	**2F**	**IOCBI**
#6 et #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 ou	controlStatusRecord = [		COR_...
#8 et #9	inputOutputControlParameter − une valeur extraite du **tableau 36**	xx	IOCP_...
	controlState − une valeur extraite du **tableau 37** (voir la remarque ci-après)]	xx	CS_…
#9 ou #10	Total de contrôle	00-FF	CS

Tableau 33 − Message de demande de contrôle des entrées/sorties par identificateur (InputOutputControlByIdentifier)

Remarque : le paramètre controlState n'apparaît que dans certains cas (voir point **7.1.3**).

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	xx	LEN
#5	**ID du service Réponse positive à une demande inputOutputControlByIdentifier**	**6F**	**IOCBIPR**
#6 et #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 ou	controlStatusRecord = [		CSR_
#8 à #9	inputOutputControlParameter (même valeur que l'octet #8 du **tableau 33**)	xx	IOCP_...
	controlState (même valeur que l'octet #9 du **tableau 33**)] (le cas échéant)	xx	CS_…
#9 ou #10	Total de contrôle	00-FF	CS

Tableau 34 − Message de réponse positive à une demande de contrôle des entrées/sorties par identificateur (InputOutputControlByIdentifier)

Octet #	*Nom du paramètre*	*Valeur hex.*	*Mnémonique*
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LEN
#5	**ID du service Réponse négative**	**7F**	**NR**
#6	ID du service Demande inputOutputControlByIdentifier	2F	IOCBI
#7	responseCode =[		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
#8	Total de contrôle	00-FF	CS

Tableau 35 − Message de réponse négative à une demande de contrôle des entrées/sorties par identificateur (InputOutputControlByIdentifier)

7.1.3 Définition des paramètres

CPR_064 Le paramètre ***inputOutputControlParameter (IOCP_)*** est défini dans le tableau ci-dessous.

Valeur hex..	*Description*	*Mnémonique*
00	**ReturnControlToECU (retour de commande à l'ECU)**	RCTECU
	Cette valeur doit indiquer au serveur (UEV) que l'appareil d'essai ne commande plus la ligne d'entrée/sortie du signal.	
01	**ResetToDefault (rétablissement de la configuration par défaut)**	RTD
	Cette valeur doit indiquer au serveur (UEV) qu'il est tenu de ramener la ligne d'entrée/sortie du signal à son état initial.	
03	**ShortTermAdjustment (réglage à court terme)**	STA
	Cette valeur doit indiquer au serveur (UEV) qu'il est tenu de régler la ligne d'entrée/sortie du signal en lui attribuant la valeur comprise dans le paramètre controlState.	

Tableau 36 − Définition des valeurs attribuées au paramètre inputOutputControlParameter

CPR_065 Le paramètre ***controlState***, défini dans le tableau ci-dessous, n'apparaît que lorsque le paramètre inputOutputControlParameter est configuré comme paramètre de réglage à court terme (ShortTermAdjustment).

Mode	*Valeur hex.*	*Description*
Désactivé	00	Ligne d'entrée/sortie désactivée (par défaut)
Activé	01	Ligne d'entrée/sortie d'étalonnage activée en mode speedSignalInput
Activé	02	Ligne d'entrée/sortie d'étalonnage activée en mode realTimeSpeedSignalOutputSensor
Activé	03	Ligne d'entrée/sortie d'étalonnage activée en mode RTCOutput

Tableau 37 − Définition des valeurs attribuées au paramètre controlState

8. Service RoutineControl (TimeAdjustment)

8.1 Description des messages

CPR_065a Le service RoutineControl (TimeAdjustment) permet de déclencher la synchronisation de l'horloge de l'UEV avec l'heure fournie par le récepteur GNSS.

Pour pouvoir exécuter le service RoutineControl (TimeAdjustment), l'UEV doit être en mode ÉTALONNAGE.

Condition préalable : il convient de s'assurer que l'UEV est en mesure de recevoir les messages de positionnement authentifiée envoyés par le récepteur GNSS.

Tant que la remise à l'heure est en cours, l'UEV répondra à une demande de résultats (requestRoutineResults), sous-fonction de la demande RoutineControl, par le paramètre routineInfo = 0 x 78.

Remarque : la remise à l'heure peut prendre un certain temps. L'appareil de diagnostic demande l'état de la remise à l'heure en utilisant la sous-fonction requestRoutineResults.

8.2 Structure des messages

CPR_065b **La structure des messages associés au service RoutineControl (TimeAdjustment) et à ses primitives fait l'objet d'une description détaillée dans les tableaux ci-après.**

Octet #	Nom du paramètre	Valeur hex.	Mnémonique
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	TGT
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	xx	LEN
#5	ID du service Demande RoutineControl	31	RC
#6	routineControlType = [startRoutine]	01	RCTP_STR
#7 et #8	routineIdentifier = [TimeAdjustment]	0100	RI_TA
#9	Total de contrôle	00-FF	CS

Tableau 37a − Message de demande RoutineControl, routine (TimeAdjustment), sous-fonction startRoutine

Octet #	Nom du paramètre	Valeur hex.	Mnémonique
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	xx	LEN
#5	ID du service Réponse positive à une demande RoutineControl	71	RCPR
#6	routineControlType = [startRoutine]	01	RCTP_STR
#7 et #8	routineIdentifier= [TimeAdjustment]	0100	RI_TA
#9	Total de contrôle	00-FF	CS

Tableau 37b − Réponse positive à une demande RoutineControl, routine (TimeAdjustment), sous-fonction startRoutine

Octet #	Nom du paramètre	Valeur hex.	Mnémonique
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	TGT
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	xx	LEN
#5	ID du service Demande RoutineControl	31	RC
#6	routineControlType = [requestRoutineResults]	03	RCTP_RRR
#7 and #8	routineIdentifier= [TimeAdjustment]	0100	RI_TA
#9	Total de contrôle	00-FF	CS

Tableau 37c − Message de demande RoutineControl, routine (TimeAdjustment), sous-fonction requestRoutineResults

Octet #	Nom du paramètre	Valeur hex.	Mnémonique
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	xx	LEN
#5	ID du service Réponse positive à une demande RoutineControl	71	RCPR
#6	routineControlType = [requestRoutineResults]	03	RCTP_RRR
#7 et #8	routineIdentifier= [TimeAdjustment]	0100	RI_TA
#9	routineInfo (voir tableau 37f)	XX	RINF_TA
#10	routineStatusRecord[] = routineStatus#1 (voir tableau 37g)	XX	RS_TA
#11	Total de contrôle	00-FF	CS

Tableau 37d − Message de réponse positive à une demande RoutineControl, routine (TimeAdjustment), sous-fonction requestRoutineResults

Octet #	Nom du paramètre	Valeur hex.	Mnémonique
#1	Octet de structure − adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	TGT
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LEN
#5	ID du service Réponse négative	7F	NR
#6	ID du service Demande inputOutputControlByIdentifier	31	RC
#7	responseCode =[sub-functionNotSupported incorrectMessageLengthOrInvalidFormat conditionsNotCorrect requestOutOfRange]	 12 13 22 31	 SFNS IMLOIF CNC ROOR
#8	Total de contrôle	00-FF	CS

Tableau 37e − Message de réponse négative à une demande RoutineControl, routine (TimeAdjustment)

routineInfo	Valeur hex.	Description
NormalExitWithResultAvailable	61	Le contrôle de routine est achevé ; des résultats supplémentaires sont disponibles.
RoutineExecutionOngoing	78	Le contrôle de routine demandé est en cours d'exécution.

Tableau 37f − RoutineControl, routine (TimeAdjustment), routineInfo

Valeur hex.	Résultats du test	Description
01	**Positif**	**La remise à l'heure a été effectuée avec succès.**
02..0F		**Réservé pour une utilisation future**
10	**Négatif**	**Aucun signal n'a été reçu en provenance du récepteur GNSS.**
11..7F		**Réservé pour une utilisation future**
80..FF		**Propre au fabricant**

Tableau 37g − RoutineControl, routine (TimeAdjustment), routineStatus

9. Structures des enregistrements de données (dataRecords)

La présente section expose en détail :

- Les règles générales applicables aux gammes de paramètres transmises par l'unité embarquée sur le véhicule à l'appareil d'essai ;
- Les structures qui sont utilisées pour les données transférées par l'intermédiaire des services de transmission de données décrits au chapitre 6.

CPR_067 Tous les paramètres indiqués sont pris en charge par l'UEV.

CPR_068 Les données transmises par l'UEV à l'appareil d'essai en réponse à une demande sont du type mesurées (c'est-à-dire la valeur actuelle du paramètre demandé telle que mesurée ou observée par l'UEV).

~~8~~9.1 Gammes des paramètres transmis

CPR_069 Le **tableau 38** définit les gammes utilisées pour déterminer la validité d'un paramètre transmis.

CPR_070 Les valeurs de la gamme « indicateur d'erreur » permettent à l'unité embarquée sur le véhicule d'indiquer immédiatement qu'aucune donnée paramétrique valable n'est actuellement disponible en raison d'une erreur quelconque au niveau du tachygraphe.

CPR_071 Les valeurs de la gamme « non disponible » permettent à l'unité embarquée sur le véhicule de transmettre un message contenant un paramètre qui n'est pas disponible ou pris en charge dans le module considéré. Les valeurs de la gamme « non demandé » permettent la transmission d'un message de commande et indiquent les paramètres pour lesquels le récepteur n'attend pas de réponse.

CPR_072 Lorsque la défaillance d'un composant empêche la transmission de données valables pour un paramètre, il convient d'utiliser l'indicateur d'erreur décrit au **tableau 38** à la place des données de ce paramètre. Toutefois, si les données mesurées ou calculées donnent une valeur valable, mais qui se situe en dehors de la gamme fixée pour ce paramètre, l'indicateur d'erreur ne devrait pas être utilisé. Il convient dans ce cas de transmettre les données en utilisant la valeur paramétrique minimale ou maximale appropriée.

Tableau 1 − Gammes de dataRecords

Nom de la gamme	*1 octet (valeur hex.)*	*2 octets (valeur hex.)*	*4 octets (valeur hex.)*	*ASCII*
Signal valable	00 à FA	0000 à FAFF	00000000 à FAFFFFFF	1 à 254
Indicateur propre au paramètre	FB	FB00 à FBFF	FB000000 à FBFFFFFF	Aucun
Gamme réservée aux futurs bits de l'indicateur	FC à FD	FC00 à FDFF	FC000000 à FDFFFFFF	Aucun
Indicateur d'erreur	FE	FE00 à FEFF	FE000000 à FEFFFFFF	0
Non disponible ou non demandé	FF	FF00 à FFFF	FF000000 à FFFFFFFF	FF

CPR_073 Pour les paramètres codés en ASCII, le caractère ASCII « * » est réservé pour servir de délimiteur.

~~8~~9.2 Structures des enregistrements de données (dataRecords)

Les **tableaux 39** à **42** ci-après exposent en détail les structures à utiliser par l'intermédiaire des services ReadDataByIdentifier et WriteDataByIdentifier.

CPR_074 Le **tableau 39** indique la longueur, la résolution et la gamme opérationnelle de chaque paramètre désigné par son recordDataIdentifier :

Nom du paramètre	*Longueur des données (en octets)*	*Résolution*	*Gamme opérationnelle*
TimeDate	8	Pour plus de précisions, voir le **tableau 40**	
HighResolutionTotalVehicleDistance	4	Gain 5 m/bit, décalage 0 m	0 à +21 055 406 km
Kfactor	2	Gain 0,001 impulsion/m/bit gain, décalage 0	0 à 64,255 impulsion/m
LfactorTyreCircumference	2	Gain 0,125 10^{-3} m /bit, décalage 0	0 à 8,031 m
WvehicleCharacteristicFactor	2	Gain 0,001 impulsion/m/bit, décalage 0	0 à 64,255 impulsion/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Pour plus de précisions, voir le **tableau 41**	
SpeedAuthorised	2	Gain 1/256 km/h/bit, décalage 0	0 à 250,996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Pour plus de précisions, voir le tableau 42	
VIN	17	ASCII	ASCII
SealDataVu	**55**	**Pour plus de précisions, voir le tableau 43**	
ByDefaultLoadType	**1**	**Pour plus de précisions, voir le tableau 44**	
VuSerialNumber	**8**	**Pour plus de précisions, voir le tableau 45**	
SensorSerialNumber	**8**	**Pour plus de précisions, voir le tableau 45**	
SensorGNSSSerialNumber	**8**	**Pour plus de précisions, voir le tableau 45**	
RemoteCommunicationModuleSerialNumber	**8**	**Pour plus de précisions, voir le tableau 45**	
TachographCardsGen1Suppression	**2**	**Pour plus de précisions, voir le tableau 46**	
VehiclePosition	**14**	**Pour plus de précisions, voir le tableau 47**	
CalibrationCountry	**3**	**ASCII**	**NationAlpha tel que défini au sous-appendice 1**

Tableau 2 − Structure des dataRecords

CPR_075 Le **tableau 40** expose en détail les structures des différents octets du paramètre TimeDate :

Octet	*Définition du paramètre*	*Résolution*	*Gamme opérationnelle*
1	Secondes	Gain 0,25 s/bit, décalage 0 s	0 à 59,75 s
2	Minutes	Gain 1 min/bit, décalage 0 min	0 à 59 min
3	Heures	Gain 1 h/bit, décalage 0 h	0 à 23 h
4	Mois	Gain 1 mois/bit, décalage 0 mois	1 à 12 mois
5	Jour	Gain 0,25 jour/bit, décalage 0 jour (voir ci-après la remarque du **tableau 41**)	0,25 à 31,75 jours
6	Année	Gain 1 année/bit, décalage +1985 (voir ci-après la remarque du **tableau 41**)	1985 à 2235
7	Correction locale des minutes	Gain 1 min/bit, décalage -125 min	-59 à + 59 min
8	Correction locale des heures	Gain 1 h/bit, décalage -125 h	- 23 à +23 h

Tableau 3 − Structure détaillée du paramètre TimeDate (valeur de recordDataIdentifier # F90B)

CPR_076 Le tableau 41 expose en détail les structures des différents octets du paramètre NextCalibrationDate :

Octet	*Définition du paramètre*	*Résolution*	*Gamme opérationnelle*
1	Mois	Gain 1 mois/bit, décalage 0 mois	1 à 12 mois
2	Jour	Gain 0,25 jour/bit, décalage 0 jour (voir la remarque ci-après)	0,25 à 31,75 jours
3	Année	Gain 1 année/bit, décalage +1985 (voir la remarque ci-après)	1985 à 2235

Tableau 4 − Structure détaillée du paramètre NextCalibrationDate (valeur de recordDataIdentifier # F922)

Remarque concernant l'utilisation du paramètre « jour » :

1. Une valeur de 0 pour la date est nulle. Les valeurs 1, 2, 3 et 4 servent à désigner le premier jour du mois ; 5, 6, 7 et 8 désignent le deuxième jour du mois, etc.

2. Ce paramètre n'influence ni ne modifie le paramètre « heure » précité.

Remarque concernant l'utilisation ~~de l'octet~~ du paramètre « année » :

Une valeur de 0 pour l'année correspond à l'année 1985, une valeur de 1 à l'année 1986, etc.

CPR_078 Le **tableau 42** expose en détail les structures des différents octets du paramètre VehicleRegistrationNumber :

Octet	*Définition du paramètre*	*Résolution*	*Gamme opérationnelle*
1	Page de code (telle que définie ~~à l'appendice~~ **au sous-appendice** 1)	~~ASCII~~ **Sans objet**	~~01 à 0A~~**VehicleRegistrationNumber**
2-14	Numéro d'immatriculation du véhicule (tel que défini ~~à l'appendice~~ **au sous-appendice** 1)	~~ASCII~~ **Sans objet**	~~ASCII~~**VehicleRegistrationNumber**

Tableau 5 − Structure détaillée du paramètre VehicleRegistrationNumber (valeur de recordDataIdentifier # F97E)

CPR_090 **Le tableau 43 expose en détail les structures des différents octets du paramètre SealDataVu :**

Octet	Définition du paramètre	Résolution	Gamme opérationnelle
1-11	sealRecord1. Structure `SealRecord` (telle que définie au sous-appendice 1)	Sans objet	`SealRecord`
12-22	sealRecord2. Structure `SealRecord` (telle que définie au sous-appendice 1)	Sans objet	`SealRecord`
23-33	sealRecord3. Structure `SealRecord` (telle que définie au sous-appendice 1)	Sans objet	`SealRecord`
34-44	sealRecord4. Structure `SealRecord` (telle que définie au sous-appendice 1)	Sans objet	`SealRecord`
45-55	sealRecord5. Structure `SealRecord` (telle que définie au sous-appendice 1)	Sans objet	`SealRecord`

Tableau 43 − Structure détaillée du paramètre SealDataVu (valeur de recordDataIdentifier # F9D3)

Remarque : s'il existe moins de 5 scellements, la valeur attribuée à EquipmentType dans tous les enregistrements de scellements (sealRecords) inutilisés doit être fixée à 15, c'est-à-dire « inutilisé ».

CPR_091 **Le tableau 44 expose en détail les structures des différents octets du paramètre ByDefaultLoadType :**

Octet	Définition du paramètre	Résolution	Gamme opérationnelle
1	loadType '00'H: type de chargement indéfini '01'H: marchandises '02'H: passagers	Sans objet	'00'H à '02'H

Tableau 44 − Structure détaillée du paramètre ByDefaultLoadType (valeur de recordDataIdentifier # F9D5)

CPR_092 **Le tableau 45 expose en détail les structures des différents octets des paramètres VuSerialNumber, SensorSerialNumber, SensorGNSSSerialNumber et RemoteCommunicationModuleSerialNumber :**

Octet	Définition du paramètre	Résolution	Gamme opérationnelle
1	VuSerialNumber, SensorSerialNumber, SensorGNSSSerialNumber et RemoteCommunicationModuleSerialNumber: structure `ExtendedSerialNumber` telle que définie au sous-appendice 1.	Sans objet	`ExtendedSerialNumber`

Tableau 45 − Structure détaillée des paramètres VuSerialNumber, SensorSerialNumber, SensorGNSSSerialNumber et RemoteCommunicationModuleSerialNumber (valeurs de recordDataIdentifier # F9D4, F9D0, F9D2, F9D1)

CPR_093 **Le tableau 46 expose en détail les structures des différents octets du paramètre TachographCardsGen1Suppression :**

Octet	Définition du paramètre	Résolution	Gamme opérationnelle
1-2	TachographCardsGen1Suppression. Structure du type `TachographCardsGen1Suppression` telle que définie au sous-appendice 1	Sans objet	'0000'H, 'A5E3'H

Tableau 46 − Structure détaillée du paramètre TachographCardsGen1Suppression (valeur de l'identificateur d'enregistrement # F9D6)

CPR_094 **Le tableau 47 expose en détail les structures des différents octets du paramètre VehiclePosition :**

Octet	Définition du paramètre	Résolution	Gamme opérationnelle
1-4	Heure et date auxquelles la position du véhicule a été déterminée	Sans objet	`TimeReal`
5	Précision GNSS	Sans objet	`GNSSAccuracy`
6-11	Position du véhicule	Sans objet	`GeoCoordinates`
12	État d'authentification	Sans objet	`PositionAuthenticationStatus`
13	Pays actuel	Sans objet	`NationNumeric`
14	Région actuelle	Sans objet	`RegionNumeric`

Tableau 47 − Structure détaillée du paramètre VehiclePosition (valeur de recordDataIdentifier # F9D7)

Remarque : après l'actualisation de la position du véhicule, la mise à jour du pays et de la région actuels peut être retardée.

~~Appendice~~ Sous-appendice 9

Homologation

LISTE DES ESSAIS MINIMAUX REQUIS

Table des matières

1. Introduction

1.1 Homologation

L'homologation CE d'un ~~équipement~~ **appareil** de contrôle (ou un composant d'appareil de contrôle) ou d'une carte tachygraphique repose sur :

- Une **certification de sécurité** basée sur les spécifications de critères communs contre une cible de sécurité parfaitement conforme ~~à l'appendice~~ **au sous-appendice** 10 ~~de la~~ **du** présente ~~annexe (à compléter ou à modifier)~~ **appendice** ;
- Une **certification de fonctionnement** exécutée par les autorités compétentes d'un**e** ~~État membre~~ **Partie contractante** et certifiant que l'élément testé satisfait aux exigences d**u**~~e la~~ présente ~~annexe~~ **appendice** sur le plan des fonctions exécutées, de la précision des mesures et des caractéristiques environnementales ;
- Une **certification d'interopérabilité** exécutée par l'organisme compétent chargé de certifier que l'appareil de contrôle (ou la carte tachygraphique) visé et la carte tachygraphique (ou l'appareil de contrôle) requise sont interopérables (voir le chapitre 8 ~~de la~~ **du** présente ~~annexe~~ **appendice**).

Le présent **sous-**appendice précise les essais minimaux que les autorités compétentes d'un**e** ~~État membre~~ **Partie contractante** doivent effectuer dans le cadre des essais de fonctionnement ainsi que les essais minimaux que l'organisme compétent doit effectuer dans le cadre des essais d'interopérabilité. Ni les procédures d'exécution de ces essais ni leur type ne font l'objet d'explications plus détaillées.

Le présent **sous-**appendice ne traite pas des différents aspects de la certification de sécurité. Si certains essais d'homologation sont effectués pendant le processus d'évaluation et de certification de la sécurité, ils n'ont pas à être répétés. En pareil cas, seuls les résultats de ces essais de sécurité sont susceptibles d'être contrôlés. À titre d'information, les exigences qui doivent faire l'objet d'essais (ou sont étroitement liées aux essais qu'il y a lieu d'exécuter) pendant la certification de sécurité sont repérées par un astérisque « * » dans le présent **sous-**appendice.

Les exigences numérotées renvoient ~~au corpus de l'annexe~~ **à l'appendice 1C**, tandis que les autres exigences renvoient aux autres **sous-**appendices (par exemple, PIC_001 correspond à l'exigence PIC_001 ~~de l'appendice~~ **du sous-appendice** 3 « Pictogrammes »).

Le présent appendice traite séparément de l'homologation du capteur de mouvement, de l'unité embarquée sur le véhicule et du dispositif GNSS externe, qui sont considérés comme des composants distincts de l'appareil de contrôle. Chaque composant obtient son propre certificat d'homologation comprenant la liste des autres composants compatibles. L'essai de fonctionnement du capteur de mouvement (ou du dispositif GNSS externe) est effectué simultanément à celui de l'unité embarquée sur le véhicule et vice versa.

L'interopérabilité entre les modèles de capteurs de mouvement (ou les dispositifs GNSS externes) et chaque modèle d'unité embarquée sur le véhicule n'est pas requise. Dans ce cas, l'homologation d'un capteur de mouvement (ou des dispositifs GNSS externes) peut être attribuée en association avec l'homologation de l'unité embarquée sur véhicule et réciproquement.

L'autorité nationale chargée des essais de fonctionnement d'une unité embarquée sur le véhicule ou d'un dispositif GNSS externe doit veiller à ce que le récepteur GNSS ait réussi les essais OSNMA spécifiés dans le présent sous-appendice. Ces essais sont considérés comme faisant partie intégrante des essais de fonctionnement de l'unité embarquée sur le véhicule ou du dispositif GNSS externe.

1.2 Références

Dans le présent s**ous-**appendice, il est fait référence aux documents suivants :

CEI 60068-2-1 : Essais d'environnement − Partie 2-1 : Essais − Essai A : Froid.

CEI 60068-2-2 : Essais d'environnement − Partie 2-2 : Essais − Essai B : Chaleur sèche.

CEI 60068-2-6 : Essais d'environnement − Partie 2-6 : Essais − Essai Fc : Vibrations (sinusoïdales).

CEI 60068-2-14 : Essais d'environnement − Partie 2-14 : Essais − Essai N : Variation de température.

CEI 60068-2-27 : Essais d'environnement − Partie 2-27 : Essais − Essai Ea et guide : Chocs.

CEI 60068-2-30 : Essais d'environnement − Partie 2-30 : Essais − Essai Db : Essai cyclique de chaleur humide (cycle de 12 h + 12 h).

CEI 60068-2-64 : Essais d'environnement − Partie 2-64 : Essais − Essai Fh : Vibrations aléatoires à large bande et guide.

CEI 60068-2-78 : Essais d'environnement − Partie 2-78 : Essais − Essai Cab : Chaleur humide, essai continu.

ISO 16750-3 − Contraintes mécaniques (2012-12).

ISO 16750-4 − Contraintes climatiques (2010-04).

ISO 20653 Véhicules routiers − Degrés de protection (codes IP) − Protection des équipements électriques contre les corps étrangers, l'eau et les contacts.

ISO 10605:2008 Véhicules routiers − Méthodes d'essai des perturbations électriques provenant de décharges électrostatiques, rectificatif technique 1:2010 et AMD 1:2014.

ISO 7637-1:2002 Véhicules routiers − Perturbations électriques par conduction et par couplage − Partie 1 : définitions et généralités, et AMD 1:2008.

ISO 7637-2 Véhicules routiers − Perturbations électriques par conduction et par couplage − Partie 2 : perturbations électriques transitoires par conduction uniquement le long des lignes d'alimentation.

ISO 7637-3 Véhicules routiers − Perturbations électriques par conduction et par couplage − Partie 3 : transmission des perturbations électriques par couplage capacitif ou inductif le long des lignes autres que les lignes d'alimentation.

ISO/CEI 7816-1 Cartes d'identification − Cartes à circuit intégré − Partie 1 : cartes à contacts - Caractéristiques physiques.

ISO/CEI 7816-2 Cartes d'identification − Cartes à circuit intégré − Partie 2 : cartes à contacts - Dimensions et emplacements des contacts.

ISO/CEI 7816-3 Cartes d'identification − Cartes à circuit intégré − Partie 3 : cartes à contacts − Interface électrique et protocoles de transmission.

ISO/CEI 10373-1:2006 Cartes d'identification − Méthodes d'essai − Partie 1 : caractéristiques générales + AMD 1:2012.

ISO/CEI 10373-3:2010 Cartes d'identification − Méthodes d'essai − Partie 3 : cartes à circuit(s) intégré(s) à contacts et dispositifs d'interface assimilés, et rectificatif technique 1:2013.

ISO 16844-3:2004 Véhicules routiers − Systèmes tachygraphes − Partie 3 : interface de capteur de mouvement (avec les unités embarquées sur le véhicule), et rectificatif technique 1:2006.

ISO 16844-4 Véhicules routiers − Systèmes tachygraphes − Partie 4 : interface CAN.

ISO 16844-6 Véhicules routiers − Systèmes tachygraphes − Partie 6 : diagnostic.

ISO 16844-7 Véhicules routiers − Systèmes tachygraphes − Partie 7 : paramètres.

ISO 534 Papier et carton − Détermination de l'épaisseur, de la masse volumique et du volume spécifique.

Règlement ONU nº 10 Prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne la compatibilité électromagnétique (Commission économique pour l'Europe).

RGODP Rapport technique du JRC : Receiver guidelines for OSNMA data processing (Lignes directrices relatives au traitement des données OSNMA par le récepteur)

2. Essais de fonctionnement de l'unité embarquée sur le véhicule

Nº	*Essai*	*Description*	*Exigences connexes*
1	**Examen administratif**		
1.1	Documentation	Exactitude de la documentation	
1.2	Résultats des essais menés par le fabricant	Résultats des essais menés par le fabricant pendant la phase d'intégration ; Démonstrations sur papier.	88, 89,91
2	**Inspection visuelle**		
2.1	Conformité à la documentation		
2.2	Identification/marquage		224 à 226
2.3	Matériaux		219 à 223
2.4	Scellement		398, 401 à 405
2.5	Interfaces externes		
3	**Essais de fonctionnement**		
3.1	Fonctions prévues		**02**, 03, 04, 05, 07, 382,
3.2	Modes de fonctionnement		09 à 11*, ~~132, 133~~ **134, 135**
3.3	Droits d'accès aux fonctions et aux données		12* 13*, 382, 383, 386 à 389
3.4	Contrôle de l'insertion et du retrait des cartes		15, 16, 17, 18, 19*, 20*, ~~132~~ **134**
3.5	Mesure de la vitesse**, de la position** et de la distance parcourue		21 à 3~~71~~
3.6	Mesure du temps (essai exécuté à 20 °C)		38 à 43
3.7	Suivi des activités du conducteur		44 à 53, ~~132~~ **134**
3.8	Suivi de la situation de conduite		54, 55, ~~132~~ **1324**
3.9	**Saisies ~~manuelles~~ par le conducteur**		56 à 62**c**
3.10	Gestion des verrouillages d'entreprise		63 à 68
3.11	Suivi des activités de contrôle		69, 70
3.12	Détection d'événements et/ou d'anomalies		71 à 88**a**, ~~132~~ **1324**
3.13	Données d'identification de l'équipement		93*, 94*, 97, 100
3.14	Données concernant l'insertion et le retrait d'une carte de conducteur **ou d'atelier**		102* à 104*
3.15	Données relatives à l'activité du conducteur		105* à 107*
3.16	Données relatives aux lieux et aux positions		108* à 112*
3.17	Kilométrage		113* à 115*
3.18	Données relatives à la vitesse du véhicule		116*
3.19	Données relatives aux événements		117*
3.20	Données relatives aux anomalies		118*
3.21	Données d'étalonnage		119* à 121*
3.22	Données relatives à la remise à l'heure		124*, 125*

N°	*Essai*	*Description*	*Exigences connexes*
3.23	Données relatives aux activités de contrôle		126*, 127*
3.24	Données relatives aux verrouillages d'entreprise		128*
3.25	Données relatives au téléchargement		129*
3.26	Données relatives aux conditions particulières		130*, 131*
3.27	**Données relatives aux cartes tachygraphiques**		**132*, 133***
3.28	**Passages de frontières**		**133a* à 133d***
3.29	**Opérations de chargement/déchargement**		**133e* à 133i***
3.30	**Carte numérique**		**133j* à 133s***
3.**31**~~27~~	Enregistrement et stockage sur les cartes tachygraphiques		~~134,135,~~ 136, 137, **138***, 139*, 141*, 142, 143, 144, 145, 146*, 147*, **147a*, 147b*** 148*, **149, 150, 150a**
3.**32**~~28~~	Affichage		90,~~ 132~~ **134**, ~~149~~ **151** à ~~166~~ **168,** PIC_001, DIS_001
3.**33**~~29~~	Impression		90, ~~132~~ **134,** ~~167~~ **169** à ~~179~~ **181**, PIC_001, PRT_001 à PRT_014
3.3**4**~~0~~	Avertissement		~~132,~~ ~~180~~ **134**, **182** à ~~189~~ **191**, PIC_001
3.3**5**~~1~~	Téléchargement de données vers des supports externes		90, ~~132,~~ ~~190~~ **134**, **192** à ~~194~~ **196**
3.3**6**~~2~~	Communication à distance pour les contrôles routiers ciblés		~~195~~ **197** à ~~197~~ **199**
3.3**7**~~3~~	**Échanges de** ~~D~~données ~~transmises à~~ avec d'autres dispositifs externes		~~198, 199~~ **200, 201**
3.3**8**~~4~~	Étalonnage		202 à 206*, 383, 384, 386 à 391
3.3**9**~~5~~	Contrôles routiers d'étalonnage		207 à 209
3.**40**~~36~~	Remise à l'heure		210 à 212*
3.41	**Surveillance des passages de frontières**		**226a à 226c**
3.42	**Mise à jour logicielle**		**226d à 226f**
3.**43**~~37~~	Absence d'interférence des fonctions supplémentaires		06, 425
3.**44**~~38~~	Interface du capteur de mouvement		02, 122
3.**45**~~39~~	Dispositif GNSS externe		03, 123
3.4**6**~~0~~	Vérifier que l'UEV détecte, enregistre et stocke les événements et/ou anomalies définis par le fabricant de l'UEV lorsqu'un capteur de mouvement couplé réagit à des champs magnétiques qui perturbent la détection des mouvements du véhicule.		217
3.4**7**~~1~~	Suite cryptographique et paramètres de domaine normalisés		CSM_48, CSM_50

N°	*Essai*	*Description*	*Exigences connexes*
4	**Essais environnementaux**		
4.1	Température	S'assurer du fonctionnement de l'unité embarquée sur le véhicule en procédant aux essais suivants : Essai conforme à la norme ISO 16750-4, chapitre 5.1.1.2 : Essai de fonctionnement à basse température (72 h à -20 °C) Cet essai satisfait à la norme CEI 60068-2-1 : Essais d'environnement − Partie 2-1 : Essais − Essai A : Froid. Essai conforme à la norme ISO 16750-4, chapitre 5.1.2.2 : Essai de fonctionnement à haute température (72 h à 70 °C) Cet essai satisfait à la norme CEI 60068-2-2 : Essais d'environnement − Partie 2-2 : Essais − Essai B : Chaleur sèche. Essai conforme à la norme ISO 16750-4, chapitre 5.3.2 : Variation rapide de température avec durée de transition spécifiée (-20 °C/70 °C, 20 cycles, temps d'exposition 2 h à chaque température) Un nombre limité d'essais (parmi ceux définis à la section 3 de ce tableau) peuvent être effectués aux températures minimale et maximale indiquées ainsi que pendant les cycles de variation de la température.	213
4.2	Humidité	Vérifier que l'unité embarquée sur le véhicule est capable de résister à un cycle de chaleur humide (essai de résistance à la chaleur) en exécutant l'essai CEI 600068-2-30 (essai Db), qui comporte six cycles de 24 heures, la température variant de +25 °C à +55 °C et le taux d'humidité relative atteignant 97 % à +25 °C et 93 % à +55 °C	214

Nº	*Essai*	*Description*	*Exigences connexes*
4.3	Mécanique	1. Vibrations sinusoïdales : Vérifier que l'unité embarquée sur le véhicule est capable de résister à des vibrations sinusoïdales possédant les caractéristiques suivantes : déplacement constant compris entre 5 et 11 Hz : 10 mm max. accélération constante comprise entre 11 et 300 Hz : 5 g L'essai CEI 60068-2-6 (essai Fc) permet de vérifier le respect de cette exigence. La durée minimale de cet essai s'élève à 3 x 12 heures (12 heures par essieu). La norme ISO n'impose pas d'essai de vibrations sinusoïdales aux dispositifs situés dans la cabine découplée du véhicule. 2. Vibrations aléatoires : Essai conforme à la norme ISO 16750-3 : chapitre 4.1.2.8 : Essai VIII : Véhicule commercial, cabine de véhicule découplée Essai de vibrations aléatoires, 10...2 000 Hz, RMS vertical 21.3 m/s², RMS longitudinal 11.8 m/s², RMS latéral 13.1 m/s², 3 essieux, 32 h par essieu, avec un cycle de température -20...70 °C Cet essai satisfait à la norme CEI 60068-2-64 : Essais d'environnement − Partie 2-64 : Essais − Essai Fh : Vibrations à large bande et guide 3. Chocs : Choc mécanique d'un demi-sinus de 3 g conformément à la norme ISO 16750 Il convient d'exécuter les essais décrits ci-dessus sur des échantillons distincts du type d'équipement testé.	219
4.4	Protection contre l'eau et les corps étrangers	Essai conforme à la norme ISO 20653 : Véhicules routiers − Degrés de protection (codes IP) − Protection des équipements électriques contre les corps étrangers, l'eau et les contacts (paramètres inchangés) ; valeur minimale IP 40	220, 221
4.5	Protection contre les surtensions	Vérifier que l'unité embarquée sur le véhicule est capable de supporter une tension d'alimentation de : Versions 24 V : 34 V à +40 °C 1 heure Versions 12 V : 17 V à +40 °C 1 heure (ISO 16750-2)	216
4.6	Protection contre les inversions de polarité	Vérifier que l'unité embarquée sur le véhicule est capable de supporter une inversion de polarité au niveau de son alimentation électrique (ISO 16750-2)	216
4.7	Protection contre les courts-circuits	Vérifier que les signaux d'entrée et de sortie sont protégés contre les courts-circuits au niveau de l'alimentation électrique et de la mise à terre (ISO 16750-2)	216
5	**Essais de compatibilité électromagnétique**		
5.1	Émissions rayonnées et susceptibilité	Conformément au Règlement ONU nº 10	218

N°	*Essai*	*Description*	*Exigences connexes*
5.2	Décharge électrostatique	Conformément à la norme ISO 10605:2008, au rectificatif technique 1:2010 et à l'amendement 1:2014 : +/- 4 kV pour le contact et +/- 8 kV pour la décharge d'air	218
5.3	Susceptibilité transitoire par conduction au niveau de l'alimentation	Pour les versions 24V : conformité avec la norme ISO 7637-2 et le Règlement ONU n° 10, révision 3 : impulsion 1a : Vs = -450V Ri = 50 ohms impulsion 2a : Vs = +37V Ri = 2 ohms impulsion 2b : Vs = +20V Ri = 0,05 ohms impulsion 3a : Vs = -150V Ri = 50 ohms impulsion 3b : Vs = +150V Ri = 50 ohms impulsion 4 : Vs = -16V Va = -12V t6 = 100 ms impulsion 5 : Vs = +120V Ri = 2,2 ohms td = 250 ms Pour les versions 12V : conformité avec la norme ISO 7637-1 et le Règlement ONU n° 10, révision 3 : impulsion 1 : Vs = -75 V Ri = 10 ohms impulsion 2a : Vs = +37 V Ri = 2 ohms impulsion 2b : Vs = +10 V Ri = 0,05 ohms impulsion 3a : Vs = -112 V Ri = 50 ohms impulsion 3b : Vs = +75V Ri = 50 ohms impulsion 4 : Vs = -6V Va = -5V t6 = 15ms impulsion 5 : Vs = +65V Ri = 3 ohms td = 100 ms L'impulsion 5 ne sera mise à l'essai que pour les unités embarquées à installer sur des véhicules dépourvus de dispositif commun de protection externe contre la perte de charge. Pour la proposition concernant la perte de charge, consulter la norme ISO 16750-2, 4e édition, chapitre 4.6.4.	218

3. Essais de fonctionnement du capteur de mouvement

N°	*Essai*	*Description*	*Exigences connexes*
1.	**Examen administratif**		
1.1	Documentation	Exactitude de la documentation	
2.	**Inspection visuelle**		
2.1.	Conformité à la documentation		
2.2.	Identification/marquage		225, 226,
2.3	Matériaux		219 à 223
2.4.	Scellement		398, 401 à 405
3.	**Essais de fonctionnement**		
3.1	Données d'identification du capteur		95 à 97*
3.2	Couplage capteur de mouvement − unité embarquée sur le véhicule		122*, 204
3.3	Détection de mouvement Précision de la mesure du mouvement		 30 à 35
3.4	Interface de l'unité embarquée sur le véhicule		02

Nº	*Essai*	*Description*	*Exigences connexes*
3.5		Vérifier que le capteur de mouvement est immunisé contre les champs magnétiques constants. Autrement, vérifier que le capteur de mouvement réagit aux champs magnétiques constants qui perturbent la détection des mouvements du véhicule, de sorte qu'une UEV connectée puisse détecter, enregistrer et stocker les anomalies du capteur.	217
4.	**Essais environnementaux**		
4.1	Température de fonctionnement	S'assurer du fonctionnement du capteur (tel que défini pour l'essai nº 3.3) dans la plage de température [-40 ºC ; +135 ºC] en exécutant les essais suivants : Essai Bd prévu par la norme CEI 60068-2-1, en appliquant une durée d'essai de 96 heures à la température minimale To_{min} Essai Bd prévu par la norme CEI 60068-2-2, en appliquant une durée d'essai de 96 heures à la température maximale To_{max} Essai conforme à la norme ISO 16750-4 : chapitre 5.1.1.2 : Essai de fonctionnement à basse température (24 h à -40 °C) Cet essai satisfait à la norme CEI 60068-2-1 : Essais d'environnement − Partie 2-1 : Essais − Essai A : Froid et CEI 68-2-2 : Essai Bd, en appliquant une durée d'essai de 96 heures à la température minimale de -40 ºC. Essai conforme à la norme ISO 16750-4 : chapitre 5.1.2.2 : Essai de fonctionnement à haute température (96 h à 135 °C) Cet essai satisfait à la norme CEI 60068-2-2 : Essais d'environnement − Partie 2 : Essais − Essai B : Chaleur sèche.	213
4.2	Cycles de température	Essai conforme à la norme ISO 16750-4 : chapitre 5.3.2 : Variation rapide de température avec durée de transition spécifiée (-40 °C/135 °C, 20 cycles, temps d'exposition de 30 min à chaque température) CEI 60068-2-14 Essais d'environnement − Partie 2-14 : Essais − Essai N : Variation de température	213
4.3	Cycles humides	S'assurer du fonctionnement du capteur (tel que défini pour l'essai nº 3.3) en procédant à l'essai CEI 600068-2-30 (essai Db) qui comporte six cycles de 24 heures, la température variant de +25 ºC à +55 ºC et le taux d'humidité relative atteignant 97 % à +25 ºC et 93 % à +55 ºC	214
4.4	Vibration	Conformément à la norme ISO 16750-3 : chapitre 4.1.2.6 : Essai VI : Véhicule commercial, moteur, engrenage Essai de vibration en mode mixte comprenant : a) un essai de vibrations sinusoïdales, 20...520 Hz, 11.4 ... 120 m/s², <= 0,5 oct/min b) un essai de vibrations aléatoires, 10...2 000 Hz, RMS 177 m/s² 94 h par essieu, avec un cycle de température -20...70 °C Cet essai satisfait à la norme CEI 60068-2-80 : Essais d'environnement − Partie 2-80 : Essais − Essai Fi : Vibration − Mode mixte	219

N°	*Essai*	*Description*	*Exigences connexes*
4.5	Chocs mécaniques	Conformément à la norme ISO 16750-3 : chapitre 4.2.3 : Essai VI − Essai pour dispositifs dans ou sur l'engrenage Choc demi-sinusoïdal, accélération à convenir dans une plage de 3 000...15 000 m/s², durée de l'impulsion à convenir, cependant <1 ms, nombre de chocs à convenir Cet essai satisfait à la norme CEI 60068-2-27 : Essais d'environnement − Partie 2 : Essais − Essai Ea et guide : Chocs	219
4.6	Protection contre l'eau et les corps étrangers	Essai conforme à la norme ISO 20653 : Véhicules routiers − Degrés de protection (codes IP) − Protection des équipements électriques contre les corps étrangers, l'eau et les contacts (paramètres inchangés) (Valeur cible IP 64)	220, 221
4.7	Protection contre les inversions de polarité	Vérifier que le capteur de mouvement est capable de supporter une inversion de polarité au niveau de son alimentation électrique	216
4.8	Protection contre les courts-circuits	Vérifier que les signaux d'entrée et de sortie sont protégés contre les courts-circuits au niveau de l'alimentation électrique et de la mise à terre	216
5.	**Essais de compatibilité électromagnétique**		
5.1	Émissions rayonnées et susceptibilité	Vérifier la conformité avec le Règlement ONU n° 10	218
5.2	Décharge électrostatique	Conformément à la norme ISO 10605:2008, au rectificatif technique 1:2010 et à l'amendement 1:2014 : +/-4 kV pour le contact et +/-8 kV pour la décharge d'air	218
5.3	Susceptibilité transitoire par conduction au niveau des lignes de transmission de données	Pour les versions 24V : conformité avec la norme ISO 7637-2 et le Règlement ONU n° 10, révision 3 : impulsion 1a : Vs = -450 V Ri = 50 ohms impulsion 2a : Vs = +37 V Ri = 2 ohms impulsion 2b : Vs = +20 V Ri = 0,05 ohms impulsion 3a : Vs = -150 V Ri = 50 ohms impulsion 3b : Vs = +150 V Ri = 50 ohms impulsion 4 : Vs = -16 V Va = -12V t6 = 100 ms impulsion 5 : Vs = +120 V Ri = 2,2 ohms td = 250 ms Pour les versions 12V : conformité avec la norme ISO 7637-1 et le Règlement ONU n° 10, révision 3 : impulsion 1 : Vs = -75 V Ri = 10 ohms impulsion 2a : Vs = +37 V Ri = 2 ohms impulsion 2b : Vs = +10 V Ri = 0,05 ohms impulsion 3a : Vs = -112 V Ri = 50 ohms impulsion 3b : Vs = +75 V Ri = 50 ohms impulsion 4 : Vs = -6V Va = -5V t6 = 15 ms impulsion 5 : Vs = +65 V Ri = 3 ohms td = 100 ms L'impulsion 5 ne sera mise à l'essai que pour les unités embarquées à installer sur des véhicules dépourvus de dispositif commun de protection externe contre la perte de charge. Pour la proposition concernant la perte de charge, consulter la norme ISO 16750-2, 4e édition, chapitre 4.6.4.	218

4. Essais de fonctionnement des cartes tachygraphiques

Les essais prévus au présent chapitre 4, à savoir

nº 5 « Essais de protocole » ;

nº 6 « Structure de la carte » ; et

nº 7 « Essais de fonctionnement » ;

peuvent être effectués par l'évaluateur ou le certificateur pendant la procédure de certification de sécurité selon les Critères communs (CC) applicables au module du circuit intégré.

Les essais numéro 2.3 et 4.2 sont identiques. Il s'agit des essais mécaniques de l'ensemble constitué du corps de la carte et du module du circuit intégré. En cas de modification de l'un de ces composants (corps de la carte ou module du circuit intégré), ces essais sont nécessaires.

Nº	**Essai**	**Description**	**Exigences connexes**
1.	**Examen administratif**		
1.1	Documentation	Exactitude de la documentation	
2	**Corps de la carte**		
2.1	Conception imprimée	S'assurer de la conformité et de la qualité d'impression de toutes les fonctions de protection et données visibles. [Indicatif] ~~Annexe~~ **Appendice** 1C, chapitre 4.1 « Données visibles », exigence 227) Le recto de la carte doit comporter : les mots « carte de conducteur », « carte de contrôleur », « carte d'atelier » ou « carte d'entreprise » imprimés en majuscules dans la ou les langues officielles de ~~l'État membre~~ **la Partie contractante** qui a délivré la carte, selon le type de carte. [Nom de ~~l'État membre~~ **la Partie contractante**] ~~Annexe~~ **Appendice** 1C, chapitre 4.1 « Données visibles », exigence 228) Le recto de la carte doit comporter : le nom de ~~l'État membre~~ **la Partie contractante** qui a délivré la carte (facultatif). [Signature] ~~Annexe~~ **Appendice** 1C, chapitre 4.1 « Données visibles », exigence 229) Le recto de la carte doit comporter : le signe distinctif de ~~l'État membre~~ **la Partie contractante** qui a délivré la carte, imprimé en négatif dans un rectangle bleu et entouré de 12 étoiles jaunes. [Énumération] ~~Annexe~~ **Appendice** 1C, chapitre 4.1 « Données visibles », exigence 232) Le verso de la carte doit comporter : une légende des numéros indiqués au recto.	227 à 229, 232, 234 à 236

		[Couleur] ~~Annexe~~ **Appendice** 1C, chapitre 4.1 « Données visibles », exigence 234) Les cartes tachygraphiques doivent être imprimées sur les fonds de couleur suivants : - carte du conducteur : blanche ; - carte d'atelier : rouge ; - carte de contrôle : bleu ; - carte d'entreprise : jaune. [Sécurité] ~~Annexe~~ **Appendice** 1C, chapitre 4.1 « Données visibles », exigence 235) Les cartes tachygraphiques présentent au moins les éléments de protection suivants contre la contrefaçon et la manipulation du corps de la carte : - impression de fond de sécurité finement guillochée et irisée ; - au moins une ligne bicolore micro-imprimée. [Marquage] ~~Annexe~~ **Appendice** 1C, chapitre 4.1 « Données visibles », exigence 236) Les ~~États membres~~ **Parties contractantes** peuvent ajouter des couleurs ou des inscriptions, tels que des symboles nationaux et des éléments de sécurité. [Marque d'homologation] Les cartes tachygraphiques portent une marque d'homologation. La marque d'homologation est composée : - d'un rectangle à l'intérieur duquel est placée la lettre « e », suivie du numéro distinctif ou de la lettre distinctive du pays qui a délivré l'homologation ; - d'un numéro d'homologation correspondant au numéro du certificat d'homologation établi pour une carte tachygraphique, placé dans une position quelconque à proximité du rectangle.	
2.2	Essais mécaniques	[Taille de la carte] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810 Cartes d'identification − Caractéristiques physiques [5] Dimension de la carte [5.1] Taille de la carte [5.1.1] Dimensions et tolérances de la carte Type de carte ID-1 Carte inutilisée [Bords de la carte] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810 Cartes d'identification − Caractéristiques physiques [5] Dimension de la carte [5.1] Taille de la carte [5.1.2] Bords de la carte	240, 243 ISO/CEI 7810

		[Construction de la carte] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810 Cartes d'identification − Caractéristiques physiques [6] Construction de la carte	
		[Matériaux des cartes] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810 Cartes d'identification − Caractéristiques physiques [7] Matériaux des cartes	
		[Rigidité à la flexion] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810 Cartes d'identification − Caractéristiques physiques [8] Caractéristiques de la carte [8.1] Rigidité à la flexion	
		[Toxicité] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810 Cartes d'identification − Caractéristiques physiques [8] Caractéristiques de la carte [8.3] Toxicité	
		[Résistance aux agents chimiques] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810 Cartes d'identification − Caractéristiques physiques [8] Caractéristiques de la carte [8.4] Résistance aux agents chimiques	
		[Stabilité de la carte] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810 Cartes d'identification − Caractéristiques physiques [8] Caractéristiques de la carte [8.5] Stabilité des dimensions de la carte et déformations à la température et à l'humidité	
		[Lumière] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810 Cartes d'identification − Caractéristiques physiques [8] Caractéristiques de la carte [8.6] Lumière	
		[Durabilité] ~~Annexe~~ **Appendice** 1C, chapitre 4.4 « Spécifications environnementales et électriques », exigence 241) Les cartes tachygraphiques doivent pouvoir fonctionner correctement pendant une période de cinq ans si elles sont utilisées conformément aux spécifications environnementales et électriques.	

		[Résistance au pelage] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810 Cartes d'identification − Caractéristiques physiques [8] Caractéristiques de la carte [8.8] Résistance au pelage	
		[Adhésion ou blocage] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810 Cartes d'identification − Caractéristiques physiques [8] Caractéristiques de la carte [8.9] Adhésion ou blocage	
		[Déformation] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810 Cartes d'identification − Caractéristiques physiques [8] Caractéristiques de la carte [8.11] Déformation globale de la carte	
		[Résistance à la chaleur] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810 Cartes d'identification − Caractéristiques physiques [8] Caractéristiques de la carte [8.12] Résistance à la chaleur	
		[Déformations de surface] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810 Cartes d'identification − Caractéristiques physiques [8] Caractéristiques de la carte [8.13] Déformations de surface	
		[Contamination] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810 Cartes d'identification − Caractéristiques physiques [8] Caractéristiques de la carte [8.14] Contamination et interaction entre les composants de la carte	
2.3	Essais mécaniques avec module de circuit intégré	[Flexion] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810:2003/AMD 1:2009 Cartes d'identification − Caractéristiques physiques − Amendement 1:2009 Critères pour les cartes contenant des circuits intégrés [9.2] Contraintes de flexion dynamique Nombre total de cycles de flexion : 4 000.	ISO/CEI 7810
		[Torsion] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810:2003/AMD 1:2009 Cartes d'identification − Caractéristiques physiques − Amendement 1:2009 Critères pour les cartes contenant des circuits intégrés [9.3] Contraintes de torsion dynamique Nombre total de cycles de torsion : 4 000.	

3	**Module**		
3.1	Module	Le module désigne l'encapsulation du circuit et la plaque de contact. [Profil de surface] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7816-1:2011 Cartes d'identification − Cartes à circuit intégré − Partie 1 : Cartes avec contacts − Caractéristiques physiques [4.2] Profil de surface des contacts [Résistance mécanique] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7816-1:2011 Cartes d'identification − Cartes à circuit intégré − Partie 1 : Cartes avec contacts − Caractéristiques physiques [4.3] Résistance mécanique (d'une carte et des contacts) [Résistance électrique] Les cartes tachygraphiques doivent satisfaire à la norme SO/CEI 7816-1:2011 Cartes d'identification − Cartes à circuit intégré − Partie 1: Cartes avec contacts − Caractéristiques physiques [4.4] Résistance électrique (des contacts) [Dimension] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7816-2:2007 Cartes d'identification − Cartes à circuit intégré − Partie 2 Cartes avec contacts − Dimensions et emplacements des contacts [3] Dimension des contacts [Emplacement] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7816-2:2007 Cartes d'identification − Cartes à circuit intégré − Partie 2 Cartes avec contacts − Dimensions et emplacements des contacts [4] Nombre et emplacements des contacts Si les modules possèdent six contacts, les contacts 'C4' et 'C8' ne sont pas soumis à cette exigence d'essai.	ISO/CEI 7816
4	**Circuit**		
4.1	Circuit	[Température de fonctionnement] Le circuit de la carte tachygraphique fonctionne dans une plage de température ambiante de -25 °C à + 85 °C.	241 à 244 Règlement ONU nº 0 ISO/CEI 7810 ISO/CEI 10373

		[Température et humidité] ~~Annexe~~ **Appendice** 1C, chapitre 4.4 « Spécifications environnementales et électriques », exigence 241) Les cartes tachygraphiques doivent pouvoir fonctionner correctement dans toutes les conditions climatiques normalement observées sur le territoire ~~communautaire~~ **des Parties contractantes**, et au minimum dans une gamme de température comprise entre -25 °C et +70 °C, avec des pointes occasionnelles à +85 °C, « occasionnelles » signifiant d'une durée inférieure ou égale à 4 heures et survenant au maximum à 100 reprises au cours de la durée de vie de la carte. Les cartes tachygraphiques sont exposées en plusieurs étapes consécutives aux températures et hygrométries suivantes pendant une période donnée. Après chaque étape, le fonctionnement électrique des cartes tachygraphiques fait l'objet d'essais. 1. Température de -20 °C pendant 2 heures. 2. Température de +/-0 °C pendant 2 heures. 3. Température de +20 °C, 50 % HR, pendant 2 heures. 4. Température de +50 °C, 50 % HR, pendant 2 heures. 5. Température de +70 °C, 50 % HR, pendant 2 heures. La température augmente par intermittence à +85 °C, 50 % HR, pendant 60 min. 6. Température de +70 °C, 85 % HR, pendant 2 heures. La température augmente par intermittence à +85 °C, 85 % HR, pendant 30 min. [Humidité] ~~Annexe~~ **Appendice** 1C, chapitre 4.4 « Spécifications environnementales et électriques », exigence 242) Les cartes tachygraphiques doivent pouvoir fonctionner correctement dans une gamme d'humidité comprise entre 10 % et 90 %. [Compatibilité électromagnétique − CEM] ~~Annexe~~ **Appendice** 1C, chapitre 4.4 « Spécifications environnementales et électriques », exigence 244) En fonctionnement, les cartes tachygraphiques doivent satisfaire au Règlement ONU nº 10 relatif à la compatibilité électromagnétique. [Électricité statique] ~~Annexe~~ **Appendice** 1C, chapitre 4.4 « Spécifications environnementales et électriques », exigence 244) En fonctionnement, les cartes tachygraphiques doivent être protégées contre les décharges électrostatiques. Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810:2003/AMD 1:2009 Cartes d'identification − Caractéristiques physiques − Amendement 1 : Critères pour les cartes contenant des circuits intégrés [9.4] Électricité statique [9.4.1] Cartes à circuit intégré avec contacts Tension d'essai : 4 000 V.	

		[Rayons X] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810:2003/AMD 1:2009 Cartes d'identification − Caractéristiques physiques − Amendement 1 : Critères pour les cartes contenant des circuits intégrés [9.1] Rayons X	
		[Lumière ultraviolette] ISO/CEI 10373-1:2006 Cartes d'identification − Méthodes d'essai − Partie 1 : Caractéristiques générales [5.11] Lumière ultraviolette	
		[3 roues] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 10373-1:2006/AMD 1:2012 Cartes d'identification − Méthodes d'essai − Partie 1 : Caractéristiques générales − Amendement 1 [5.22] CCI − Résistance mécanique : Essai 3 roues pour les cartes à circuit intégré avec contacts	
		[Enveloppe] Les cartes tachygraphiques doivent satisfaire à la norme MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8 : Essai de robustesse de l'enveloppe [13.2.1.32] TM-422 : Fiabilité mécanique : Essai d'enveloppe	
4.2	Essais mécaniques avec module de circuit intégré dans le corps de la carte -> identique au point 2.3	[Flexion] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810:2003/AMD 1:2009 Cartes d'identification − Caractéristiques physiques − Amendement 1:2009 Critères pour les cartes contenant des circuits intégrés [9.2] Contraintes de flexion dynamique Nombre total de cycles de flexion : 4 000.	ISO/CEI 7810
		[Torsion] Les cartes tachygraphiques doivent satisfaire à la norme ISO/CEI 7810:2003/AMD 1:2009 Cartes d'identification − Caractéristiques physiques − Amendement 1:2009 Critères pour les cartes contenant des circuits intégrés [9.3] Contraintes de torsion dynamique Nombre total de cycles de torsion : 4 000.	
5	**Essais de protocole**		
5.1	ATR	S'assurer de la conformité de l'ATR	ISO/CEI 7816-3 TCS_14, TCS_17, TCS_18
5.2	T = 0	S'assurer de la conformité du protocole T = 0	ISO/CEI 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	S'assurer de la conformité de la commande PTS en passant de T = 0 à T = 1	ISO/CEI 7816-3 TCS_12, TCS_19, TCS_20, TCS_21

5.4	T = 1	S'assurer de la conformité du protocole T = 1	ISO/CEI 7816-3 TCS_11, TCS_13, TCS_16
6	**Structure de la carte**		
6.1		Vérifier la conformité de la structure des fichiers enregistrés sur la carte en contrôlant la présence des fichiers obligatoires ainsi que leurs conditions d'accès	TCS_22 à TCS_28 TCS_140 à TCS_179
7	**Essais de fonctionnement**		
7.1	Fonctionnement normal	Tester au moins une fois chaque usage autorisé de chaque commande (par exemple, essayer la commande UPDATE BINARY avec les octets CLA = '00', CLA = '0C' et avec différents paramètres P1, P2 et Lc). Vérifier que les opérations voulues ont été correctement exécutées sur la carte (par exemple, en extrayant le fichier sur lequel la commande considérée a été exécutée)	TCS_29 à TCS_139
7.2	Messages d'erreur	Tester une fois au moins chaque message d'erreur (comme indiqué ~~à l'appendice~~ **au sous-appendice** 2) pour chaque commande Tester une fois au moins chaque erreur générique (à l'exception des erreurs d'intégrité '**6400**' contrôlées dans le cadre de la certification de sécurité).	
7.3	Suite cryptographique et paramètres de domaine normalisés		CSM_48, CSM_50
8	**Personnalisation**		
8.1	Personnalisation visuelle	~~Annexe~~ **Appendice** 1C, chapitre 4.1 « Données visibles », exigence 230) Le recto de la carte doit comporter : des indications particulières concernant la carte délivrée. ~~Annexe~~ **Appendice** 1C, chapitre 4.1 « Données visibles », exigence 231) Le recto de la carte doit comporter : les dates sont indiquées sous la forme « jj/mm/aaaa » ou « jj.mm.aaaa » (jour, mois, année). ~~Annexe~~ **Appendice** 1C, chapitre 4.1 « Données visibles », exigence 235) Les cartes tachygraphiques présentent au moins les éléments de protection suivants contre la contrefaçon et la manipulation du corps de la carte : - chevauchement de l'impression de fond de sécurité et de la photographie.	230, 231, 235

5. Essais du dispositif GNSS externe

Nº	Essai	Description	Exigences connexes
1.	**Examen administratif**		
1.1	Documentation	Exactitude de la documentation	
2.	**Inspection visuelle d'un dispositif GNSS externe**		
2.1.	Conformité avec la documentation		
2.2.	Identification/marquage		224 à 226
2.3	Matériaux		219 à 223
3.	**Essais de fonctionnement**		
3.1	Données d'identification du capteur		**98, 99**
3.2	Couplage module GNSS externe − unité embarquée sur le véhicule		**123, 205**
3.3	Position GNSS		**36, 37**
3.4	Interface de l'unité embarquée sur le véhicule lorsque le récepteur GNSS est externe à l'unité embarquée sur le véhicule		03
3.5	Suite cryptographique et paramètres de domaine normalisés		CSM_48, CSM_50
4.	**Essais environnementaux**		
4.1	Température	S'assurer du fonctionnement du dispositif en procédant aux essais suivants : Essai conforme à la norme ISO 16750-4, chapitre 5.1.1.2 : Essai de fonctionnement à basse température (72 h à -20 °C) Cet essai satisfait à la norme CEI 60068-2-1 : Essais d'environnement − Partie 2-1 : Essais − Essai A : Froid. Essai conforme à la norme ISO 16750-4 : chapitre 5.1.2.2 : Essai de fonctionnement à haute température (72 h à 70 °C) Cet essai satisfait à la norme CEI 60068-2-2 : Essais d'environnement − Partie 2 : Essais - Essai B : Chaleur sèche. Essai conforme à la norme ISO 16750-4 : chapitre 5.3.2 : Variation rapide de température avec durée de transition spécifiée (-20 °C/70 °C, 20 cycles, temps d'exposition de 1 h à chaque température) Un nombre limité d'essais (parmi ceux définis à la section 3 de ce tableau) peuvent être effectués aux températures minimale et maximale indiquées ainsi que pendant les cycles de variation de la température.	213
4.2	Humidité	Vérifier que l'unité embarquée sur le véhicule est capable de résister à un cycle de chaleur humide (essai de résistance à la chaleur) en exécutant l'essai CEI 60068-2-30 (essai Db), qui comporte six cycles de 24 heures, la température variant de +25 °C à +55 °C et le taux d'humidité relative atteignant 97 % à +25 °C et 93 % à +55 °C	214

4.3	Mécanique	Vibrations sinusoïdales : S'assurer que l'unité embarquée sur le véhicule est capable de résister à des vibrations sinusoïdales possédant les caractéristiques suivantes : déplacement constant compris entre 5 et 11 Hz : 10 mm max. ; accélération constante comprise entre 11 et 300 Hz : 5 g. L'essai CEI 60068-2-6 (essai Fc) permet de vérifier le respect de cette exigence. La durée minimale de cet essai s'élève à 3 x 12 heures (12 heures par essieu). La norme ISO 16750-3 n'impose pas d'essai de vibrations sinusoïdales aux dispositifs situés dans la cabine découplée du véhicule. Vibrations aléatoires : Essai conforme à la norme ISO 16750-3 : chapitre 4.1.2.8 : Essai VIII : Véhicule commercial, cabine de véhicule découplée Essai de vibrations aléatoires, 10...2 000 Hz, RMS vertical 21,3 m/s², RMS longitudinal 11,8 m/s², RMS latéral 13,1 m/s², 3 essieux, 32 h par essieu, avec un cycle de température -20...70 °C. Cet essai satisfait à la norme CEI 60068-2-64 : Essais d'environnement − Partie 2-64 : Essais − Essai Fh : Vibrations à large bande et guide. Chocs : Choc mécanique d'un demi-sinus de 3 g conformément à la norme ISO 16750. Il convient d'exécuter les essais décrits ci-dessus sur des échantillons distincts du type d'équipement faisant l'objet des essais.	219
4.4	Protection contre l'eau et les corps étrangers	Essai conforme à la norme ISO 20653 : Véhicules routiers − Degrés de protection (codes IP) − Protection des équipements électriques contre les corps étrangers, l'eau et les contacts (paramètres inchangés)	220, 221
4.5	Protection contre les surtensions	Vérifier que l'unité embarquée sur le véhicule est capable de supporter une tension d'alimentation de : Versions 24 V : 34 V à +40 °C 1 heure Versions 12 V : 17 V à +40 °C 1 heure (ISO 16750-2, chap. 4.3)	216
4.6	Protection contre les inversions de polarité	Vérifier que l'unité embarquée sur le véhicule est capable de supporter une tension d'alimentation de : Versions 24 V : 34V à +40°C 1 heure Versions 12V : 17V à +40°C 1 heure (ISO 16750-2, chap. 4.7)	216
4.7	Protection contre les courts-circuits	Vérifier que les signaux d'entrée et de sortie sont protégés contre les courts-circuits au niveau de l'alimentation électrique et de la mise à terre (ISO 16750-2, chapitre 4.10)	216
5	**Essais de compatibilité électromagnétique**		
5.1	Émissions rayonnées et susceptibilité	Conformément au Règlement ONU nº 10	218

5.2	Décharge électrostatique	Conformément à la norme ISO 10605:2008, au rectificatif technique 1:2010 et à l'amendement 1:2014 : +/-4 kV pour le contact et +/-8 kV pour la décharge d'air	218
5.3	Susceptibilité transitoire par conduction au niveau de l'alimentation	Pour les versions 24V : conformité avec la norme ISO 7637-2 et le Règlement ONU nº 10, révision 3 : impulsion 1a : Vs = -450 V Ri = 50 ohms impulsion 2a : Vs = +37 V Ri = 2 ohms impulsion 2b : Vs = +20 V Ri = 0,05 ohms impulsion 3a : Vs = -150 V Ri = 50 ohms impulsion 3b : Vs = +150 V Ri = 50 ohms impulsion 4 : Vs = -16 V Va = -12 V t6 = 100 ms impulsion 5 : Vs = +120 V Ri = 2,2 ohms td = 250 ms Pour les versions 12 V : conformité avec la norme ISO 7637-1 et le Règlement ONU nº 10, révision 3 : impulsion 1 : Vs = -75V Ri = 10 ohms impulsion 2a : Vs = +37 V Ri = 2 ohms impulsion 2b : Vs = +10 V Ri = 0,05 ohms impulsion 3a : Vs = -112 V Ri = 50 ohms impulsion 3b : Vs = +75 V Ri = 50 ohms impulsion 4 : Vs = -6 V Va = -5 V t6 = 15ms impulsion 5 : Vs = +65 V Ri = 3 ohms td = 100 ms L'impulsion 5 ne sera mise à l'essai que pour les unités embarquées à installer sur des véhicules dépourvus de dispositif commun de protection externe contre la perte de charge. Pour la proposition concernant la perte de charge, consulter la norme ISO 16750-2, 4e édition, chapitre 4.6.4.	218

6. Essais du dispositif de communication à distance

Nº	**Essai**	**Description**	**Exigences connexes**
1.	**Examen administratif**		
1.1	Documentation	Exactitude de la documentation	
2.	**Inspection visuelle**		
2.1	Conformité avec la documentation		
2.2	Identification/marquage		225, 226
2.3	Matériel		219 à 223
3.	**Essais de fonctionnement**		
3.1	**Communication à distance aux fins des contrôles routiers ciblés**		**4, 197 à 199**
3.2	**Enregistrement et stockage dans la mémoire**		**91**
3.3	**Communication ~~au sein de~~ avec l'unité embarquée sur le véhicule**		**Sous-appendice 14, DCS_66 à DCS_70, DCS_71 à DCS_76**
4.	**Essais environnementaux**		

4.1	Température	S'assurer du fonctionnement du dispositif en procédant aux essais suivants : Essai conforme à la norme ISO 16750-4, chapitre 5.1.1.2 : Essai de fonctionnement à basse température (72 h à -20 °C) Cet essai satisfait à la norme CEI 60068-2-1 : Essais d'environnement − Partie 2-1 : Essais − Essai A : Froid. Essai conforme à la norme ISO 16750-4 : chapitre 5.1.2.2 : Essai de fonctionnement à haute température (72 h à 70 °C) Cet essai satisfait à la norme CEI 60068-2-2 : Essais d'environnement − Partie 2 : Essais − Essai B : Chaleur sèche. Essai conforme à la norme ISO 16750-4 : chapitre 5.3.2 : Variation rapide de température avec durée de transition spécifiée (-20 °C/70 °C, 20 cycles, temps d'exposition de 1 h à chaque température) Un nombre limité d'essais (parmi ceux définis à la section 3 de ce tableau) peuvent être effectués aux températures minimale et maximale indiquées ainsi que pendant les cycles de variation de la température.	213
4.2	Protection contre l'eau et les corps étrangers	Essai conforme à la norme ISO 20653 : Véhicules routiers − Degrés de protection (codes IP) − Protection des équipements électriques contre les corps étrangers, l'eau et les contacts (valeur cible IP 40)	220, 221
5	**Essais EMC**		
5.1	Émissions rayonnées et susceptibilité	Conforme au Règlement ONU nº 10	218
5.2	Décharge électrostatique	Conformément à la norme ISO 10605:2008, au rectificatif technique 1:2010 et à l'amendement 1:2014 : +/-4 kV pour le contact et +/-8 kV pour la décharge d'air	218
5.3	Susceptibilité transitoire par conduction au niveau de l'alimentation	Pour les versions 24V : conformité avec la norme ISO 7637-2 et le Règlement ONU nº 10, révision 3 : impulsion 1a : Vs = -450 V Ri = 50 ohms impulsion 2a : Vs = +37 V Ri = 2 ohms impulsion 2b : Vs = +20 V Ri = 0,05 ohms impulsion 3a : Vs = -150 V Ri = 50 ohms impulsion 3b : Vs = +150 V Ri = 50 ohms impulsion 4 : Vs = -16 V Va = -12 V t6 = 100 ms impulsion 5 : Vs = +120 V Ri = 2,2 ohms td = 250 ms Pour les versions 12V : conformité avec la norme ISO 7637-1 et le Règlement ONU nº 10, révision 3 : impulsion 1 : Vs = -75 V Ri = 10 ohms impulsion 2a : Vs = +37 V Ri = 2 ohms impulsion 2b : Vs = +10 V Ri = 0,05 ohms impulsion 3a : Vs = -112 V Ri = 50 ohms impulsion 3b : Vs = +75 V Ri = 50 ohms impulsion 4 : Vs = -6 V Va = -5 V t6 = 15 ms impulsion 5 : Vs = +65 V Ri = 3 ohms td = 100 ms L'impulsion 5 ne sera mise à l'essai que pour les unités embarquées à installer sur des véhicules dépourvus de dispositif commun de protection externe contre la perte de charge. Pour la proposition concernant la perte de charge, consulter la norme ISO 16750-2, 4e édition, chapitre 4.6.4.	218

7. Essais fonctionnels des tirages papier

Nº	Essai	Description	Exigences connexes
1.	**Examen administratif**		
1.1	Documentation	Exactitude de la documentation	
2	**Essais généraux**		
2.1	Nombre de caractères par ligne	Inspection visuelle des tirages papier.	172
2.2	Taille minimum des caractères	Inspection visuelle des tirages papier et contrôle des caractères.	173
2.3	Jeux de caractères compatibles	L'imprimante doit prendre en charge les caractères spécifiés au chapitre 4 (Jeux de caractères) ~~de l'appendice~~ **du sous-appendice** 1.	174
2.4	Définition des impressions	Contrôle de l'homologation du tachygraphe et inspection visuelle des tirages papier	174
2.5	Lisibilité et identification des impressions	Inspection des tirages papier Étayé par des rapports et des protocoles d'essai fournis par le fabricant. Tous les numéros d'homologation des tachygraphes avec lesquels il est possible d'utiliser le papier d'impression sont imprimés sur le papier.	175, 177, 178
2.6	Ajout de commentaires manuscrits	Inspection visuelle : un champ destiné à la signature du conducteur est disponible. D'autres champs destinés à la saisie d'informations manuscrites sont disponibles.	180
2.7	Informations supplémentaires au recto et au verso du papier	Le recto et le verso du papier peuvent fournir des précisions et des informations supplémentaires. Ces précisions et ces informations supplémentaires n'interfèrent pas avec la lisibilité des impressions. Inspection visuelle.	177, 178
3	**Essais de stockage**		
3.1	Chaleur sèche	Préconditionnement : 16 heures à +23 °C ± 2 °C/55 % ± 3 % d'humidité relative Environnement d'essai : 72 h à +70 °C ± 2 °C Récupération : 16 heures à +23 °C ± 2 °C/55 % ± 3 % d'humidité relative	176, 178 CEI 60068-2-2-Bb
2.2	Chaleur humide	Préconditionnement : 16 heures à +23 °C ± 2 °C/55 % ± 3 % d'humidité relative Environnement d'essai : 144 heures à +55 °C ± 2 °C et 93 % ± 3 % d'humidité relative Récupération : 16 heures à +23 °C ± 2 °C/55 % ± 3 % d'humidité relative	176, 178 CEI 60068-2-78-Cab
4	**Essais sur le papier en circulation**		
4.1	Résistance à l'humidité du support (papier non imprimé)	Préconditionnement : 16 heures à +23 °C ± 2 °C/55 % ± 3 % d'humidité relative Environnement d'essai : 144 heures à +55 °C ± 2 °C et 93 % ± 3 % d'humidité relative Récupération : 16 heures à +23 °C ± 2 °C/55 % ± 3 % d'humidité relative	176, 178 CEI 60068-2-78-Cab

4.2	Imprimabilité	Préconditionnement : 24 heures à +40 °C ± 2 °C/93 % ± 3 % d'humidité relative Environnement d'essai : impression produite à +23 °C ± 2 °C Récupération : 16 heures à +23 °C ± 2 °C/55 % ± 3 % d'humidité relative	176, 178
4.3	Résistance à la chaleur	Préconditionnement : 16 heures à +23 °C ± 2 °C/55 % ± 3 % d'humidité relative Environnement d'essai : 2 heures at +70 °C ± 2 °C, chaleur sèche Récupération : 16 heures à +23 °C ± 2 °C/55 % ± 3 % d'humidité relative	176, 178 CEI 60068-2-2-Bb
4.4	Résistance aux basses températures	Préconditionnement : 16 heures à +23 °C ± 2 °C/55 % ±3 % d'humidité relative Environnement d'essai : 24 heures at -20 °C ± 3 °C, chaleur sèche Récupération : 16 heures à +23 °C ± 2 °C/55 % ± 3 % d'humidité relative	176, 178 ISO 60068-2-1-Ab
4.5	Résistance à la lumière	Préconditionnement : 16 heures à +23 °C ± 2 °C/55 % ± 3 % d'humidité relative Environnement d'essai : 100 heures sous une lumière de 5 000 Lux à +23 °C ± 2 °C/55 % ± 3 % d'humidité relative Récupération : 16 heures à +23 °C ± 2 °C/55 % ± 3 % d'humidité relative	176, 178

Critère de lisibilité pour les essais 3.x et 4.x :

La lisibilité des tirages papier est garantie si la densité optique respecte les contraintes suivantes :

Caractères imprimés : min. 1,0 ;

Fond (papier non imprimé) : max. 0,2.

La densité optique des tirages papier doit être mesurée conformément à la norme DIN EN ISO 534.

Les tirages papier ne doivent subir aucune modification de dimension et demeurer parfaitement lisibles.

8. Essais d'interopérabilité

Nº	**Essai**	**Description**
8.1 Essais d'interopérabilité entre les unités embarquées et les cartes tachygraphiques		
1	Authentification mutuelle	S'assurer de la bonne exécution de la procédure d'authentification mutuelle entre l'unité embarquée et la carte tachygraphique
2	Essais de lecture/écriture	Mettre à exécution un scénario d'activité classique sur l'unité embarquée. Le scénario doit être adapté au type de carte à l'essai et comporter l'exécution d'opérations d'écriture dans le plus grand nombre possible d'EF présents sur la carte Procéder à un téléchargement à partir de l'UEV pour vérifier que tous les enregistrements correspondants ont été effectués correctement Procéder à un téléchargement à partir de la carte pour vérifier que tous les enregistrements correspondants ont été effectués correctement Procéder à des tirages quotidiens pour s'assurer de la bonne lisibilité des enregistrements correspondants

8.2 Essais d'interopérabilité entre les unités embarquées et les capteurs de mouvement		
1	Couplage	S'assurer de la bonne exécution de l'appariement entre l'unité embarquée et le capteur de mouvement
2	Essais d'activité	Exécuter un scénario d'activité classique sur le capteur de mouvement. Le scénario implique une activité normale et la création d'un nombre d'événements et d'anomalies aussi élevé que possible. Procéder à un téléchargement à partir de l'unité embarquée pour vérifier que tous les enregistrements correspondants ont été effectués correctement Procéder à un téléchargement à partir de la carte pour vérifier que tous les enregistrements correspondants ont été effectués correctement Procéder à un tirage quotidien pour s'assurer de la bonne lisibilité des enregistrements correspondants
8.3 Essais d'interopérabilité entre les unités embarquées et les dispositifs GNSS externes (le cas échéant)		
1	Authentification mutuelle	S'assurer de la bonne exécution de la procédure d'authentification mutuelle (couplage) entre l'unité embarquée et le module GNSS externe.
2	Essais d'activité	Exécuter un scénario d'activité classique sur le dispositif GNSS externe. Le scénario implique une activité normale et la création d'un nombre d'événements et d'anomalies aussi élevé que possible. Procéder à un téléchargement à partir de l'unité embarquée pour vérifier que tous les enregistrements correspondants ont été effectués correctement. Procéder à un téléchargement à partir de la carte pour vérifier que tous les enregistrements correspondants ont été effectués correctement. Procéder à un tirage quotidien pour s'assurer de la bonne lisibilité des enregistrements correspondants.

9. Essais OSNMA

9.1 Introduction

Le présent chapitre décrit les essais visant à démontrer la bonne mise en œuvre du service ouvert d'authentification des messages de navigation (OSNMA) au sein du récepteur GNSS. Étant donné que l'authentification du signal satellite est effectuée exclusivement par le récepteur GNSS en toute indépendance par rapport aux autres composants du tachygraphe, les essais décrits dans le présent chapitre peuvent être effectués sur le récepteur GNSS en tant qu'élément autonome. Dans ce cas, le fabricant du tachygraphe doit présenter aux autorités d'homologation un rapport détaillant le déroulement et les résultats des essais effectués sous la responsabilité du fabricant du récepteur GNSS.

9.2 Conditions applicables

- **Les critères de réussite et d'échec définis dans la procédure d'essai OSNMA ne sont considérés comme valables que pour les conditions d'essai indiquées ;**
- **Les critères pourraient être révisés au moment de la déclaration de mise en service OSNMA et compte tenu des engagements en matière de performance des services associés.**

9.3 Définitions et abréviations

9.3.1 Définitions

Démarrage GNSS froid/chaud/très chaud : Désigne l'état d'un récepteur GNSS au démarrage en fonction de la disponibilité de l'heure (T), de l'almanach (A) et de l'éphéméride (E) actuels, et de la position (P) :

- **Démarrage GNSS froid : aucun**
- **Démarrage GNSS chaud : T, A, P**
- **Démarrage GNSS très chaud : T, A, E, P**

Démarrage OSNMA froid/chaud/très chaud : Désigne l'état de la fonction OSNMA au démarrage en fonction de la disponibilité de la clé publique (P) et du DSM-KROOT (K) (tels que définis dans les lignes directrices OSNMA relatives aux récepteurs visées au sous-appendice 12) :

- **Démarrage OSNMA froid : aucun**
- **Démarrage OSNMA chaud : P**
- **Démarrage OSNMA très chaud : P, K**

9.3.2 Abréviations

ADKD	**Données d'authentification et délai de clé *(Authentication Data & Key Delay*)**
DSM-KROOT	**Message de signature numérique contenant la KROOT *(Digital Signature Message KROOT*)**
GNSS	**Système mondial de navigation par satellite *(Global Navigation Satellite System)***
KROOT	**Clé racine *(Root Key)* de la chaîne de clés TESLA**
MAC	**Code d'authentification des messages *(Message Authentication Code)***
NMAC	**Nombre de MAC et de blocs de clés (par 30 secondes)**
OSNMA	**Service ouvert ~~Galileo~~ d'authentification des messages de navigation *(Open Service Navigation Message Authentication)***
SLMAC	**MAC lent *(Slow MAC)***
TESLA	**Protocole *Timed Efficient Stream Loss-tolerant Authentication* (utilisé dans l'OSNMA)**

9.4 Équipement pour la génération des signaux GNSS

La génération des signaux GNSS nécessaire au bon fonctionnement du récepteur GNSS peut être réalisée à l'aide d'un générateur de signaux GNSS multi-constellations, ainsi que des messages de navigation, de l'heure de début et de la durée du scénario définis par l'utilisateur. Il est également possible d'utiliser un lecteur de signaux radioélectriques capable de reproduire les échantillons de signaux GNSS extraits des fichiers. La profondeur de bit et la fréquence d'échantillonnage caractéristiques sont respectivement de 4 bits I/Q et 10 MHz.

On suppose que le récepteur GNSS dispose d'interfaces permettant d'ordonner l'effacement de sa mémoire (pour supprimer de manière indépendante la clé publique, la KROOT, les informations d'horloge et de position, les éphémérides et les almanachs), de régler la réalisation temporelle en heure locale du récepteur pour satisfaire l'exigence de vérification de la synchronisation OSNMA et de charger les informations

cryptographiques. Ces commandes peuvent être limitées à des fins d'essai et donc ne pas être disponibles dans des conditions de fonctionnement nominal du récepteur.

9.5 Conditions d'essai

9.5.1 Conditions GNSS

Les signaux GNSS simulés ou répétés doivent présenter les caractéristiques suivantes :

- **Un scénario de récepteur utilisateur statique ;**
- **Une fréquence E1/L1 ;**
- **Au moins 4 satellites transmettant des données OSNMA et ayant un angle d'élévation supérieur à 5 °;**
- **La durée prescrite pour chaque essai ;**
- **Les éphémérides de navigation constante des satellites utilisés pendant l'essai.**

9.5.2 Conditions OSNMA

Le message OSNMA transmis dans le signal RF doit présenter les caractéristiques suivantes :

- **Un message HKROOT avec l'état OSNMA réglé sur « opérationnel » ou « à l'essai » et un message DSM-KROOT fixe de 8 blocs pour la chaîne en vigueur ;**
- **Au moins 4 satellites transmettant des données OSNMA ;**
- **Un message MACK comprenant un bloc MACK (soit NMACK=1), et au moins un ADKD=0 et un ADKD=12 par satellite et bloc MACK ;**
- **Une taille de balise de 40 bits ;**
- **La longueur minimale équivalente de la balise prescrite dans les lignes directrices OSNMA relatives aux récepteurs (actuellement 80 bits).**

Sauf indication contraire, la réalisation temporelle du récepteur interne doit être connue avec une précision suffisante et correctement alignée sur l'heure simulée. Cela garantit que l'exigence de synchronisation temporelle initiale OSNMA pour chaque condition d'essai, c'est-à-dire la synchronisation nominale pour tous les essais, à l'exception de l'essai SLMAC. Pour plus d'informations concernant l'initialisation temporelle, voir les lignes directrices OSNMA relatives aux récepteurs.

9.6 Spécifications d'essai

Nº	Essai	Description	Exigences connexes
1.	Examen administratif		
1.1	Documentation	Exactitude de la documentation	
2	Essais généraux		

2.1	**Démarrage OSNMA très chaud**	**Objectif : vérifier que le récepteur GNSS calcule une position à l'aide du service OSNMA après un démarrage très chaud.** **Procédure :** **Le récepteur GNSS est allumé dans des conditions de démarrage GNSS et OSNMA très chaud et acquiert les signaux des satellites visibles.** **Le récepteur authentifie les données de navigation à l'aide du service OSNMA (ADKD=0) et fournit une position avec les données authentifiées.** **Critères de réussite et d'échec : le récepteur calcule une position authentifiée dans un délai de 160 secondes.**	**Appendice 12, GNS_3b**
2.2	**Démarrage OSNMA chaud**	**Objectif : vérifier que le récepteur GNSS calcule une position à l'aide du service OSNMA après un démarrage chaud.** **Procédure : avant de lancer l'essai, les éphémérides et les données KROOT doivent être effacées de la mémoire du récepteur GNSS afin de forcer le démarrage GNSS et OSNMA chaud.** **Le récepteur GNSS démarre et acquiert les signaux des satellites visibles.** **Le message DSM-KROOT est reçu et vérifié.** **Le récepteur authentifie les données de navigation à l'aide du service OSNMA (ADKD=0) et fournit une position avec les données authentifiées.** **Critères de réussite et d'échec : le récepteur calcule une position authentifiée valide dans un délai de 430 secondes.**	**Appendice 12, GNS_3b**
2.3	**Démarrage OSNMA chaud avec SLMAC**	**Objectif : vérifier que le récepteur GNSS calcule une position à l'aide du service OSNMA après un démarrage chaud avec une initialisation temporelle qui nécessite le mode SLMAC, tel que défini dans les lignes directrices OSNMA relatives aux récepteurs.** **Procédure : la réalisation temporelle du récepteur interne doit être configurée de manière à avoir une incertitude initiale comprise entre 2 et 2,5 minutes, de telle sorte que, conformément aux lignes directrices OSNMA relatives aux récepteurs, le mode « Slow MAC » soit activé.** **Avant de commencer les essais, les éphémérides et la KROOT doivent être effacées de la mémoire du récepteur GNSS afin de forcer le démarrage GNSS et OSNMA chaud.** **Le récepteur GNSS démarre et acquiert les signaux des satellites visibles.** **Le message DSM-KROOT est reçu et vérifié.** **Le récepteur authentifie les données de navigation à l'aide du service OSNMA limité au mode « Slow MAC » (ADKD=12 et fournit une position avec les données authentifiées.** **Critères de réussite et d'échec : le récepteur calcule une position authentifiée valide dans un délai de 730 secondes.**	**Appendice 12, GNS_3b**

2.4	**Démarrage OSNMA très chaud avec répétition du signal**	**Objectif : vérifier que le récepteur GNSS détecte un signal répété.** **Procédure :** **Le récepteur GNSS est allumé dans des conditions de démarrage GNSS et OSNMA très chaud et acquiert les signaux des satellites visibles.** **Le récepteur authentifie les données de navigation à l'aide du service OSNMA (ADKD=0) et fournit une position avec les données authentifiées.** **Une fois que le récepteur a fourni une solution PVT avec des données authentifiées, il est éteint.** **Un signal répété avec un retard de 40 secondes par rapport au signal précédent est simulé, puis le récepteur est allumé.** **Le récepteur détecte que l'heure du système qui correspond à l'heure du signal dans l'espace et l'heure locale réelle ne satisfont pas à l'exigence de synchronisation et il cesse de traiter les données OSNMA comme prévu dans les lignes directrices OSNMA relatives aux récepteurs.** **Critères de réussite et d'échec : le récepteur détecte le signal répété et ne calcule pas de position authentifiée valide depuis le début de la répétition jusqu'à la fin de l'essai.**	**Appendice 12, GNS_3b**
2.5	**Démarrage OSNMA très chaud avec des données erronées**	**Objectif : vérifier que l'OSNMA détecte les données erronées.** **Procédure :** **Le récepteur GNSS est allumé dans des conditions de démarrage GNSS et OSNMA très chaud.** **Le récepteur doit être en mesure d'acquérir le signal de tous les satellites visibles et de vérifier l'authenticité de leurs messages de navigation au moyen du service OSNMA.** **Au moins un bit des données d'éphémérides fournies par chaque satellite ne correspond pas aux données originales et authentifiées, mais le message I/NAV est cohérent, y compris le CRC.** **Critères de réussite et d'échec : le récepteur détecte les données erronées dans un délai de 160 secondes et ne calcule pas de position authentifiée valide jusqu'à la fin de l'essai.**	**Appendice 12, GNS_3b**

~~Appendice~~ Sous-appendice 10

Exigences en matière de sécurité

Le présent **sous-**appendice définit les exigences en matière de sécurité informatique applicables aux composants du tachygraphe intelligent (tachygraphe de seconde génération).

SEC_001 Les composants suivants du tachygraphe intelligent doivent faire l'objet d'une certification de sécurité selon les Critères communs :

- Unité embarquée sur le véhicule ;
- Carte tachygraphique ;
- Capteur de mouvement ;
- Dispositif GNSS externe.

SEC_002 Les exigences minimales de sécurité informatique à satisfaire par chaque composant soumis à une certification de sécurité doivent être définies dans un profil de protection propre au composant, conformément aux Critères communs.

SEC_003 ~~La Commission européenne doit s'assurer que~~ **Les** quatre profils de protection suivants, conformes **au présent sous-appendice**, doivent être parrainés, développés et approuvés par les organismes gouvernementaux de certification de la sécurité informatique faisant partie du groupe de travail d'interprétation conjointe (JIWG) qui encourage la reconnaissance mutuelle des certificats dans le cadre de l'accord européen SOG-IS MRA (accord sur la reconnaissance mutuelle des certificats d'évaluation de la sécurité en matière de technologie de l'information), et faire l'objet d'un enregistrement :

- Profil de protection de l'unité embarquée sur le véhicule ;
- Profil de protection de la carte tachygraphique ;
- Profil de protection du capteur de mouvement ;
- Profil de protection du dispositif GNSS externe.

Le profil de protection de l'unité embarquée sur le véhicule doit couvrir les cas où l'unité embarquée a été conçue pour être utilisée avec un dispositif GNSS externe et ceux où elle a été conçue pour être utilisée sans dispositif GNSS externe. Dans le premier cas, les exigences de sécurité du dispositif GNSS externe seront définies dans le profil de protection dédié.

SEC_004 Afin d'établir les objectifs de sécurité en vue de l'obtention des certificats de sécurité, les fabricants de composants habilités affineront et compléteront, selon les besoins, le profil de protection des composants appropriés, sans supprimer ni modifier les spécifications concernant les menaces, les objectifs, les procédures et les fonctions de maintien de la sécurité.

SEC_005 La stricte conformité d'un objectif de sécurité avec le profil de protection correspondant doit être déclaré au cours du processus d'évaluation.

SEC_006 Le niveau de garantie exigé par chaque profil de protection doit être le niveau EAL4 auquel s'ajoutent les composants de garantie ATE_DPT.2 et AVA_VAN.5.

~~Appendice~~ Sous-appendice 11

Mécanismes de sécurité communs

Table des matières

Préambule

Le présent **sous-**appendice définit les mécanismes de sécurité garantissant :

- L'authentification mutuelle entre les différents composants du tachygraphe ;
- La confidentialité, l'intégrité, l'authenticité et/ou la non-répudiation des données transférées entre les différents composants du tachygraphe ou téléchargées vers un support de mémoire externe.

Le présent **sous-**appendice se compose de deux parties. La partie A définit les mécanismes de sécurité applicables au tachygraphe de première génération (tachygraphe numérique). La partie B définit les mécanismes de sécurité applicables au tachygraphe de deuxième génération (tachygraphe intelligent).

Les mécanismes spécifiés dans la partie A du présent **sous-**appendice s'appliquent si au moins l'un des composants du tachygraphe concerné par une authentification mutuelle et/ou un processus de transfert de données est de première génération.

Les mécanismes spécifiés dans la partie B du présent **sous-**appendice s'appliquent si les deux composants concernés par une authentification mutuelle et/ou un processus de transfert de données sont de deuxième génération.

~~L'appendice~~**Le sous-appendice** 15 fournit de plus amples informations sur l'utilisation des composants de première génération avec ceux de deuxième génération.

PARTIE A TACHYGRAPHE DE PREMIÈRE GÉNÉRATION

1. Introduction

1.1 Références

Dans le présent **sous-**appendice, il est fait référence aux documents suivants :

SHA-1	National Institute of Standards and Technology (NIST), *FIPS Publication 180-1: Secure Hash Standard*, avril 1995.
PKCS1	RSA Laboratories, PKCS # 1 : *RSA Encryption Standard*, version 2.0, octobre 1998.
TDES	National Institute of Standards and Technology (NIST), *FIPS Publication 46-3 : Data Encryption Standard*, projet 1999.
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation, 1998.
ISO/CEI 7816-4	Technologies de l'information − Cartes d'identification − Cartes à circuit(s) intégré(s) à contacts − Partie 4 : commandes intersectorielles pour les échanges, première édition : 1995, et amendement 1:1997.
ISO/CEI 7816-6	Technologies de l'information − Cartes d'identification − Cartes à circuit(s) intégré(s) à contacts − Partie 6 : éléments de données intersectoriels, première édition : 1996, et rectificatif technique 1: 1998.
ISO/CEI 7816-8	Technologies de l'information − Cartes d'identification − Cartes à circuit(s) intégré(s) à contacts − Partie 8 : commandes intersectorielles de sécurité, première édition : 1999.
ISO/CEI 9796-2	Technologies de l'information − Techniques de sécurité − Schémas de signature numérique rétablissant le message − Partie 2 : mécanismes utilisant une fonction de hachage, première édition : 1997.

ISO/CEI 9798-3	Technologies de l'information − Techniques de sécurité − Mécanismes d'authentification d'entité − Partie 3 : authentification d'entité utilisant un algorithme à clé publique, seconde édition : 1998.
ISO 16844-3	Véhicules routiers − Systèmes tachygraphes − Partie 3 : interface de capteur de mouvement.

1.2 Notations et abréviations

Les notations et abréviations qui suivent apparaissent dans le présent **sous-**appendice :

(K_a, K_b, K_c)	Faisceau de clés destiné au triple DES (*Data Encryption Standard*)
AC	Autorité de certification
RAC	Référence de l'autorité de certification
CC	Contrôle cryptographique
CG	Cryptogramme
EC	En-tête de commande
ADC	Autorisation du détenteur de certificat
RDC	Référence du détenteur de certificat
D()	Déchiffrement avec DES (*Data Encryption Standard*)
DE	Élément de données
OD	Objet de données
d	Clé privée − exposant privé RSA
e	Clé publique − exposant public RSA
E()	Chiffrement avec DES
EQT	Équipement
Hash()	Valeur de hachage, en tant que sortie de *Hash*
Hash	Fonction hachage
KID	Identificateur de clé
Km	Clé TDES, clé maîtresse définie dans la norme ISO 16844-3
Km_{UEV}	Clé TDES insérée dans les unités embarquées
Km_{CAT}	Clé TDES insérée dans les cartes d'ateliers *(Km_{wc}, en anglais)*
m	Représentant de message, nombre entier compris entre 0 et *n*-1
n	Clés RSA, modulo
OR	Octet de remplissage
IR	Octet indicateur de remplissage (employé dans les cryptogrammes destinés aux objets de données d'instructions de confidentialité)
VC	Valeur en clair
s	Représentant de signature, nombre entier compris entre 0 et n-1
CSE	Compteur de séquences d'envoi
TCBC	Mode d'opération par chaînage de blocs de données chiffrées TDEA
TDEA	Algorithme Triple DES *(Triple Data Encryption Algorithm)*
TLV	Structure balise-longueur-valeur *(Tag-Length-Value)*
UEV	Unité embarquée sur le véhicule *(VU, en anglais)*

X.C	Certificat de l'utilisateur X émis par une autorité de certification
X.AC	Autorité de certification de l'utilisateur X
$X.AC.PK_o X.C$	Opération de dévoilement d'un certificat pour en extraire une clé publique. Il s'agit d'un opérateur infixe dont l'opérande de gauche correspond à la clé publique d'une autorité de certification et l'opérande de droite au certificat émis par ce même organisme. On obtient comme résultat la clé publique de l'utilisateur X, dont le certificat est l'opérande de droite.
X.PK	Clé publique RSA d'un utilisateur X
X.PK[I]	Chiffrement RSA de certaines informations I à l'aide de la clé publique de l'utilisateur X
X.SK	Clé privée RSA d'un utilisateur X
X.SK[I]	Chiffrement RSA d'informations I à l'aide de la clé privée de l'utilisateur X
′xx′	Valeur hexadécimale
||	Opérateur de concaténation

2. Systèmes et algorithmes cryptographiques

2.1 Systèmes cryptographiques

CSM_001 Les unités embarquées et les cartes tachygraphiques utilisent un système cryptographique classique à clé publique RSA pour mettre en œuvre les mécanismes de sécurité suivants :

- Authentification mutuelle entre unités embarquées et cartes tachygraphiques ;
- Acheminement des clés de session Triple DES (*Data Encryption Standard*) entre unités embarquées et cartes tachygraphiques.
- Signature numérique des données téléchargées sur des supports externes à partir d'unités embarquées ou de cartes tachygraphiques.

CSM_002 Les unités embarquées et les cartes tachygraphiques ont recours à un système cryptographique symétrique Triple DES pour garantir l'intégrité des données lors des échanges de données d'utilisateur entre elles et pour assurer, le cas échéant, la confidentialité de ces échanges de données.

2.2 Algorithmes cryptographiques

2.2.1 Algorithme RSA

CSM_003 L'algorithme RSA est entièrement défini par les relations suivantes :

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

Une description plus détaillée de la fonction RSA figure dans le document de référence [PKCS1]. L'exposant public « e » pour les calculs de l'algorithme RSA est un nombre entier compris entre 3 et n-1 et tel que gcd[e, lcm(p-1, q-1)] = 1.

2.2.2 Algorithme de hachage

CSM_004 Les mécanismes de signature numérique utilisent l'algorithme de hachage SHA-1 tel qu'il est défini dans le document de référence [SHA-1].

2.2.3 Algorithme de chiffrement de données

CSM_005 Des algorithmes fondés sur les normes de chiffrement DES sont utilisés dans le mode de chiffrement par chaînage de blocs (CBC).

3. Clés et certificats

3.1 Génération et distribution de clés

3.1.1 Génération et distribution de clés RSA

CSM_006 Des clés RSA sont générées selon trois niveaux hiérarchiques de fonctionnement :

- Niveau ~~européen~~ **racine ;**
- Niveau ~~État membre~~ **Partie contractante ;**
- Niveau équipement.

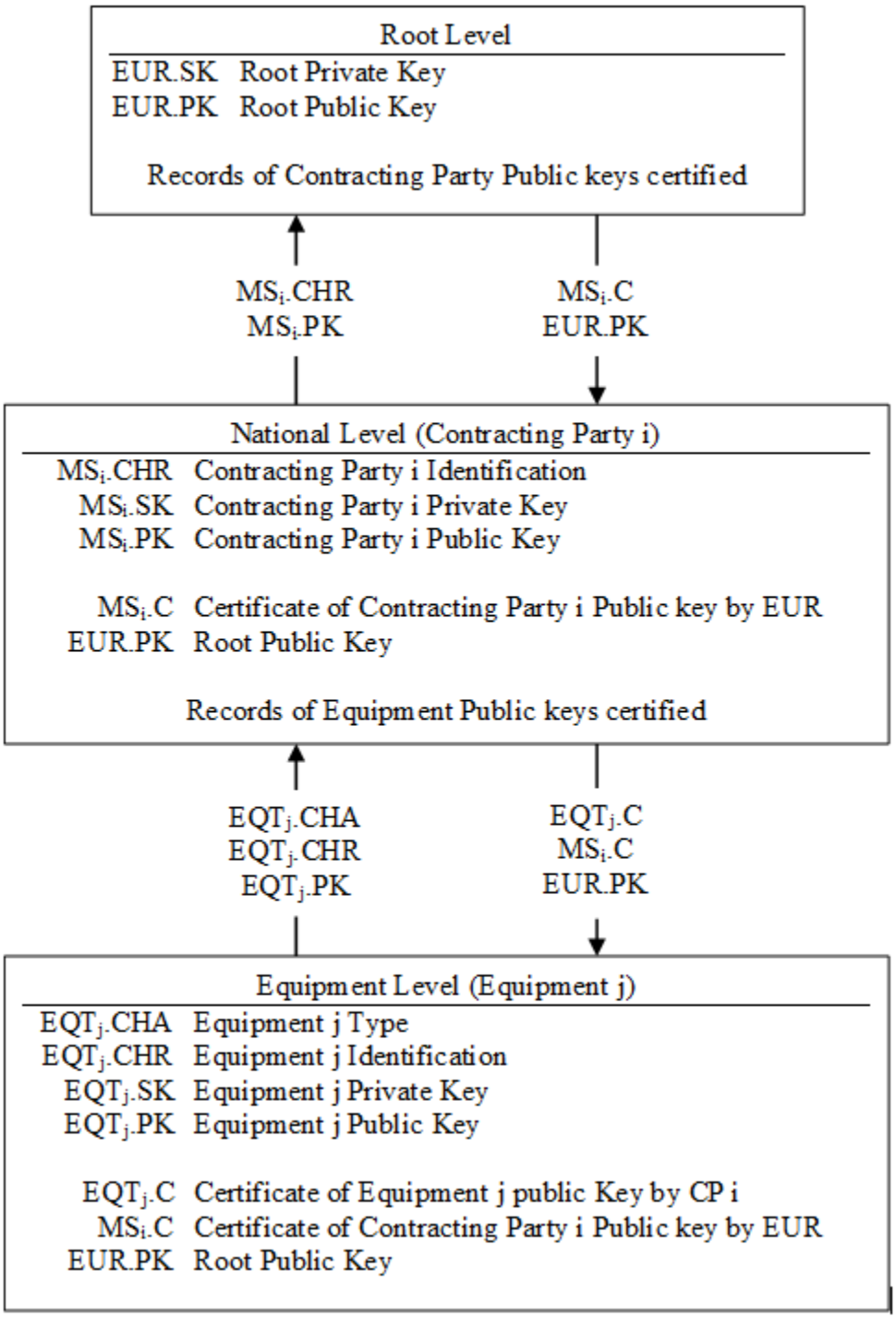
CSM_007 Au niveau ~~européen~~ **racine**, une seule paire de clés ~~européenne~~ **racine** (EUR.SK et EUR.PK) est générée. La clé privée ~~européenne~~ **racine** permet de certifier les clés publiques des ~~États membres~~ **Parties contractantes**. L'ensemble des clés certifiées doivent être sauvegardées. Ces tâches sont exécutées par une autorité de certification ~~européen~~ **racine**~~, placé sous l'autorité et la responsabilité de la Commission européenne~~.

CSM_008 Au niveau ~~État membre~~ **Partie contractante**, une paire de clés par ~~État membre~~ **Partie contractante** (MS.SK et MS.PK) est générée. Les clés publiques des ~~États membres~~ **Parties contractantes** doivent être certifiées par l'autorité de certification ~~européen~~ **racine**. La clé privée d'un**e** ~~État membre~~ **Partie contractante** permet de certifier les clés publiques à introduire dans l'équipement (unité embarquée ou carte tachygraphique). L'ensemble des clés publiques certifiées sont sauvegardées avec les données d'identification de l'équipement auquel elles sont destinées. Ces tâches sont effectuées par une autorité de certification ~~nationale~~ **de la Partie contractante concernée**. Les ~~États membres~~ **Parties contractantes** sont habilitées à changer régulièrement de paire de clés.

CSM_009 Au niveau équipement, une seule paire de clés (EQT.SK et EQT.PK) est générée et introduite dans chaque équipement. Les clés publiques des équipements doivent être certifiées par une autorité de certification ~~nationale~~ **de la Partie contractante concernée**. Ces tâches peuvent être effectuées par les fabricants d'équipements, les adaptateurs d'équipement ou les autorités ~~nationales~~ compétentes **de la Partie contractante concernée**. Cette paire de clés est utilisée dans les procédures d'authentification, de signature numérique et de chiffrement.

CSM_010 La confidentialité des clés privées doit être préservée durant leur génération, leur acheminement (le cas échéant) et leur stockage.

Le schéma ci-dessous présente une synthèse du cheminement des données caractérisant ce processus :



3.1.2 Clés de contrôle RSA

CSM_011 Aux fins des essais sur les équipements (y compris les essais d'interopérabilité), l'autorité de certification ~~européenne~~ **racine** génère une paire de clés de contrôle ~~européenne~~ **racine** distincte et au moins deux paires de clés de contrôle nationales, dont les clés publiques seront certifiées à l'aide de la clé de contrôle privée ~~européenne~~ **racine**. Les fabricants introduisent dans les équipements en cours d'homologation des clés de contrôle certifiées par l'une des clés de contrôle nationales.

3.1.3 Clés du capteur de mouvement

La confidentialité des trois clés Triple DES décrites ci-après doit être protégée de manière appropriée durant la génération, l'acheminement (le cas échéant) et le stockage.

Afin de permettre l'utilisation des composants de tachygraphe conformes à la norme ISO 16844, l'autorité de certification ~~européenne~~ **racine** et les autorités de certification ~~de l'État membre~~ **des Parties contractantes** veillent au respect des exigences qui suivent.

CSM_036 L'autorité de certification ~~européenne~~ **racine** génère les clés Km_{UEV} et Km_{CAT}, deux clés Triple DES uniques et indépendantes, ainsi que la clé Km selon la formule : $Km = Km_{UEV}$ XOR Km_{CAT}. L'autorité de certification ~~européen~~ **racine** transmet ensuite ces clés, en respectant les procédures sécurisées appropriées, aux autorités de certification des ~~États membres~~ **Parties contractantes** qui en font la demande.

CSM_037 Les autorités de certification des ~~États membres~~ **Parties contractantes** :

- Utilisent la clé Km pour chiffrer les données du capteur de mouvement demandées par les fabricants de capteurs de mouvement (les données à chiffrer avec la clé Km sont définies dans la norme ISO 16844-3) ;
- Transmettent la clé Km_{UEV} aux fabricants d'unités embarquées, selon les procédures sécurisées appropriées, afin qu'elle soit insérée dans les UEV ;
- Veillent à ce que la clé Km_{CAT} soit insérée dans toutes les cartes d'atelier (sous SensorInstallationSecData dans le fichier élémentaire Sensor_Installation_Data) lors de leur configuration.

3.1.4 Génération et distribution de clés de session T-DES

CSM_012 Dans le cadre du processus d'authentification mutuelle, les unités embarquées et les cartes tachygraphiques génèrent et échangent les données nécessaires à l'élaboration d'une clé de session T-DES commune. La confidentialité de cet échange de données doit être protégée par un mécanisme de chiffrement RSA.

CSM_013 Cette clé doit être utilisée lors de toutes les opérations cryptographiques ultérieures faisant appel à la messagerie sécurisée. Sa validité expire à la fin de la session (retrait ou réinitialisation de la carte) et/ou après 240 utilisations (une utilisation de la clé correspond à une commande envoyée par messagerie sécurisée vers une carte et la réponse associée).

3.2 Clés

CSM_014 Les clés RSA ont les longueurs suivantes (quel que soit le niveau) : modulo *n* 1024 bits, exposant public *e* 64 bits maximum et exposant privé *d* 1024 bits.

CSM_015 Les clés Triple DES prennent la forme (K_a, K_b, K_a), où K_a et K_b sont des clés indépendantes de 64 bits. Aucun bit de parité destiné à la détection d'erreur ne doit être défini.

3.3 Certificats

CSM_016 Les certificats associés aux clés publiques RSA sont vérifiables, mais ne sont pas autodescriptifs (voir ISO/CEI 7816-8).

3.3.1 Contenu des certificats

CSM_017 Les certificats associés aux clés publiques RSA comportent les données ci-après dans l'ordre suivant :

Données	*Format*	*Octets*	*Observations*
CPI	INTEGER	1	Identificateur de profil de certificat (‘01’ pour cette version)
RAC	OCTET STRING	8	Référence de l’autorité de certification
ADC	OCTET STRING	**7**	Autorisation du détenteur de certificat
EOV	TimeReal	4	Expiration du certificat. Peut être complété par des octets de remplissage ‘FF’ en cas de non-utilisation.
RDC	OCTET STRING	8	Référence du détenteur de certificat
n	OCTET STRING	128	Clé publique (modulo)
e	OCTET STRING	8	Clé publique (exposant public)
		164	

Remarques :

1. L’« identificateur de profil de certificat » (CPI) détermine la structure précise d’un certificat d’authentification. Il peut servir d’identificateur interne d’équipement au sein d’une liste en-tête appropriée qui décrit la concaténation des éléments de données du certificat.

La liste en-tête associée au contenu de ce certificat se présente ainsi :

‘4D’	‘16’	‘5F 29’	‘01’	‘42’	‘08’	‘5F 4B’	‘07’	‘5F 24’	‘04’	‘5F 20’	‘08’	‘7F 49’	‘05’	‘81’	‘81 80’	‘82’	‘08’
Balise de liste en-tête étendue	Longueur de la liste en-tête	Balise CPI	Longueur CPI	Balise RAC	Longueur RAC	Balise ADC	Longueur ADC	Balise EOV	Longueur EOV	Balise RDC	Longueur RDC	Balise de clé publique (construite)	Longueur des objets de données suivants	Balise modulo	Longueur modulo	Balise exposant public	Longueur exposant public

2. La « référence de l’autorité de certification » (RAC) permet d’identifier l’autorité de certification qui émet le certificat, de telle manière que cet élément de données puisse être utilisé avec un identificateur de clé associé à une autorité pour désigner la clé publique de l’autorité de certification (pour plus d’informations concernant le codage, voir la définition de l’identificateur de clé ci-dessous).

3. L’« autorisation du détenteur de certificat » (ADC) permet de définir les droits du détenteur de certificat. Elle est composée de l’ID d’application du tachygraphe et du type d’équipement auquel le certificat considéré est destiné (en fonction de l’élément de données `EquipmentType`, ‘00’ pour un**e** ~~État membre~~ **Partie contractante**).

4. La « référence du détenteur de certificat » (RDC) permet d’identifier le détenteur du certificat de manière unique, de telle manière que cet élément de données puisse être utilisé avec un identificateur de clé associé à un sujet pour désigner la clé publique du détenteur de certificat.

5. Les identificateurs de clé permettent d’identifier de manière unique le détenteur du certificat ou l’autorité de certification. Ils sont codés comme suit :

5.1 Équipement (UEV ou carte) :

Données	*Numéro de série de l’équipement*	*Date*	*Type*	*Fabricant*
Longueur	4 octets	2 octets	1 octet	1 octet

Données	*Numéro de série de l'équipement*	*Date*	*Type*	*Fabricant*
Valeur	Entier	Codage DCB mm aa	Propre au fabricant	Code du fabricant

Lors de la demande d'un certificat concernant une UEV, le fabricant peut connaître ou non les données d'identification de l'équipement au sein duquel les clés seront introduites.

Dans le premier cas de figure, le fabricant enverra les données d'identification de l'équipement accompagnées de la clé publique à l'autorité de certification ~~nationale~~ compétente **de la Partie contractante concernée**. Le certificat contiendra donc les données d'identification de l'équipement concerné. Le fabricant devra veiller à ce que les clés et le certificat appropriés soient introduits dans l'équipement voulu. L'identificateur de clé se présente sous la forme indiquée ci-dessus.

Dans le second cas de figure, le fabricant doit identifier chaque demande de certificat de manière unique et envoyer les données d'identification correspondantes accompagnées de la clé publique à l'autorité de certification ~~nationale~~ compétente **de la Partie contractante concernée**. Le certificat contiendra donc les données d'identification de la demande de certificat concernée. Le fabricant doit communiquer en retour à l'autorité de certification nationale compétente les informations relatives à l'attribution des clés à un équipement donné (c'est-à-dire les données d'identification de la demande de certificat et d'identification de l'équipement) après l'introduction des clés dans cet équipement. L'identificateur de clé se présente sous la forme suivante :

Données	*Numéro de série de l'équipement*	*Date*	*Type*	*Fabricant*
Longueur	4 octets	2 octets	1 octet	1 octet
Valeur	Entier	Codage DCB mm aa	'FF'	Code du fabricant

5.2 Autorité de certification :

Données	*Identification de l'autorité*	*Numéro de série de la clé*	*Informations complémentaires*	*Identificateur*
Longueur	4 octets	1 octet	2 octets	1 octet
Valeur	Code numérique national sur un octet Code alphanumérique national sur trois octets	Entier	Codage additionnel (propre à l'AC) 'FF FF' en cas de non-utilisation	'01'

Le numéro de série d'une clé permet de faire la distinction entre les différentes clés d'un**e** ~~État membre~~ **Partie contractante**, en cas de changement de clé.

6. Les vérificateurs de certificat savent implicitement que la clé publique certifiée est une clé RSA destinée à l'authentification, à la vérification et au chiffrement de signatures numériques à des fins de confidentialité (le certificat ne contient aucun identificateur d'objet qui permette de l'indiquer).

3.3.2 Certificats émis

CSM_018 Le certificat émis se présente comme une signature numérique avec récupération partielle du contenu du certificat conformément à la norme ISO/CEI 9796-2 (annexe A.4 non comprise), la « référence de l'autorité de certification » clôturant le certificat.

$$X.C = X.AC.SK[\text{'6A'} \parallel C_r \parallel \mathit{Hash}(Cc) \parallel \text{'BC'}] \parallel C_n \parallel X.RAC$$

Avec contenu de certificat = Cc = C_r || C_n

106 octets 58 octets

Remarques :

1. Ce certificat est constitué de 194 octets.

2. La RAC, masquée par la signature, est ajoutée à cette dernière, afin que la clé publique de l'autorité de certification puisse être sélectionnée pour procéder à la vérification du certificat.

3. Le vérificateur du certificat connaît implicitement l'algorithme employé par l'autorité de certification pour signer le certificat.

4. La liste en-tête associée à ce certificat se présente comme suit :

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Balise certificat VC (construite)	Longueur des objets de données suivants	Balise de la signature	Longueur de la signature	Balise du reste	Longueur du reste	Balise RAC	Longueur RAC

3.3.3 Vérification et dévoilement des certificats

La vérification et le dévoilement des certificats consistent à vérifier la signature conformément à la norme ISO/CEI 9796-2, à extraire le contenu du certificat et la clé publique qu'il contient (X.PK = X.AC.PK o X.C), et à vérifier la validité du certificat.

CSM_019 Cette procédure comporte les opérations suivantes :

Vérification de la signature et extraction du contenu :

– À partir de X.C, extraire Sign., C_n' et RAC' : X.C = Sign || C_n' || RAC'
128 octets 58 octets 8 octets

À partir de RAC', sélectionner la clé publique de l'autorité de certification appropriée (dans l'éventualité où cette opération n'aurait pas été exécutée par d'autres moyens)

– Ouvrir Sign avec la clé publique de l'autorité de certification : Sr'= X.AC.PK [Sign]

– S'assurer que le Sr' commence par '6A' et se termine par 'BC'

– Calculer C_r' et H' à partir de : Sr' = '6A' || C_r' || H' || 'BC'
106 octets 20 octets

– Récupérer le contenu du certificat C'= C_r' || C_n' ;

– Vérifier *Hash*(C') = H'

Si les vérifications sont concluantes, le certificat est un original et son contenu est C'.

Vérification de la validité, à partir de C' :

– Contrôler, le cas échéant, la date d'expiration.

Extraction et stockage de la clé publique, de l'identificateur de clé, de l'autorisation du détenteur de certificat et de la date d'expiration du certificat à partir du certificat C' :

– X.PK = *n* || *e*

– X.KID = RDC

– X.ADC = ADC

– X.EOV = EOV

4. Mécanisme d'authentification mutuelle

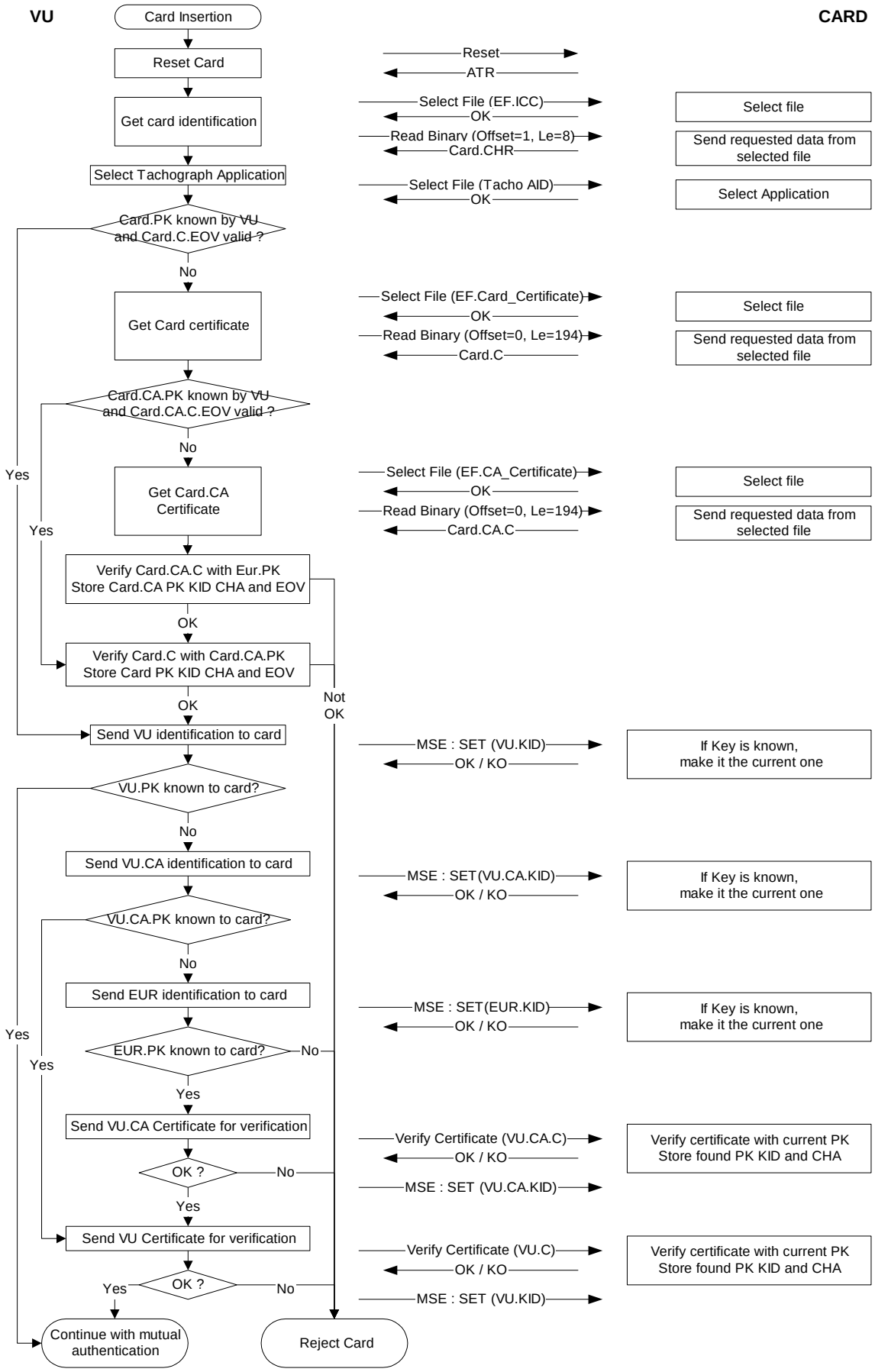
L'authentification mutuelle entre les cartes et les UEV repose sur le principe suivant :

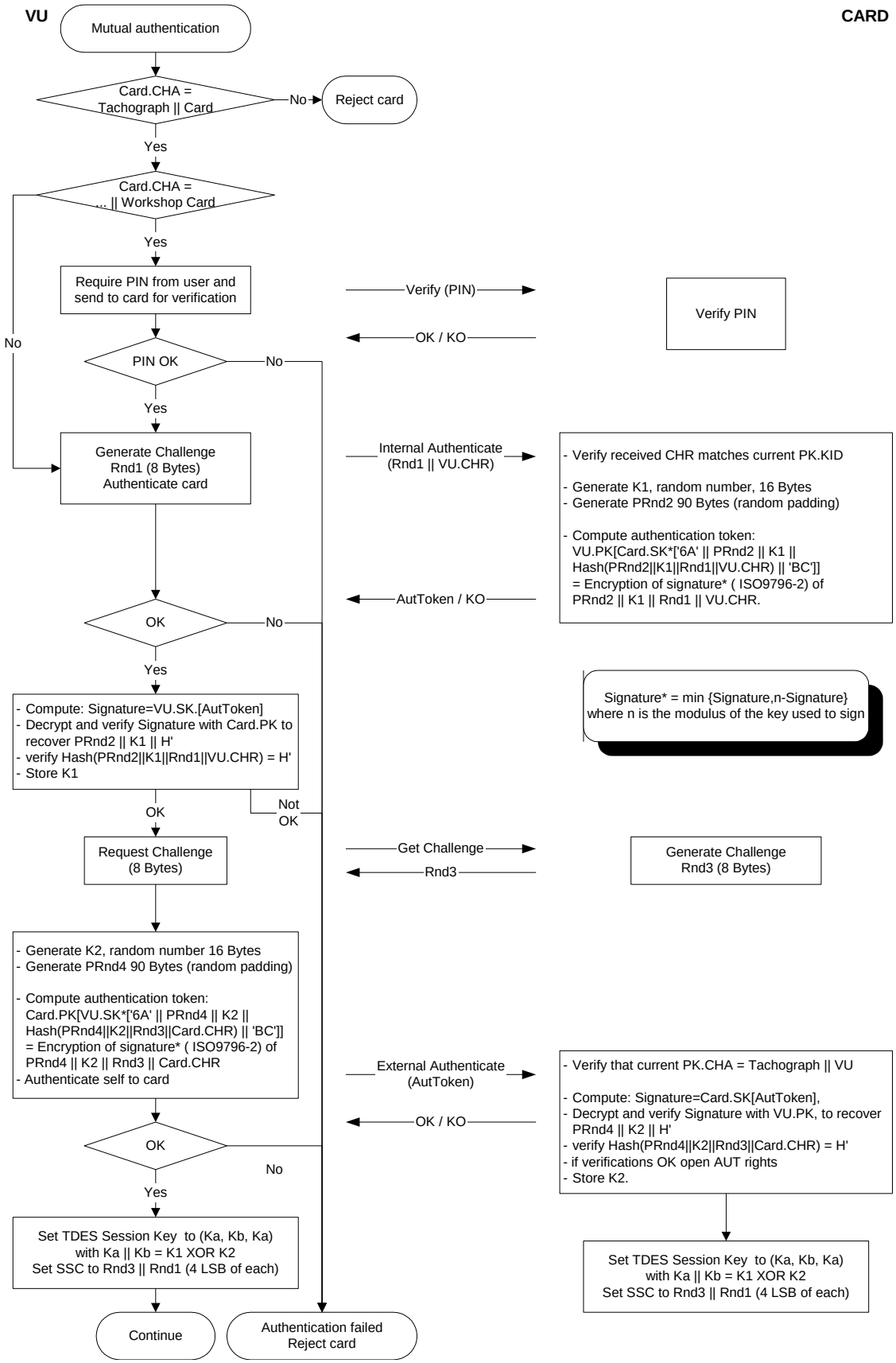
Chacune des parties doit démontrer à l'autre qu'elle possède une paire de clés valide, dont la clé publique a été certifiée par l'autorité de certification ~~nationale~~ compétente **de la Partie contractante concernée**, agréée par l'~~autorité de certification européenne~~**autorité de certification racine.**

Cette démonstration consiste à signer avec la clé privée un nombre aléatoire envoyé par l'autre partie, laquelle doit récupérer, lors de la vérification de cette signature, le nombre aléatoire préalablement envoyé.

L'UEV concernée déclenche le mécanisme d'authentification à l'insertion de la carte. La procédure commence par l'échange des certificats et le dévoilement des clés publiques ; elle prend fin avec la définition d'une clé de session.

CSM_020 On utilisera le protocole ci-après [les flèches indiquent les commandes et données échangées (voir **sous-**appendice 2)] :


VU
CARD
Card Insertion
Reset Card
Reset
ATR
Get card identification
Select File (EF.ICC)
OK
Select file
Read Binary (Offset=1, Le=8)
Card.CHR
Send requested data from selected file
Select Tachograph Application
Select File (Tacho AID)
OK
Select Application
Card.PK known by VU and Card.C.EOV valid ?
No
Get Card certificate
Select File (EF.Card_Certificate)
OK
Select file
Read Binary (Offset=0, Le=194)
Card.C
Send requested data from selected file
Card.CA.PK known by VU and Card.CA.C.EOV valid ?
No
Yes
Get Card.CA Certificate
Select File (EF.CA_Certificate)
OK
Select file
Read Binary (Offset=0, Le=194)
Card.CA.C
Send requested data from selected file
Yes
Verify Card.CA.C with Eur.PK
Store Card.CA PK KID CHA and EOV
OK
Verify Card.C with Card.CA.PK
Store Card PK KID CHA and EOV
OK
Not OK
Send VU identification to card
MSE : SET (VU.KID)
OK / KO
If Key is known, make it the current one
VU.PK known to card?
No
Send VU.CA identification to card
MSE : SET(VU.CA.KID)
OK / KO
If Key is known, make it the current one
VU.CA.PK known to card?
No
Send EUR identification to card
MSE : SET(EUR.KID)
OK / KO
If Key is known, make it the current one
Yes
EUR.PK known to card?
No
Yes
Yes
Send VU.CA Certificate for verification
Verify Certificate (VU.CA.C)
OK / KO
Verify certificate with current PK Store found PK KID and CHA
OK ?
No
MSE : SET (VU.CA.KID)
Yes
Send VU Certificate for verification
Verify Certificate (VU.C)
OK / KO
Verify certificate with current PK Store found PK KID and CHA
Yes
OK ?
No
MSE : SET (VU.KID)
Continue with mutual authentication
Reject Card


VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
No
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
OK
Not OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

5. Mécanismes de confidentialité, d'intégrité et d'authentification des données transférées entre les UEV et les cartes

5.1 Messagerie sécurisée

CSM_021 L'intégrité des transferts de données entre les UEV et les cartes doit être préservée par un dispositif de messagerie sécurisée, conformément aux normes de référence [ISO/CEI 7816-4] et [ISO/CEI 7816-8].

CSM_022 Si la protection de données s'impose pendant leur transfert, le système adjoint un objet de données du type total de contrôle cryptographique aux objets de données transmis dans la commande ou la réponse. Le récepteur procède à la vérification du total de contrôle cryptographique.

CSM_023 Le total de contrôle cryptographique des données transmises dans une commande comprend l'en-tête de commande ainsi que la totalité des objets de données envoyés (= > CLA = '0C' et tous les objets de données sont encapsulés avec des balises au sein desquelles b1=1).

CSM_024 Les octets d'état et les octets de données transmis en réponse sont protégés par un total de contrôle cryptographique lorsque cette réponse ne comporte aucune zone de données.

CSM_025 Les totaux de contrôle cryptographiques mesurent 4 octets de long.

Par conséquent, en cas de recours à la messagerie sécurisée, les commandes et réponses présentent la structure suivante :

Les objets de données utilisés sont un jeu partiel des objets de données de messagerie sécurisée décrits dans la norme ISO/CEI 7816-4.

Balise	*Mnémonique*	*Signification*
'81'	T_{VC}	Valeur en clair non codée en BER-TLV (à protéger par CC)
'97'	**T_{LE}**	Valeur de Le dans la commande non sécurisée (à protéger par CC)
'99'	T_{ME}	Informations d'état (à protéger par CC)
'8E'	T_{CC}	Total de contrôle cryptographique
'87'	$T_{IR\ CG}$	Octet indicateur de remplissage || Cryptogramme (valeur en clair non codée en BER-TLV)

Étant donné une paire de réponses à une commande non sécurisée :

En-tête de commande				*Corps de la commande*		
CLA	INS	P1	P2	[Zone L_c]	[Zone de données]	[Zone L_e]
4 octets				Octets L, indiquant B_1 à B_L		

Corps de la réponse	*En queue de réponse*	
[Zone de données]	ME1	ME2
Octets de données L_r	2 octets	

La paire de réponses à une commande sécurisée correspondante se présente comme suit :

Commande sécurisée :

En-tête de commande (EC)				**Corps de la commande**											
CLA	INS	P1	P2	[Nouvelle zone L_c]	[Nouvelle zone de données]										[Nouvelle zone L_e]
‘OC’				Longueur de la nouvelle zone de données	T_{VC}	L_{VC}	VC	**T_{LE}**	L_{LE}	L_e	T_{CC}	L_{CC}	CC		‘00’
					‘81’	L_c	Zone de données	‘97’	‘01’	L_e	‘8E’	‘04’	CC		

Données à intégrer dans le total de contrôle = EC || OR || T_{VC} || L_{VC} || VC || T_{LE} || L_{LE} || L_e || OR

OR = Octets de remplissage (80 .. 00) selon la méthode n° 2 définie dans les normes ISO/CEI 7816-4 et ISO 9797.

Les objets de données VC et LE ne sont présents que si la commande non sécurisée comporte un certain nombre de données correspondantes.

Réponse sécurisée :

1. Cas où la zone de données de la réponse n’est pas vide et ne nécessite aucune protection à des fins de confidentialité :

Corps de la réponse						*En queue de réponse*
		[Nouvelle zone de données]				Nouveaux ME1 ME2
T_{VC}	L_{VC}	VC	T_{CC}	L_{CC}	CC	
‘81’	L_r	Zone de données	‘8E’	‘04’	CC	

Données à intégrer dans le total de contrôle = T_{VC} || L_{VC} || VC || OR

2. Cas où la zone de données de la réponse n’est pas vide et nécessite une protection garantissant sa confidentialité :

Corps de la réponse						*En queue de réponse*
		[Nouvelle zone de données]				Nouveaux ME1 ME2
$T_{IR\ CG}$	$L_{IR\ CG}$	IR CG	T_{CC}	L_{CC}	CC	
‘87’		IR || CG	‘8E’	‘04’	CC	

Données à acheminer par CG : données non codées en BER-TLV et octets de remplissage.

Données à intégrer dans le total de contrôle = $T_{IR\ CG}$ || $L_{IR\ CG}$ || IR CG || OR

3. Cas où la zone de données de la réponse est vide :

Corps de la réponse						*En queue de réponse*
		[Nouvelle zone de données]				Nouveaux ME1 ME2
T_{ME}	L_{ME}	ME	T_{CC}	L_{CC}	CC	
‘99’	‘02’	Nouveaux ME1 ME2	‘8E’	‘04’	CC	

Données à intégrer dans le total de contrôle = T_{ME} || L_{ME} || ME || OR

5.2 Traitement des erreurs de messagerie sécurisée

CSM_026 Si la carte tachygraphique détecte une erreur de messagerie sécurisée lors de l’interprétation d’une commande, les octets d’état correspondants doivent être renvoyés sans messagerie sécurisée.

Conformément à la norme ISO/CEI 7816-4, les octets d'état suivants sont prévus pour indiquer les erreurs de messagerie sécurisée :

'66 88' : échec de la vérification du total de contrôle cryptographique ;

'69 87' : objets de données de messagerie sécurisée attendus manquants ;

'69 88' : objets de données de messagerie sécurisée incorrects.

CSM_027 Si la carte tachygraphique renvoie des octets d'état sans objet de données de messagerie sécurisée ou avec un objet de données de messagerie sécurisée erroné, l'UEV doit mettre fin à la session en cours.

5.3 Algorithme de calcul des totaux de contrôle cryptographique

CSM_028 La constitution des totaux de contrôle cryptographiques se fait à l'aide d'un code d'authentification de message (Retail MAC) chiffré DES, conformément à la norme ANSI X9.19 :

- Phase initiale : le bloc de contrôle initial y0 est E(Ka, CSE) ;
- Phase séquentielle : les blocs de contrôle y1, .. , yn se calculent à l'aide de Ka ;
- Phase finale : le total de contrôle cryptographique se calcule à partir du dernier bloc de contrôle yn en procédant comme suit : E(Ka, D(Kb, yn)).

Où l'abréviation E() signifie chiffrement avec DES et l'abréviation D() déchiffrement avec DES.

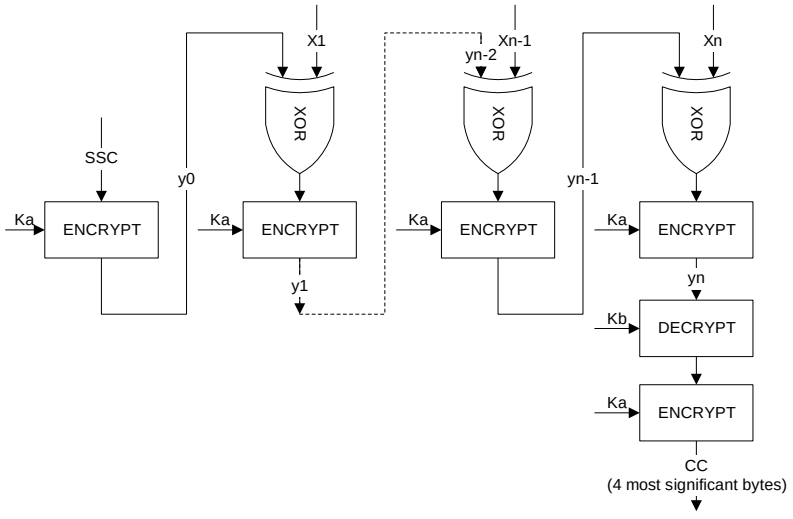
Les quatre octets les plus significatifs du total de contrôle cryptographique sont transférés.

CSM_029 Le compteur de séquences d'envoi (CSE) est lancé pendant la procédure de concordance de clés :

CSE initial : Rnd3 (4 octets les moins significatifs) || Rnd1 (4 octets les moins significatifs).

CSM_030 Le compteur de séquences d'envoi est incrémenté d'une unité avant le calcul de chaque MAC (en d'autres termes, le CSE associé à la première commande correspond au CSE initial + 1, tandis que le CSE associé à la première réponse correspond au CSE initial + 2).

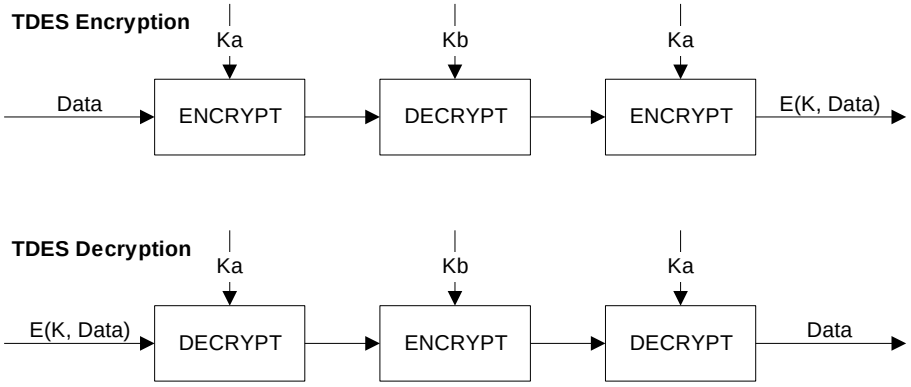
La figure ci-après illustre le calcul du Retail MAC :



5.4 Algorithme de calcul des cryptogrammes garantissant la confidentialité des objets de données

CSM_031 Les cryptogrammes se calculent à l'aide de l'algorithme TDES en mode de chiffrement TCBC conformément aux normes [TDES] et [TDES-OP] de référence et avec le vecteur nul comme bloc de valeur initial.

La figure qui suit illustre l'application des clés chiffrées TDES : *(voir la traduction à la fin du présent sous-appendice)*



6. Mécanismes de signature numérique des téléchargements de données

CSM_032 L'équipement spécialisé intelligent (ESI) enregistre dans un seul fichier physique les données transmises à partir d'un équipement (UEV ou carte) donné pendant une session de téléchargement. Ce fichier doit contenir les certificats MS_i.C et EQT.C. Il contient également les signatures numériques associées aux blocs de données conformément aux indications fournies dans ~~l'appendice~~ **le sous-appendice** 7 (Protocoles de téléchargement des données).

CSM_033 Les signatures numériques des données téléchargées doivent reposer sur une structure de signature numérique avec appendice, de sorte que les données téléchargées puissent être lues sans aucun déchiffrement, le cas échéant.

6.1 Génération des signatures

CSM_034 La génération de signatures de données par l'équipement doit respecter la structure de signature avec appendice défini dans le document de référence [PKCS1] et se faire au moyen de la fonction de hachage SHA-1 :

Signature = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(Données))]

PS = chaîne d'octets de remplissage de valeur ‘FF’ dont la longueur équivaut à 128.

DER(SHA-1(*M*)) correspond au codage de l'ID de l'algorithme pour la fonction de hachage et la valeur de hachage dans une valeur ASN.1 de type `DigestInfo` (distinguished encoding rules) :

‘30’||’21’||’30’||’09’||’06’||’05’||’2B’||’0E’||’03’||’02’||’1A’||’05’||’00’||’04’||’14’‖valeur de hachage.

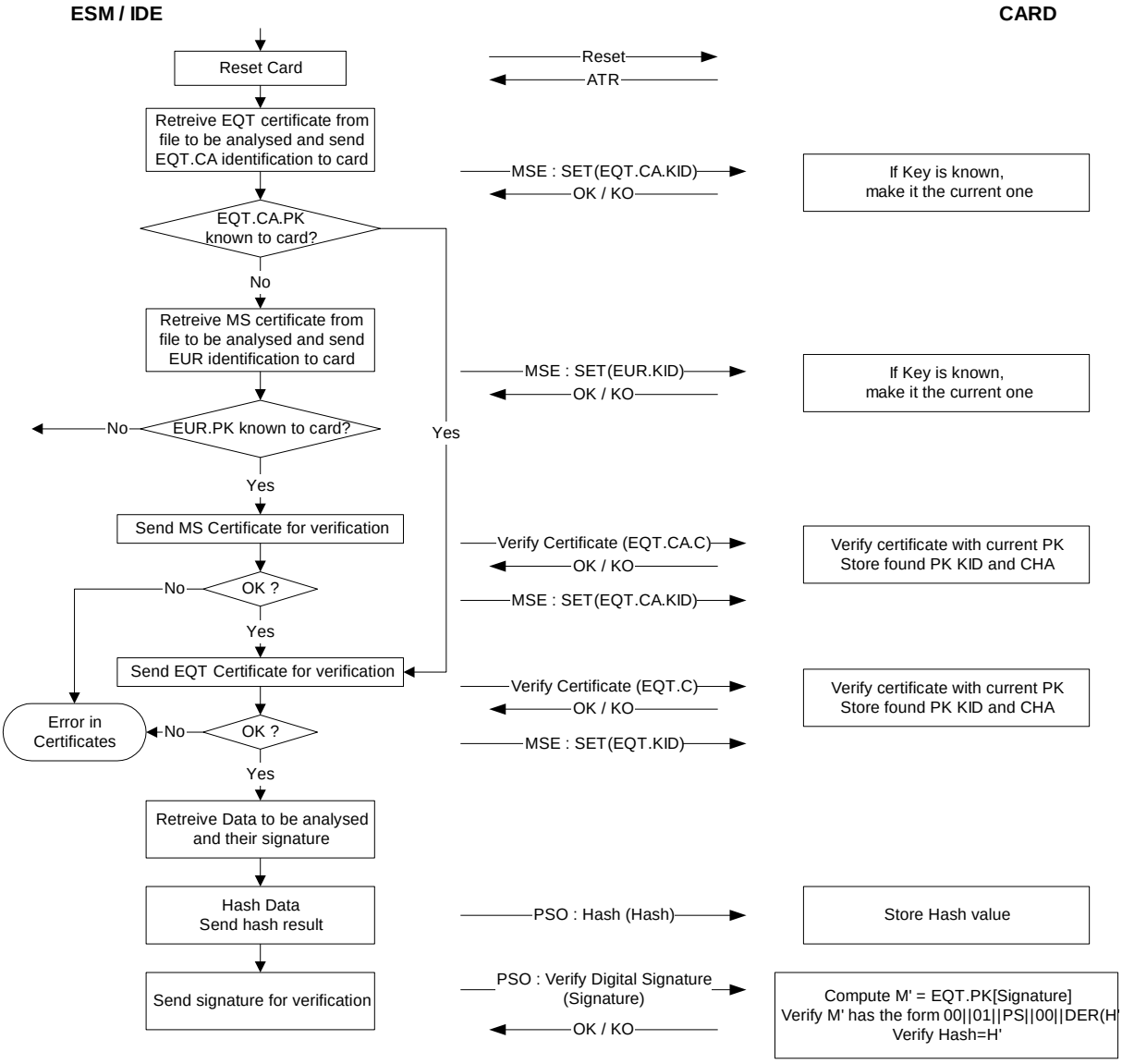
6.2 Vérification des signatures

CSM_035 La vérification de la signature des données téléchargées doit respecter la structure de signature avec appendice défini dans le document de référence [PKCS1] et se faire au moyen de la fonction de hachage SHA-1.

Le vérificateur doit connaître de façon indépendante (et approuver) la clé publique ~~européenne~~ **racine** EUR.PK.

Le tableau qui suit illustre le protocole qu'un ESI associé à une carte de contrôleur peut appliquer pour vérifier l'intégrité des données téléchargées et enregistrées sur le support de mémoire externe. La carte de contrôleur permet de déchiffrer les signatures numériques. De ce fait, cette fonction n'est pas nécessairement implémentée dans l'ESI.

L'équipement qui a téléchargé et signé les données à analyser est désigné par l'abréviation EQT.



PARTIE B TACHYGRAPHES DE DEUXIÈME GÉNÉRATION

7. Introduction

7.1 Références

Dans le présent **sous-**appendice, il est fait référence aux documents suivants :

AES	National Institute of Standards and Technology (NIST), FIPS PUB 197: Advanced Encryption Standard, 26 novembre 2001.
DSS	National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), juillet 2013.
ISO 7816-4	ISO/CEI 7816-4 Cartes d'identification − Cartes à circuit intégré − Partie 4 : organisation, sécurité et commandes pour les échanges, troisième édition, 15 avril 2013.
ISO 7816-8	ISO/CEI 7816-8 Cartes d'identification − Cartes à circuit intégré − Partie 8 : commandes pour des opérations de sécurité, seconde édition, 1er juin 2004.
ISO 8825-1	ISO/CEI 8825-1 Technologies de l'information − Règles de codage ASN.1 : Spécification des règles de codage de base (BER), des règles de codage canoniques (CER) et des règles de codage distinctives (DER), quatrième édition, 15 décembre 2008.
ISO 9797-1	ISO/CEI 9797-1 Technologies de l'information − Techniques de sécurité − Codes d'authentification de message (MAC) − Partie 1 : mécanismes utilisant un chiffrement par blocs, seconde édition, 1er mars 2011.
ISO 10116	ISO/CEI 10116 Technologies de l'information − Techniques de sécurité − Modes opératoires pour un chiffrement par blocs de *n* bits, troisième édition, 1er février 2006.
ISO16844-3	ISO/CEI 16844-3 Véhicules routiers − Systèmes tachygraphes − Partie 3 : interface de capteur de mouvement, première édition, 2004, et rectificatif technique 1:2006
RFC 5480	Elliptic Curve Cryptography Subject Public Key Information, mars 2009
RFC 5639	Elliptic Curve Cryptography (ECC) - Brainpool Standard Curves and Curve Generation, 2010
RFC 5869	HMAC-based Extract-and-Expand Key Derivation Function (HKDF), mai 2010.
SHS	National Institute of Standards and Technology (NIST), FIPS PUB 180-4: Secure Hash Standard, mars 2012.
SP 800-38B	National Institute of Standards and Technology (NIST), Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005.
TR-03111	BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 28 juin 2012.

7.2 Notations et abréviations

Les notations et abréviations qui suivent apparaissent dans le présent **sous-**appendice :

AES	Norme de chiffrement avancé (*Advanced Encryption Standard*)
AC	Autorité de certification
RAC	Référence de l'autorité de certification
CBC	Chiffrement par chaînage de blocs (mode opératoire)
EC	En-tête de commande
ADC	Autorisation du détenteur de certificat
RDC	Référence du détenteur de certificat *(Certificate Holder Reference)*
VC	Vecteur constant
DER	Règles de codage distinctives (*Distinguished Encoding Rules*)
OD	Objet de données
DSRC	Communication spécialisée à courte portée
ECC	Cryptographie à courbe elliptique (*Elliptic Curve Cryptography*)
ECDSA	Algorithme de signature numérique à courbe elliptique (*Elliptic Curve Digital Signature Algorithm*)
ECDH	Courbe elliptique de Diffie-Hellman (algorithme de concordance de clé)
DGE	Dispositif GNSS externe *(EGF, en anglais)*
EQT	Équipement
SID	Identificateur de service
K_M	Clé maîtresse du capteur de mouvement permettant le couplage d'une unité embarquée avec un capteur de mouvement
$K_{M\text{-}UEV}$	Clé insérée dans les unités embarquées et permettant à une UEV d'extraire la clé maîtresse du capteur de mouvement si une carte d'atelier est insérée dans l'un de ses lecteurs
$K_{M\text{-}CAT}$	Clé insérée dans les cartes d'atelier et permettant à une UEV d'extraire la clé maîtresse du capteur de mouvement si une carte d'atelier est insérée dans l'un de ses lecteurs
MAC	Code d'authentification de message
PKI	Infrastructure à clés publiques (ICP) ou infrastructure de gestion de clés (IGC)
RCF	Dispositif de communication à distance
CSE	Compteur de séquences d'envoi
MS	Messagerie sécurisée
TDES	Triple DES (*Triple Data Encryption Standard*)
TLV	Structure balise-longueur-valeur (*Tag-Length-Value*)
UEV	Unité embarquée sur le véhicule *(VU, en anglais)*
X.C	Certificat de clé publique d'un utilisateur X
X.AC	Autorité de certification qui a émis le certificat d'un utilisateur X
X.RAC	Référence de l'autorité de certification mentionnée dans le certificat d'un utilisateur X

X.RDC	Référence du détenteur du certificat mentionné dans le certificat d'un utilisateur X
X.PK	Clé publique d'un utilisateur X
X.SK	Clé privée d'un utilisateur X
$X.PK_{eph}$	Clé publique éphémère d'un utilisateur X
$X.SK_{eph}$	Clé privée éphémère d'un utilisateur X
′xx′	Valeur hexadécimale
||	Opérateur de concaténation

7.3 Définitions

Les définitions des termes utilisés dans le présent **sous-**appendice figurent au chapitre 1 de ~~l'annexe~~ **l'appendice** 1C.

8. Systèmes et algorithmes cryptographiques

8.1 Systèmes cryptographiques

CSM_38 Les unités embarquées et les cartes tachygraphiques ont recours à un système cryptographique à clé publique fondé sur les courbes elliptiques pour assurer les services de sécurité suivants :

- Authentification mutuelle entre une unité embarquée et une carte ;
- Concordance des clés de session AES entre une unité embarquée et une carte ;
- Garantie de l'authenticité, de l'intégrité et de la non-répudiation des données téléchargées depuis les unités embarquées ou les cartes tachygraphiques vers un support de mémoire externe.

CSM_39 Les unités embarquées et les dispositifs GNSS externes ont recours à un système cryptographique à clé publique fondé sur les courbes elliptiques pour assurer les services de sécurité suivants :

- Couplage d'une unité embarquée et d'un dispositif GNSS externe ;
- Authentification mutuelle entre une unité embarquée et un dispositif GNSS externe ;
- Concordance d'une clé de session AES entre une unité embarquée et un dispositif GNSS externe.

CSM_40 Les unités embarquées et les cartes tachygraphiques ont recours à un système cryptographique AES symétrique pour assurer les services de sécurité suivants :

- Garantie de l'authenticité et de l'intégrité des données échangées entre une unité embarquée et une carte tachygraphique ;
- Le cas échéant, garantie de la confidentialité des données échangées entre une unité embarquée et une carte tachygraphique.

CSM_41 Les unités embarquées et les dispositifs GNSS externes ont recours à un système cryptographique AES symétrique pour assurer les services de sécurité suivants :

- Garantie de l'authenticité et de l'intégrité des données échangées entre une unité embarquée et un dispositif GNSS externe.

CSM_42 Les unités embarquées et les capteurs de mouvement ont recours à un système cryptographique AES symétrique pour assurer les services de sécurité suivants :

- Couplage d'une unité embarquée et d'un capteur de mouvement ;
- Authentification mutuelle entre une unité embarquée et un capteur de mouvement ;
- Garantie de la confidentialité des données échangées entre une unité embarquée et un capteur de mouvement.

CSM_43 Les unités embarquées et les cartes de contrôleur ont recours à un système cryptographique AES symétrique pour assurer les services de sécurité suivants :

- Garantie de la confidentialité, de l'authenticité et de l'intégrité des données transmises par une unité embarquée à une carte de contrôleur.

Remarques :

- Plus précisément, les données sont transmises par une unité embarquée à un interrogateur à distance sous le contrôle d'un agent de contrôle, au moyen d'un dispositif de communication à distance interne ou externe à l'UEV (voir **sous-**appendice 14). L'interrogateur à distance envoie les données reçues à une carte de contrôleur qui les déchiffre et confirme leur authenticité. Du point de vue de la sécurité, le dispositif de communication à distance et l'interrogateur à distance sont entièrement transparents ;
- Une carte d'atelier offre les mêmes services de sécurité au niveau de l'interface DSRC qu'une carte de contrôleur. Cela permet à un atelier de garantir le bon fonctionnement, ainsi que la sécurité, de l'interface de communication à distance d'une UEV. Pour de plus amples informations, voir la section **9.2.2**~~9.2.3~~.

8.2 Algorithmes cryptographiques

8.2.1 Algorithmes symétriques

CSM_44 Les unités embarquées, les cartes tachygraphiques, les capteurs de mouvement et les dispositifs GNSS externes doivent être compatibles avec l'algorithme AES défini dans la norme [AES], avec des longueurs de clés de 128, 192 et 256 bits.

8.2.2 Algorithmes asymétriques et paramètres de domaine normalisés

CSM_45 Les unités embarquées, les cartes tachygraphiques et les dispositifs GNSS externes doivent être compatibles avec la cryptographie à courbe elliptique et respecter les longueurs de clés de 256, 384 et 512/521 bits.

CSM_46 Les unités embarquées, les cartes tachygraphiques et les dispositifs GNSS externes doivent prendre en charge l'algorithme de signature ECDSA défini dans la norme [DSS].

CSM_47 Les unités embarquées, les cartes tachygraphiques et les dispositifs GNSS externes doivent prendre en charge l'algorithme de concordance de clé ECKA-EG défini dans la norme [TR 03111].

CSM_48 Les unités embarquées, les cartes tachygraphiques et les dispositifs GNSS externes doivent prendre en charge tous les paramètres de domaines normalisés définis dans le **tableau 1** ci-dessous pour la cryptographie à courbe elliptique.

Tableau 1
Paramètres de domaine normalisés

Nom	*Taille (en bits)*	*Référence*	*Identificateur d'objet*
NIST P-256	256	[DSS], [RFC 5480]	secp256r1
BrainpoolP256r1	256	[RFC 5639]	brainpoolP256r1

Nom	*Taille (en bits)*	*Référence*	*Identificateur d'objet*
NIST P-384	384	[DSS], [RFC 5480]	secp384r1
BrainpoolP384r1	384	[RFC 5639]	brainpoolP384r1
BrainpoolP512r1	512	[RFC 5639]	brainpoolP512r1
NIST P-521	521	[DSS], [RFC 5480]	secp521r1

Remarque : les identificateurs d'objet mentionnés dans la dernière colonne du ~~tableau 43~~ **tableau 1** sont spécifiés dans le document [RFC 5639] pour les courbes Brainpool et dans le document [RFC 5480] pour les courbes NIST.

Exemple 1 : l'identificateur d'objet de la courbe de BrainpoolP256r1 est {iso(1) identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8) ellipticCurve(1) versionOne(1) 7}.

En notation par points : 1.3.36.3.3.2.8.1.1.7.

Exemple 2 : l'identificateur d'objet de la courbe NIST P-384 est

{iso(1) identified-organization(3) certicom(132) curve(0) 34}.

En notation par points : 1.3.132.0.34.

8.2.3 Algorithmes de hachage

CSM_49 Les unités embarquées**,** ~~et~~ les cartes tachygraphiques **et les dispositifs GNSS externes** doivent être compatibles avec les algorithmes SHA-256, SHA-384 et SHA-512 définis dans la norme [SHS].

8.2.4 Suite cryptographique

CSM_50 Dans le cas où un algorithme symétrique, un algorithme asymétrique et/ou un algorithme de hachage sont associés pour former un protocole de sécurité, leur longueur de clé et taille de hachage respectives doivent être de force (à peu près) égale. Le ~~tableau 44~~ **tableau 2 ci-dessous** montre les suites cryptographiques autorisées.

Tableau 2
Suites cryptographiques autorisées

ID de la suite cryptographique	*Taille de clé ECC (en bits)*	*Longueur de clé AES (en bits)*	*Algorithme de hachage*	*Longueur MAC (en octets)*
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Remarque : les clés ECC de 512 et de 521 bits sont considérées comme étant de force égale aux fins du présent **sous-**appendice.

9. Clés et certificats

9.1 Paires de clés asymétriques et certificats de clé publique

9.1.1 Généralités

Remarque : les clés décrites dans cette section servent à l'authentification mutuelle et aux échanges par messagerie sécurisée entre les unités embarquées et les cartes tachygraphiques, ainsi qu'entre les unités embarquées et les dispositifs GNSS externes. Ces processus sont décrits en détail dans les chapitres 0 et 0 du présent **sous-**appendice.

CSM_51 Au sein du système ~~européen~~ de tachygraphe intelligent, les paires de clés ECC et leurs certificats sont générés et gérés selon trois niveaux hiérarchiques de fonctionnement :

- Niveau ~~européen~~ **racine ;**
- Niveau ~~État membre~~ **Partie contractante ;**
- Niveau équipement.

CSM_52 Dans l'ensemble du système ~~européen~~ de tachygraphe intelligent, les clés privées et publiques ainsi que les certificats correspondants sont générés, gérés et communiqués à l'aide de méthodes normalisées et sécurisées.

9.1.2 ~~Niveau européen~~ Niveau racine

CSM_53 Au niveau ~~européen~~ **racine**, une seule paire de clés ECC, désignée par l'abréviation EUR, est générée. Elle se compose d'une clé privée (EUR.SK) et d'une clé publique (EUR.PK). Cette paire de clés forme la paire racine de la PKI de l'ensemble des tachygraphes intelligents ~~européens~~. Cette tâche est assurée par une autorité de certification racine ~~européenne~~ (ERCA)~~, placée sous l'autorité et la responsabilité de la Commission européenne~~.

CSM_54 L'ERCA utilise la clé privée ~~européenne~~ **racine** pour signer un certificat racine (auto-signé) de la clé publique ~~européenne~~ **racine** et communique ce certificat racine ~~européen~~ à ~~tous les États membres~~ **toutes les Parties contractantes.**

CSM_55 L'ERCA utilise la clé privée ~~européenne~~ **racine** pour signer les certificats des clés publiques des ~~États membres~~ **Parties contractantes** qui en font la demande. L'ERCA tient un registre de tous les certificats de clé publique signés qu'elle a délivrés aux ~~États membres~~ **Parties contractantes**.

CSM_56 Comme le montre la figure 1 de la section 9.1.7, l'ERCA génère une nouvelle paire de clés racine ~~européenne~~ tous les 17 ans. Chaque fois que l'ERCA génère une nouvelle paire de clés racine ~~européenne~~, elle crée un nouveau certificat racine auto-signé pour la nouvelle clé publique ~~européenne~~ **racine**. La durée de validité d'un certificat racine ~~européen~~ est de 34 ans plus trois mois.

Remarque : l'introduction d'une nouvelle paire de clés racine implique également que l'ERCA génère une nouvelle clé maîtresse pour le capteur de mouvement et une nouvelle clé maîtresse DSRC (voir sect. ~~9.2.2.2 et 9.2.3.2~~ **9.2.1.2 et 9.2.2.2**).

CSM_57 Avant de générer une nouvelle paire de clés racine ~~européenne~~, l'ERCA doit évaluer la force cryptographique dont aura besoin la nouvelle paire de clés, étant donné que celle-ci devra rester sécurisée pendant les 34 prochaines années. Si cela se révèle nécessaire, l'ERCA adopte une suite cryptographique plus puissante que la suite actuelle, comme indiqué au point ~~TCS_192~~ **CSM_50**.

CSM_58 Chaque fois qu'elle génère une nouvelle paire de clés racine ~~européenne~~, l'ERCA crée un nouveau certificat de lien destiné à la nouvelle clé publique ~~européenne~~ **racine** et le signe avec la clé privée ~~européenne~~ **racine** précédente. La durée de validité du certificat de lien est de 17 ans **plus trois mois**. La **figure 1** de la section **9.1.7** illustre ce processus.

Remarque : un certificat de lien contient la clé publique ERCA de génération *X* et il est signé avec la clé privée ERCA de génération *X-1*. Il offre donc aux équipements de génération *X-1* une méthode pour s'assurer de la fiabilité d'un équipement de génération *X*.

CSM_59 L'ERCA n'utilise pas la clé privée d'une paire de clés racine à d'autres fins après le début de validité d'un nouveau certificat de clé racine.

CSM_60 À tout moment, l'ERCA doit disposer des clés et des certificats cryptographiques suivants :

- La paire de clés EUR en vigueur et le certificat correspondant ;
- Tous les certificats EUR antérieurs à utiliser pour vérifier les certificats MSCA toujours valables ;
- Les certificats de lien de toutes les générations de certificats EUR à l'exception du premier.

9.1.3 Niveau ~~État membre~~ Partie contractante

CSM_61 Au niveau ~~État membre~~ **Partie contractante**, ~~tous les États membres~~ **toutes les Parties** contractantes tenues de signer les certificats des cartes tachygraphiques génèrent une ou plusieurs paires de clés ECC uniques, désignées par l'appellation MSCA_Card. ~~Tous les États membres~~ **Toutes les Parties contractantes** tenues de signer les certificats des unités embarquées ou des dispositifs GNSS externes génèrent en plus une ou plusieurs paires de clés ECC uniques, désignées par l'appellation MSCA_UEV-DGE.

CSM_62 La tâche consistant à générer des paires de clés destinée à un**e** ~~État membre~~ **Partie contractante** incombe à l'autorité de certification de ~~l'État membre~~ **la Partie contractante** (MSCA). Chaque fois qu'une MSCA génère une paire de clés pour un**e** ~~État membre~~ **Partie contractante**, elle doit envoyer la clé publique à l'ERCA afin d'obtenir un certificat propre à ~~l'État membre~~ **la Partie contractante** correspondant**e**, signé par l'ERCA.

CSM_63 Une MSCA choisit pour la paire de clés de ~~l'État membre~~ **la Partie contractante** une force égale à celle de la paire de clés racine ~~européenne~~ servant à signer le certificat de ~~l'État membre~~ **la Partie contractante** correspondant**e**.

CSM_64 Une paire de clés MSCA_UEV-DGE, le cas échéant, se compose d'une clé privée MSCA_UEV-DGE.SK et d'une clé publique MSCA_UEV-DGE.PK. Une MSCA utilise la clé privée MSCA_UEV-DGE.SK exclusivement pour signer les certificats de clé publique des unités embarquées et des dispositifs GNSS externes.

CSM_65 Une paire de clés MSCA_Card se compose d'une clé privée MSCA_Card.SK et d'une clé publique MSCA_Card.PK. Une MSCA utilise la clé privée MSCA_Card.SK exclusivement pour signer les certificats de clé publique des cartes tachygraphiques.

CSM_66 Une MSCA archive tous les certificats d'UEV, de dispositifs GNSS externes et de cartes signées ainsi que l'identification de l'équipement auquel chacun de ces certificats est destiné.

CSM_67 La durée de validité d'un certificat MSCA_UEV-DGE est de 17 ans plus trois mois. La durée de validité d'un certificat MSCA_Card est de 7 ans plus un mois.

CSM_68 Comme l'illustre la **figure 1** de la section **9.1.7**, la clé privée d'une paire de clés MSCA_UEV-DGE et la clé privée d'une paire de clé MSCA_Card ont une période d'utilisation de deux ans.

CSM_69 Une MSCA ne doit pas utiliser la clé privée d'une paire de clés MSCA_UEV-DGE à quelque fin que ce soit après l'expiration de sa période d'utilisation. De même, une MSCA ne doit pas utiliser la clé

privée d'une paire de clés MSCA_Card à quelque fin que ce soit après l'expiration de sa période d'utilisation.

CSM_70 À tout moment, une MSCA doit disposer des clés et des certificats cryptographiques suivants :

- La paire de clés MSCA_Card en vigueur et le certificat correspondant ;
- Tous les certificats MSCA_Card antérieurs à utiliser pour vérifier les certificats des cartes tachygraphiques toujours valides ;
- Le certificat EUR en vigueur nécessaire pour vérifier le certificat MSCA en vigueur ;
- Tous les certificats EUR antérieurs nécessaires pour vérifier tous les certificats MSCA toujours valables.

CSM_71 Si une MSCA doit signer des certificats pour des unités embarquées ou pour des dispositifs GNSS externes, elle doit en outre disposer des clés et certificats suivants :

- La paire de clés MSCA_UEV-DGE en vigueur et le certificat correspondant ;
- Toutes les clés publiques MSCA_UEV-DGE antérieures à utiliser pour vérifier les certificats des UEV ou des dispositifs GNSS externes toujours valables.

9.1.4 Niveau équipement : unités embarquées sur le véhicule

CSM_72 Deux paires de clés ECC uniques, désignées par UEV_MA et UEV_Sign, sont générées pour chaque unité embarquée. Cette tâche incombe aux fabricants d'UEV. Chaque fois qu'une paire de clés destinée à une UEV est générée, la partie qui la génère doit envoyer la clé publique à la MSCA **compétente** ~~de son pays de résidence~~ afin d'obtenir le certificat d'UEV correspondant, signé par la MSCA. La clé privée n'est utilisée que par l'unité embarquée sur le véhicule.

CSM_73 Les certificats UEV_MA et UEV_Sign attribués à une unité embarquée donnée ont la même date d'entrée en vigueur.

CSM_74 Un fabricant d'UEV doit attribuer à une paire de clés d'UEV une force égale à celle de la paire de clés MSCA servant à signer le certificat d'UEV correspondant.

CSM_75 Une unité embarquée utilise sa paire de clés UEV_MA, composée d'une clé privée UEV_MA.SK et d'une clé publique UEV_MA.PK, exclusivement pour procéder à l'authentification des cartes tachygraphiques et des dispositifs GNSS externes, comme indiqué aux sections **10.3 et 11.4 du présent sous-appendice**.

CSM_76 Une unité embarquée doit pouvoir générer des paires de clés ECC éphémères, qu'elle utilisera exclusivement pour procéder à la concordance des clés de session avec une carte tachygraphique ou un dispositif GNSS externe, comme indiqué aux sections **10.4 et 11.4 du présent sous-appendice**.

CSM_77 Une unité embarquée utilise la clé privée UEV_Sign.SK de sa paire de clés UEV_Sign exclusivement pour signer des fichiers de données téléchargés, comme prévu au chapitre **14** du présent **sous-**appendice. La clé publique UEV_Sign.PK correspondante sert exclusivement à vérifier les signatures créées par l'UEV.

CSM_78 Comme le montre la figure **1** de la section **9.1.7**, la durée de validité d'un certificat UEV_MA est de 15 ans et trois mois. La durée de validité d'un certificat UEV_Sign est également de 15 ans et trois mois.

Remarques :

La durée de validité étendue d'un certificat UEV_Sign permet à une unité embarquée de créer des signatures valables pour des données téléchargées pendant les trois premiers mois qui suivent sa date d'expiration~~, comme l'exige le règlement n° 581/2010~~.

La durée de validité étendue d'un certificat UEV_MA est nécessaire pour permettre à l'UEV d'authentifier une carte de contrôleur ou une carte d'entreprise pendant les trois premiers mois qui suivent sa date d'expiration, de sorte qu'il soit possible de télécharger des données.

CSM_79 Une UEV ne doit pas utiliser la clé privée d'une paire de clés d'UEV à quelque fin que ce soit après l'expiration du certificat correspondant.

CSM_80 Les paires de clés d'une UEV donnée (à l'exception des paires de clés éphémères) et les certificats correspondants ne sont ni remplacés ni renouvelés sur le terrain une fois que l'UEV a été mise en service.

Remarques :

Les paires de clés éphémères ne sont pas soumises à cette exigence, car une nouvelle paire de clés éphémères est générée par l'UEV à chaque authentification de circuit et à chaque concordance de clé de session (voir sect. **10.4**). Il convient de noter que les paires de clés éphémères ne possèdent pas de certificats correspondants.

Cette exigence n'interdit pas la possibilité de remplacer les paires de clés d'UEV statiques lors d'une maintenance ou d'une réparation dans un environnement contrôlé et sécurisé par le fabricant de l'UEV.

CSM_81 Lorsqu'elle est mise en service, l'UEV doit contenir les clés et les certificats cryptographiques suivants :

- La clé privée UEV_MA et le certificat correspondant ;
- La clé privée UEV_Sign et le certificat correspondant ;
- Le certificat MSCA_UEV-DGE comprenant la clé publique MSCA_UEV-DGE.PK à utiliser pour vérifier les certificats UEV_MA et UEV_Sign ;
- Le certificat EUR comprenant la clé publique EUR.PK à utiliser pour vérifier le certificat MSCA_UEV-DGE ;
- Le certificat EUR dont la durée de validité précède directement celle du certificat EUR à utiliser pour vérifier le certificat MSCA_UEV-DGE, le cas échéant ;
- Le certificat de lien reliant ces deux certificats EUR, le cas échéant.

CSM_82 Outre les clés et les certificats cryptographiques énumérés au point ~~TCS_223~~ **CSM_81**, les unités embarquées contiennent également les clés et les certificats spécifiés dans la partie A du présent **sous-**appendice, qui permettent à une unité embarquée d'interagir avec les cartes tachygraphiques de première génération.

9.1.5 Niveau équipement : cartes tachygraphiques

CSM_83 Une paire de clés ECC unique, désignée par Card_MA, est générée pour chaque carte tachygraphique. Une deuxième paire de clés ECC unique, désignée par Card_Sign, est générée en plus pour chaque carte de conducteur et chaque carte d'atelier. Cette tâche peut être confiée aux fabricants ou aux configurateurs de cartes. Chaque fois qu'une paire de clés destinée à une carte est générée, la partie qui la génère doit envoyer la clé publique à la MSCA **compétente** ~~de son pays de résidence~~ afin d'obtenir le certificat de carte correspondant, signé par la MSCA. La clé privée est utilisée uniquement par la carte tachygraphique.

CSM_84 Les certificats Card_MA et Card_Sign attribués à une carte de conducteur ou d'atelier donnée ont la même date d'entrée en vigueur.

CSM_85 Un fabricant ou un configurateur de carte doit attribuer à une paire de clés associée à une carte une force égale à celle de la paire de clés MSCA servant à signer le certificat de carte correspondant.

CSM_86 Une carte tachygraphique utilise sa paire de clés Card_MA, composée d'une clé privée Card_MA.SK et d'une clé publique Card_MA.PK, exclusivement pour effectuer des opérations d'authentification mutuelle et de concordance de clés de session avec les UEV, comme indiqué aux sections **10.3 et 10.4 du présent sous-appendice**.

CSM_87 Une carte de conducteur ou d'atelier utilise la clé privée Card_Sign.SK de sa paire de clés Card_Sign exclusivement pour signer des fichiers de données téléchargés, comme prévu au chapitre **14** du présent **sous-**appendice. La clé publique Card_Sign.PK correspondante sert exclusivement à vérifier les signatures créées par la carte.

CSM_88 La durée de validité d'un certificat Card_MA est la suivante :

Pour les cartes de conducteur : 5 ans

Pour les cartes d'entreprise : ~~2~~**5** ans

Pour les cartes de contrôleur : 2 ans

Pour les cartes d'atelier : 1 an

CSM_89 La durée de validité d'un certificat Card_Sign est la suivante :

Pour les cartes de conducteur : 5 ans et 1 mois

Pour les cartes d'atelier : 1 an et 1 mois

Remarque : la durée de validité étendue d'un certificat Card_Sign permet à une carte de conducteur de créer des signatures valables pour des données téléchargées pendant le premier mois qui suit sa date d'expiration. ~~Cela est nécessaire en vertu du règlement (UE) n° 581/2010 qui exige qu'un téléchargement de données depuis une carte de conducteur soit possible jusqu'à 28 jours après la mémorisation des dernières données.~~

CSM_90 Les paires de clés d'une carte tachygraphique donnée et les certificats correspondants ne sont ni remplacés ni renouvelés après l'émission de ladite carte.

CSM_91 Une fois émises, les cartes tachygraphiques doivent contenir les clés et les certificats cryptographiques suivants :

- La clé privée Card_MA et le certificat correspondant ;
- En sus, pour les cartes de conducteur et d'atelier : la clé privée Card_Sign et le certificat correspondant ;
- Le certificat MSCA_Card comprenant la clé publique MSCA_Card.PK à utiliser pour vérifier les certificats Card_MA et Card_Sign ;
- Le certificat EUR comprenant la clé publique EUR.PK à utiliser pour vérifier le certificat MSCA_Card ;
- Le certificat EUR dont la durée de validité précède directement celle du certificat EUR à utiliser pour vérifier le certificat MSCA_Card, le cas échéant ;
- Le certificat de lien reliant ces deux certificats EUR, le cas échéant ;
- **En sus, pour les cartes de contrôleur, d'entreprise et d'atelier uniquement, et seulement si ces cartes sont délivrées au cours des trois premiers mois de la période de validité d'un nouveau certificat EUR : le certificat EUR antérieur de deux générations, le cas échéant.**

Exemple concernant ce dernier point : Au cours des trois premiers mois de validité du certificat ERCA (3) (voir fig. 1), les cartes susmentionnées doivent contenir le certificat ERCA (1). Cette disposition est nécessaire pour garantir que ces cartes puissent être

utilisées pour effectuer des téléchargements de données à partir des UEV certifiées par l'ERCA (1) dont la durée de vie normale est de 15 ans, plus la période de téléchargement de données de 3 mois (voir le dernier point de l'exigence 13 de l'appendice 1C).

CSM_92 Outre les clés et les certificats cryptographiques énumérés au point ~~233~~ **CSM_91**, les cartes tachygraphiques contiennent également les clés et les certificats spécifiés dans la partie A du présent **sous-**appendice, qui leur permettent d'interagir avec les UEV de première génération.

9.1.6 Niveau équipement : dispositifs GNSS externes

CSM_93 Une paire de clés ECC unique, désignée par l'appellation DGE_MA, est générée pour chaque dispositif GNSS externe. Cette tâche incombe aux fabricants de dispositifs GNSS externes. Chaque fois qu'une paire de clés DGE_MA est générée, **la partie qui la génère doit envoyer la clé publique** à la MSCA **compétente** ~~du pays de résidence~~ afin d'obtenir le certificat DGE_MA correspondant, signé par la MSCA. La clé privée est utilisée uniquement par le dispositif GNSS externe.

CSM_94 Un fabricant de dispositifs GNSS externes doit attribuer à une paire de clés DGE_MA une force égale à celle de la paire de clés MSCA servant à signer le certificat DGE_MA correspondant.

CSM_95 Un dispositif GNSS externe utilise sa paire de clés DGE_MA, composée d'une clé privée DGE_MA.SK et d'une clé publique DGE_MA.PK, exclusivement pour effectuer des opérations d'authentification mutuelle et de concordance de clés de session avec les UEV, comme indiqué à la section **11.4 du présent sous-appendice**.

CSM_96 La durée de validité d'un certificat DGE_MA est de 15 ans.

CSM_97 Un dispositif GNSS externe ne doit pas utiliser la clé privée d'une paire de clés DGE_MA pour se coupler avec une UEV après l'expiration du certificat correspondant.

Remarque : comme expliqué à la section **11.3.3**, un dispositif GNSS externe peut éventuellement utiliser sa clé privée pour procéder à une authentification mutuelle avec l'UEV à laquelle il est couplé, y compris après l'expiration du certificat correspondant.

CSM_98 La paire de clés DGE_MA d'un dispositif GNSS externe donné et les certificats correspondants ne sont ni remplacés ni renouvelés sur le terrain une fois que le dispositif a été mis en service.

Remarque : cette exigence n'interdit pas la possibilité de remplacer les paires de clés DGE lors d'une maintenance ou d'une réparation dans un environnement contrôlé et sécurisé par le fabricant d'DGE.

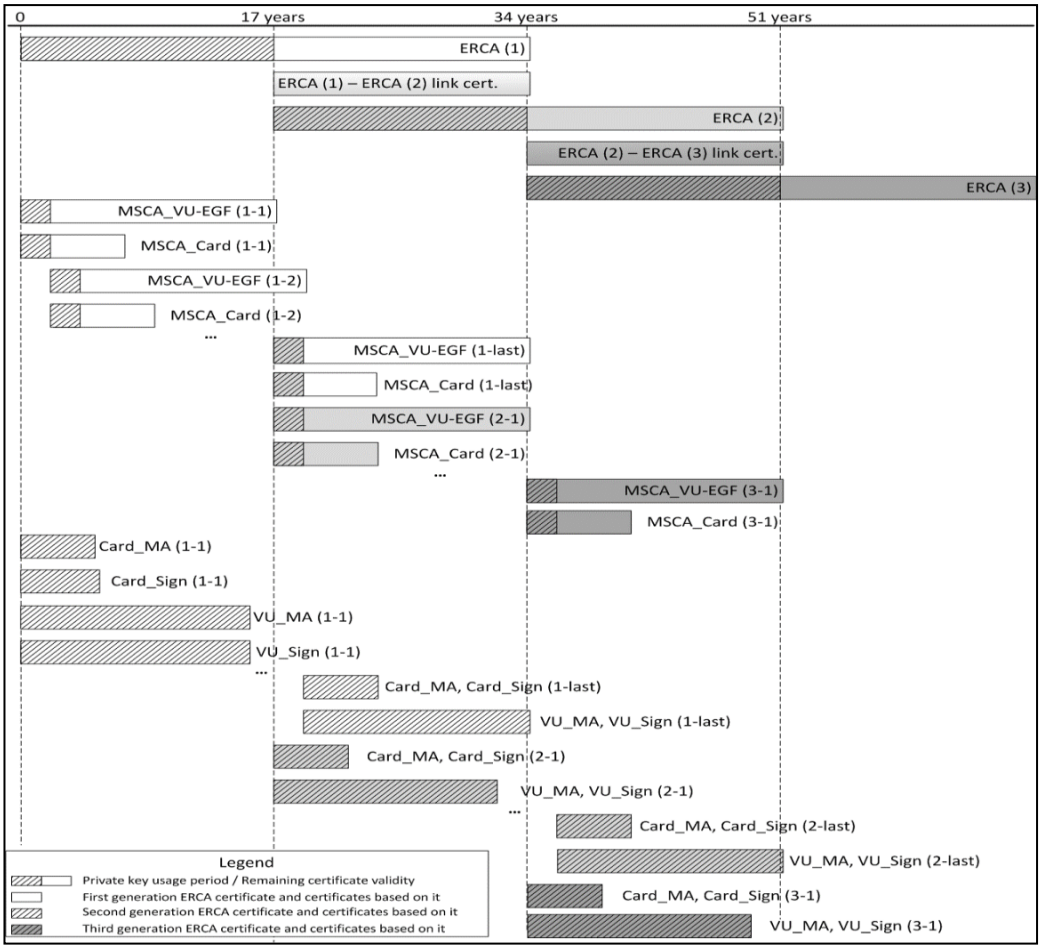
CSM_99 Lorsqu'il entre en fonctionnement, le dispositif GNSS externe doit contenir les clés et les certificats cryptographiques suivants :

- La clé privée DGE_MA et le certificat correspondant ;
- Le certificat MSCA_UEV-DGE comprenant la clé publique MSCA_UEV-DGE.PK à utiliser pour vérifier le certificat DGE_MA ;
- Le certificat EUR comprenant la clé publique EUR.PK à utiliser pour vérifier le certificat MSCA_UEV-DGE ;
- Le certificat EUR dont la durée de validité précède directement celle du certificat EUR à utiliser pour vérifier le certificat MSCA_UEV-DGE, le cas échéant ;
- Le certificat de lien reliant ces deux certificats EUR, le cas échéant.

9.1.7 Généralités : certificat de remplacement

La **figure 1** ci-après montre comment différentes générations de certificats racine ERCA, de certificats de lien ERCA, de certificats MSCA et de certificats d'équipement (UEV et carte) sont émises et utilisées au fil du temps :

Figure 1
Émission et utilisation de différentes générations de certificats racine ERCA, de certificats de lien ERCA, de certificats MSCA et de certificats d'équipement



Remarques concernant la **figure 1** :

1. Le nombre entre parenthèses indique les différentes générations du certificat racine. Par exemple, ERCA (1) désigne le certificat racine ERCA de première génération, ERCA (2) celui de deuxième génération, etc.

2. D'autres certificats sont suivis de deux nombres entre parenthèses. Le premier indique la génération du certificat racine sous lequel ils ont été émis, le second la génération du certificat lui-même. Par exemple, MSCA_Card (1-1) désigne le premier certificat MSCA_Card émis sous le certificat ERCA (1) ; MSCA_Card (2-1) désigne le premier certificat MSCA_Card émis sous le certificat ERCA (2) ; MSCA_Card (2-last) désigne le dernier certificat MSCA_Card émis sous le certificat ERCA (2) ; Card_MA(2-1) désigne le premier certificat de carte destiné à l'authentification mutuelle émis sous le certificat ERCA (2), etc.

3. Les certificats MSCA_Card (2-1) et MSCA_Card (1-last) sont émis quasiment à la même date. MSCA_Card (2-1) désigne le premier certificat MSCA_Card émis sous le certificat ERCA (2) et sera émis peu de temps après le certificat MSCA_Card (1-last), c'est-à-dire le dernier certificat MSCA_Card émis sous le certificat ERCA (1).

4. Comme le montre la figure, les premiers certificats d'UEV et de carte émis sous le certificat ERCA (2) apparaissent presque deux ans avant que n'apparaissent les derniers certificats d'UEV et de carte émis sous le certificat ERCA (1). Cela s'explique par le fait que les certificats d'UEV et de carte sont émis sous un certificat MSCA et pas directement sous le certificat ERCA. Le certificat MSCA (2-1) est émis immédiatement après l'entrée en validité du certificat ERCA (2), mais le certificat MSCA (1-last) est émis légèrement avant, à la toute fin de validité du certificat ERCA (1). Par conséquent, ces deux certificats MSCA ont à peu près la même durée de validité, malgré le fait qu'ils soient de générations différentes.

5. La durée de validité indiquée pour les cartes correspond à celle des cartes de conducteur (5 ans).

6. Pour gagner de l'espace, la différence entre les durées de validité des certificats Card_MA et Card_Sign ~~et les certificats UEV_MA et UEV_Sign~~ n'est précisée que pour la première génération.

9.2 Clés symétriques

9.2.1 Clés de sécurisation de la communication entre l'UEV et le capteur de mouvement

~~9.2.2 Clés de sécurisation de la communication DSRC~~

9.2.1.1 Généralités

Remarque : les lecteurs de la présente section sont censés être au fait du contenu de la norme [ISO 16844-3] qui décrit l'interface entre une UEV et un capteur de mouvement. La procédure de couplage entre une UEV et un capteur de mouvement est présentée en détail au chapitre **12** du présent **sous-**appendice.

CSM_100 Un nombre de clés symétriques déterminé est nécessaire pour coupler des UEV et des capteurs de mouvement, en vue de leur authentification mutuelle et afin de chiffrer la communication entre eux, comme l'illustre le ~~tableau 45~~ **tableau 3**. Toutes ces clés sont des clés AES dont la longueur est égale à celle de la clé maîtresse du capteur de mouvement, cette dernière étant liée à la longueur de la paire de clés **racine** ~~européenne~~ (prévue), comme indiqué au point ~~TCS_192~~**CSM_50**.

Tableau ~~45~~ **3**
Clés de sécurisation de la communication entre l'UEV et le capteur de mouvement

Clé	*Symbole*	*Générée par*	*Méthode de génération*	*Stockée par*
Clé maîtresse du capteur de mouvement − partie UEV	$K_{M\text{-}UEV}$	ERCA	Aléatoire	ERCA, MSCA impliquées dans l'émission des certificats d'UEV, fabricants d'UEV, UEV
Clé maîtresse du capteur de mouvement − partie atelier	$K_{M\text{-}CAT}$	ERCA	Aléatoire	ERCA, MSCA, fabricants de cartes, cartes d'atelier
Clé maîtresse du capteur de mouvement	K_M	Générée de manière non indépendante	Calculée selon $K_M = K_{M\text{-}UEV}$XOR $K_{M\text{-}CAT}$	ERCA, MSCA impliquées dans l'émission des clés de capteurs de mouvement (facultatif)*
Clé d'identification	K_{ID}	Générée de manière non indépendante	Calculée selon $K_{ID} = K_M$ XOR VC, où VC est défini dans ~~TCS_248~~**CSM_106**	ERCA, MSCA impliquées dans l'émission des clés de capteurs de mouvement (facultatif)*

Clé	*Symbole*	*Générée par*	*Méthode de génération*	*Stockée par*
Clé de couplage	K_P	Fabricant du capteur de mouvement	Aléatoire	Un capteur de mouvement
Clé de session	K_S	UEV (pendant le couplage de l'UEV et du capteur de mouvement)	Aléatoire	Une UEV et un capteur de mouvement

* Le stockage de K_M et K_{ID} est facultatif, car ces clés peuvent être dérivées de $K_{M\text{-}UEV}$, de $K_{M\text{-}CAT}$ et du VC.

CSM_101 L'autorité de certification racine ~~européenne~~ génère $K_{M\text{-}UEV}$ et $K_{M\text{-}CAT}$, deux clés AES aléatoires et uniques à partir desquelles la clé maîtresse du capteur de mouvement K_M peut être calculée selon $K_{M\text{-}UEV}$ XOR $K_{M\text{-}CAT}$. L'ERCA communique K_M, $K_{M\text{-}UEV}$ et $K_{M\text{-}CAT}$ aux autorités de certification de ~~l'État membre~~ **la Partie contractante** concerné**e** sur leur demande.

CSM_102 L'ERCA attribue à chaque clé maîtresse d'un capteur de mouvement K_M un numéro de version unique, qui s'applique également aux clés $K_{M\text{-}UEV}$ et $K_{M\text{-}CAT}$ qui la constitue ainsi qu'à la clé d'identification K_{ID} associée. L'ERCA informe les MSCA du numéro de version lorsqu'elle leur envoie $K_{M\text{-}UEV}$ et $K_{M\text{-}CAT}$.

Remarque : le numéro de version sert à distinguer les différentes générations de ces clés, comme expliqué en détail dans la section ~~9.2.2.2~~**9.2.1.2**.

CSM_103 L'autorité de certification ~~de l'État membre~~ **d'une Partie contractante** transmet $K_{M\text{-}UEV}$ et son numéro de version aux fabricants d'UEV qui en font la demande. Les fabricants d'UEV insèrent $K_{M\text{-}UEV}$ et son numéro de version dans toutes les UEV fabriquées.

CSM_104 L'autorité de certification ~~de l'État membre~~ **d'une Partie contractante** vérifie que $K_{M\text{-}CAT}$ et son numéro de version sont insérés dans chaque carte d'atelier émise sous leur responsabilité.

Remarques :

- Voir la description du type de données `SensorInstallationSecData` ~~à l'appendice~~ **au sous-appendice** 2.
- Comme expliqué à la section ~~9.2.2.2~~**9.2.1.2**, il se peut que plusieurs générations de $K_{M\text{-}CAT}$ doivent être insérées dans une même carte d'atelier.

CSM_105 Outre la clé AES visée au point ~~TCS_246~~**CSM_104**, la MSCA doit veiller à ce que la clé TDES Km_{CAT}, définie à l'exigence CSM_037 dans la partie A du présent **sous-**appendice, soit insérée dans chaque carte d'atelier émise sous sa responsabilité.

Remarques :

- Cela permet d'utiliser une carte d'atelier de deuxième génération pour coupler une UEV de première génération ;
- Une carte d'atelier de deuxième génération contient deux applications distinctes : l'une conforme à la partie B du présent **sous-**appendice et l'autre à la partie A. Cette dernière contient la clé TDES Km_{CAT}.

CSM_106 Une MSCA impliquée dans la distribution de capteurs de mouvement calcule la clé d'identification de la clé maîtresse du capteur de mouvement en appliquant la fonction XOR ainsi qu'un vecteur constant, VC. La valeur du vecteur constant est la suivante :

Pour les clés maîtresses du capteur de mouvement codées sur 128 bits : VC = ‘B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 **5~~E~~D** 83’

Pour les clés maîtresses du capteur de mouvement codées sur 192 bits : VC = ‘72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25’

Pour les clés maîtresses du capteur de mouvement codées sur 256 bits : VC = ‘1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60’

Remarque : les vecteurs constants sont générés de la manière suivante :

Pi_10 = 10 premiers octets de la partie décimale de la constante mathématique π = ‘24 3F 6A 88 85 A3 08 D3 13 19’

VC_128-bits = 16 premiers octets de SHA-256(Pi_10)

VC_192-bits = 24 premiers octets de SHA-384(Pi_10)

VC_256-bits = 32 premiers octets de SHA-512(Pi_10)

CSM_107 Les fabricants de capteurs de mouvement doivent générer une clé de couplage K_P aléatoire et unique pour chaque capteur de mouvement et envoyer chaque clé de couplage à l’autorité de certification ~~de l’État membre~~ **de la Partie contractante** concernée. La MSCA chiffre chaque clé de couplage séparément à l’aide de la clé maîtresse du capteur de mouvement K_M et renvoie la clé chiffrée au fabricant de capteurs de mouvement. Pour chaque clé chiffrée, la MSCA doit communiquer au fabricant de capteurs de mouvement le numéro de version de la clé maîtresse associée.

Remarque : comme expliqué à la section ~~9.2.2.2~~ **9.2.1.2**, il se peut qu’un fabricant de capteurs de mouvement doive générer plusieurs clés de couplage uniques pour un même capteur de mouvement.

CSM_108 Les fabricants de capteurs de mouvement doivent générer un numéro de série unique pour chaque capteur de mouvement et envoyer tous les numéros de série à l’autorité de certification ~~de l’État membre~~ **de la Partie contractante** concernée. La MSCA chiffre chaque numéro de série séparément à l’aide de la clé d’identification K_{ID} et renvoie le numéro de série chiffré au fabricant de capteurs de mouvement. Pour chaque numéro de série chiffré, la MSCA doit communiquer au fabricant de capteurs de mouvement le numéro de version du K_{ID} associé.

CSM_109 En ce qui concerne les exigences ~~TCS_249~~**CSM_107** et ~~TCS_250~~**CSM_108**, la MSCA a recours à l’algorithme AES en mode de chiffrement par chaînage de blocs (CBC), tel que défini dans la norme [ISO 10116], avec un paramètre d’entrelacement de *m* = 1 et un vecteur d’initialisation SV = ’00’ {16}, c’est-à-dire seize octets de valeur binaire 0. Lorsque cela se révèle nécessaire, la MSCA utilise la méthode de remplissage 2 définie dans la norme [ISO 9797-1].

CSM_110 Le fabricant de capteurs de mouvement stocke la clé de couplage et le numéro de série chiffrés dans le capteur de mouvement auquel ils sont destinés. Il y stocke également les valeurs en clair correspondantes et le numéro de version de K_M et de K_{ID} utilisées pour le chiffrement.

Remarque : comme expliqué à la section ~~9.2.2.2~~**9.2.1.2**, il se peut qu’un fabricant de capteurs de mouvement doive enregistrer plusieurs clés de couplage uniques chiffrées et plusieurs numéros de série chiffrés dans un même capteur de mouvement.

CSM_111 Outre le matériel cryptographique AES visé au point ~~TCS_252~~**CSM_110**, le fabricant de capteurs de mouvement peut également stocker dans chaque capteur de mouvement le matériel

cryptographique TDES spécifié à l'exigence CSM_037 dans la partie A du présent **sous-**appendice.

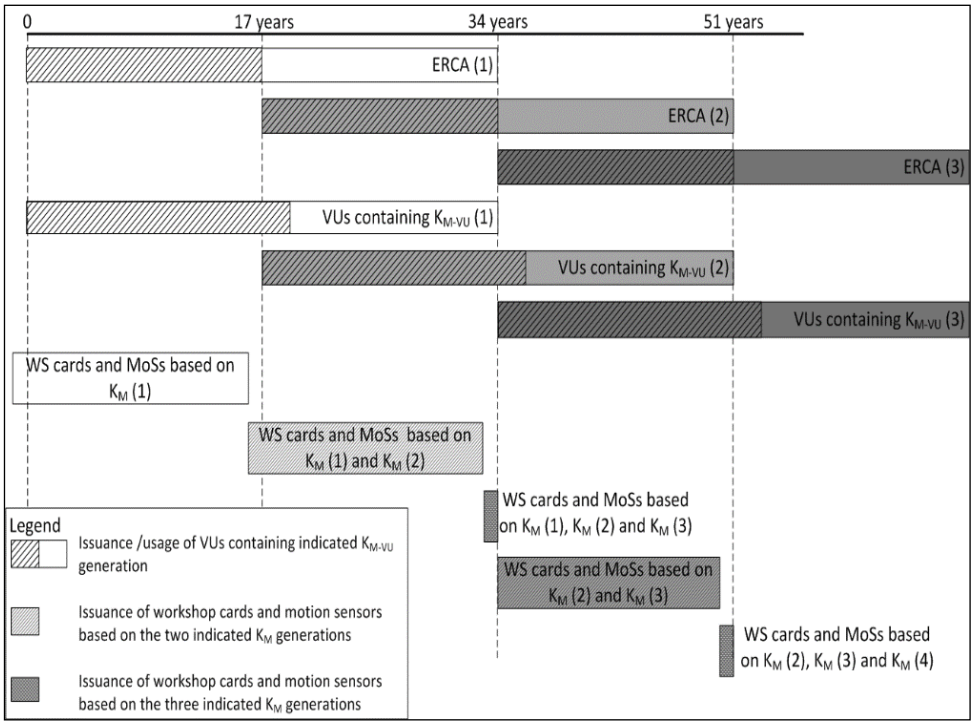
Remarque : ce faisant, il permet le couplage d'un capteur de mouvement de deuxième génération avec une UEV de première génération.

CSM_112 La longueur de la clé de session K_S générée par une UEV pendant le couplage avec un capteur de mouvement est liée à la longueur de sa $K_{M\text{-}UEV}$, comme décrit au point ~~TCS_192~~**CSM_50**.

9.2.1.2 Remplacement de la clé maîtresse du capteur de mouvement dans un équipement de deuxième génération

CSM_113 Toutes les clés maîtresses des capteurs de mouvement et toutes les clés associées (voir ~~tableau 45~~ **tableau 3**) sont liées à une génération donnée de paire de clés racine ERCA. Ces clés doivent donc être remplacées tous les 17 ans. La durée de validité de chaque génération de clés maîtresses de capteur de mouvement commence un an avant que la paire de clés racine ERCA associée n'entre en validité et elle finit à l'expiration de la paire de clés racine ERCA associée. La **figure 2** illustre ce principe.

Figure 2
Émission et utilisation de différentes générations de clés maîtresses de capteurs de mouvement dans des UEV, des capteurs de mouvement et des cartes d'ateliers



CSM_114 Au moins un an avant la génération d'une nouvelle paire de clés racine ~~européenne~~, conformément à l'exigence ~~TCS_198~~**CSM_56**, l'ERCA génère une nouvelle clé maîtresse de capteur de mouvement K_M en générant de nouvelles $K_{M\text{-}UEV}$ et $K_{M\text{-}CAT}$. La longueur de la clé maîtresse du capteur de mouvement est liée à la force anticipée de la nouvelle paire de clés racine ~~européenne~~ conformément à l'exigence ~~TCS_192~~**CSM_50**. L'ERCA communique les nouvelles K_M, $K_{M\text{-}UEV}$ et $K_{M\text{-}CAT}$ ainsi que leur numéro de version aux MSCA sur leur demande.

CSM_115 Les MSCA veillent à ce que toutes les générations valides de $K_{M\text{-}CAT}$ soient stockées dans chaque carte d'atelier émise sous leur autorité, de même que leurs numéros de version, comme illustré à la figure 2.

Remarque : cela implique qu'au cours de la dernière année de validité d'un certificat ERCA, les cartes d'atelier sont émises avec trois générations de $K_{M\text{-}CAT}$, comme illustré à la figure 2.

CSM_116 À propos de la procédure décrite aux points ~~TCS_249~~**CSM_107** et ~~TCS_250~~**CSM_108** ci-dessus : la MSCA chiffre chaque paire de clés de couplage K_P reçue des fabricants de capteurs de mouvement séparément selon chaque génération valable de clé maîtresse de capteur de mouvement K_M. La MSCA chiffre également chaque numéro de série reçu des fabricants de capteurs de mouvement séparément selon chaque génération valable de clé d'identification K_{ID}. Le fabricant de capteurs de mouvement stocke toutes les clés de couplage et les numéros de série chiffrés dans le capteur de mouvement auquel ils sont destinés. Il y stocke également les valeurs en clair correspondantes et le ou les numéros de version de K_M et K_{ID} qui ont servi au chiffrement.

Remarque : cela implique qu'au cours de la dernière année de validité d'un certificat ERCA, les capteurs de mouvement sont émis avec des données chiffrées avec trois générations de K_M, comme illustré à la figure 2.

CSM_117 À propos de la procédure décrite au point ~~TCS_249~~**CSM_107** ci-dessus : du fait que la longueur de la clé de couplage K_P doit être liée à celle de K_M (voir ~~TCS_253~~**CSM_100**), il se peut que le fabricant de capteurs de mouvement doive générer jusqu'à trois clés de couplage distinctes (de longueurs différentes) pour un même capteur de mouvement, pour anticiper les éventuelles longueurs des générations futures de K_M. Dans ce cas, le fabricant doit envoyer chaque clé de couplage à la MSCA. La MSCA vérifie que chaque clé de couplage est chiffrée selon la génération adéquate de la clé maîtresse du capteur de mouvement, c'est-à-dire celle présentant la même longueur.

Remarque : si le fabricant de capteurs de mouvement choisit de générer une clé de couplage TDES pour un capteur de mouvement de deuxième génération (voir ~~TCS_253~~**CSM_111**), il doit indiquer à la MSCA que la clé maîtresse du capteur de mouvement TDES doit être utilisée pour chiffrer cette clé de couplage. Cela s'impose parce que la longueur de la clé TDES pourrait être égale à celle de la clé AES. La MSCA ne pourrait alors pas les distinguer sur la seule base de leurs longueurs respectives.

CSM_118 Les fabricants d'UEV insèrent uniquement une génération de $K_{M\text{-}UEV}$ dans chaque UEV, accompagnée de son numéro de version. Cette génération de $K_{M\text{-}UEV}$ est liée au certificat ERCA duquel découlent les certificats de l'UEV.

Remarques :

- Une UEV liée à un certificat ERCA de génération *X* contient uniquement une $K_{M\text{-}UEV}$ de génération *X* même si elle est émise après le début de la durée de validité du certificat ERCA de génération *X+1*. La figure 2 illustre ce principe ;
- Une UEV de génération *X* ne peut pas être couplée avec un capteur de mouvement de génération *X-1* ;
- Du fait que les cartes d'atelier ont une durée de validité d'un an, les exigences ~~TCS_255 – TCS_260~~**CSM_113 à CSM_118** font que toutes les cartes d'atelier contiennent la nouvelle $K_{M\text{-}CAT}$ à l'émission de la première UEV contenant la nouvelle $K_{M\text{-}UEV}$. Par conséquent, une telle UEV pourra toujours calculer la nouvelle K_M. De plus, à ce moment-là, la plupart des nouveaux capteurs de mouvement contiendront également des données chiffrées sur la base de la nouvelle K_M.

9.2.2 Clés de sécurisation de la communication DSRC

9.2.2.1 Généralités

CSM_119 L'authenticité et la confidentialité des données communiquées par l'UEV aux autorités de contrôle par un canal de communication à

distance DSRC sont garanties au moyen d'un jeu de clés AES propres à l'UEV dérivées d'une clé maîtresse DSRC unique, KM_{DSRC}.

CSM_120 La clé maîtresse DSRC KM_{DSRC} est une clé AES générée, stockée et distribuée de manière sécurisée par l'ERCA. La longueur de la clé peut être de 128, 192 ou 256 bits. Elle dépend de la longueur de la paire de clés racine ~~européenne~~, comme prévu au point ~~TCS_192~~**CSM_50**.

CSM_121 L'ERCA communique la clé maîtresse DSRC aux autorités de certification ~~de l'État membre~~ **de la Partie contractante** concerné**e**, sur leur demande et de manière sécurisée. Cela leur permet de calculer les clés DSRC propres aux UEV et de s'assurer que la clé maîtresse DSRC est insérée dans toutes les cartes de contrôleur et d'atelier émises sous leur responsabilité.

CSM_122 L'ERCA attribue un numéro de version unique à chaque clé maîtresse DSRC. L'ERCA informe les MSCA du numéro de version lorsqu'elle leur envoie la clé maîtresse DSRC.

Remarque : le numéro de version sert à distinguer les différentes générations de ces clés maîtresses DSRC, comme expliqué en détail dans la section ~~9.2.3.2~~ **9.2.2.2**.

CSM_123 Pour chaque unité embarquée, le fabricant d'unités embarquées crée un numéro de série unique qu'il envoie aux autorités de certification ~~de l'État membre~~ **de la Partie contractante** concerné**e** en vue d'obtenir un jeu de deux clés DSRC propre aux UEV. Le numéro de série de l'UEV relève du type de données `VuSerialNumber` ~~et les règles de codage distinctives (DER) conformes à la norme [ISO 8825-1] servent à son cryptage~~.

Remarques :

- **Le numéro de série de l'UEV doit être identique à l'élément vuSerialNumber de VuIdentification (voir sous-appendice 1) et à la référence du détenteur de certificat figurant dans les certificats de l'UEV ;**
- **Le fabricant de l'unité embarquée peut ne pas connaître le numéro de série d'une UEV lorsqu'il fait une demande de clés DSRC pour celle-ci. Dans ce cas, le fabricant envoie à la place l'identificateur unique de la demande de certificat qu'il a utilisé lors de la demande de certificat pour l'UEV (voir CSM_153). Cet identificateur de demande de certificat doit donc correspondre à la référence du détenteur de certificat figurant dans les certificats de l'UEV.**

CSM_124 Dès réception d'une demande de clés DSRC propres aux UEV, la MSCA calcule deux clés AES pour l'UEV, nommées K_UEV_{DSRC}_ENC et K_UEV_{DSRC}_MAC. Ces clés propres aux UEV doivent avoir la même longueur que la clé maîtresse DSRC. La MSCA utilise la fonction de dérivation de clé définie dans le document [RFC 5869]. La fonction de hachage nécessaire pour instancier la fonction de hachage HMAC est liée à la longueur de la clé maîtresse DSRC, conformément au point 0. La fonction de dérivation de clé définie dans le document [RFC 5869] doit être utilisée de la manière suivante :

Étape n° 1 (extraction) :

- *PRK* = HMAC-Hash (*salt, IKM*) où *salt* représente une chaîne vide '' et *IKM* correspond à KM_{DSRC}.

Étape n° 2 (expansion) :

- *OKM = T(1)*, où

T(1) = HMAC-Hash (*PRK, T(0)* || *info* || '01') avec

T(0) = chaîne vide ('')

info = numéro de série de l'UEV **ou ID de la demande de certificat**, comme spécifié au point ~~TCS_265~~ **CSM_123**

K_UEV_{DSRC}_ENC = premiers octets *L* de *OKM* et

K_UEV_{DSRC}_MAC = derniers octets *L* de *OKM*

où *L* est la longueur requise de K_UEV_{DSRC}_ENC et K_UEV_{DSRC}_MAC en octets.

CSM_125 La MSCA communique K_UEV_{DSRC}_ENC et K_UEV_{DSRC}_MAC aux fabricants d'UEV de manière sécurisée en vue de leur insertion dans les UEV auxquelles elles sont destinées.

CSM_126 Après leur émission, l'UEV enregistre les clés K_UEV_{DSRC}_ENC et K_UEV_{DSRC}_MAC dans sa mémoire sécurisée, de façon à pouvoir garantir l'intégrité, l'authenticité et la confidentialité des données envoyées au moyen du canal de communication à distance. L'UEV enregistre également le numéro de version de la clé maîtresse DSRC servant à calculer les clés propres aux UEV.

CSM_127 Après leur émission, les cartes de contrôleur et d'atelier enregistrent la clé KM_{DSRC} dans leur mémoire sécurisée, de façon à pouvoir vérifier l'intégrité et l'authenticité des données envoyées par l'UEV par le canal de communication à distance et de façon à pouvoir déchiffrer ces données. Les cartes de contrôleur et d'atelier enregistrent également le numéro de version de la clé maîtresse DSRC.

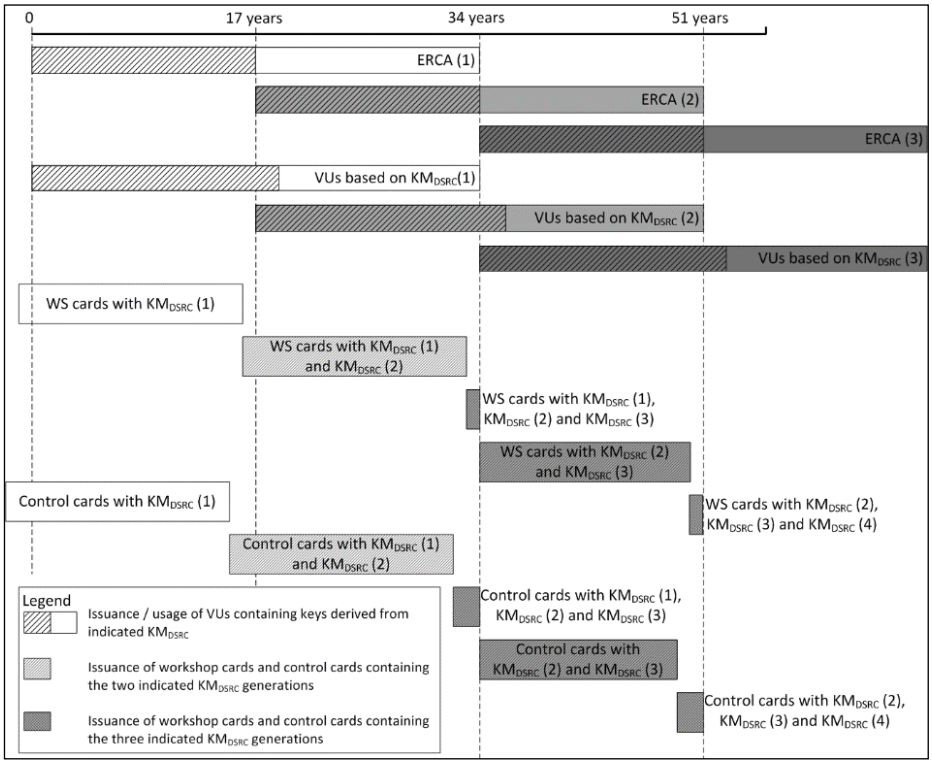
Remarque : comme expliqué à la section ~~9.2.3.2~~ **9.2.2.2**, il se peut que plusieurs générations de KM_{DSRC} doivent être insérées dans une même carte d'atelier ou de contrôleur.

CSM_128 La MSCA archive toutes les clés DSRC propres aux UEV qu'elle a générées, ainsi que leur numéro de version et ~~l'identificateur de l'UEV destinés à chaque jeu de clés~~ le numéro de version de l'UEV ou l'ID de la demande de certificat utilisé pour obtenir ces clés.

9.2.2.2 ~~9.2.3.2~~ Remplacement des clés maîtresses DSRC

CSM_129 Toutes les clés maîtresses DSRC sont liées à une génération donnée de paire de clés racine ERCA. L'ERCA doit donc remplacer chaque clé maîtresse DSRC tous les 17 ans. La durée de validité de chaque génération de clés maîtresses DSRC commence deux ans avant que la paire de clés racine ERCA associée n'entre en validité et elle finit à l'expiration de la paire de clés racine ERCA associée. La figure 3 illustre ce principe.

Figure 3
Émission et utilisation de différentes générations de clés maîtresses DSRC sur des UEV, des cartes d'ateliers et de contrôleur



CSM_130 Au moins deux ans avant la génération d'une nouvelle paire de clés racine ~~européenne~~, comme décrit au point ~~TCS_198~~**CSM_56**, l'ERCA génère une nouvelle clé maîtresse DSRC. La longueur de la clé maîtresse DSRC est liée à la force anticipée de la nouvelle paire de clés racine ~~européenne~~ conformément au point ~~TCS_192~~ **CSM_50**. L'ERCA communique la nouvelle clé maîtresse DSRC ainsi que son numéro de version aux MSCA sur leur demande.

CSM_131 Les MSCA veillent à ce que toutes les générations valides de KM_{DSRC} soient stockées dans chaque carte de contrôleur émise sous leur autorité, de même que leurs numéros de version, comme illustré à la **figure 3**.

Remarque : cela implique qu'au cours des deux dernières années de validité d'un certificat ERCA, les cartes de contrôleur sont émises avec trois générations de KM_{DSRC}, comme illustré à la **figure 3**.

CSM_132 Les MSCA veillent à ce que toutes les générations de KM_{DSRC} valides depuis au moins un an et toujours en cours de validité soient stockées dans chaque carte d'atelier émise sous leur autorité, de même que leurs numéros de version, comme illustré à la **figure 3**.

Remarque : cela implique qu'au cours de la dernière année de validité d'un certificat ERCA, les cartes d'atelier sont émises avec trois générations de KM_{DSRC}, comme illustré à la **figure 3**.

CSM_133 Les fabricants d'UEV insèrent uniquement un jeu de clés DSRC propres aux UEV dans chaque UEV, accompagné de son numéro de version. Ce jeu de clés est dérivé de la génération KM_{DSRC} liée au certificat ERCA duquel découlent les certificats UEV.

Remarques :

Cela implique qu'une UEV fondée sur un certificat ERCA de génération *X* contient uniquement une $K\_UEV_{DSRC}\_ENC$ et une $K\_UEV_{DSRC}\_MAC$ de génération *X* même si

l'UEV est délivrée après le début de la période de validité du certificat ERCA de génération *X+1*. La **figure 3** illustre ce principe.

Du fait que les cartes d'atelier ont une validité d'un an et les cartes de contrôleur une validité de deux ans, les exigences ~~TCS_273 TCS_275~~**CSM_131 à CSM_133** font que toutes les cartes d'atelier et de contrôleur contiennent la nouvelle clé maîtresse DSRC à la délivrance de la première UEV contenant les clés propres aux UEV relevant de cette clé maîtresse.

9.3 Certificats

9.3.1 Généralités

CSM_134 Tous les certificats inscrits dans le système ~~européen~~ de tachygraphe intelligent sont de type autodescriptif et vérifiable par carte conformément aux normes [ISO 7816-4] et [ISO 7816-8].

CSM_135 Les règles de codage distinctives (DER) conformes à la norme [ISO 8825-1] doivent servir à encoder ~~les structures de données ASN.1 et (selon l'application)~~ les objets de données au sein des certificats. **Le tableau 4 montre l'ensemble du codage des certificats, y compris les balises et les octets de longueur.**

Remarque : ce codage donne la structure TLV suivante :

- Balise : la balise est codée sur un ou deux octets et indique le contenu ;
- Longueur : la longueur est codée comme un entier non signé sur un, deux ou trois octets, soit une longueur maximale de 65 535 octets. On utilisera le moins d'octets possible ;
- Valeur : la valeur est codée sur zéro octet ou plus.

9.3.2 Contenu du certificat

CSM_136 Tous les certificats possèdent la structure présentée dans le profil de certificat au **tableau 4**~~46~~.

Tableau 4
Profil de certificat version 1

Champ	*ID de champ*	*Balise*	*Longueur (en octets)*	*Type de données ASN.1 (voir sous-appendice 1)*
Certificat ECC	C	'7F 21'	var	
Corps du certificat ECC	B	'7F 4E'	var	
Identificateur de profil de certificat	CPI	'5F 29'	'01'	INTEGER(0..255)
Référence de l'autorité de certification	RAC	'42'	'08'	KeyIdentifier
Autorisation du détenteur de certificat	ADC	'5F 4C'	'07'	CertificateHolderAuthorisation
Clé publique	PK	'7F 49'	var	
Paramètres de domaine	DP	'06'	var	OBJECT IDENTIFIER
Point public	PP	'86'	var	OCTET STRING
Référence du détenteur de certificat	RDC	'5F 20'	'08'	KeyIdentifier
Date d'entrée en vigueur du certificat	CEfD	'5F 25'	'04'	TimeReal
Date d'expiration du certificat	CExD	'5F 24'	'04'	TimeReal
Signature du certificat ECC	S	'5F 37'	var	OCTET STRING

Remarque : dans les sections ultérieures du présent **sous-**appendice, l'ID de champ est utilisé pour désigner les différents champs d'un certificat, par exemple X.RAC correspond à la référence des autorités de certification mentionnées dans le certificat d'un utilisateur X.

9.3.2.1 Identificateur de profil de certificat

CSM_137 Les certificats comportent un identificateur de profil de certificat qui sert à indiquer le profil utilisé. Comme précisé au tableau **4**~~46~~, la version 1 est identifiée par une valeur de '00'.

9.3.2.2~~9.3.2.1~~ Référence de l'autorité de certification

CSM_138 La référence de l'autorité de certification (RAC) permet d'identifier la clé publique à utiliser pour vérifier la signature du certificat. La référence des autorités de certification doit être identique à celle du détenteur de certificat dans le certificat de l'autorité de certification correspondant.

CSM_139 Le certificat racine ERCA est autosigné, c'est-à-dire que la RAC et la référence du détenteur de certificat figurant sur le certificat doivent être identiques.

CSM_140 Pour un certificat de lien ERCA, la référence du détenteur du certificat est identique à la RAC du nouveau certificat racine ERCA. La RAC d'un certificat de lien est identique à la référence du détenteur du précédent certificat racine ERCA.

9.3.2.3 Autorisation du détenteur de certificat

CSM_141 L'autorisation du détenteur de certificat permet d'identifier le type de certificat. Elle se compose des six octets les plus significatifs de l'ID de l'application tachygraphique, concaténés à EquipmentType ~~auquel est destiné le certificat~~**, qui indique le type d'équipement auquel le certificat est destiné. Dans le cas d'un certificat d'UEV, d'un certificat de carte de conducteur ou d'un certificat de carte d'atelier, le type d'équipement permet également de faire la distinction entre un certificat d'authentification mutuelle et un certificat de création de signatures numériques (voir sect. 9.1 et sous-appendice 1, type de données EquipmentType).**

9.3.2.4 Clé publique

La clé publique comprend deux éléments de données : les paramètres de domaine normalisés à utiliser avec la clé publique du certificat et la valeur du point public.

CSM_142 L'élément de données Paramètres de domaine contient l'un des identificateurs d'objet spécifié au **tableau 1**~~4~~3 afin de référencer à un jeu de paramètres de domaine normalisés.

CSM_143 L'élément de données PublicPoint contient le point public. Les points publics de la courbe elliptique sont convertis en chaînes d'octets comme spécifié dans le document [TR-03111]. On utilise la structure de codage non compressée. La validation décrite dans le document [TR-03111] doit toujours être effectuée lors du décodage d'un point de la courbe elliptique.

9.3.2.5 Référence du détenteur de certificat

CSM_144 La référence du détenteur de certificat sert d'identificateur pour la clé publique fournie avec le certificat. Elle est utilisée pour référencer cette clé publique dans d'autres certificats.

CSM_145 Concernant les certificats de cartes et de dispositifs GNSS externes, la référence du détenteur de certificat est du type `ExtendedSerialNumber` tel que défini ~~à l'appendice~~ **au sous-appendice** 1.

CSM_146 Concernant les UEV, le fabricant, lorsqu'il demande un certificat, peut connaître ou non le numéro de série propre au fabricant de l'UEV à

laquelle ce certificat et la clé privée associée sont destinés. Dans le premier cas, la référence du détenteur du certificat sera du type `ExtendedSerialNumber` tel que défini ~~à l'appendice~~ **au sous-appendice** 1. Dans le dernier cas, la référence du détenteur de certificat sera du type `CertificateRequestID` tel que défini ~~à l'appendice~~ **au sous-appendice** 1.

Remarque : pour les certificats de carte, la valeur de la RDC est identique à la valeur de cardExtendedSerialNumber dans l'EF_ICC (voir sous-appendice 2). Pour les certificats de dispositifs GNSS externes, la valeur de la RDC est identique à la valeur de sensorGNSSSerialNumber dans l'EF_ICC (voir sous-appendice 14). Pour les certificats d'UEV, la valeur de la RDC est identique à la valeur de vuSerialNumber dans VuIdentification (voir sous-appendice 1), sauf si le fabricant ne connaît pas le numéro de série spécifique au moment où il demande le certificat.

CSM_147 Concernant les certificats ERCA et MSCA, la référence du détenteur de certificat est du type CertificationAuthorityKID tel que défini ~~à l'appendice~~ **au sous-appendice** 1.

9.3.2.6 Date d'entrée en vigueur du certificat (Certificate Effective Date)

CSM_148 La date d'entrée en vigueur du certificat indique la date et l'heure de début de la période de validité du certificat. ~~La date d'entrée en vigueur du certificat correspond à la date de génération du certificat.~~

9.3.2.7 Date d'expiration du certificat (Certificate Expiration Date)

CSM_149 La date d'expiration du certificat indique la date et l'heure de fin de la période de validité du certificat.

9.3.2.8 Signature du certificat (Certificate Signature)

CSM_150 La signature du certificat est créée en fonction du corps du certificat codé, y compris la balise et la longueur de ce dernier. On utilise l'algorithme de signature ECDSA, conformément aux règles [DSS], combiné avec l'algorithme de hachage associé à la taille de la clé de l'autorité de signature, comme indiqué au point ~~TCS_192~~**CSM_50**. La structure de la signature doit être en clair comme spécifié dans le document [TR-03111].

9.3.3 Demande de certificat

CSM_151 Lors de la demande d'un certificat, ~~le demandeur~~ **une MSCA** doit envoyer les données suivantes à ~~l'autorité de certification compétente~~ **l'ERCA** :

L'identificateur de profil de certificat du certificat faisant l'objet de la demande ;

La référence de l'autorité de certification à utiliser pour signer le certificat ;

La clé publique à signer.

CSM_152 En plus des données énoncées au point ~~TCS_293~~**CSM_151**, une MSCA envoie les données suivantes dans une demande de certificat à l'ERCA, afin de permettre à celle-ci de créer la référence du détenteur du nouveau certificat MSCA :

Le code numérique national de l'autorité de certification (type de données NationNumeric défini ~~à l'appendice~~ **au sous-appendice** 1) ;

Le code alphanumérique national de l'autorité de certification (type de données NationAlpha défini ~~à l'appendice~~ **au sous-appendice** 1) ;

Le numéro de série sur un octet permettant de faire la distinction entre les différentes clés de l'autorité de certification lorsque certaines clés font l'objet de modifications ;

Le champ de deux octets contenant les informations complémentaires spécifiques à l'autorité de certification.

CSM_153 ~~En plus des données énoncées au point 0, u~~**Un** fabricant d'équipement envoie les données suivantes dans une demande de certificat à une MSCA, afin de permettre à celle-ci de créer la référence du détenteur du certificat d'un nouvel équipement :

~~Un identificateur propre au fabricant pour le type d'équipement considéré ;~~

S'il est connu (voir ~~TCS_296~~ **CSM_154**), le numéro de série de l'équipement, propre au fabricant, ainsi que le type d'équipement et le mois de sa fabrication. Sinon, un identificateur unique de demande de certificat ;

Le mois et l'année de fabrication de l'équipement ou de la demande de certificat.

Le fabricant s'assure de l'exactitude de ces données et du fait que le certificat renvoyé par la MSCA est inséré dans l'équipement auquel il est destiné.

CSM_154 Pour ce qui est des UEV, le fabricant, lorsqu'il demande un certificat, peut connaître ou non le numéro de série propre au fabricant de l'UEV à laquelle le certificat et la clé privée associée sont destinés. S'il est connu, le fabricant d'UEV envoie le numéro de série à la MSCA. S'il n'est pas connu, le fabricant identifie de manière distincte chaque demande de certificat et envoie le numéro de série de la demande de certificat à la MSCA. Le certificat produit contient donc le numéro de série de la demande de certificat. Après insertion du certificat dans une UEV donnée, le fabricant communique la connexion entre le numéro de série de la demande de certificat et l'ID de l'UEV à la MSCA.

10. Authentification mutuelle de la carte et de l'UEV et messagerie sécurisée

10.1 Généralités

CSM_155 À haut niveau, la sécurité des communications entre une UEV et une carte tachygraphique repose sur les étapes suivantes :

- Premièrement, chaque partie montre à l'autre qu'elle détient un certificat de clé publique valable, signé par l'autorité de certification d'un**e** ~~État membre~~ **Partie contractante**. En retour, le certificat de clé publique de la MSCA doit être signé par l'autorité de certification racine ~~européen~~. Cette étape correspond à la vérification de la chaîne de certificats et fait l'objet d'une description détaillée à la section **10.2 ;**
- Deuxièmement, l'UEV montre à la carte qu'elle détient la clé privée correspondant à la clé publique du certificat présenté. Cela revient à signer un numéro aléatoire envoyé par la carte. La carte vérifie la signature par rapport au numéro aléatoire. Si cette vérification aboutit, l'UEV est authentifiée. Cette étape correspond à l'authentification de l'UEV et fait l'objet d'une description détaillée à la section **10.3 ;**
- Troisièmement, les deux parties calculent indépendamment deux clés de session AES en utilisant un algorithme de concordance de clé asymétrique. À l'aide de l'une de ces clés de session, la carte crée un code d'authentification de message (MAC) en rapport avec des données envoyées par l'UEV. L'UEV vérifie le MAC. Si cette vérification aboutit, la carte est authentifiée. Cette étape correspond à l'authentification de la carte et fait l'objet d'une description détaillée à la section **10.4 ;**
- Quatrièmement, l'UEV et la carte utilisent les clés de session convenues pour assurer la confidentialité, l'intégrité et l'authenticité de tous les messages échangés. Cette

étape correspond à la messagerie sécurisée et fait l'objet d'une description détaillée à la section **10.5.**

CSM_156 Le mécanisme décrit au point ~~TCS_297~~**CSM_155** est déclenché par l'UEV dès lors qu'une carte est insérée dans l'un de ses lecteurs.

10.2 Vérification mutuelle de la chaîne de certificats

10.2.1 Vérification de la chaîne de certificats de la carte par l'UEV

CSM_157 Les UEV suivent le protocole prévu à la figure 4 pour vérifier la chaîne de certificats d'une carte tachygraphique. **Pour chaque certificat qu'elle lit d'une carte tachygraphique, l'UEV vérifie que le champ ADC (autorisation du détenteur de certificat) est correct :**

- **Le champ ADC du certificat indique un certificat de carte destiné à l'authentification mutuelle (voir sous-appendice 1, type de données EquipmentType) ;**
- **Le champ ADC du certificat Card.AC indique une MSCA ;**
- **Le champ ADC du certificat Card.Link indique l'ERCA.**

Remarques concernant la **figure 4** :

- Les certificats et les clés publiques associés à la carte mentionnés dans la figure sont ceux destinés à l'authentification mutuelle. La section **9.1.5** précise leur intitulé : Card_MA ;
- Les certificats Card.AC et les clés publiques mentionnées dans la figure sont ceux destinés à la signature des certificats de carte ; cela est indiqué dans la RAC du certificat Card. La section **9.1.3** précise leur intitulé : MSCA_Card ;
- Le certificat Card.AC.EUR mentionné dans la figure est le certificat racine européen indiqué dans la RAC du certificat Card.AC ;
- Le certificat Card.Link mentionné dans la figure est le certificat de lien de la carte, le cas échéant. Comme le précise la section **9.1.2**, il s'agit d'un certificat de lien pour une nouvelle paire de clés racine ~~européenne~~ créé par l'ERCA et signé par la précédente clé privée **racine** ~~européenne~~ ;
- Le certificat Card.Link.EUR est le certificat racine ~~européen~~ indiqué dans la RAC du certificat Card.Link.

CSM_158 Comme le montre la **figure 4**, la vérification de la chaîne de certificats de la carte commence dès l'insertion de la carte. L'UEV extrait la référence du détenteur de la carte (`cardExtendedSerialNumber`) à partir de l'EF ICC. Elle vérifie si elle connaît la carte, c'est-à-dire si elle a déjà vérifié la chaîne de certificats de la carte dans le passé et l'a enregistrée en vue d'une utilisation ultérieure. Si tel est le cas et que le certificat de la carte est toujours valable, la procédure se poursuit avec la vérification de la chaîne de certificats de l'UEV. Autrement, l'UEV extrait successivement de la carte le certificat MSCA_Card à utiliser pour vérifier le certificat de la carte, Card.AC, le certificat EUR à utiliser pour vérifier le certificat MSCA_Card et éventuellement le certificat de lien, jusqu'à trouver un certificat reconnu ou vérifiable. Si elle trouve un tel certificat, l'UEV utilise ce certificat pour vérifier les certificats de carte sous-jacents qu'elle a extraits à partir de la carte. En cas de réussite, la procédure se poursuit avec la vérification de la chaîne de certificats de l'UEV. En cas d'échec, l'UEV ignore la carte.

Remarque : l'UEV peut connaître le certificat Card.AC.EUR pour trois raisons :

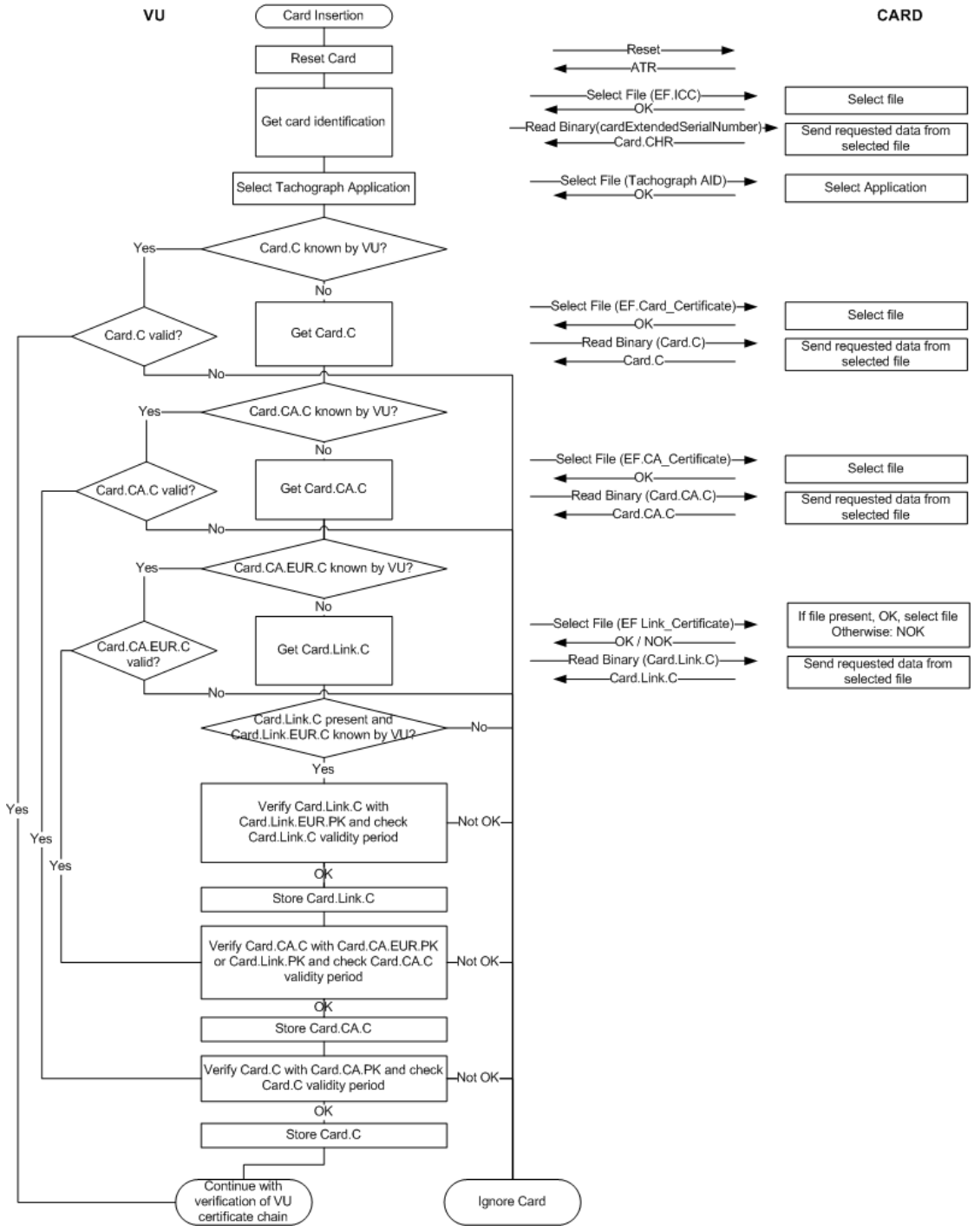
- Le certificat Card.AC.EUR est identique à celui de l'UEV ;

- Le certificat Card.AC.EUR précède celui de l'UEV et l'UEV contenait déjà ce certificat lors de sa mise en service (voir CSM_81) ;
- Le certificat Card.AC.EUR succède à celui de l'UEV et l'UEV a reçu par le passé un certificat de lien d'une autre carte tachygraphique, l'a vérifié et enregistré en vue d'une utilisation ultérieure.

CSM_159 Comme l'indique la **figure 4**, une fois que l'UEV a vérifié l'authenticité et la validité d'un certificat encore inconnu, elle peut l'enregistrer en vue d'une utilisation ultérieure, de manière à ne pas devoir le vérifier à nouveau s'il lui est représenté. Au lieu de stocker l'intégralité du certificat, l'UEV peut choisir de ne stocker que le contenu du corps du certificat, comme spécifié à la section **9.3.2. Alors que le stockage des certificats de tous les autres types est facultatif, l'UEV est tenue de stocker tout nouveau certificat de lien présenté par une carte.**

CSM_160 L'UEV vérifie la validité temporelle de tout certificat extrait de la carte ou stocké dans sa mémoire et refuse les certificats expirés. Pour vérifier la validité temporelle d'un certificat présenté par la carte, l'UEV utilise son horloge interne.

Figure 4
Protocole de vérification de la chaîne de certificats d'une carte par une UEV



10.2.2 Vérification de la chaîne de certificats de l'UEV par la carte

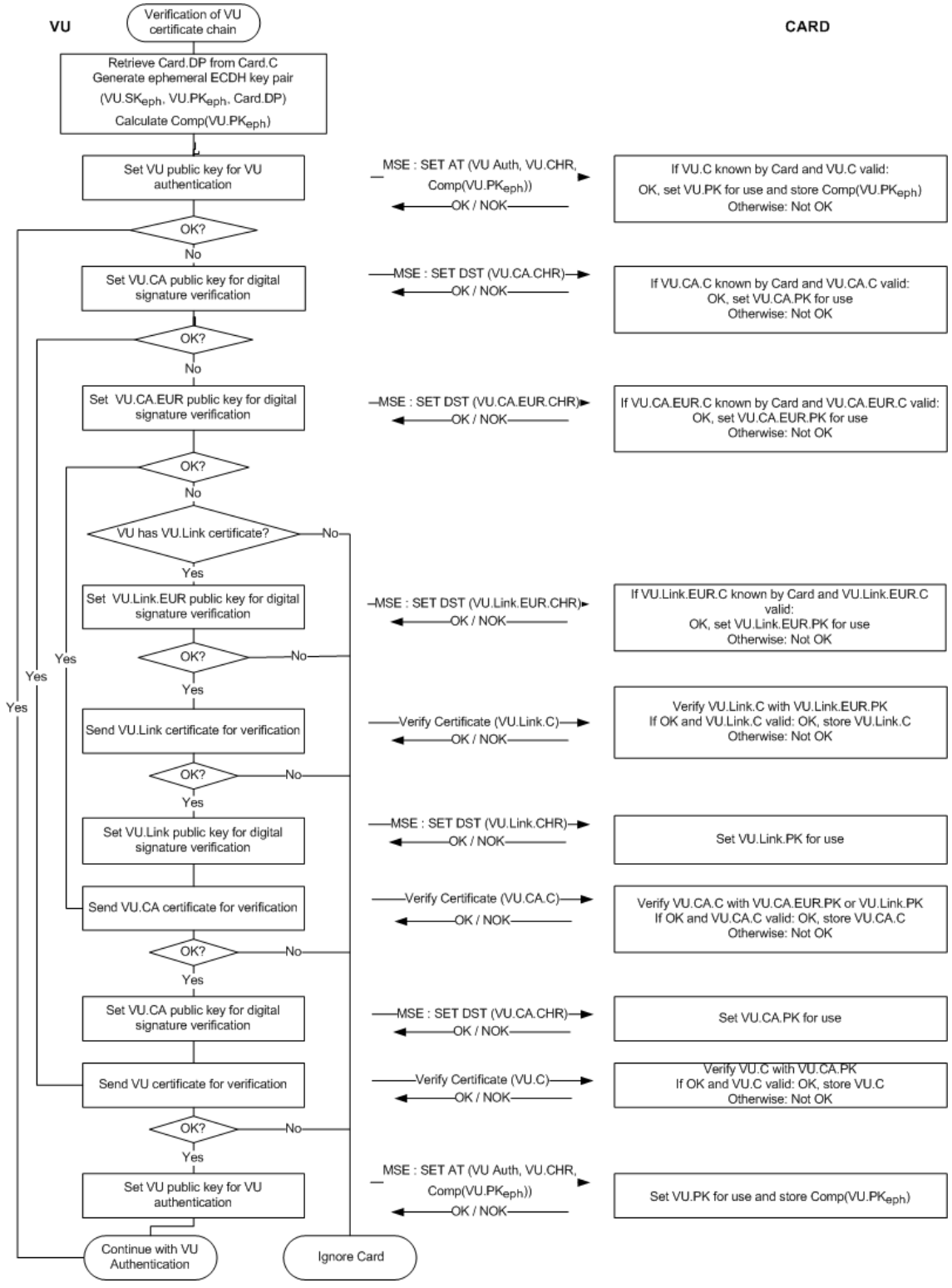
CSM_161 Les cartes tachygraphiques suivent le protocole prévu à la figure 5 pour vérifier la chaîne de certificats d'une UEV. **Pour chaque certificat présenté par une UEV, la carte vérifie que le champ ADC (autorisation du détenteur de certificat) est correct :**

- **Le champ ADC du certificat UEV.Link indique l'ERCA ;**
- **Le champ ADC du certificat UEV.AC indique une MSCA.**

Figure 5

Protocole de vérification de la chaîne de certificats d'une UEV par une carte

- **Le champ ADC du certificat de l'UEV indique un certificat d'UEV destiné à l'authentification mutuelle (voir sous-appendice 1, type de données EquipmentType).**



Remarques concernant la **figure 5** :

- Les certificats et les clés publiques associés à l'UEV mentionnés dans la figure sont ceux destinés à l'authentification mutuelle. La section **9.1.4** précise leur intitulé : UEV_MA ;

- Les certificats UEV.AC et les clés publiques mentionnés dans la figure sont ceux destinés la signature des certificats de l'UEV et du dispositif GNSS externe. La section **9.1.3** précise leur intitulé : MSCA_UEV-DGE ;
- Le certificat UEV.AC.EUR mentionné dans la figure est le certificat racine ~~européen~~ indiqué dans la RAC du certificat UEV.AC ;
- Le certificat UEV.Link mentionné dans la figure est le certificat de lien de l'UEV, le cas échéant. Comme le précise la section **9.1.2**, il s'agit d'un certificat de lien pour une nouvelle paire de clés racine ~~européenne~~ créé par l'ERCA et signé par la précédente clé privée **racine** ~~européenne~~ ;
- Le certificat UEV.Link.EUR est le certificat racine ~~européen~~ indiqué dans la RAC du certificat UEV.Link.

CSM_162 Comme le montre la **figure 5**, la vérification de la chaîne de certificats de l'UEV commence par la tentative de l'UEV de définir sa propre clé publique afin de l'utiliser dans la carte tachygraphique. Si cette tentative aboutit, cela signifie que la carte a déjà vérifié avec succès la chaîne de certificats de l'UEV dans le passé et a enregistré le certificat de l'UEV en vue d'une utilisation ultérieure. Dans ce cas, le certificat de l'UEV est prêt à servir et la procédure se poursuit avec l'authentification de l'UEV. Si la carte ne reconnaît par le certificat de l'UEV, l'UEV présente successivement le certificat MSCA_UEV servant à vérifier son certificat, le certificat UEV.AC.EUR servant à vérifier le certificat MSCA_UEV et éventuellement le certificat de lien, afin de trouver un certificat que la carte puisse reconnaître ou vérifier. Si un tel certificat est trouvé, la carte utilise ce certificat pour vérifier les certificats d'UEV sous-jacents qui lui sont présentés. En cas de réussite, l'UEV fixe définitivement la clé publique à utiliser dans la carte tachygraphique. En cas d'échec, l'UEV ignore la carte.

Remarque : la carte peut connaître le certificat UEV.AC.EUR pour trois raisons :

- Le certificat UEV.AC.EUR est identique à celui de l'UEV ;
- Le certificat UEV.AC.EUR précède celui de l'UEV et la carte contenait déjà ce certificat lors de son émission (voir CSM_91) ;
- Le certificat UEV.AC.EUR succède à celui de la carte et la carte a reçu par le passé un certificat de lien d'une autre UEV, l'a vérifié et enregistré en vue d'une utilisation ultérieure.

CSM_163 L'UEV utilise la commande MSE: SET AT pour définir sa clé publique et l'utiliser dans la carte tachygraphique. Conformément ~~à l'appendice~~ **au sous-appendice** 2, cette commande comporte une indication du mécanisme cryptographique à utiliser avec la clé définie. Ce mécanisme correspond à l'authentification de l'UEV au moyen de l'algorithme ECDSA, en combinaison avec l'algorithme de hachage associé à la taille de clé de la paire de clés UEV_MA de l'UEV, comme spécifié au point ~~TCS_192~~ **CSM_50**.

CSM_164 La commande MSE: SET AT comporte également une indication de la paire de clés éphémères que l'UEV utilise dans le cadre de la procédure de concordance de clés de session (voir sect. **10.4**). Par conséquent, avant d'envoyer la commande MSE: SET AT, l'UEV doit générer une paire de clés ECC éphémères. Pour générer la paire de clés éphémères, l'UEV utilise les paramètres de domaine normalisés indiqués dans le certificat de la carte. La paire de clés éphémères est désignée comme $UEV.SK_{eph}$, $UEV.PK_{eph}$ et Card.DP. L'UEV utilise l'abscisse du point public éphémère ECDH comme identification de clé ; il s'agit de la représentation comprimée de la clé publique appelée $Comp(UEV.PK_{eph})$.

CSM_165 Si la commande MSE: SET AT aboutit, la carte définit l'UEV .PK indiquée pour une utilisation ultérieure dans le cadre de l'authentification du véhicule et stocke temporairement Comp(UEV.PK_{eph}). Si deux commandes MSE: SET AT ou plus sont envoyées et aboutissent avant de procéder à la concordance des clés de session, la carte n'enregistre que le dernier Comp(UEV.PK_{eph}) reçu. **La carte réinitialise Comp(UEV.PKeph) lorsqu'une commande GENERAL AUTHENTICATE est traitée avec succès.**

CSM_166 La carte vérifie la validité temporelle de tout certificat présenté par l'UEV ou référencé par l'UEV pendant qu'il est stocké dans la mémoire de la carte et refuse les certificats expirés.

CSM_167 Afin de vérifier la validité temporelle d'un certificat présenté par l'UEV, chaque carte tachygraphique stocke dans sa mémoire des données temporelles à jour. Ces données ne sont pas directement actualisables par une UEV. Lors de son émission, les données temporelles d'une carte sont fixées de manière à correspondre à la date d'entrée en vigueur du certificat Card_MA de la carte. Une carte met à jour ses données temporelles si la date d'entrée en vigueur d'un certificat authentique représentant une « source temporelle valide » présenté par une UEV est plus récente que les données temporelles actuelles de la carte. Dans ce cas, la carte aligne ses données temporelles actuelles sur la date effective dudit certificat. La carte accepte uniquement les certificats suivants comme source temporelle valide :

- Certificats de lien ERCA de deuxième génération ;
- Certificats MSCA de deuxième génération ;
- Certificats d'UEV de deuxième génération émis par le même pays que le ou les certificats de carte de ladite carte.

Remarque : la dernière exigence implique qu'une carte doit pouvoir reconnaître la RAC du certificat de l'UEV, c'est-à-dire le certificat MSCA_UEV-DGE. Il ne s'agira pas de la même RAC que celle de son propre certificat, qui est le certificat MSCA_Card.

CSM_168 Comme l'indique la **figure 5**, une fois que la carte a vérifié l'authenticité et la validité d'un certificat encore inconnu, elle peut l'enregistrer en vue d'une utilisation ultérieure, de manière à ne pas devoir le vérifier à nouveau s'il lui est représenté. Au lieu de stocker l'intégralité du certificat, une carte peut choisir de ne stocker que le contenu du corps du certificat, comme spécifié à la section 9.3.2.

10.3 Authentification d'UEV

CSM_169 Les unités embarquées et les cartes suivent le protocole d'authentification d'UEV prévu à la **figure 6** pour authentifier l'UEV par rapport à la carte. La procédure d'authentification d'UEV permet à la carte tachygraphique de vérifier explicitement l'authenticité d'une UEV. Pour ce faire, l'UEV doit se servir de sa clé privée pour signer un défi généré par la carte.

CSM_170 Dans sa signature, l'UEV inclut, à côté du défi de la carte, la référence du détenteur de la carte qu'elle extrait du certificat de la carte.

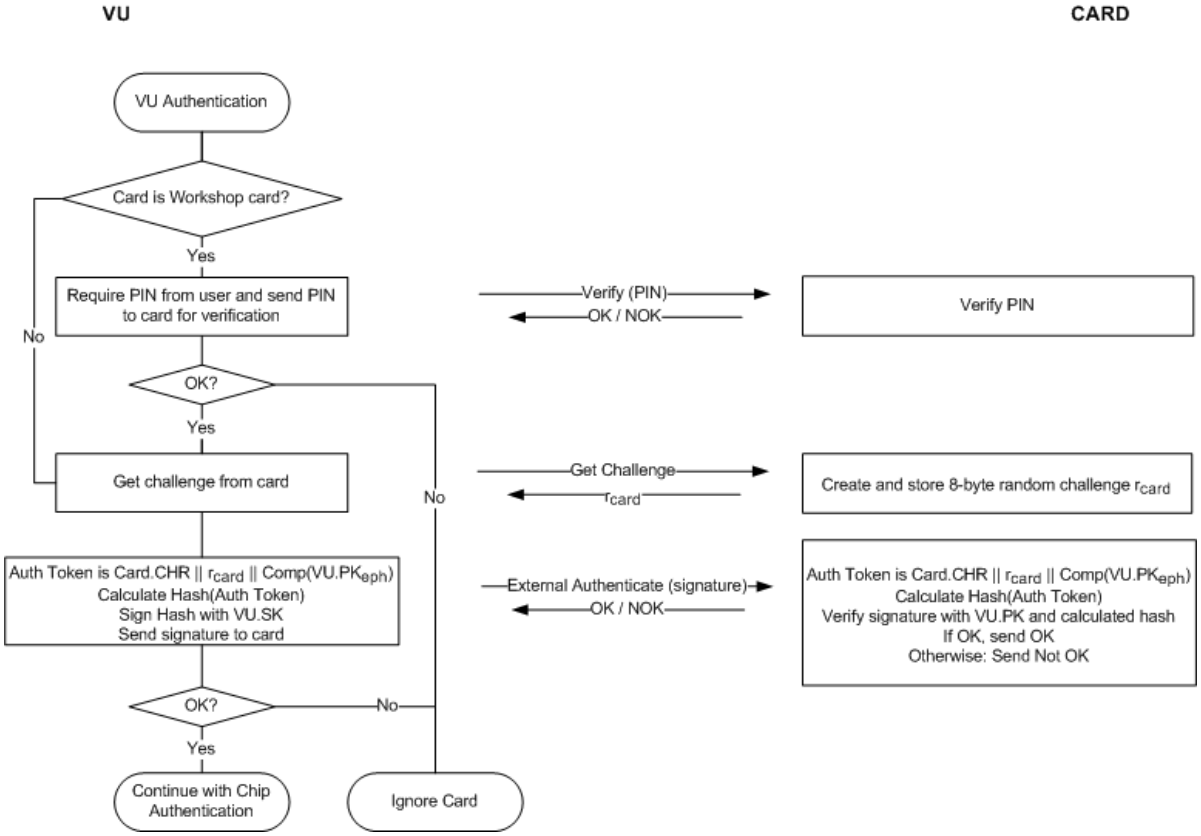
Remarque : cela garantit que la carte auprès de laquelle l'UEV s'authentifie est la même que celle dont elle a préalablement vérifié la chaîne de certificat.

CSM_171 L'UEV insère également dans la signature l'identificateur de la clé publique éphémère Comp(UEV.PK_{eph}) qu'elle utilisera pour configurer

la messagerie sécurisée pendant la procédure d'authentification de circuit décrite à la section **10.4**.

Remarque : cela garantit que l'UEV avec laquelle une carte communique au cours d'une session de messagerie sécurisée est la même UEV que celle qu'elle a authentifiée.

Figure 6
Protocole d'authentification d'UEV



CSM_172 Si l'UEV envoie plusieurs commandes GET CHALLENGE pendant son authentification, la carte renvoie un nouveau défi aléatoire sur 8 octets à chaque fois, mais enregistre uniquement le dernier.

CSM_173 L'algorithme de signature utilisé par l'UEV dans le cadre de la procédure d'authentification d'UEV est l'ECDSA, conformément aux règles [DSS], combiné avec l'algorithme de hachage associé à la taille de clé de la paire de clés UEV_MA de l'UEV, comme indiqué au point ~~TCS_192~~**CSM_50**. La structure de la signature doit être en clair, comme spécifié dans le document [TR-03111]. L'UEV envoie la signature produite à la carte.

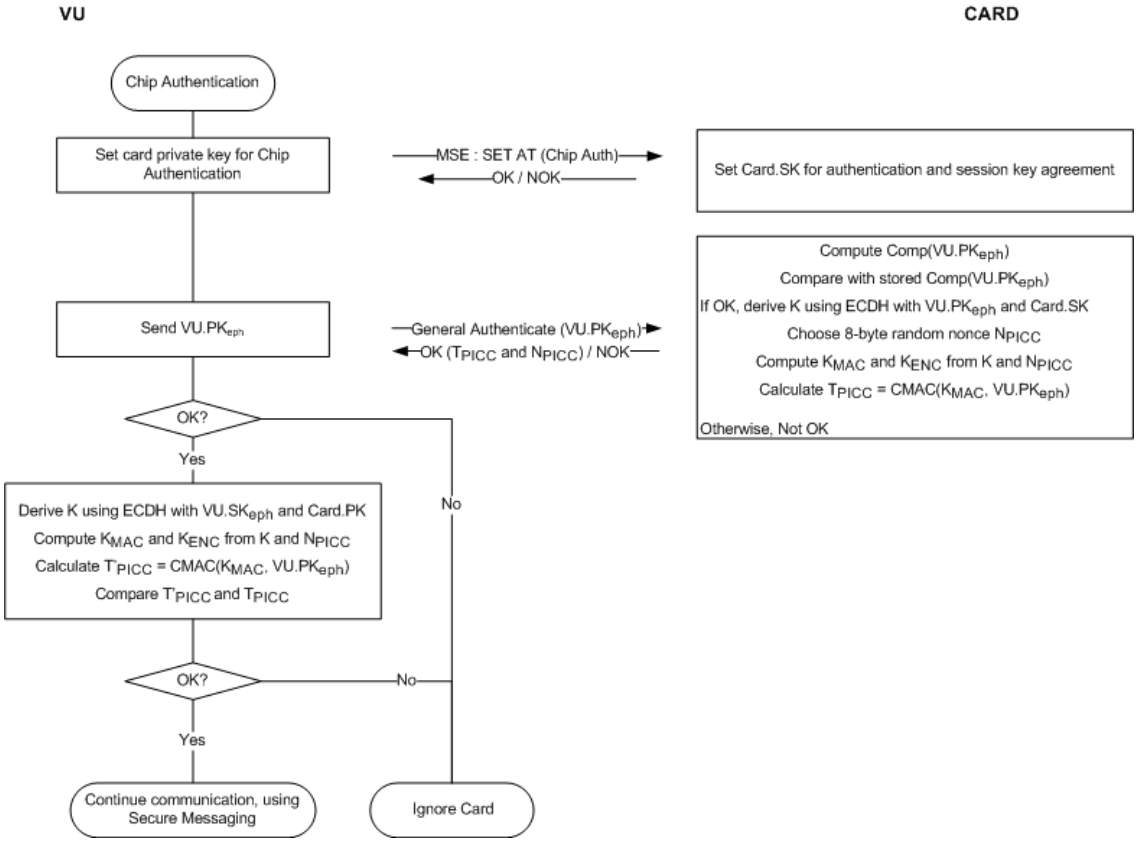
CSM_174 À la réception de la signature de l'UEV dans une commande EXTERNAL AUTHENTICATE, la carte :

- Calcule le jeton d'authentification en concaténant Card.RDC, le lanceur de défis de la carte r_{card} et l'identificateur de la clé publique éphémère de l'UEV Comp(UEV.PK_{eph}) ;
- ~~Calcule~~ **Vérifie** ~~le hachage en fonction du jeton d'authentification~~ **la signature de l'UEV** à l'aide de l'algorithme ECDSA et de l'algorithme de hachage associé à la taille de clé de la paire de clés UEV_MA de l'UEV comme indiqué au point ~~TCS_192~~**CSM_50** ;
- Vérifie la signature de l'UEV à l'aide de l'algorithme ECDSA **CSM_50**, combiné à l'UEV.PK et au ~~hachage~~ **jeton d'authentification** calculé.

10.4 Authentification du circuit et concordance de clés de session

CSM_175 Les unités embarquées et les cartes suivent le protocole d'authentification du circuit illustré à la **figure 7** pour authentifier la carte par rapport à l'UEV. L'authentification du circuit permet à l'unité embarquée de vérifier explicitement l'authenticité de la carte.

Figure 7
Authentification du circuit et concordance de clés de session



CSM_176 L'UEV et la carte suivent les étapes suivantes :

1. L'UEV lance la procédure d'authentification du circuit en envoyant la commande MSE: SET AT indiquant « authentification du circuit à l'aide de l'algorithme ECDH produisant une longueur de clés de session AES liée à la taille de clé de la paire de clés Card_MA de la carte, conformément à l'exigence ~~TCS_192~~**CSM_50** ». L'UEV détermine la taille de clé de la paire de clés de la carte d'après le certificat de la carte.
2. L'UEV envoie le point public UEV.PK_{eph} de sa paire de clés éphémères à la carte. **Le point public est converti en une chaîne d'octets comme spécifié dans le document [TR-03111]. On utilise la structure de codage non compressée.** Comme expliqué au point ~~TCS_306~~**CSM_164**, l'UEV a généré cette paire de clés éphémères avant la vérification de sa chaîne de certificats et a envoyé l'identificateur de la clé publique éphémère Comp(UEV.PK_{eph}) à la carte qui l'a enregistré dans sa mémoire.
3. La carte calcule Comp(UEV.PK_{eph}) d'après UEV.PK_{eph} et compare le résultat avec la valeur de Comp(UEV.PK_{eph}) stockée dans sa mémoire.
4. À l'aide de l'algorithme ECDH combiné à la clé privée statique de la carte et à la clé publique éphémère de l'UEV, la carte calcule une K secrète.
5. La carte choisit un nonce aléatoire sur 8 octets NPICC et l'utilise pour dériver les deux clés de session AES KMAC et KENC à partir de K (voir ~~TCS_321~~**CSM_179**).
6. En utilisant KMAC, la carte calcule un jeton d'authentification en fonction de l'identificateur de la clé publique éphémère de l'UEV : TPICC = CMAC(KMAC,

UEV.PK_{eph}). **La structure du point public doit être celle utilisée par l'UEV (voir point 2 ci-dessus).** La carte envoie NPICC et TPICC à l'unité embarquée.

7. À l'aide de l'algorithme ECDH combiné à la clé publique statique de la carte et à la clé privée éphémère de l'UEV, l'UEV calcule le même K secret que la carte à l'étape **3**0.
8. L'UEV dérive les clés de session KMAC et KENC d'après K et NPICC (voir ~~TCS_321~~ **CSM_179**).
9. L'UEV vérifie le jeton d'authentification TPICC.

CSM_177 À l'étape 2 ci-dessus, la carte calcule Comp(UEV.PKeph) comme l'abscisse du point public dans UEV.PKeph.

CSM_178 Aux étapes 3 et 6 ci-dessus, la carte et l'unité embarquée utilisent l'algorithme ECKA-EG défini dans le document [TR-03111].

CSM_179 Aux étapes 4 et 7 ci-dessus, la carte et l'unité embarquée utilisent la fonction de dérivation de clé pour les clés de session AES définie dans le document [TR-03111], en respectant les spécifications et ajustements suivants :

- La valeur du compteur est de '00 00 00 01' pour K_{ENC} et de '00 00 00 02' pour K_{MAC} ;
- Le numéro à usage unique/nonce *r* doit être utilisé et est égal à N_{PICC} ;
- Pour calculer les clés AES 128 bits, l'algorithme de hachage à utiliser est SHA-256 ;
- Pour calculer les clés AES 192 bits, l'algorithme de hachage à utiliser est SHA-384 ;
- Pour calculer les clés AES 256 bits, l'algorithme de hachage à utiliser est SHA-512.

La longueur des clés de session (c'est-à-dire la longueur à laquelle le hachage est tronqué) est liée à la taille de la paire de clés Card_MA, comme spécifié au point ~~TCS_192~~ **CSM_50**.

CSM_180 **Aux étapes 6 et 9** ci-dessus, la carte et l'unité embarquée utilisent l'algorithme AES en mode CMAC, conformément aux recommandations [SP 800-38B]. La longueur de T_{PICC} est liée à la longueur des clés de session AES, comme spécifié au point ~~TCS_192~~ **CSM_50**.

10.5 Messagerie sécurisée

10.5.1 Généralités

CSM_181 Toutes les commandes et réponses échangées entre une unité embarquée sur le véhicule et une carte tachygraphique après authentification réussie du circuit et jusqu'à la fin de la session sont protégées par la messagerie sécurisée.

CSM_182 À l'exception de l'extraction d'un fichier avec des règles d'accès MS-R-ENC-MAC-G2 (voir **sous-**appendice 2, chap. 4), la messagerie sécurisée doit être utilisée en mode authentification uniquement (*authentication-only*). Dans ce mode, un total de contrôle cryptographique (MAC) s'ajoute à toutes les commandes et réponses pour garantir l'authenticité et l'intégrité du message.

CSM_183 Lors de la lecture de données provenant d'un fichier soumis aux règles d'accès MS-R-ENC-MAC-G2, la messagerie sécurisée doit être utilisée en mode chiffrement puis authentification (*encrypt-then-authenticate*), c'est-à-dire que les données de réponse sont d'abord chiffrées pour garantir la confidentialité du message, puis qu'un MAC est calculé par rapport aux données chiffrées et structurées pour en garantir l'authenticité et l'intégrité.

CSM_184 La messagerie sécurisée utilise l'algorithme AES tel que défini dans la norme [AES] avec les clés de session K_{MAC} et K_{ENC} convenues lors de l'authentification du circuit.

CSM_185 Un entier non signé sert de compteur de séquences d'envoi (CSE) pour empêcher les attaques par réinsertion. La taille du CSE doit être égale à la taille du bloc AES, soit 128 bits. Le CSE respecte la structure MSB-first (octet le plus significatif en premier). Le compteur de séquences d'envoi est remis à zéro (c'est-à-dire '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00') au lancement de la messagerie sécurisée. Le CSE est incrémenté avant chaque APDU de commande ou de réponse, c'est-à-dire que la valeur de départ du CSE dans une session de messagerie sécurisée est égale à zéro et qu'à la première commande, la valeur du CSE est égale à un. La valeur du CSE pour la première réponse est égale à deux.

CSM_186 En ce qui concerne le chiffrement des messages, la clé K_{ENC} est utilisée avec l'algorithme AES en mode de chiffrement par chaînage de blocs (CBC), tel que défini dans la norme [ISO 10116], avec un paramètre d'entrelacement de $m = 1$ et un vecteur d'initialisation $SV = E(K_{ENC}, CSE)$, soit la valeur actuelle du compteur de séquences d'envoi chiffrée au moyen de K_{ENC}.

CSM_187 En ce qui concerne l'authentification des messages, la clé K_{MAC} est utilisée avec l'algorithme AES en mode CMAC comme spécifié dans le document [SP 800-38B]. La longueur du MAC est liée à la longueur des clés de session AES, conformément à l'exigence ~~TCS_192~~ **CSM_50**. Le compteur de séquence d'envoi est inclus dans le MAC et préfixé au datagramme à authentifier.

10.5.2 Structure de message sécurisée

CSM_188 La messagerie sécurisée n'utilise que les objets de données de messagerie sécurisée (voir la norme [ISO 7816-4]) énumérés au **tableau 5**~~47~~. Dans tous les messages, ces objets de données doivent être agencés dans l'ordre défini dans ce tableau.

Tableau 5
Objets de données de messagerie sécurisée

		Présence obligatoire (O), conditionnelle (C) ou interdite (I) dans	
Nom de l'objet de données	*Balise*	*Commandes*	*Réponses*
Valeur en clair non codée en BER-TLV	'81'	C	C
Valeur en clair codée BER-TLV, sans objet de données de messagerie sécurisée	'B3'	C	C
Indicateur de contenu de remplissage par cryptogramme, valeur en clair non codée en BER-TLV	'87'	C	C
Le protégée	'97'	C	I
État de traitement	'99'	I	O
Total de contrôle cryptographique	'8E'	O	O

Remarque : comme le spécifie ~~l'appendice~~ **le sous-appendice** 2, les cartes tachygraphiques prennent en charge les commandes READ BINARY et UPDATE BINARY avec un octet INS impair ('B1' resp. 'D7'). Ces variantes de commande sont nécessaires pour extraire et mettre à jour des fichiers de 32 768 octets et davantage. Si une telle variante est utilisée, un objet de données avec la balise 'B3' sera substitué à un objet avec la balise '81'. Pour toute information complémentaire, se référer ~~à l'appendice~~ **au sous-appendice** 2.

CSM_189 Tous les objets de données de messagerie sécurisée sont codés en DER-TLV conformément à la norme [ISO 8825-1]. Ce chiffrement produit la structure TLV suivante :

Balise : la balise est chiffrée sur un ou deux octets et indique le contenu ;

Longueur : la longueur est chiffrée comme un entier non signé sur un, deux ou trois octets, soit une longueur maximale de 65 535 octets. On utilise le nombre minimal d'octets ;

Valeur : la valeur est chiffrée sur zéro octet ou plus.

CSM_190 Les APDU protégés par messagerie sécurisée sont conçus de la manière suivante :

- L'en-tête de commande est inclus dans le calcul du MAC, par conséquent la valeur '0C'sert pour l'octet de classe CLA ;
- Comme spécifié ~~à l'appendice~~ **au sous-appendice 2**, tous les octets INS sont pairs, sauf éventuellement les octets INS impairs des commandes READ BINARY et UPDATE BINARY ;
- La valeur réelle de Lc est modifiée en Lc' après l'application de la messagerie sécurisée ;
- La zone de données se compose d'objets de données de messagerie sécurisée ;
- Dans l'APDU de commande protégée, le nouvel octet Le est défini à '00'. Si nécessaire, un objet de données '97' est inséré dans la zone de données afin de transmettre la valeur initiale de Le.

CSM_191 Tout objet de données à chiffrer doit être complété conformément à la norme [ISO 7816-4] en utilisant l'indicateur de contenu de remplissage '01'. Concernant le calcul du MAC, ~~chaque~~ **les** objet**s** de données de l'APDU ~~doit~~ **doivent** ~~également~~ être complétés ~~séparément~~ conformément à la norme [ISO 7816-4].

Remarque : le remplissage à des fins de messagerie sécurisée est toujours affecté à la couche de messagerie sécurisée, et non aux algorithmes CMAC ou CBC.

Synthèse et exemples

Une APDU de commande avec messagerie sécurisée aura la structure suivante, selon la commande non sécurisée correspondante (OD correspond à l'objet de données) :

Cas 1 : CLA INS P1 P2 || Lc' || OD '8E' || Le
Cas 2 : CLA INS P1 P2 || Lc' || OD '97' || OD '8E' || Le
Cas 3 (octet INS pair) : CLA INS P1 P2 || Lc' || OD '81' || DO'8E' || Le

Cas 3 (octet INS impair) : CLA INS P1 P2 || Lc' || OD 'B3' || OD '8E' || Le
Cas 4 (octet INS pair) : CLA INS P1 P2 || Lc' || OD '81' || OD '97' || OD '8E' || Le

Cas 4 (octet INS impair) : CLA INS P1 P2 || Lc' || OD 'B3' || OD '97' || OD '8E' || Le

Où Le = '00' ou '00 00' selon que l'on utilise des zones de longueur courte ou étendue (voir [ISO 7816-4]).

Une APDU de réponse avec messagerie sécurisée aura la structure suivante, selon la réponse non sécurisée correspondante :

Cas 1 ou 3 : OD '99' || OD '8E' || ME1ME2
Cas 2 ou 4 (octet INS pair) avec codage : OD '81' || OD '99' || OD '8E' || ME1ME2

Cas 2 ou 4 (octet INS pair) sans codage : OD '87' || OD '99' || OD '8E' || ME1ME2

Cas 2 ou 4 (octet INS impair) sans codage : OD 'B3' || OD '99' || OD '8E' || ME1ME2

Remarque : le cas 2 ou 4 (octet INS impair) avec codage ne sert jamais dans la communication entre une UEV et une carte.

Ci-après suivent trois exemples de transformations APDU pour des commandes avec un code INS pair. La **figure 8** montre une APDU de commande authentifiée relevant du cas 4, la **figure 9** montre une APDU de réponse authentifiée relevant des cas **1** ou **3** et la **figure 10** montre une APDU de réponse chiffrée et authentifiée relevant des cas 2 ou 4.

Figure 8

Transformation d'une APDU de commande authentifiée relevant du cas 4

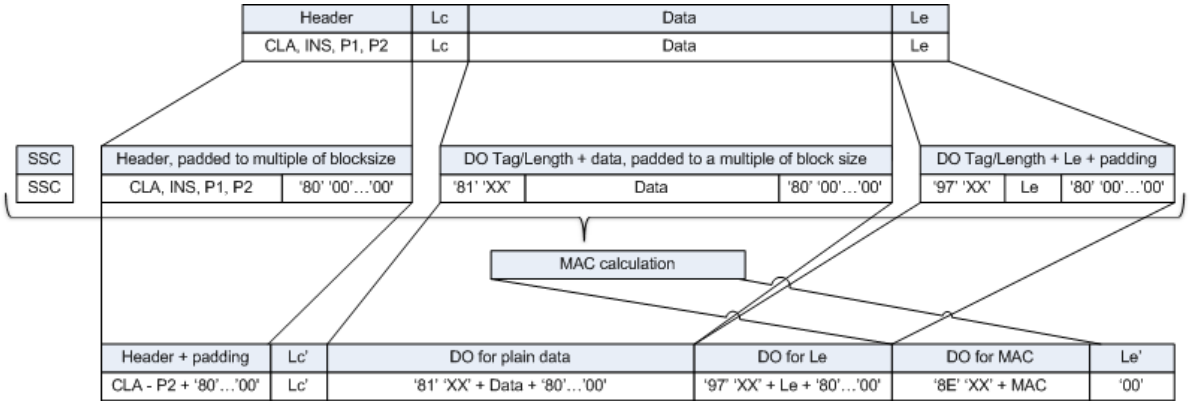


Figure 9

Transformation d'une APDU de réponse authentifiée relevant des cas 1 ou 3

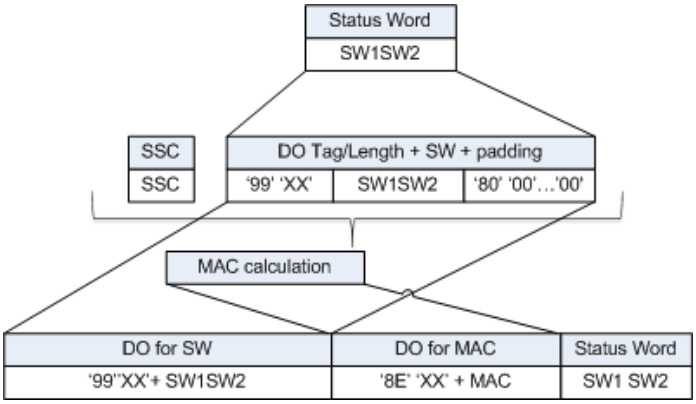
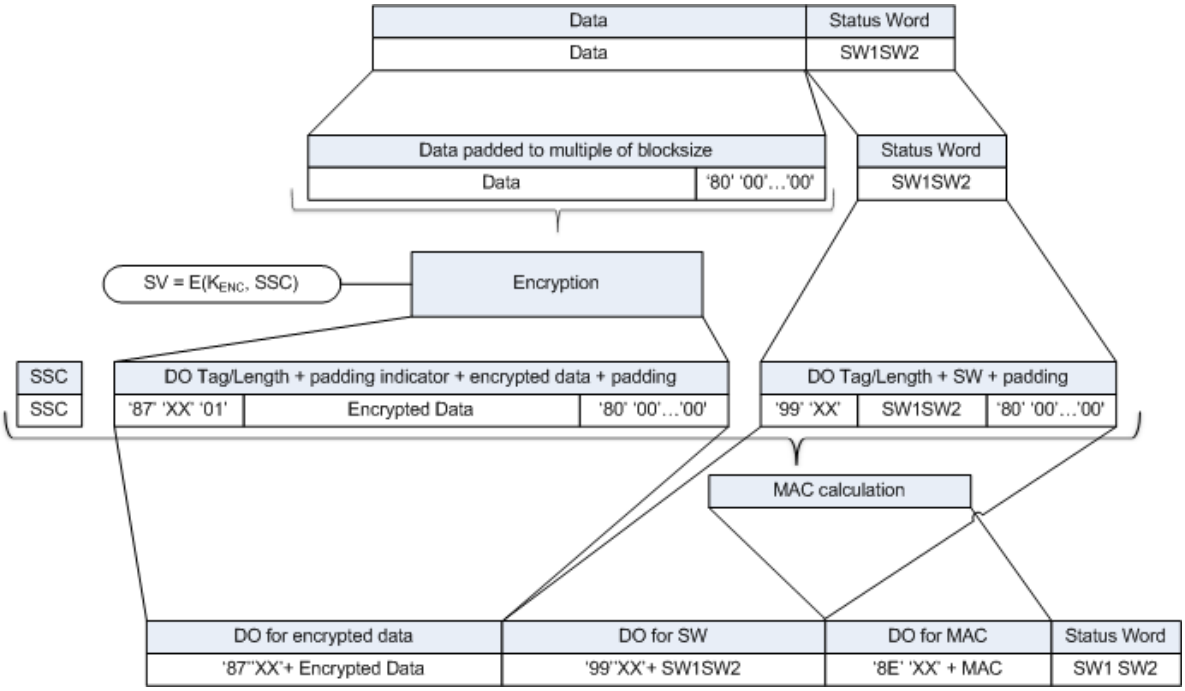


Figure 10
Transformation d'une APDU de réponse chiffrée et authentifiée relevant des cas 2 ou 4



10.5.3 Interruption de la session de messagerie sécurisée

CSM_192 Les unités embarquées interrompt une session de messagerie sécurisée en cours si et seulement si l'une des conditions suivantes survient :

- Elle reçoit une APDU de réponse en clair ;
- Elle détecte une erreur de messagerie sécurisée dans une APDU de réponse :
  - Un objet de données de messagerie sécurisée attendu est manquant, l'ordre des objets de données est erroné ou un objet de données inconnu est présent ;
  - Un objet de données de messagerie sécurisée est erroné, par exemple la valeur du MAC est erronée, la structure TLV est erronée ou l'indicateur de remplissage de la balise '87' n'est pas égal à '01' ;
- La carte envoie un octet d'état indiquant qu'elle a détecté une erreur de messagerie sécurisée (voir ~~TCS_336~~ **CSM_194**) ;
- La limite pour le nombre de commandes et de réponses associées de la session en cours est atteinte. Pour une UEV donnée, cette limite est définie par le fabricant, compte tenu des exigences en matière de sécurité du matériel utilisé et avec une valeur maximale de 240 commandes et réponses associées de messagerie sécurisée par session.

CSM_193 Une carte tachygraphique interrompt une session de messagerie sécurisée en cours si et seulement si l'une des conditions suivantes survient :

- Elle reçoit une APDU de réponse en clair ;
- Elle détecte une erreur de messagerie sécurisée dans une APDU de commande :
  - Un objet de données de messagerie sécurisée est manquant, l'ordre des objets de données est erroné ou un objet de données inconnu est présent ;
  - Un objet de données de messagerie sécurisée est erroné, par exemple la valeur du MAC est erronée ou la structure TLV est erronée ;
- L'alimentation est coupée ou la carte est réinitialisée ;

~~— L'UEV sélectionne une application sur la carte ;~~

- L'UEV lance la procédure d'authentification d'UEV ;
- La limite pour le nombre de commandes et de réponses associées de la session en cours est atteinte. Pour une carte donnée, cette limite est définie par le fabricant, compte tenu des exigences en matière de sécurité du matériel utilisé et avec une valeur maximale de 240 commandes et réponses associées de messagerie sécurisée par session.

CSM_194 Concernant la gestion des erreurs de messagerie sécurisée par une carte tachygraphique :

- Si, dans une APDU de commande, certains objets de données de messagerie sécurisée attendus sont manquants, l'ordre des objets de données est erroné ou des objets de données inconnus sont présents, la carte tachygraphique répond en envoyant les octets d'état '69 87' ;
- Si un objet de données de messagerie sécurisée dans une APDU de commande est erroné, la carte tachygraphique répond en envoyant les octets d'état '69 88'.

Dans ce cas, les octets d'état doivent être renvoyés sans utiliser la messagerie sécurisée.

CSM_195 Si une session de messagerie sécurisée entre une UEV et une carte tachygraphique est interrompue, l'UEV et la carte tachygraphique :

- Détruisent de façon sécurisée les clés de sessions stockées en mémoire ;
- Établissent immédiatement une nouvelle session de messagerie sécurisée, conformément aux dispositions des sections **10.2** à **10.5**.

CSM_196 Si pour une raison quelconque, l'UEV décide de relancer une procédure d'authentification mutuelle vis-à-vis d'une carte insérée, il faudra recommencer à partir de la vérification de la chaîne de certificats de la carte, conformément aux dispositions de la section **10.2**, et poursuivre conformément aux dispositions des sections **10.2** à **10.5**.

11. Couplage de l'UEV et du dispositif GNSS externe, authentification mutuelle et messagerie sécurisée

11.1 Généralités

CSM_197 Le dispositif GNSS qu'utilise une UEV pour déterminer sa position peut être interne (c'est-à-dire intégré au boîtier de l'UEV et inamovible) ou externe (module indépendant). Dans le premier cas, il n'est pas nécessaire de normaliser la communication interne entre le dispositif GNSS et l'UEV. Les exigences du présent chapitre ne s'appliquent donc pas. Dans le deuxième cas, la communication entre le dispositif GNSS externe (DGE) et l'UEV doit être normalisée et protégée tel que le décrit le présent chapitre.

CSM_198 La communication sécurisée entre les unités embarquées et un dispositif GNSS externe s'effectue de la même manière que la communication sécurisée entre les unités embarquées et une carte tachygraphique, le dispositif GNSS externe jouant le rôle de la carte tachygraphique. Toutes les exigences énoncées au chapitre **10** pour les cartes tachygraphiques doivent être satisfaites par le DGE, compte tenu des modifications, clarifications et ajouts mentionnés au présent chapitre. En particulier, la vérification mutuelle de la chaîne de certificats, l'authentification de l'UEV et l'authentification du circuit doivent être exécutées conformément aux dispositions des sections **11.3 et 11.4**.

CSM_199 La communication entre les unités embarquées et un dispositif GNSS externe se distingue de la communication entre les unités embarquées et une carte tachygraphique en cela qu'une UEV et un DGE doivent être couplés une fois dans l'atelier avant qu'ils puissent échanger des données GNSS en fonctionnement normal. Le processus de couplage fait l'objet d'une description détaillée à la section **11.2**.

CSM_200 Pour la communication entre les unités embarquées et un dispositif GNSS externe, on utilise les commandes et les réponses APDU relevant des normes [ISO 7816-4] et [ISO 7816-8]. La structure exacte de ces APDU fait l'objet d'une description détaillée ~~à l'appendice~~**au sous-appendice** 2 ~~de la~~ **du** présente ~~Annexe~~ **appendice**.

11.2 Couplage d'une UEV et d'un dispositif GNSS externe

CSM_201 Une unité embarquée sur véhicule et un dispositif GNSS externe doivent être couplés par un atelier. Seuls une UEV et un DGE couplés peuvent communiquer en fonctionnement normal.

CSM_202 Le couplage d'une UEV et d'un DGE n'est possible que si l'UEV est en mode étalonnage. Le couplage est lancé par l'unité embarquée sur le véhicule.

CSM_203 Un atelier peut à tout moment coupler de nouveau les unités embarquées à un autre dispositif GNSS externe ou au même. Pendant le nouveau couplage, l'UEV détruit de façon sécurisée le certificat DGE_MA présent dans sa mémoire et enregistre le certificat DGE_MA du DGE auquel elle vient d'être couplée.

CSM_204 Un atelier peut à tout moment coupler de nouveau un dispositif GNSS externe à une autre UEV ou à la même. Pendant le nouveau couplage, le DGE détruit de façon sécurisée le certificat UEV_MA présent dans sa mémoire et enregistre le certificat UEV_MA de la UEV à laquelle il vient d'être couplé.

11.3. Vérification mutuelle de la chaîne de certificats

11.3.1 Généralités

CSM_205 La vérification mutuelle de la chaîne de certificats entre une UEV et un DGE prend place uniquement durant le couplage de l'UEV et du DGE par un atelier. Pendant le fonctionnement normal d'une UEV et d'un DGE couplés, aucun certificat n'est vérifié. L'UEV et le DGE font confiance aux certificats enregistrés pendant le couplage, après avoir vérifié leur validité temporelle. L'UEV et le DGE ne font confiance à aucun autre certificat pour protéger la communication entre eux en fonctionnement normal.

11.3.2 Pendant le couplage UEV − dispositif GNSS externe

CSM_206 Pendant le couplage à un dispositif GNSS externe, l'unité embarquée sur le véhicule utilise le protocole décrit à la **figure 4** (sect. 10.2.1) pour vérifier la chaîne de certificats du dispositif GNSS externe.

Remarques concernant la **figure 4** dans ce contexte :

- Le contrôle de la communication n'entre pas dans le champ d'application du présent **sous-**appendice. Cependant, un DGE n'est pas une carte intelligente. L'UEV n'enverra donc vraisemblablement pas de commande RESET (réinitialisation) pour lancer la communication et ne recevra pas d'ATR ;

- Les certificats et les clés publiques de la carte mentionnés dans la figure doivent être interprétés comme ceux du DGE destinés à l'authentification mutuelle. La section **9.1.6** précise leur intitulé : DGE_MA ;
- Les certificats Card.AC et les clés publiques mentionnés dans la figure doivent être interprétés comme ceux de la MSCA destinés à la signature des certificats du DGE. La section **9.1.3** précise leur intitulé : MSCA_UEV-DGE ;
- Le certificat Card.AC.EUR mentionné dans la figure est le certificat racine ~~européen~~ indiqué dans la RAC du certificat MSCA_UEV-DGE ;
- Le certificat Card.Link mentionné dans la figure correspond au certificat de lien du DGE, le cas échéant. Comme le précise la section **9.1.2**, il s'agit d'un certificat de lien pour une nouvelle paire de clés racine ~~européenne~~ créé par l'ERCA et signé par la précédente clé privée **racine** ~~européenne~~ ;
- Le certificat Card.Link.EUR est le certificat racine ~~européen~~ indiqué dans la RAC du certificat Card.Link ;
- Au lieu de l'élément cardExtendedSerialNumber, l'UEV extrait l'élément sensorGNSSserialNumber depuis l'EF ICC ;
- Au lieu de sélectionner l'AID de la carte tachygraphique, l'UEV sélectionne l'AID du DGE :
- La mention « Ignorer la carte » devient « Ignorer le DGE ».

CSM_207 Une fois le certificat DGE_MA vérifié, l'unité embarquée sur le véhicule l'enregistre dans sa mémoire pour l'utiliser en fonctionnement normal (voir sect. **11.3.3**).

CSM_208 Pendant le couplage à une UEV, un dispositif GNSS externe utilise le protocole décrit à la figure 5 (sect. 10.2.2) pour vérifier la chaîne de certificats de l'UEV.

Remarques concernant la **figure 5** dans ce contexte :

- L'UEV génère une nouvelle paire de clés éphémères en utilisant les paramètres de domaine figurant dans le certificat DGE ;
- Les certificats et les clés publiques associés à l'UEV mentionnés dans la figure sont ceux destinés à l'authentification mutuelle. La section **9.1.4** précise leur intitulé : UEV_MA ;
- Les certificats UEV.AC et les clés publiques mentionnés dans la figure sont ceux destinés à la signature des certificats de l'UEV et du dispositif GNSS externe. La section **9.1.3** précise leur intitulé : MSCA_UEV-DGE ;
- Le certificat UEV.AC.EUR mentionné dans la figure est le certificat racine ~~européen~~ indiqué dans la RAC du certificat UEV.AC ;
- Le certificat UEV.Link mentionné dans la figure est le certificat de lien de l'UEV, le cas échéant. Comme le précise la section **9.1.2**, il s'agit d'un certificat de lien pour une nouvelle paire de clés racine ~~européenne~~ créé par l'ERCA et signé par la précédente clé privée **racine** ~~européenne~~ ;
- Le certificat UEV.Link.EUR est le certificat racine européen indiqué dans la RAC du certificat UEV.Link.

CSM_209 À titre d'exception à l'exigence du ~~TCS_309~~ **CSM_167**, un DGE utilise la date et l'heure GNSS pour vérifier la validité temporelle de tout certificat présenté.

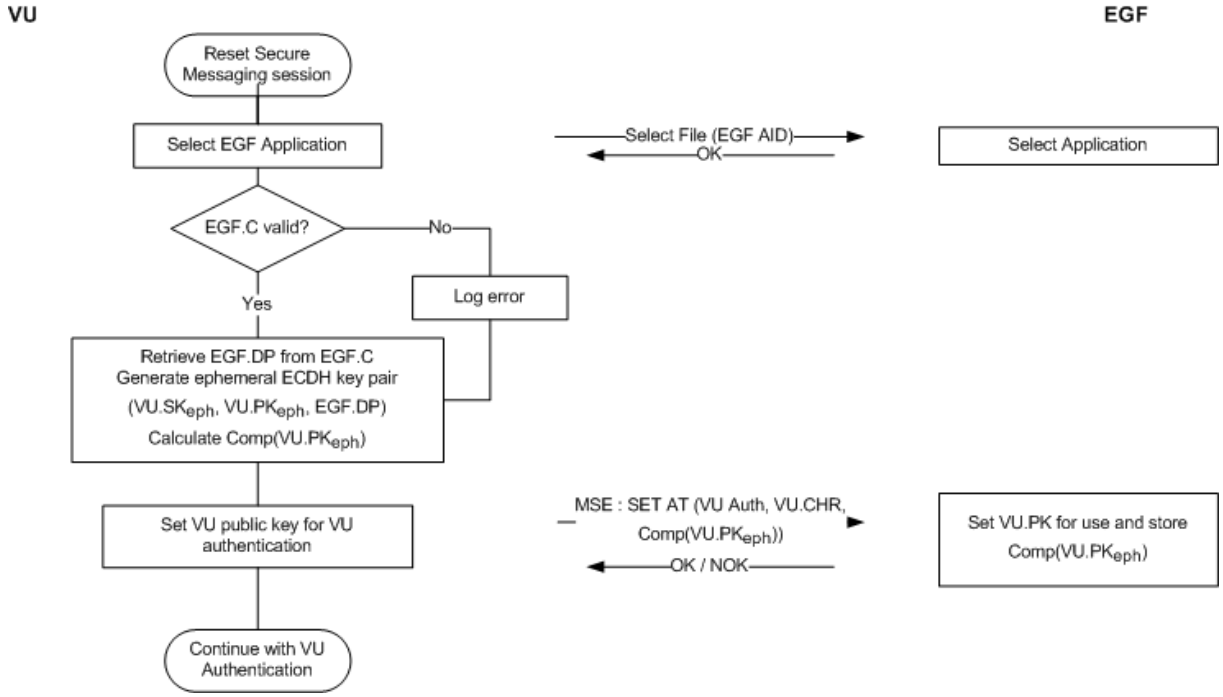
CSM_210 Une fois le certificat UEV_MA vérifié, le dispositif GNSS externe enregistre ce certificat dans sa mémoire pour l'utiliser en fonctionnement normal (voir sect. **11.3.3**).

11.3.3 Pendant le fonctionnement normal

CSM_211 En fonctionnement normal, l'unité embarquée sur le véhicule et le dispositif GNSS externe suivent le protocole décrit à la figure 11 pour vérifier la validité temporelle des certificats du DGE, ~~MA et UEV_MA~~ en mémoire et pour définir la clé publique UEV_MA en vue de l'authentification ultérieure de l'UEV. Aucune autre vérification mutuelle des chaînes de certificats n'a lieu en fonctionnement normal.

Remarque : la **figure 11** reprend essentiellement les premières étapes présentées aux figures **4** et **5**. Il convient de souligner à nouveau que, dans la mesure où le DGE n'est pas une carte intelligente, l'UEV n'enverra vraisemblablement pas de commande RESET pour lancer la communication et ne recevra pas d'ATR. Dans tous les cas, cela sort du champ d'application du présent **sous-**appendice.

Figure 11
Vérification mutuelle de la validité temporelle du certificat en fonctionnement normal entre l'UEV et le DGE



CSM_212 Comme le montre la **figure 11**, l'unité embarquée sur le véhicule enregistre une erreur si le certificat DGE_MA n'est plus valable. Toutefois, l'authentification mutuelle, la concordance de clés et la communication ultérieure par messagerie sécurisée se déroulent normalement.

11.4 Authentification de l'UEV, authentification du circuit et concordance de clés de session

CSM_213 L'authentification de l'UEV, l'authentification du circuit et la concordance des clés de la session entre une UEV et un DGE ont lieu pendant le couplage et chaque fois qu'une session de messagerie sécurisée est rouverte en fonctionnement normal. L'UEV et le DGE exécutent les procédures décrites aux sections **10.3 et 10.4**. Toutes les exigences prévues dans ces sections s'appliquent.

11.5 Messagerie sécurisée

CSM_214 Toutes les commandes et réponses échangées entre les unités embarquées et un dispositif GNSS externe après l'authentification réussie du circuit et jusqu'à la fin de la session sont protégées par la messagerie sécurisée en mode authentification uniquement. Toutes les exigences prévues à la section **10.5** s'appliquent.

CSM_215 Si une session de messagerie sécurisée entre une UEV et un DGE est interrompue, l'UEV ouvre immédiatement une nouvelle session de messagerie sécurisée, comme décrit aux sections **11.3.3 et 11.4**.

12. Couplage et communication entre l'UEV et le capteur de mouvement

12.1 Généralités

CSM_216 Les unités embarquées et un capteur de mouvement communiquent à l'aide du protocole d'interface prévu dans la norme [ISO 16844-3] pendant le couplage et en fonctionnement normal. Cela inclut les modifications décrites dans le présent chapitre et à la section **9.2.1**.

Remarque : les lecteurs de la présente section sont censés être au fait du contenu de la norme [ISO 16844-3].

12.2 Couplage de l'UEV et du capteur de mouvement à l'aide de générations de clés différentes

Comme expliqué à la section **9.2.1**, la clé maîtresse du capteur de mouvement et toutes les clés associées sont régulièrement remplacées. Cela entraîne la présence de jusqu'à trois clés AES $K_{M\text{-}CAT}$ liées au capteur de mouvement (de générations de clés consécutives) sur les cartes d'atelier. De même, un maximum de trois différents chiffrements de données de type AES (fondés sur des générations consécutives de la clé maîtresse K_M du capteur de mouvement) peuvent être présents dans les capteurs de mouvement. Une unité embarquée ne contient qu'une seule clé $K_{M\text{-}UEV}$ associée au capteur de mouvement.

CSM_217 Le couplage d'une UEV et d'un capteur de mouvement de deuxième génération se déroule de la manière suivante (voir le tableau 6 de la norme [ISO 16844-3]) :

1. Une carte d'atelier de deuxième génération est insérée dans le lecteur approprié de l'UEV et celle-ci est connectée au capteur de mouvement ;

2. L'UEV lit toutes les clés $K_{M\text{-}CAT}$ disponibles sur la carte d'atelier, inspecte leur numéro de version et choisit celui qui correspond au numéro de version de sa clé $K_{M\text{-}UEV}$. Si la clé $K_{M\text{-}CAT}$ correspondante est absente de la carte d'atelier, l'UEV interrompt la procédure de couplage et affiche le message d'erreur approprié à l'intention du détenteur de la carte d'atelier ;

3. L'UEV calcule la clé maîtresse du capteur de mouvement K_M à partir des clés $K_{M\text{-}UEV}$ et $K_{M\text{-}CAT}$, ainsi que la clé d'identification K_{ID} à partir de K_M, comme prévu à la section **9.2.1** ;

4. L'UEV envoie les instructions pour lancer la procédure de couplage avec le capteur de mouvement, conformément à la norme [ISO 16844-3], et chiffre le numéro de série reçu du capteur de mouvement avec la clé d'identification K_{ID}. L'UEV renvoie le numéro de série chiffré au capteur de mouvement ;

5. Le capteur de mouvement compare le numéro de série chiffré avec chacun des numéros de série chiffrés dont il dispose en interne. S'il trouve une correspondance, l'UEV est authentifiée. Le capteur de mouvement relève la génération de K_{ID} utilisée

par l'UEV et renvoie la version chiffrée correspondante de sa clé de couplage, c'est-à-dire celle chiffrée avec la même génération de K_M ;

6. L'UEV déchiffre la clé de couplage à l'aide de K_M, génère une clé de session K_S, la chiffre à l'aide de la clé de couplage et envoie le résultat au capteur de mouvement. Le capteur de mouvement déchiffre K_S ;

7. L'UEV assemble les informations relatives au couplage comme le prévoit la norme [ISO 16844-3], chiffre les informations à l'aide de la clé de couplage et envoie le résultat au capteur de mouvement. Le capteur de mouvement déchiffre les informations de couplage ;

8. Le capteur de mouvement chiffre les informations relatives au couplage reçues à l'aide de la K_S qu'il a reçue et les renvoie à l'UEV. L'UEV vérifie que les informations de couplage sont identiques à celles qu'elle a envoyées au capteur de mouvement à l'étape précédente. Dans l'affirmative, cela prouve que le capteur de mouvement a utilisé la même K_S que l'UEV. Par conséquent, à l'étape **5**, il a envoyé sa clé de couplage chiffrée avec la bonne génération de K_M. Le capteur de mouvement est ainsi authentifié.

Remarque : les étapes 2 et 5 divergent de la procédure normalisée [ISO 16844-3] ; les autres étapes sont standard.

Exemple : imaginons qu'un couplage ait lieu durant la première année de validité du certificat ERCA (3) (voir fig. **2 de la section** ~~9.2.2.2~~ **9.2.1.2**). Imaginons en outre que :

- Le capteur de mouvement ait été émis pendant la dernière année de validité du certificat ERCA (1). Il contiendra alors les clés et les données suivantes :
- $N_s[1]$: son numéro de série chiffré avec K_{ID} de génération 1 ;
- $N_s[2]$: son numéro de série chiffré avec K_{ID} de génération 2 ;
- $N_s[3]$: son numéro de série chiffré avec K_{ID} de génération 3 ;
- $K_P[1]$: sa clé de couplage[13] de génération 1, chiffrée avec K_M de génération 1 ;
- $K_P[2]$: sa clé de couplage de génération 2, chiffrée avec K_M de génération 2 ;
- $K_P[3]$: sa clé de couplage de génération 3, chiffrée avec K_M de génération 3 ;
- La carte d'atelier ait été émise pendant la première année de validité du certificat ERCA (3). Elle contiendra donc les générations 2 et 3 de la clé $K_{M\text{-}CAT}$;
- L'UEV soit de génération 2 et contienne $K_{M\text{-}UEV}$ de génération 2. Dans ce cas, voici le déroulement des étapes 2 à 5 :
- Étape 2 : l'UEV lit les $K_{M\text{-}CAT}$ de génération 2 et de génération 3 de la carte d'atelier et inspecte leurs numéros de version ;
- Étape 3 : l'UEV associe la $K_{M\text{-}CAT}$ de génération 2 avec sa $K_{M\text{-}UEV}$ afin de calculer les clés K_M et K_{ID} ;
- Étape 4 : l'UEV chiffre le numéro de série qu'elle reçoit du capteur de mouvement à l'aide de K_{ID} ;
- Étape 5 : le capteur de mouvement compare les données reçues avec $N_s[1]$ sans trouver de correspondance. Il compare ensuite les données avec $N_s[2]$ et trouve une correspondance. Il conclut que l'UEV est de génération 2 et renvoie donc $K_P[2]$.

[13] Remarque : les clés de couplage de génération 1, 2 et 3 peuvent être identiques ou il peut s'agir de trois clés distinctes de longueur différente, comme expliqué au point ~~TCS_259~~ **CSM_117**.

12.3 Couplage et communication entre l'UEV et le capteur de mouvement à l'aide de l'algorithme AES

CSM_218 Comme indiqué dans le ~~tableau 45~~ **tableau 3** de la section **9.2.1**, toutes les clés intervenant dans le couplage d'une UEV et d'un capteur de mouvement de deuxième génération et dans leur communication ultérieure doivent être des clés AES, plutôt que des clés TDES à double longueur tel que prévu dans la norme [ISO 16844-3]. La longueur de ces clés AES peut être de 128, 192 ou 256 bits. La taille des blocs AES étant de 16 octets, la longueur d'un message chiffré doit être un multiple de 16 octets, au lieu de 8 octets pour les clés TDES. Par ailleurs, certains de ces messages seront utilisés pour transporter des clés AES, dont la longueur peut être de 128, 192 ou 256 bits. Par conséquent, le nombre d'octets de données par instruction indiqué dans le tableau 5 de la norme [ISO 16844-3] doit être modifié selon le **tableau 6** ~~48~~.

Tableau 6
Nombre d'octets de données chiffrées et en clair par instruction tel que prévu dans la norme [ISO 16844-3]

Instruction	*Demande/ Réponse*	*Description des données*	*Nombre d'octets de données en clair Selon [ISO 16844-3]*	*Nombre d'octets de données en clair chiffrée avec des clés AES*	*Nombre d'octets de données chiffrées avec des clés AES d'une longueur de*		
					128 bits	**192 bits**	**256 bits**
10	Demande	Données d'authentification + numéro de fichier	8	8	16	16	16
11	Réponse	Données d'authentification + contenu de fichier	16 ou 32 bits selon le fichier	16 ou 32 bits selon le fichier	~~16~~ 32/**48**	~~16~~ 32/**48**	~~16~~ 32/**48**
41	Demande	Numéro de série du capteur de mouvement	8	8	16	16	16
41	Réponse	Clé de couplage	16	16/ 24 / 32	16	32	32
42	Demande	Clé de session	16	16 / 24 / 32	16	32	32
43	Demande	Informations de couplage	24	24	32	32	32
50	Réponse	Informations de couplage	24	24	32	32	32
70	Demande	Données d'authentification	8	8	16	16	16
80	Réponse	Valeur du compteur du capteur de mouvement + données d'authentification	8	8	16	16	16

CSM_219 Les informations relatives au couplage envoyées dans les instructions 43 (demande de l'UEV) et 50 (réponse du capteur de mouvement) sont assemblées comme prévu dans la section 7.6.10 de la norme [ISO 16844-3], à l'exception de l'utilisation de l'algorithme AES au lieu de l'algorithme TDES dans la procédure de chiffrement des données de couplage. Cela donne lieu à deux chiffrements AES et au recours au remplissage spécifié au point ~~TCS_362~~**CSM_220** pour

correspondre à la taille des blocs AES. La clé K'_p servant à ce chiffrement est générée comme suit :

- Dans le cas où la clé de couplage K_P a une longueur de 16 octets : $K'_p = K_P$ XOR $(N_s||N_s)$;
- Dans le cas où la clé de couplage K_P a une longueur de 24 octets : $K'_p = K_P$ XOR $(N_s||N_s||N_s)$;
- Dans le cas où la clé de couplage K_P a une longueur de 32 octets : $K'_p = K_P$ XOR $(N_s||N_s||N_s||N_s)$;

Où N_s correspond au numéro de série sur 8 octets du capteur de mouvement.

CSM_220 Si la longueur des données en clair (utilisant les clés AES) n'est pas un multiple de 16 octets, la méthode de remplissage nº 2 définie dans la norme [ISO 9797-1] doit être utilisée.

Remarque : conformément à la norme [ISO 16844-3], le nombre d'octets de données en clair doit être un multiple de 8, de sorte que le remplissage n'est pas nécessaire lorsque des clés TDES sont utilisées. Le présent **sous-**appendice ne modifie pas la définition des données et des messages figurant dans la norme [ISO 16844-3]. Il reste donc nécessaire de procéder au remplissage.

CSM_221 Concernant l'instruction 11 et lorsque plusieurs blocs de données doivent être chiffrés, il convient d'utiliser le mode de chiffrement par chaînage de blocs, tel que défini dans la norme [ISO 10116], avec un paramètre d'entrelacement *m* = 1. L'IV à utiliser est :

- Pour l'instruction 11 : le bloc d'authentification sur 8 octets spécifié à la section 7.6.3.3 de la norme [ISO 16844-3], complété selon la méthode de remplissage nº 2 définie dans la norme [ISO 9797-1] (voir également les sections 7.6.5 et 7.6.6 de la norme [ISO 16844-3]) ;
- Pour toutes les autres instructions dans lesquelles plus de 16 octets sont transférés, comme spécifié dans le **tableau 6** ~~48~~ : '00' {16}, soit 16 octets de valeur binaire 0.

Remarque : comme indiqué aux sections 7.6.5 et 7.6.6 de la norme [ISO 16844-3], lorsque le capteur de mouvement chiffre des fichiers de données pour insertion dans l'instruction 11, le bloc d'authentification est à la fois :

- Utilisé comme vecteur d'initialisation pour le chiffrement en mode CBC des fichiers de données ;
- Chiffré et inclus comme premier bloc dans les données envoyées à l'UEV.

12.4 Couplage de l'UEV et du capteur de mouvement pour des équipements de générations différentes

CSM_222 Comme expliqué à la section **9.2.1**, un **deuxième** ~~capteur de mouvement de deuxième génération peut prendre en charge le~~ chiffrement ~~TDES~~ des données de couplage (comme défini dans la partie A du présent **sous-**appendice)~~, ce qui~~ permet de coupler le capteur de mouvement avec une UEV de première génération. Si tel est le cas, ~~une UEV de première génération et un capteur de mouvement de deuxième génération sont couplés~~ **le couplage s'effectue conformément aux descriptions figurant** ~~comme décrit~~ dans la partie A du présent **sous-**appendice et dans la norme [ISO 16844-3]. Concernant la procédure de couplage, on peut utiliser indifféremment une carte d'atelier de première ou de deuxième génération.

Remarques :

- Il n'est pas possible de coupler une UEV de deuxième génération avec un capteur de mouvement de première génération ;

- Il n'est pas possible d'utiliser une carte d'atelier de première génération pour coupler une UEV de deuxième génération avec capteur de mouvement.

13. Sécurité des communications à distance par DSRC

13.1 Généralités

Comme prévu ~~à l'appendice~~ **au sous-appendice** 14, une UEV génère régulièrement des données du contrôle à distance des tachygraphes (RTM) qu'elle envoie au dispositif (interne ou externe) de communication à distance. Le dispositif de communication à distance est responsable de l'envoi de ces données vers l'interrogateur distant via l'interface DSRC décrite ~~à l'appendice~~ **au sous-appendice** 14. ~~L'appendice~~ **Le sous-appendice** 1 spécifie que les données RTM résultent de la concaténation des :

Données utiles chiffrées du tachygraphe	le chiffrement en clair des données utiles du tachygraphe
Données de sécurité DSRC	décrites ci-dessous

Les **sous-**appendices 1 et 14 spécifient la structure des données utiles en clair du tachygraphe. La présente section décrit la structure des données de sécurité DSRC ; les spécifications formelles figurent dans ~~l'appendice~~ **le sous-appendice** 1.

CSM_223 Les données en clair de type TachographPayload communiquées par une UEV à un dispositif de communication à distance (si le dispositif de communication à distance est externe à l'UEV) ou par une UEV à l'interrogateur distant au moyen de l'interface DSRC (si le dispositif de communication à distance est interne à l'UEV) sont protégées en mode chiffrement puis authentification. Cela signifie que les données utiles du tachygraphe sont d'abord chiffrées pour protéger la confidentialité du message, puis qu'un MAC est calculé pour garantir l'authenticité et l'intégrité des données.

CSM_224 Les données de sécurité DSRC correspondent à une concaténation des éléments de données suivants dans l'ordre indiqué (voir **fig. 12**) :

Date et heure actuelles	la date et l'heure actuelles de l'UEV (type de données TimeReal)
Compteur	un compteur sur trois octets (voir TCS_CSM_)
Numéro de série de l'UEV	le numéro de série de l'UEV ou l'ID de la demande de certificat (type de données **VuSerialNumber ou CertificateRequestID) (voir CSM_123)**
Numéro de version de la clé maîtresse DSRC	le numéro de version sur un octet de la clé maîtresse DSRC de laquelle découlent les clés DSRC propres à l'UEV (voir sect. 9.2.2).
MAC	le MAC calculé en fonction de tous les octets précédents dans les données RTM.

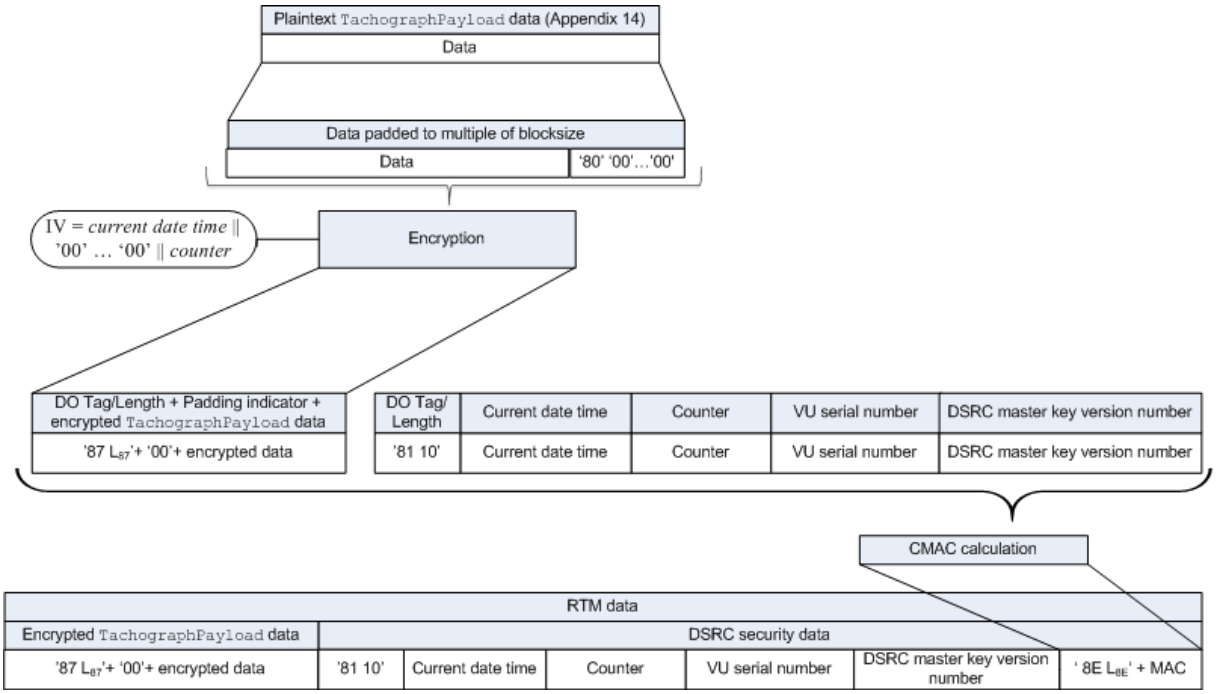
CSM_225 Le compteur sur trois octets inclus dans les données de sécurité DSRC respecte la structure MSB-first (octet le plus significatif en premier). La première fois qu'une UEV calcule un jeu de données RTM après sa mise en service, elle attribue la valeur zéro au compteur. L'UEV incrémente le compteur d'une unité avant chaque calcul d'un nouveau de jeu de données RTM.

13.2 Chiffrement des données utiles du tachygraphe et génération du MAC

CSM_226 Étant donné un élément de données en clair de type TachographPayload tel que décrit ~~à l'appendice~~ **au sous-appendice** 14, l'UEV chiffre ces données comme illustré dans la figure 12 : la clé DSRC de l'UEV destinée au codage $K\_UEV_{DSRC}\_ENC$ (voir sect. ~~9.2.3~~ **9.2.2**) est utilisée avec l'algorithme AES en mode opératoire de chiffrement par chaînage de blocs (CBC), tel que défini dans la norme [ISO 10116], avec un paramètre d'entrelacement m = 1. Le vecteur d'initialisation doit être égal à *IV = date et heure actuelles* || *'00 00 00 00 00 00 00 00'* || *compteur*, les valeurs des *date et heure actuelles* ainsi que du *compteur* étant indiquée au point ~~TCS_366~~ **CSM_224**. Les données à chiffrer sont complétées selon la méthode n° 2 définie dans la norme [ISO 9797-1].

CSM_227 L'UEV calcule le MAC correspondant aux données de sécurité DSRC comme illustré dans la figure 12 : le MAC est calculé sur tous les octets précédents des données RTM, jusqu'au numéro de version de la clé maîtresse DSRC incluse, y compris les balises et les longueurs des objets de données. L'UEV utilise sa clé d'authentification DSRC $K\_VU_{DSRC}\_MAC$ (voir sect. ~~9.2.3~~ **9.2.2**) avec l'algorithme AES en mode CMAC comme spécifié dans le document [SP 800-38B]. La longueur du MAC est liée à la longueur des clés DSRC propres à l'UEV, comme spécifié au point ~~RCS_192~~ **CSM_50**.

Figure 12
Chiffrement des données utiles du tachygraphe et génération du MAC



13.3 Vérification et déchiffrement des données utiles du tachygraphe

CSM_228 Lorsqu'un interrogateur distant reçoit les données RTM d'une UEV, il envoie la totalité de ces données RTM à une carte de contrôleur dans la zone de données d'une commande PROCESS DSRC MESSAGE, conformément ~~à l'appendice~~ **au sous-appendice** 2. Puis :

1. La carte de contrôleur inspecte le numéro de version de la clé maîtresse DSRC incluse dans les données de sécurité DSRC. Si la carte de contrôleur ne connaît pas la clé

maîtresse DSRC indiquée, elle envoie un des messages d'erreur prévus ~~à l'appendice~~ **au sous-appendice** 2 et interrompt la procédure ;

2. La carte de contrôleur utilise la clé maîtresse DSRC indiquée en combinaison avec le numéro de série de l'UEV ou l'ID de la demande de certificat figurant dans les données de sécurité DSRC pour calculer les clés DSRC propres à l'UEV K_UEV_{DSRC}_ENC et K_UEV_{DSRC}_MAC, comme précisé au point ~~TCS_266~~ **CSM_124** ;

3. La carte de contrôleur utilise la K_UEV_{DSRC}_MAC pour vérifier le MAC dans les données de sécurité DSRC, comme spécifié au point ~~TCS_369~~ **CSM_227**. Si le MAC est erroné, la carte de contrôleur envoie un des messages d'erreur prévus ~~à l'appendice 2~~ **au sous-appendice 2** et interrompt la procédure ;

4. La carte de contrôleur utilise la K_UEV_{DSRC}_ENC pour déchiffrer les données utiles chiffrées du tachygraphe, comme spécifié au point ~~TCS_368~~ **CSM_226**. La carte de contrôleur supprime le remplissage et envoie les données utiles du tachygraphe déchiffrées à l'interrogateur distant.

CSM_229 Afin d'éviter les attaques par réinsertion, l'interrogateur distant vérifie la récence des données RTM en contrôlant que *la date et l'heure actuelles* incluses dans les données de sécurité DSRC ne diffèrent pas trop de ses propres date et heure actuelles.

Remarques :

- L'interrogateur distant doit pour ce faire disposer d'une source horaire précise et fiable ;
- ~~L'appendice~~ **Le sous-appendice** 14 exigeant qu'une UEV calcule un nouveau jeu de données RTM toutes les 60 secondes et que l'horloge de l'UEV ait une marge d'erreur autorisée d'une minute par rapport à l'heure exacte, la limite inférieure de récence des données RTM est fixée à deux minutes. La récence effective dépend également du degré de précision de l'horloge de l'interrogateur distant.

CSM_230 Lorsqu'un atelier vérifie le bon fonctionnement de la fonction DSRC d'une UEV, il envoie la totalité des données RTM reçues de l'UEV à une carte d'atelier dans la zone de données d'une commande PROCESS DSRC MESSAGE, conformément ~~à l'appendice~~ **au sous-appendice** 2. La carte d'atelier effectue tous les contrôles et toutes les actions spécifiées au point ~~TCS_370~~ **CSM_228**.

14. Signature des téléchargements de données et contrôle des signatures

14.1 Généralités

CSM_231 L'équipement spécialisé intelligent (ESI) enregistre les données reçues d'une UEV ou d'une carte donnée pendant une session de téléchargement au sein d'un fichier de données physiques. Les données peuvent être stockées sur un support ~~de stockage externe~~. Ce fichier contient les signatures numériques associées aux blocs de données, comme spécifié ~~à l'appendice~~ **au sous-appendice** 7. Ce fichier contient également les certificats suivants (voir sect. **9.1**) :

- En cas de téléchargement à partir d'une UEV :
  - Le certificat UEV_Sign ;
  - Le certificat MSCA_UEV-DGE comprenant la clé publique à utiliser pour vérifier le certificat UEV_Sign.
- En cas de téléchargement à partir d'une carte :

- Le certificat Card_Sign ;
- Le certificat MSCA_Card comprenant la clé publique à utiliser pour vérifier le certificat Card_Sign.

CSM_232 L'ESI dispose également des éléments suivants :

- En cas d'utilisation d'une carte de contrôleur pour vérifier la signature, comme illustré dans la **figure 13** : le certificat de lien reliant le plus récent certificat EUR à celui dont la période de validité précède immédiatement la sienne, le cas échéant ;
- Dans le cas où il vérifie la signature : tous les certificats racines européens valides.

Remarque : la méthode qu'utilise l'ESI pour lire ces certificats n'est pas précisée dans le présent **sous-**appendice.

14.2 Génération de signatures

CSM_233 L'algorithme de signature permettant de créer des signatures numériques pour les données téléchargées est l'ECDSA conformément aux règles [DSS], combiné à l'algorithme de hachage associé à la taille de la clé de l'UEV ou de la carte, comme indiqué au point ~~TCS_192~~ **CSM_50**. La structure de la signature doit être en clair, comme spécifié dans le document [TR-03111].

14.3 Vérification de signatures

CSM_234 Un ESI peut procéder lui-même à la vérification d'une signature se rapportant à des données téléchargées ou utiliser une carte de contrôleur à cette fin. S'il utilise une carte de contrôleur, la vérification de la signature doit se dérouler selon la procédure indiquée à la **figure 13**. **Pour vérifier la validité temporelle d'un certificat présenté par un IDE, la carte de contrôleur utilise son heure actuelle interne, comme spécifié au point CSM_167. La carte de contrôleur doit mettre à jour son heure si la date d'entrée en vigueur d'un certificat authentique considéré comme une « source temporelle valable » est plus récente que l'heure courante de la carte. Seuls les certificats suivants sont acceptés comme des sources temporelles valables par la carte :**

- **Certificats de lien ERCA de deuxième génération ;**
- **Certificats MSCA de deuxième génération ;**
- **Certificats UEV_Sign ou Card_Sign de deuxième génération émis par le même pays que le certificat de carte de la carte de contrôleur**.

S'il procède lui-même à la vérification de la signature, l'ESI doit vérifier l'authenticité et la validité de tous les certificats de la chaîne de certificats contenus dans le fichier de données ainsi que la signature se rapportant à ces données conformément à la procédure relative aux signatures définie par les règles [DSS]. **Dans les deux cas, pour tout certificat extrait d'un fichier de données, il sera nécessaire de vérifier que le champ ADC (autorisation du détenteur de certificat) est rempli correctement, c'est-à-dire que :**

- **Le champ ADC du certificat EQT indique un certificat d'UEV ou de carte (selon le cas) à signer (voir sous-appendice 1, type de données EquipmentType) ;**
- **Le champ ADC du certificat EQT.AC indique une MSCA ;**
- **Le champ ADC du certificat EQT.Link indique l'ERCA.**

Remarques concernant la **figure 13** :

- L'équipement qui a signé les données à analyser est désigné par l'abréviation EQT.

- Les certificats et les clés publiques EQT mentionnées sur la figure sont destinés à la signature, c'est-à-dire UEV_Sign ou Card_Sign ;
- Les certificats et les clés publiques EQT.AC mentionnés dans la figure sont ceux destinés à la signature des certificats d'UEV ou de carte, selon le cas ;
- Le certificat EQT.AC.EUR mentionné dans la figure est le certificat racine européen indiqué dans la RAC du certificat EQT.AC ;
- Le certificat EQT.Link mentionné dans la figure est le certificat de lien de l'EQT, le cas échéant. Comme précisé à la section **9.1.2**, il s'agit d'un certificat de lien pour une nouvelle paire de clés racine ~~européenne~~ créé par l'ERCA et signé par la précédente clé privée **racine** ~~européenne~~ ;
- Le certificat EQT.Link.EUR désigne le certificat racine européen indiqué dans la RAC du certificat EQT.Link.

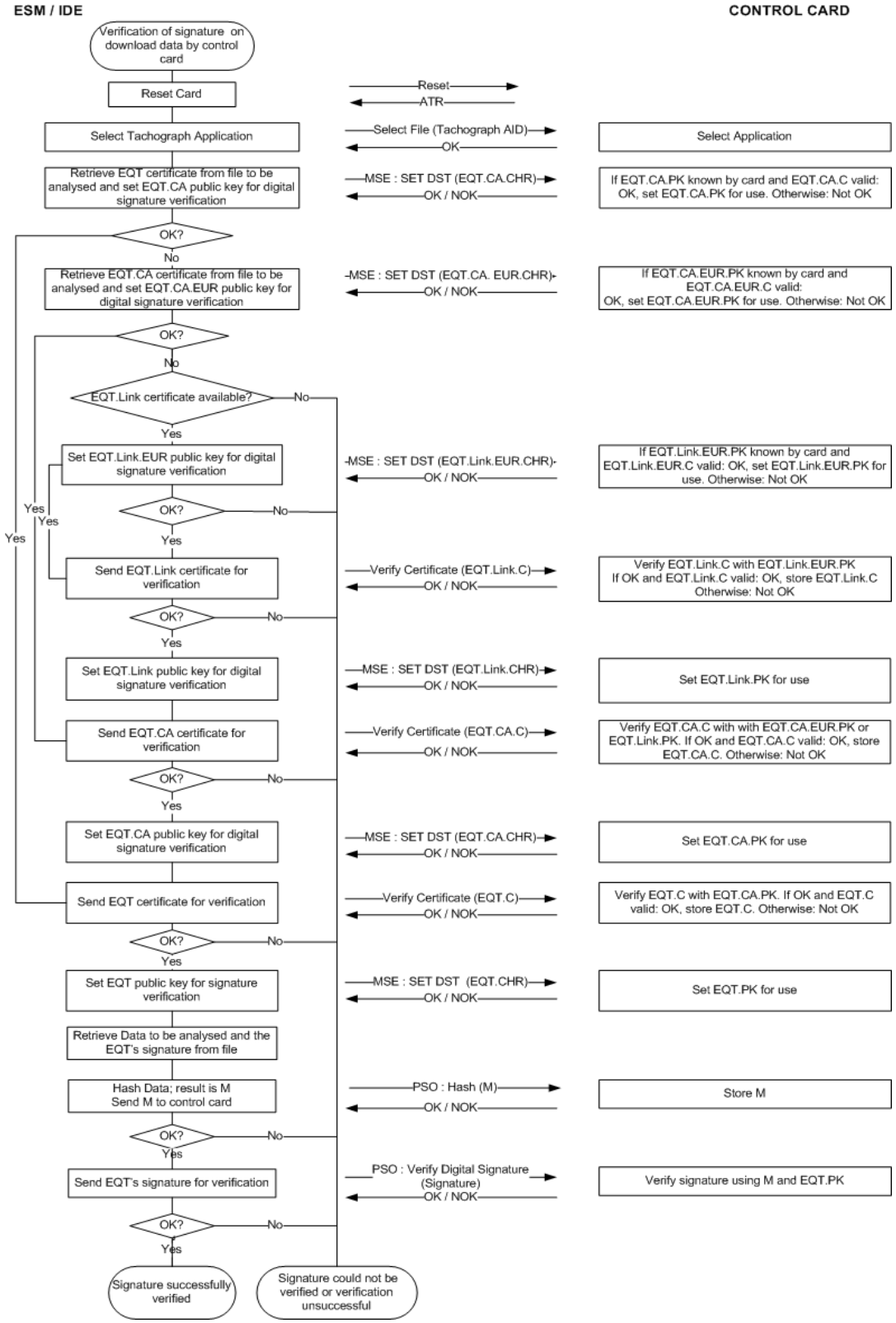
CSM_235 Pour calculer le M de hachage envoyé à la carte de contrôleur dans la commande PSO:HASH, l'ESI utilise l'algorithme de hachage associé à la taille de la clé de l'UEV ou de la carte à partir de laquelle les données sont téléchargées, comme spécifié au point ~~TCS_192~~ **CSM_50**.

CSM_236 Pour vérifier la signature EQT, la carte de contrôleur suit la procédure relative aux signatures définies par les règles [DSS].

Remarque : le présent document ne spécifie aucune action à entreprendre dans le cas où il est impossible de vérifier une signature associée à un fichier de données téléchargé ou si cette vérification échoue.

Figure 13

Protocole de vérification de la signature associée à un fichier de données téléchargé



Sous-appendice 12

Positionnement basé sur le système mondial de navigation par satellite (GNSS)

Table des matières

1. Introduction

Le présent **sous-**appendice présente les exigences techniques applicables au récepteur GNSS et aux données GNSS qu'utilise l'unité embarquée sur le véhicule, y compris les protocoles à appliquer pour garantir la sécurité et l'exactitude du transfert de données relatives au positionnement.

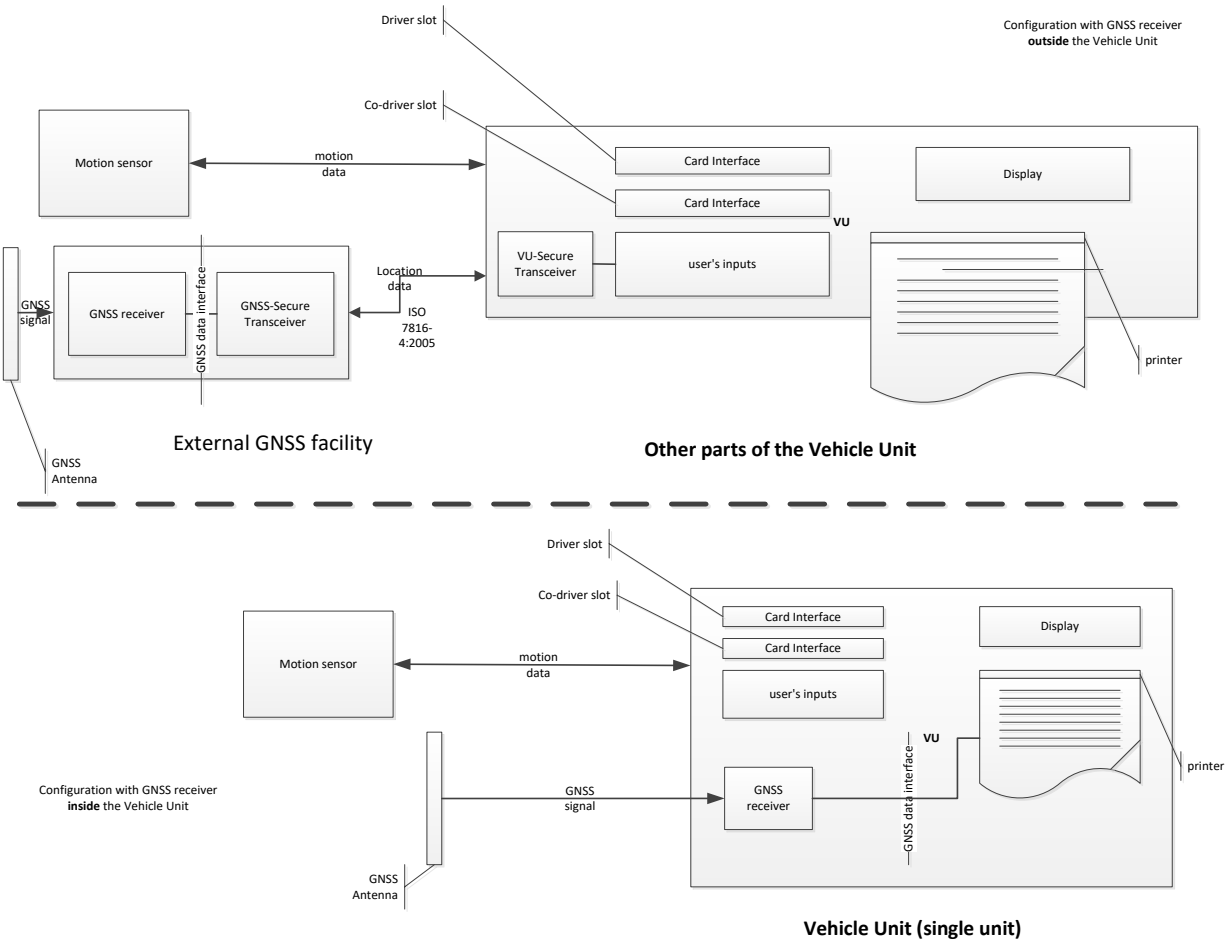
~~Les principaux articles du règlement (UE) n° 165/2014 dont découlent les présentes exigences sont les suivants : « Article 8 Enregistrement de la position du véhicule à certains points de la période de travail journalière», «Article 10 Interface avec les systèmes de transport intelligents» et «Article 11 Dispositions détaillées relatives au tachygraphe intelligent ».~~

1.1 Champ d'application

GNS_1 L'unité embarquée sur le véhicule recueille des données de localisation à partir d'au moins un **réseau satellite** GNSS ~~afin de prendre en charge l'application de l'article 8~~.

L'unité embarquée sur le véhicule peut disposer ou non d'un dispositif GNSS externe, comme illustré à la figure 1.

Figure 1
Différentes configurations du récepteur GNSS



1.1.1 Références

Dans cette partie du présent sous-appendice, il est fait référence au document suivant :

NMEA **Norme d'interface NMEA (« National Marine Electronics Association ») 0183 Interface Standard, V4.11.**

1.2 Abréviations et notations

Dans le présent **sous-**appendice, les abréviations suivantes sont utilisées :

DOP	Coefficient d'affaiblissement de la précision (*Dilution of Precision*)
DGE	Dispositif GNSS externe *(EGF, en anglais)*
EGNOS	Système européen de navigation par recouvrement géostationnaire
GNSS	Système mondial de navigation par satellite (*Global Navigation Satellite System*)
GSA	Coefficient d'affaiblissement de la précision du GPS et satellites actifs
HDOP	Coefficient d'affaiblissement de la précision du positionnement horizontal
NMEA	National Marine Electronics Association
PDOP	Coefficient d'affaiblissement de la précision du positionnement
RMC	Minimum spécifique recommandé (*Recommended Minimum Specific*)
VDOP	Coefficient d'affaiblissement de la précision du positionnement vertical
UEV	Unité embarquée sur le véhicule *(VU, en anglais)*
OSNMA	**Service ouvert Galileo d'authentification des messages de navigation (*Galileo Open Service Navigation Message Authentication*)**
RTC	**Horloge en temps réel (*Real Time Clock*)**

2. ~~Spécifications~~ Caractéristiques de base du récepteur GNSS

~~Indépendamment de la configuration du tachygraphe intelligent, avec ou sans dispositif GNSS externe, la délivrance d'informations de positionnement précises et fiables constitue un critère fondamental du fonctionnement efficace du tachygraphe intelligent. Il convient donc d'exiger sa compatibilité avec les services fournis par le programme Galileo et le programme EGNOS (European Geostationary Navigation Overlay Service) tels qu'ils sont définis par le règlement (UE) n° 1285/2013 du Parlement Européen et du Conseil[14]. Le système établi en vertu du programme Galileo est un système mondial de radionavigation par satellite indépendant et celui établi en vertu du programme EGNOS est un système régional de radionavigation par satellite destiné à améliorer la qualité du signal du système de positionnement mondial (GPS).~~

GNS_2 Les fabricants veillent à ce que les récepteurs GNSS des tachygraphes intelligents soient compatibles avec les services de positionnement fournis par les systèmes **GPS, GLONASS et** Galileo ~~et EGNOS~~. Les fabricants ont la possibilité de garantir, en plus, la compatibilité avec d'autres systèmes de navigation par satellite.

GNS_3 Le récepteur GNSS doit être capable de prendre en charge l'authentification **des messages de navigation** sur le service ouvert Galileo **(OSNMA)** ~~lorsque ledit service est fourni par le système Galileo et pris en charge par les fabricants de récepteurs GNSS. Cependant, en ce qui concerne les tachygraphes intelligents introduits sur le marché avant que les conditions précitées ne deviennent effectives et qui ne prennent pas en charge le service ouvert d'authentification de Galileo, aucune mise à niveau ne sera requise.~~

GNS_3a Le récepteur GNSS doit effectuer un certain nombre de contrôles de cohérence afin de vérifier que les mesures calculées par le récepteur GNSS sur la base

~~[14] Règlement (UE) n° 1285/2013 du Parlement européen et du Conseil du 11 décembre 2013 relatif à la mise en place et à l'exploitation des systèmes européens de radionavigation par satellite et abrogeant le règlement (CE) du Conseil n° 876/2002 et le règlement (CE) n° 683/2008 du Parlement européen et du Conseil (OJ L 347, 20.12.2013, p. 1).~~

des données OSNMA ont permis d'obtenir des informations correctes sur la position, la vitesse et les données du véhicule et n'ont donc pas été influencées par une attaque externe telle que des opérations de transplexion. Ces contrôles de cohérence consistent, par exemple, en :

- **La détection des émissions de puissance anormales au moyen de la surveillance combinée du système de contrôle automatique de gain (AGC) et du rapport porteuse/densité de bruit (C/N0) ;**
- **La vérification de la cohérence des mesures de la pseudo-distance et des mesures Doppler dans le temps, y compris la détection de variations brusques des mesures ;**
- **Des techniques de surveillance autonome de l'intégrité par récepteur (RAIM), y compris la détection de mesures que ne cadrent pas avec la position estimée ;**
- **Des contrôles de position et de vitesse, y compris les solutions en cas de positions et de vitesses anormales, les variations brusques et les comportements qui ne cadrent pas avec la dynamique du véhicule ;**
- **Des contrôles de la cohérence entre les valeurs de temps et de fréquence, y compris les variations brusques de temps et les dérivations qui ne cadrent pas avec les caractéristiques de l'horloge du récepteur.**

GNS_3b La Commission européenne doit élaborer et approuver les documents suivants :

- **Un document de contrôle des signaux dans les interfaces spatiales (SIS ICD pour « Signal in Space Interface Control Document ») décrivant en détail les informations OSNMA transmises dans le signal Galileo ;**
- **Des lignes directrices OSNMA relatives aux récepteurs, qui définissent les exigences et les procédures applicables aux récepteurs afin de garantir une mise en œuvre sûre du service OSNMA, ainsi que des recommandations visant à améliorer les performances du service OSNMA.**

Les récepteurs GNSS, internes comme externes, installés dans les tachygraphes sont construits conformément au SIS ICD et aux lignes directrices OSNMA relatives aux récepteurs.

GNS_3c Le récepteur GNSS fournit des messages de position, appelés messages de position authentifiée, qui sont élaborés exclusivement à l'aide de messages de navigation satellites dont l'authenticité a été vérifiée avec succès.

GNS_3d Le récepteur GNSS fournit également des messages de position standard, élaborés à l'aide des satellites en vue, que ceux-ci soient authentifiés ou non.

GNS_3e Le récepteur GNSS utilise l'horloge en temps réel (RTC) de l'UEV comme référence temporelle pour la synchronisation du temps nécessaire au service OSNMA.

GNS_3f L'heure de la RTC de l'UEV est fournie au récepteur GNSS par l'UEV.

GNS_3g La dérive temporelle maximale spécifiée à l'exigence 41 de l'appendice 1C est fournie au récepteur GNSS par l'UEV, avec l'heure de la RTC de l'UEV.

~~**Les récepteurs GNSS peuvent également être capables de recevoir et de traiter les signaux SBAS.**~~

3. Phrases ~~NMEA~~ fournies par le récepteur GNSS

Le présent chapitre décrit les phrases ~~NMEA~~ utilisées pendant le fonctionnement du tachygraphe intelligent **pour transmettre des messages de position standard et authentifiée**. Cette section est applicable à la configuration du tachygraphe intelligent avec et sans dispositif GNSS externe.

GNS_4 Les données de ~~localisation~~ **positionnement standard** reposent sur les données GNSS transmises dans la phrase NMEA de type minimum spécifique recommandé (RMC), à savoir les informations de positionnement (latitude et longitude), l'heure au format UTC (~~hhmmss~~hh**mmss.ss** ~~**Partie contractante.**~~ss) et la vitesse sur le fond en nœuds plus d'autres valeurs complémentaires.

La structure de la phrase RMC est la suivante (d'après la norme NMEA V4.1) :

Figure 2
Structure de la phrase RMC

$--RMC,hhmmss.ss,A,llll.ll,a,yyyyy.yy,a,x.x,x.x,xxxx,x.x,a* hh
1) Time (UTC)
2) Status, A = Valid position, V = Warning
3) Latitude
4) N or S
5) Longitude
6) E or W
7) Speed over ground in knots
8) Track made good, degrees true
9) Date, ddmmyy
10) Magnetic Variation, degrees
11) E or W
12) Checksum

L'état indique la disponibilité du signal GNSS. Tant que la valeur de l'état n'est pas fixée à « A », les données reçues (par exemple l'heure, la latitude ou la longitude) ne peuvent pas servir à enregistrer la position du véhicule dans l'UEV.

La résolution de la position repose sur la structure de la phrase RMC décrite ci-dessus. La première partie des champs 3) et 5) ~~(les deux premiers chiffres)~~ correspondent aux degrés. Le reste correspond aux minutes avec trois décimales. La résolution est donc de 1/1 000 minute ou 1/60 000 degré (parce qu'une minute correspond à 1/60 degré).

GNS_4a Les données de positionnement authentifiées reposent sur une phrase de type NMEA, les données spécifiques minimales authentifiées (AMC), qui contiennent les informations de positionnement (latitude et longitude), l'heure au format UTC (hhmmss.ss) et la vitesse sur le fond en nœuds plus d'autres valeurs complémentaires.

La structure de la phrase AMC est la suivante (d'après la norme NMEA V4.11, sauf pour la valeur n° 2) :

Figure 3
Structure de la phrase AMC

$--AMC,hhmmss.ss,A,llll.ll,a,yyyyy.yy,a,x.x,x.x,xxxx,x.x,a*hh

1) Heure (UTC) ;

2) État : A = position authentifiée (établie au moyen de messages de navigation provenant d'au moins 4 satellites dont l'authenticité a été vérifiée avec succès), J = brouillage ou O = autre attaque GNSS en l'absence d'échec de l'authentification des messages de navigation (par des contrôles de cohérence mis en œuvre conformément à l'exigence GNS_3a), F = échec de l'authentification des messages de navigation (détecté par les vérifications OSNMA spécifiées dans les documents visés à l'exigence GNS_3b), V = sans objet (la position authentifiée n'est pas disponible pour tout autre motif) ;

3) Latitude ;

4) N ou S ;

5) Longitude ;

6) E ou O ;

7) Vitesse sur le fond en nœuds ;

8) Route suivie (TMG) en degrés vrais ;

9) Date (jjmmaa) ;

10) Déclinaison magnétique en degrés ;

11) E ou O ;

12) Total de contrôle ;

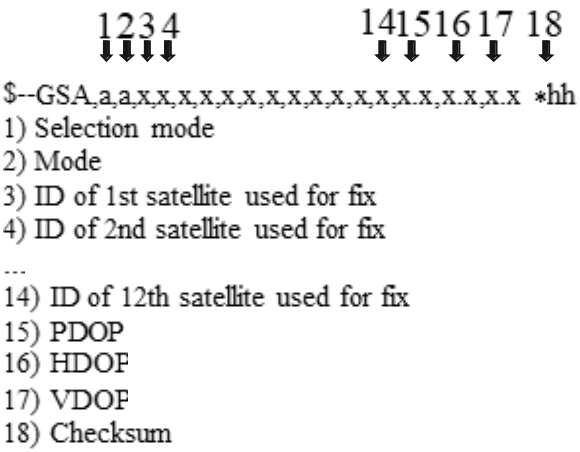
L'état indique si une position GNSS authentifiée est disponible, si une attaque contre les signaux GNSS a été détectée, si l'authentification des messages de navigation a échoué ou si la position GNSS est indisponible. Tant que la valeur de l'état n'est pas fixée à « A », les données reçues (par exemple l'heure, la latitude ou la longitude) sont considérées comme non valides et ne peuvent pas servir à enregistrer la position du véhicule dans l'UEV. Lorsque la valeur de l'état est fixée à « J » (brouillage), « O » (autre attaque GNSS) ou « F » (échec de l'authentification des messages de navigation), un événement du type « anomalie GNSS » est enregistré dans l'UEV, comme défini à l'appendice 1C et au sous-appendice 1 (EventFaultCode).

GNS_5 L'unité embarquée sur le véhicule enregistre dans sa base de données les informations relatives au positionnement en termes de latitude et de longitude selon une résolution d'1/10 minute ou 1/600 degré, comme décrit ~~à l'appendice~~ **au sous-appendice** 1 pour les coordonnées géographiques (type de données GeoCoordinates).

L'UEV peut utiliser la commande GPS DOP et satellites actifs (GSA), conformément à la norme NMEA V4.11, pour déterminer et enregistrer la disponibilité du signal et l'exactitude des positions standard. En particulier, le HDOP donne une indication sur le degré de précision des données de localisation enregistrées (voir 4.2.2). L'UEV enregistre la valeur du coefficient d'affaiblissement de la précision de positionnement horizontal (HDOP) calculée comme étant la minimale des valeurs HDOP recueillies sur les systèmes GNSS disponibles.

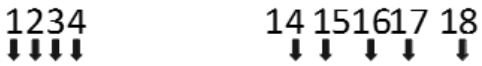
L'identificateur du système GNSS indique ~~GPS, Glonass, Galileo, Beidou ou~~ **l'identificateur NMEA correspondant pour chaque constellation GNSS et** pour le système de renforcement satellitaire (SBAS).

Figure **4**~~3~~
Structure de la phrase GSA (positionnements standard)



De même, l'UEV peut utiliser la phrase satellites actifs authentifiés (ASA) de type NMEA pour déterminer et enregistrer la disponibilité du signal et l'exactitude des positionnements authentifiés. Les valeurs 1 à 18 sont définies dans la norme NMEA V4.11.

Figure 5
Structure de la phrase ASA (positionnements authentifiés)



$--ASA,a,a,x,x,x,x,x,x,x,x,x,x,x,x,x,x.x,x.x,x.x*hh

1) Mode de sélection (A = sélection automatique, M = inutilisé) ;

2) Mode ;

3) ID du 1er satellite utilisé comme point de repère ;

4) ID du 2e satellite utilisé comme point de repère ;

…

14) ID du 12e satellite utilisé comme point de repère ;

15) PDOP ;

16) HDOP ;

17) VDOP ;

18) Total de contrôle ;

~~Ici, le Mode (2) indique que certains points de repère (fix) sont indisponibles (Mode = 1) ou qu'ils sont disponibles en 2D (Mode = 2) ou en 3D (Mode = 3).~~

GNS_6 **Lorsqu'un dispositif GNSS externe est utilisé, ~~L~~l**a phrase GSA doit être stockée **dans l'émetteur-récepteur GNSS sécurisé** avec le**s** numéro**s** d'enregistrement '02' **à '06', et la phrase ASA est enregistrée avec les numéros d'enregistrement '12' à '16'.**

GNS_7 La taille maximale des phrases ~~NMEA~~ (par exemple RMC, **AMC,** GSA**, ASA** ou autres), qui peut servir à l'étalonnage de la commande READ RECORD, est de 85 octets (voir ~~tableau 49~~ **tableau 1**).

4. Unité embarquée sur le véhicule avec un dispositif GNSS externe

4.1 Configuration

4.1.1 Principaux composants et principales interfaces

Dans cette configuration, le récepteur GNSS fait partie du dispositif GNSS externe.

GNS_8 Le dispositif GNSS externe doit être alimenté par une interface de véhicule spécifique.

GNS_9 Le dispositif GNSS externe se compose des éléments suivants (voir fig. **6**~~4~~**4**~~17~~) :

a) Un récepteur GNSS commercial pour fournir les données de positionnement par l'intermédiaire de l'interface de données GNSS. Par exemple, l'interface de données GNSS peut être conforme à la norme NMEA V4.1**~~0~~1** selon laquelle le récepteur GNSS tient le rôle de l'émetteur et transmet les phrases NMEA à l'émetteur-récepteur GNSS sécurisé sur une fréquence de 1 Hz pour le jeu prédéfini de phrases NMEA, lequel doit comprendre au moins les phrases RMC**, AMC,** ~~et~~ GSA **et ASA**. Le choix de la mise en œuvre de l'interface de données GNSS revient aux fabricants du dispositif GNSS externe ;

b) Un dispositif émetteur-récepteur (émetteur-récepteur GNSS sécurisé) compatible avec la norme ISO/CEI 7816-4:2013 (voir ~~5.2.1~~**4.2.1**) qui permet la communication avec l'unité embarquée sur le véhicule et la prise en charge de l'interface de données GNSS faisant le lien avec le récepteur GNSS. Ce dispositif est doté d'une mémoire pour le stockage des données relatives à l'identification du récepteur GNSS et du dispositif GNSS externe ;

c) Un système clos doté d'une fonction de détection des fraudes qui englobe le récepteur GNSS et l'émetteur-récepteur GNSS sécurisé. La fonction de détection des fraudes met en application les mesures de protection de la sécurité définies dans le profil de protection du tachygraphe intelligent ;

d) Une antenne GNSS installée sur le véhicule et connectée au récepteur GNSS par l'intermédiaire du système clos.

GNS_10 Le dispositif GNSS externe dispose au minimum des interfaces externes suivantes :

a) L'interface avec l'antenne GNSS installée sur le véhicule, dans le cas où l'on utilise une antenne externe ;

b) L'interface avec l'unité embarquée sur le véhicule.

GNS_11 Dans l'UEV, l'émetteur-récepteur sécurisé de l'UEV est à l'autre extrémité de la communication sécurisée avec l'émetteur-récepteur GNSS sécurisé. Il doit être conforme à la norme ISO/CEI 7816-4:2013 relative à la connexion au dispositif GNSS externe.

GNS_12 Pour la couche physique de communication avec le dispositif GNSS externe, l'UEV doit respecter la norme ISO/CEI 7816-12:2005 ou toute autre norme compatible avec la norme ISO/CEI 7816-4:2013 (voir ~~5.2.1~~ **4.2.1**)

4.1.2 État du dispositif GNSS externe à la fin de la production

GNS_13 Le dispositif GNSS externe doit enregistrer les valeurs suivantes dans la mémoire non volatile de l'émetteur-récepteur GNSS sécurisé au moment où il quitte l'usine :

- La paire de clé DGE_MA et le certificat correspondant ;
- Le certificat MSCA_UEV-DGE comprenant la clé publique MSCA_UEV-DGE.PK à utiliser pour vérifier le certificat DGE_MA ;
- Le certificat EUR comprenant la clé publique EUR.PK à utiliser pour vérifier le certificat MSCA_UEV-DGE ;
- Le certificat EUR dont la durée de validité précède directement celle du certificat EUR à utiliser pour vérifier le certificat MSCA_UEV-DGE, le cas échéant ;
- Le certificat de lien reliant ces deux certificats EUR, le cas échéant ;
- Le numéro de série étendu du dispositif GNSS externe ;
- L'identificateur du système d'exploitation du dispositif GNSS ;
- Le numéro d'homologation du dispositif GNSS externe ;
- L'identificateur du composant de sécurité du dispositif GNSS externe.

4.2 Communication entre le dispositif GNSS externe et l'unité embarquée sur le véhicule

4.2.1 Protocole de communication

GNS_14 Le protocole de communication entre le dispositif GNSS externe et l'unité embarquée sur le véhicule remplit les fonctions suivantes :

1. La collecte et la distribution des données GNSS (par exemple la position, l'heure et la vitesse) ;

2. La collecte des données de configuration du dispositif GNSS externe ;

3. Le rôle de protocole de gestion à l'appui du couplage, de l'authentification mutuelle et de la concordance des clés de session entre le dispositif GNSS externe et l'UEV ;

4. La transmission au dispositif GNSS externe de l'heure de la RTC de l'UEV et de la différence maximale entre celle-ci et l'heure réelle.

GNS_15 Le protocole de communication repose sur la norme ISO/CEI 7816-4:2013 qui prévoit que l'émetteur-récepteur sécurisé de l'UEV tient le rôle du maître et l'émetteur-récepteur GNSS sécurisé le rôle de l'esclave. La connexion physique entre le dispositif GNSS externe et l'UEV est fondé sur la norme ISO/CEI 7816-12:2005 ou une autre norme compatible avec la norme ISO/CEI 7816-4:2013.

GNS_16 Le protocole de communication ne prend pas en charge les zones de longueur étendue.

GNS_17 Conformément à la norme ISO 7816 (parties 4:2013 et 12:2005), le protocole de communication entre le dispositif GNSS externe et l'UEV doit être défini à T = 1.

GNS_18 Concernant les fonctions **1)** de collecte et de distribution des données GNSS, 2) de collecte des données de configuration du dispositif GNSS externe et 3) de protocole de gestion, l'émetteur-récepteur GNSS sécurisé simule le fonctionnement d'une carte intelligente dont l'architecture de fichiers comprend un fichier maître (MF), un fichier spécialisé (DF) doté de l'identificateur d'application spécifié ~~à l'appendice~~ **au sous-appendice** 1, section 6.2 ('FF 44 54 45 47 4D'), trois fichiers élémentaires (EF) contenant des certificats et un fichier élémentaire unique (EF.EGF) dont l'identificateur de fichier correspond à '2F2F' comme indiqué dans le ~~tableau 49~~ **tableau 1**.

GNS_18a En ce qui concerne la fonction 4) de transmission au dispositif GNSS externe de l'heure de la RTC de l'UEV et de la différence maximale entre celle-ci et l'heure réelle, l'émetteur-récepteur GNSS sécurisé utilise un EF (EF VU) figurant dans le même DF et dont l'identificateur de fichier correspond à '2F30' comme indiqué dans le tableau 1.

GNS_19 L'émetteur-récepteur GNSS sécurisé doit enregistrer les données provenant du récepteur GNSS et les données de configuration dans le fichier EF.EGF. Il s'agit d'un fichier d'enregistrement d'une longueur variable et linéaire associé à un identificateur équivalant à '2F2F' au format hexadécimal.

GNS_19a L'émetteur-récepteur GNSS sécurisé doit enregistrer les données provenant de l'UEV dans le fichier EF VU. Il s'agit d'un fichier d'enregistrement d'une longueur fixe et linéaire associé à un identificateur équivalant à '2F30' au format hexadécimal.

GNS_20 L'émetteur-récepteur GNSS sécurisé utilise une mémoire pour stocker les données et pour pouvoir effectuer ~~au moins 20 millions~~ **autant de** cycles de lecture/écriture **que nécessaire pendant une durée de vie d'au moins 15 ans**. Hormis cet aspect, la conception interne et la mise en service de l'émetteur-récepteur GNSS sécurisé incombent aux fabricants.

Le ~~tableau 49~~ **tableau 1** dresse un inventaire des numéros d'enregistrement et des données.

Remarque : il existe ~~quatre~~ **cinq** phrases GSA correspondant aux ~~quatre systèmes de satellite~~ **constellations GNSS** et au système SBAS (*Satellite-Based Augmentation System*).

GNS_21 Le ~~tableau 49~~ **tableau 1** présente la structure de fichiers. Pour des informations concernant les règles d'accès TJR, JMS et MS-MAC, voir **sous-**appendice 2, section 3.5.

Tableau 1
Structure des fichiers

		Règles d'accès		
Fichier	ID de fichier	Lecture	Actualisation	Codage
MF	3F00			
EF.ICC	0002	TJR	JMS (par l'UEV)	Non
DF GNSS Facility	0501	TJR	JMS	Non
EF EGF_MACertificate	C100	TJR	JMS	Non
EF CA_Certificate	C108	TJR	JMS	Non
EF Link_Certificate	C109	TJR	JMS	Non
EF ~~.~~EGF	2F2F	MS-MAC	JMS (par l'UEV)	Non
EF VU	**2F30**	**MS-MAC**	**MS-MAC**	**Non**

Fichier/Élément de données	*N° d'enregistrement*	*Taille (en octets)*		*Valeurs par défaut*
		Min	**Max**	
MF		552	1031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF GNSS Facility		*612*	*1023*	
EF EGF_MACertificate		*204*	*341*	
EGFCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF ~~.~~EGF				
Phrase NMEA RMC	'01'	85	85	
1re phrase NMEA GSA	'02'	85	85	
2e phrase NMEA GSA	'03'	85	85	
3e phrase NMEA GSA	'04'	85	85	
4e phrase NMEA GSA	'05'	85	85	
5e phrase NMEA GSA	'06'	85	85	
Numéro de série étendu du dispositif GNSS externe défini ~~à l'appendice~~ **au sous-appendice** 1 comme SensorGNSSSerialNumber.	'07'	8	8	
Identificateur du système d'exploitation de l'émetteur-récepteur GNSS sécurisé défini ~~à l'appendice~~ **au sous-appendice** 1 comme SensorOSIdentifier.	'08'	2	2	
Numéro d'homologation du dispositif GNSS externe défini ~~à l'appendice~~ **au sous-appendice** 1 comme SensorExternalGNSSApprovalNumber.	'09'	16	16	

Fichier/Élément de données	*N° d'enregistrement*	*Taille (en octets)*		*Valeurs par défaut*
Identificateur du composant de sécurité du dispositif GNSS externe défini ~~à l'appendice~~ **au sous-appendice** 1 comme SensorExternalGNSSSCIdentifier	'10'	8	8	
Phrase AMC	**'11'**	**85**	**85**	
1re phrase ASA	**'12'**	**85**	**85**	
2e phrase ASA	**'13'**	**85**	**85**	
3e phrase ASA	**'14'**	**85**	**85**	
4e phrase ASA	**'15'**	**85**	**85**	
5e phrase ASA	**'16'**	**85**	**85**	
Réservé pour une utilisation future	De '17~~1~~' à 'FD'			
EF VU				
VuRtcTime (voir sous-appendice 1)	**'01'**	**4**	**4**	**{00..00}**
VuGnssMaximalTimeDifference (voir sous-appendice 1)	**'02'**	**2**	**2**	**{00..00}**

4.2.2 Transfert sécurisé de données GNSS

GNS_22 Le transfert sécurisé des données de positionnement GNSS**, de l'heure de la RTC de l'UEV et de la différence de temps maximale entre l'heure réelle et l'heure de la RTC** n'est autorisé que dans les conditions suivantes :

1. La procédure de couplage a abouti conformément aux dispositions ~~de l'appendice~~ **du sous-appendice** 11 (Mécanismes de sécurité communs) ;

2. Les procédures d'authentification mutuelle régulière et de concordance des clés de session entre l'UEV et le dispositif GNSS externe également décrites ~~à l'appendice~~ **au sous-appendice** 11 (Mécanismes de sécurité communs) ont été effectuées à la fréquence indiquée.

GNS_23 Toutes les T secondes, où T est une valeur inférieure ou égale à ~~1~~**2**0, sauf pendant le déroulement d'une procédure de couplage ou d'authentification mutuelle et de concordance de clés de session, l'UEV demande au dispositif GNSS externe les informations de positionnement selon la séquence suivante :

1. L'UEV demande au dispositif GNSS externe les données de localisation ainsi que les données relatives à l'affaiblissement de la précision (provenant de**s** ~~la~~ phrase**s** GSA **et ASA**~~NMEA~~). L'émetteur-récepteur sécurisé de l'UEV utilise les commandes SELECT et READ RECORD(S) définies dans la norme ISO/CEI 7816-4:2013 en mode authentification uniquement de la messagerie sécurisée, comme prévu ~~à l'appendice~~ **au sous-appendice** 11, section 11.5, avec l'identificateur de fichier '2F2F' et un numéro d'enregistrement égal à '01' pour la phrase NMEA RMC**, à** ~~et~~ '02','03','04','05' ou '06' pour la phrase NMEA GSA **, à '11' pour la phrase AMC et à '12','13','14','15' ou '16' pour la phrase ASA.**

2. Les dernières données de ~~localisation~~ **positionnement** reçues sont enregistrées dans l'EF correspondant à l'identificateur '2F2F' et les enregistrements décrits au ~~tableau 49~~ **tableau 1** dans l'émetteur-récepteur GNSS sécurisé car ce dernier reçoit les données NMEA du récepteur GNSS par l'intermédiaire de l'interface de données GNSS sur une fréquence d'au moins 1 Hz.

3. L'émetteur-récepteur GNSS sécurisé envoie la réponse à l'émetteur-récepteur sécurisé de l'UEV à l'aide d'une APDU de réponse en mode authentification uniquement de la messagerie sécurisée, comme prévu ~~à l'appendice~~ **au sous-appendice** 11, section 11.5.

4. L'émetteur-récepteur sécurisé de l'UEV contrôle l'authenticité et l'intégrité de la réponse reçue. En cas de résultat positif, les données de ~~localisation~~ **positionnement** sont transférées au processeur de l'UEV par l'intermédiaire de l'interface de données GNSS.

5. Le processeur de l'UEV vérifie les données reçues en extrayant les informations (par exemple la latitude, la longitude ou l'heure) de la phrase NMEA RMC. La phrase NMEA

RMC contient les informations si le positionnement **non authentifié** est valide. Si tel ~~n'est pas~~ **est** le cas, ~~les données de localisation ne sont pas encore mises à disposition et ne peuvent pas servir à enregistrer la position du véhicule. Si le positionnement est valide,~~ le processeur de l'UEV extrait également les valeurs HDOP des phrases NMEA GSA et calcule la valeur ~~moyenne~~ **minimale** d'après les systèmes satellites disponibles (c'est-à-dire lorsque les points de repère sont disponibles).

6. Le processeur de l'UEV **extrait également les informations (par exemple la latitude, la longitude ou l'heure) de la phrase AMC. La phrase AMC contient les informations si le positionnement authentifié n'est pas valide ou si le signal GNSS a été attaqué. Si le positionnement est valide, le processeur de l'UEV extrait également les valeurs HDOP des phrases ASA et calcule la valeur minimale d'après les systèmes de satellites disponibles (c'est-à-dire lorsque les points de repère sont disponibles).** ~~enregistre les informations reçues et traitées comme la latitude, la longitude, l'heure et la vitesse dans l'UEV, selon la structure définie à l'appendice **au sous-appendice** 1 (Dictionnaire de données), comme coordonnées géographiques avec la valeur HDOP calculée selon le minimum des valeurs HDOP recueillies sur les systèmes GNSS disponibles.~~

GNS_23a L'UEV enregistre également l'heure de l'horloge de l'UEV et l'écart temporel maximal entre celle-ci et l'heure réelle, le cas échéant, en utilisant les commandes SELECT et WRITE RECORD définies dans la norme ISO/CEI 7816-4:2013 en mode authentification uniquement de la messagerie sécurisée, comme prévu au sous-appendice 11, section 11.5, avec l'identificateur de fichier '2F30' et un numéro d'enregistrement égal à '01' pour VuRtcTime et à '02' pour MaximalTimeDifference.

4.2.3 Structure de la commande READ RECORD

La présente section décrit en détail la structure de la commande READ RECORD. La messagerie sécurisée (en mode authentification uniquement) est ajoutée conformément aux dispositions ~~de l'appendice~~**du sous-appendice** 11 (Mécanismes de sécurité communs).

GNS_24 La commande doit être compatible avec le mode authentification uniquement de la messagerie sécurisée (voir **sous-**appendice 11).

GNS_25 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'0Ch'	Messagerie sécurisée demandée
INS	1	'B2h'	READ RECORD
P1	1	'XXh'	Numéro d'enregistrement ('00' correspond à l'enregistrement en cours)
P2	1	'04h'	Lire l'enregistrement correspondant au numéro d'enregistrement indiqué en P1
Le	1	'XXh'	Longueur des données attendue. Nombre d'octets à extraire

GNS_26 L'enregistrement indiqué en P1 devient l'enregistrement en cours.

Octet	*Longueur*	*Valeur*	*Description*
#1-#X	X	'XX..XXh'	Données extraites
ME	2	'XXXXh'	Mots d'état (ME1, ME2)

- Si la commande aboutit, l'émetteur-récepteur GNSS sécurisé renvoie '**9000**' ;
- Si le fichier actif n'est pas destiné aux enregistrements, l'émetteur-récepteur GNSS sécurisé renvoie **'6981'** ;

- Si la commande est utilisée avec P1 = ’00’, mais qu’aucun EF n’est actif, l’émetteur-récepteur GNSS sécurisé renvoie **‘6986’** (commande interdite) ;
- Si l’enregistrement est introuvable, l’émetteur-récepteur GNSS sécurisé renvoie **‘6A83’** ;
- Si le dispositif GNSS externe détecte une manipulation, il renvoie les mots d’état **‘6690’**.

~~**GNS_7** L’émetteur récepteur GNSS sécurisé doit prendre en charge les commandes suivantes de la deuxième génération de tachygraphes définies à l’appendice **au sous-appendice** 2 :~~

~~*Commande*~~	~~*Référence*~~
~~SELECT~~	~~Appendice **Sous-appendice** 2 chapitre 3.5.1~~
~~READ BINARY~~	~~Appendice **Sous-appendice** 2 chapitre 3.5.2~~
~~GET CHALLENGE~~	~~Appendice **Sous-appendice** 2 chapitre 3.5.4~~
~~PSO: VERIFY CERTIFICATE~~	~~Appendice **Sous-appendice** 2 chapitre 3.5.7~~
~~EXTERNAL AUTHENTICATE~~	~~Appendice **Sous-appendice** 2 chapitre 3.5.9~~
~~GENERAL AUTHENTICATE~~	~~Appendice **Sous-appendice** 2 chapitre 3.5.10~~
~~MSE:SET~~	~~Appendice **Sous-appendice** 2 chapitre 3.5.11~~

4.2.4 Structure de la commande WRITE RECORD

La présente section décrit en détail la structure de la commande WRITE RECORD. La messagerie sécurisée (en mode authentification uniquement) est ajoutée conformément aux dispositions du sous-appendice 11 (Mécanismes de sécurité communs).

GNS_26a La commande doit être compatible avec le mode authentification uniquement de la messagerie sécurisée (voir sous-appendice 11).

GNS_26b Message de commande

Octet	Longueur	Valeur	Description
CLA	**1**	**‘0Ch’**	**Messagerie sécurisée demandée**
INS	**1**	**‘D2h’**	**WRITE RECORD**
P1	**1**	**‘XXh’**	**Numéro d’enregistrement (‘00’ correspond à l’enregistrement en cours)**
P2	**1**	**‘04h’**	**Écrire des données dans l’enregistrement correspondant au numéro indiqué en P1**
Données	**X**	**‘XXh’**	**Données**

GNS_26c L’enregistrement indiqué en P1 devient l’enregistrement en cours.

Octet	Longueur	Valeur	Description
ME	**2**	**‘XXXXh’**	**Mots d’état (ME1, ME2)**

- **Si la commande aboutit, l’émetteur-récepteur GNSS sécurisé renvoie ‘9000’ ;**
- **Si le fichier actif n’est pas destiné aux enregistrements, l’émetteur-récepteur GNSS sécurisé renvoie ‘6981’ ;**
- **Si la commande est utilisée avec P1 = ‘00’, mais qu’aucun EF n’est actif, l’émetteur-récepteur GNSS sécurisé renvoie ‘6986 (commande interdite) ;**
- **Si l’enregistrement est introuvable, l’émetteur-récepteur GNSS sécurisé renvoie ‘6A83’ ;**
- **Si le dispositif GNSS externe détecte une fraude, il renvoie les mots d’état ‘6690’.**

4.2.5 Autres commandes

GNS_27 L'émetteur-récepteur GNSS sécurisé doit prendre en charge les commandes suivantes de la deuxième génération de tachygraphes, définies au sous-appendice 2 :

Commande	Référence
SELECT	**Sous-appendice 2, section 3.5.1**
READ BINARY	**Sous-appendice 2, section 3.5.2**
GET CHALLENGE	**Sous-appendice 2, section 3.5.4**
PSO: VERIFY CERTIFICATE	**Sous-appendice 2, section 3.5.7**
EXTERNAL AUTHENTICATE	**Sous-appendice 2, section 3.5.9**
GENERAL AUTHENTICATE	**Sous-appendice 2, section 3.5.10**
MSE:SET	**Sous-appendice 2, section 3.5.11**

4.3 Couplage, authentification mutuelle et concordance de clés de session entre le dispositif GNSS externe et l'UEV

Le couplage, l'authentification mutuelle et la concordance des clés de session entre le dispositif GNSS externe et l'UEV sont décrits ~~à l'appendice~~ **au sous-appendice** 11 (Mécanismes de sécurité communs), chapitre 11.

4.4 Traitement des erreurs

La présente section décrit comment les éventuelles erreurs en rapport avec le dispositif GNSS externe sont traitées et enregistrées dans l'UEV.

4.4.1 Erreur de communication avec le dispositif GNSS externe

GNS_28 Si l'UEV ne parvient pas à communiquer avec le dispositif GNSS externe auquel elle est couplée pendant plus de 20 minutes consécutives, elle génère et enregistre dans sa mémoire un événement de type EventFaultType ayant pour valeur enum ~~*'53'H External*~~ ***'0E'H Erreur de communication avec le*** *dispositif GNSS* ***externe*** et dont l'horodatage est réglé sur l'heure actuelle. L'événement n'est généré que si les deux conditions suivantes sont satisfaites : a) le tachygraphe intelligent n'est pas en mode étalonnage ; et b) le véhicule est en mouvement. Dans ce contexte, une erreur de communication survient lorsque l'émetteur-récepteur sécurisé de l'UEV ne reçoit pas de message de réponse après un message de demande comme décrit à la section ~~5.2~~ **4.2**.

4.4.2 Atteinte à l'intégrité physique du dispositif GNSS externe

GNS_29 En cas d'atteinte au dispositif GNSS externe, l'émetteur-récepteur GNSS sécurisé **veille à ce que le matériel cryptographique ne soit pas disponible** ~~efface toute sa mémoire, y compris le matériel cryptographique~~. Conformément aux exigences GNS_25 et GNS_26, l'UEV détecte une manipulation si l'état '6690' est envoyé en réponse. L'UEV génère ensuite un événement ~~de type~~ **conformément à l'exigence 85 de l'appendice 1C et au sous-appendice 1 (**EventFaultType**)** ~~enum *'55'H* *'19'H*~~ pour la détection d'une atteinte au dispositif GNSS. **Le dispositif GNSS ~~ne~~ peut ~~plus~~ quant à lui répondre aux demandes de l'UEV sans messagerie sécurisée et en envoyant l'état '6A88' ~~à des demandes externes~~.**

4.4.3 Absence d'informations de positionnement en provenance du récepteur GNSS

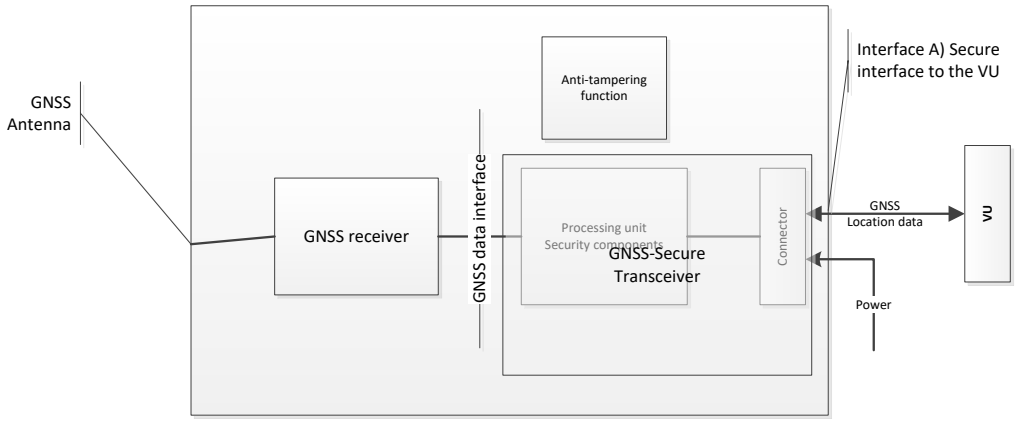
GNS_30 Si l'émetteur-récepteur GNSS sécurisé ne reçoit aucune donnée du récepteur GNSS ~~pendant plus de trois heures successives~~, il génère un message de réponse à la commande READ RECORD avec un numéro d'enregistrement égal à '01' et une zone de

données de 12 octets, tous définis par 0xFF. Dès la réception du message de réponse comprenant une zone de données de cette valeur, l'UEV génère et enregistre ~~un événement de type EventFaultType enum *'52'H* **'0D'H*~~ **l'absence d'informations de positionnement en provenance du** récepteur GNSS ~~externe~~**, conformément à l'exigence 81 de l'appendice 1C et au sous-appendice 1 (EventFaultType)**~~ assorti d'un horodatage indiquant l'heure actuelle uniquement si les deux conditions suivantes sont satisfaites: a) le tachygraphe intelligent n'est pas en mode étalonnage et b) le véhicule circule~~.

4.4.4 Expiration du certificat du dispositif GNSS externe

GNS_31 Si l'UEV détecte que le certificat DGE utilisé pour l'authentification mutuelle n'est plus valable, l'UEV génère et enregistre **une tentative d'atteinte à la sécurité conformément à l'exigence 85 de l'appendice 1C et au sous-appendice 1 (EventFaultType) pour l'expiration du certificat du dispositif GNSS externe** ~~une anomalie de l'équipement d'enregistrement~~ **l'appareil de contrôle** ~~de type EventFaultType enum *'56'H* **'1B'H** *External GNSS facility certificate expired* assorti d'un horodatage indiquant l'heure actuelle~~. L'UEV continue d'utiliser les données de positionnement GNSS reçues.

Figure ~~6-4~~
Schéma du dispositif GNSS externe



5. Unité embarquée sur le véhicule sans dispositif GNSS externe

5.1 Configuration

Dans cette configuration, le récepteur GNSS est situé à l'intérieur de l'UEV tel qu'illustré à la ~~figure 14~~ **figure 1**.

GNS_32 **Pour la transmission des données de position, des données DOP et des données satellites,** ~~Ll~~**e** récepteur GNSS tient le rôle de l'émetteur qui transmet les phrases NMEA ou de type NMEA au processeur de l'UEV, qui tient le rôle de récepteur sur une fréquence d'1/10 Hz ou supérieure pour le jeu prédéfini de phrases ~~NMEA~~, lequel doit comprendre au moins les phrases RMC**,** ~~et~~ GSA**, AMC et ASA**. **Le processeur de l'UEV et le récepteur GNSS externe peuvent également utiliser d'autres structures de données pour échanger les données contenues dans les phrases NMEA ou de type NMEA spécifiées aux points GNS_4, GNS_4a et GNS_5.**

GNS_33 Une antenne GNSS externe installée sur le véhicule ou une antenne GNSS interne doit être connectée à l'UEV.

5.2 Transfert d'informations du récepteur GNSS vers l'UEV

GNS_34 Le processeur de l'UEV vérifie les données reçues en extrayant les informations (par exemple la latitude, la longitude ou l'heure) de la phrase NMEA RMC et de la phrase AMC.

GNS_35 La phrase NMAE RMC contient les informations si le positionnement non authentifié est valide. Si tel n'est pas le cas, les données de positionnement ne sont pas mises à disposition et ne peuvent pas être utilisées pour enregistrer la position du véhicule. Si le positionnement non authentifié est valide, le processeur de l'UEV extrait également les valeurs HDOP de la phrase NMEA GSA.

GNS_36 Le processeur de l'UEV extrait également les informations (par exemple la latitude, la longitude ou l'heure) de la phrase AMC. La phrase AMC contient les informations si le positionnement non authentifié est valide conformément à l'exigence GNS_4a. Si le positionnement non authentifié est valide, le processeur de l'UEV extrait également les valeurs HDOP des phrases NMEA ASA.

5.3 Transfert d'informations de l'UEV vers le récepteur GNSS

GNS_37 Le processeur de l'UEV fournit au récepteur GNSS l'heure de la RTC de l'UEV et l'écart temporel maximal entre celle-ci et l'heure réelle, conformément aux exigences GNS_3f et GNS_3g.

~~5.2.~~5.4 Traitement des erreurs

~~5.2.1~~5.4.1 Absence d'informations de positionnement en provenance du récepteur GNSS

GNS_3~~8~~34 **L'UEV génère et enregistre un événement de type « absence d'informations de positionnement en provenance du récepteur GNSS », conformément à l'exigence 81 de l'appendice 1C et au sous-appendice 1 (EventFaultType)** ~~Si l'UEV ne reçoit aucune donnée du récepteur GNSS pendant plus de trois heures successives, l'UEV génère et mémorise un événement de type EventFaultType enum *'51'H Internal GNSS receiver fault* assorti d'un horodatage indiquant l'heure actuelle uniquement si les deux conditions suivantes sont satisfaites : a) le tachygraphe intelligent n'est pas en mode étalonnage et b) le véhicule circule~~.

6. Traitement et enregistrement des données de positionnement par l'UEV ~~Conflit temporel GNSS~~

Cette section s'applique à la configuration des tachygraphes intelligents avec et sans dispositif GNSS externe. ~~Si l'UEV détecte un écart de plus d'une minute entre le temps indiqué par sa fonction de mesure du temps et le temps indiqué par le récepteur GNSS, l'UEV mémorise un événement de type EventFaultType enum *'0B'H Time conflict (GNSS versus VU internal clock)*. Cet événement est enregistré avec la valeur de l'horloge interne de l'unité embarquée sur le véhicule et s'accompagne d'une remise à l'heure automatique. Après le déclenchement d'un événement «Conflit temporel», l'UEV ne vérifie plus les écarts temporels pendant les 12 heures suivantes. Cet événement n'est pas déclenché lorsqu'aucun signal GNSS valable n'a pu être détecté par le récepteur GNSS au cours des 30 derniers jours. Cependant, lorsque les informations de positionnement fournies par le récepteur GNSS sont à nouveau disponibles, la remise à l'heure automatique est effectuée.~~

GNS_39 Les données de positionnement sont stockées dans l'UEV avec un marqueur indiquant si le positionnement a été authentifié. Lorsque des données de positionnement doivent être enregistrées dans l'UEV, les règles suivantes s'appliquent :

a) Si les positionnements authentifiés et standard sont valides et cohérents, le positionnement standard et la précision correspondante sont enregistrés dans l'UEV, et le marqueur indique « authentifié » ;

b) Si les positionnements authentifiés et standard sont valides mais divergents, l'UEV stocke le positionnement authentifié et la précision correspondante, et le marqueur indique « authentifié » ;

c) Si le positionnement authentifié est valide et que le positionnement standard n'est pas valide, l'UEV enregistre le positionnement authentifié et la précision correspondante, et le marqueur indique « authentifié » ;

d) Si le positionnement standard est valide et que le positionnement authentifié n'est pas valide, l'UEV enregistre le positionnement standard et la précision correspondante, et le marqeur indique « authentifié ».

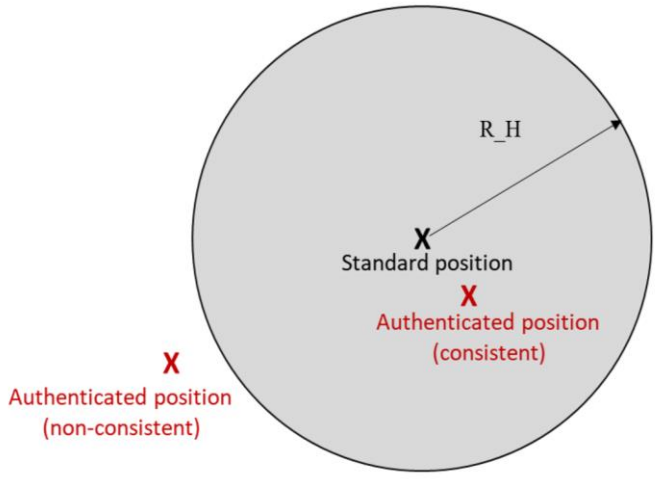
Les positionnements authentifiés et standard sont considérés comme cohérents, comme le montre la figure 7, lorsque le positionnement horizontal authentifié se trouve dans un cercle centré sur le positionnement horizontal standard, le rayon correspondant à l'arrondi au nombre entier supérieur le plus proche de la valeur R_H calculée selon la formule suivante :

$$R\_H = 1.74 \cdot \sigma_{UERE} \cdot HDOP$$

Où :

- **R_H est le rayon relatif d'un cercle autour de la position horizontale estimée, en mètres. Il s'agit d'un indicateur utilisé pour vérifier la cohérence entre les positionnements standard et les positionnements authentifiés ;**
- **σ_{UERE} est l'écart type correspondant à la gamme d'erreurs converties en équivalent utilisateur UERE *(User Equivalent Range Error*), qui modélise toutes les erreurs de mesure pour l'application cible, y compris les environnements urbains. On utilise une valeur constante de σ_{UERE} = 10 mètres ;**
- **HDOP est le coefficient d'affaiblissement de la précision horizontale calculée par le récepteur GNSS ;**
- **σ_{UERE} . HDOP est l'estimation de l'erreur quadratique moyenne dans le domaine horizontal.**

Figure 7
Positionnements authentifiés et positionnements standard (non authentifiés) cohérents



GNS_40 Lorsque l'état dans une phrase AMC reçue prend la valeur 'J', 'O' ou 'F', conformément à l'exigence GNS_4a, l'UEV génère et enregistre un événement de type « anomalie GNSS », conformément à l'exigence 88a de l'appendice 1C et au sous-appendice 1 (EventFaultType). L'unité embarquée sur le véhicule peut effectuer des vérifications supplémentaires avant de stocker un événement « anomalie GNSS » après la réception d'un état 'J' ou 'O'.

7. Conflit temporel GNSS

GNS_41 Si l'UEV détecte un écart entre l'heure de la fonction de mesure du temps de l'unité embarquée sur le véhicule et l'heure provenant des signaux GNSS, elle génère et enregistre un événement « Conflit temporel GNSS », conformément à l'exigence 86 de l'appendice 1C et au sous-appendice 1 (EventFaultType).

8. Conflit concernant le mouvement du véhicule

GNS_42~~35~~ L'UEV déclenche et enregistre un événement de type « conflit concernant le mouvement du véhicule » ~~(voir~~ **conformément à** l'exigence 84 de ~~l'annexe~~ **l'appendice** 1C~~)~~ ~~assorti d'un horodatage indiquant l'heure actuelle~~ si les informations relatives au mouvement calculées par le capteur de mouvement entrent en conflit avec les informations relatives au mouvement calculées par le récepteur GNSS interne, le dispositif GNSS externe **ou par d'autres sources indépendantes d'informations relatives au mouvement, conformément à l'exigence 26 de l'annexe 1C**.

L'événement « conflit concernant le mouvement du véhicule » est déclenché lorsque l'une des conditions de déclenchement présentée ci-après se produit.

Condition de déclenchement 1 :

~~Pour détecter ces conflits, o~~**O**n utilise la valeur ~~médiane~~ **moyenne tronquée** des différences de vitesse entre ces sources **lorsque les informations de positionnement du récepteur GNSS sont disponibles et que le contact du véhicule est allumé**, comme indiqué ci-dessous :

- Toutes les dix secondes maximum, la valeur absolue de la différence entre la vitesse du véhicule estimée par le dispositif GNSS et celle estimée par le capteur de mouvement est calculée ;
- Toutes les données calculées dans une fenêtre horaire comportant les cinq dernières minutes de mouvement servent à calculer la valeur ~~médiane~~ **moyenne tronquée ;**
- La valeur ~~médiane~~ **moyenne tronquée** est calculée comme la moyenne de 80 % des valeurs restantes, après élimination des plus élevées en valeur absolue.

L'événement « conflit concernant le mouvement du véhicule » est déclenché si la valeur ~~médiane~~ **moyenne tronquée** dépasse 10 km/h pendant cinq minutes de circulation du véhicule ininterrompues. ~~On peut également utiliser d'autres sources indépendantes de détection du mouvement du véhicule afin de renforcer la fiabilité de détection des manipulations du tachygraphe.~~ (Remarque : l'utilisation de la valeur ~~médiane~~ **moyenne tronquée** des cinq dernières minutes limite le risque de valeurs aberrantes et de valeurs transitoires dans les mesures.) ~~Cet événement ne se déclenche pas dans les cas suivants : a) lors d'un trajet en ferry/train, b) lorsque les informations de positionnement fournies par le récepteur GNSS ne sont pas disponibles et c) en mode étalonnage.~~

Pour le calcul de la moyenne tronquée, le véhicule est considéré comme en mouvement si au moins une valeur de vitesse du véhicule estimée soit par le capteur de mouvement soit par le récepteur GNSS n'est pas égale à zéro.

<u>Condition de déclenchement 2 :</u>

L'événement « conflit concernant le mouvement du véhicule » est également déclenché si la condition suivante est vraie :

$$\boldsymbol{GnssDistance} > \left[\boldsymbol{OdometerDifference} \times \boldsymbol{OdometerToleranceFactor} + \boldsymbol{Minimum}\left(\boldsymbol{SlipDistanceUpperlimit}\,;\,(\boldsymbol{OdometerDifference} \times \boldsymbol{SlipFactor})\right) + \boldsymbol{GnssTolerance} + \boldsymbol{FerryTrainDistance}\right]$$

Où :

- ***GnssDistance*** **est la distance entre la position actuelle du véhicule et la position précédente, toutes deux obtenues à partir des messages de position authentifiée valides, sans tenir compte de la hauteur ;**
- ***OdometerDifference*** **est la différence entre le kilométrage actuel et le kilométrage correspondant au précédent message de position authentifiée valide ;**
- ***OdometerToleranceFactor*** **est égal à 1,1 (facteur de tolérance le plus défavorable pour toutes les tolérances de mesure du compteur kilométrique du véhicule) ;**
- ***GnssTolerance*** **est égal à 1 km (tolérance GNSS la plus défavorable) ;**
- **Minimum (SlipDistanceUpperLimit ; (OdometerDifference * SlipFactor)) est la valeur la plus faible entre :**
  - **SlipDistanceUpperLimit, soit 10 km (limite supérieure de la distance de glissement due aux effets de glissement pendant le freinage) ;**
  - **OdometerDifference * SlipFactor, où SlipFactor est égal à 0,2 (influence maximale des effets de glissement pendant le freinage) ;**
  - **FerryTrainDistance est calculé comme suit : FerryTrainDistance = 200 km/h * tFerryTrain, où tFerryTrain est la somme des durées en heures de trajet en ferry/train dans l'intervalle de temps considéré. La durée d'un trajet en ferry/train est définie comme la différence de temps entre le marqueur de fin et le marqueur de début.**

Les vérifications ci-dessus doivent être effectuées toutes les 15 minutes si les données de positionnement nécessaires sont disponibles, ou dès que celles-ci sont disponibles.

Pour cette condition de déclenchement :

- **La date et l'heure du début de l'événement sont égales à la date et à l'heure de réception du message de position précédent ;**
- **La date et l'heure de la fin de l'événement sont égales à la date et à l'heure auxquelles la condition contrôlée redevient fausse.**

Condition de déclenchement 3 :

L'unité embarquée sur le véhicule constate une discordance entre le capteur de mouvement qui ne détecte aucun mouvement et la source indépendante qui détecte des mouvements pendant une période déterminée. Les conditions d'enregistrement d'une discordance ainsi que la période de détection de cette discordance sont fixées par le fabricant de l'unité embarquée, mais la discordance doit être détectée dans un délai maximal de trois heures.

~~Appendice~~Sous-appendice 13

Interface STI

Table des matières

1. Introduction

1.1 Champ d'application

ITS_01 Le présent **sous-**appendice pose **les bases de la communication par l'intermédiaire de** ~~la conception et les procédures à respecter pour mettre en œuvre~~ l'interface **tachygraphique** avec les systèmes de transport intelligent (STI) ~~tel que le préconise l'article 10 du règlement (UE) n° 165/2014 (le règlement)~~.

ITS_02 L'interface STI doit permettre aux dispositifs externes d'obtenir des données du tachygraphe, d'utiliser les services assurés par les tachygraphes et de fournir des données aux tachygraphes.

D'autres interfaces tachygraphiques (par exemple, bus CAN) peuvent également être utilisées à cette fin.

Le présent sous-appendice ne précise pas :

- **Les modalités de collecte et de gestion des données fournies par l'intermédiaire de l'interface STI se rapportant au tachygraphe ;**
- **La forme de la présentation des données collectées pour les applications hébergées sur le dispositif externe ;**
- **La spécification de sécurité STI, au-delà de ce qui est prévu dans la norme Bluetooth® ;**
- **Les protocoles Bluetooth® qu'utilise l'interface STI.**

1.2 Abréviations et définitions

Dans le présent sous-appendice, les abréviations et définitions suivantes sont utilisées :

GNSS	**Système mondial de navigation par satellite (*Global Navigation Satellite System*)**
STI	**Système de transport intelligent**
OSI	**Interconnexion de systèmes ouverts (*Open Systems Interconnection*)**
UEV	**Unité embarquée sur le véhicule**
Unité STI	**Dispositif ou application externe utilisant l'interface STI de l'UEV**

2. Normes de référence

ITS_03 Le présent sous-appendice renvoie aux règlements et normes ci-après, et dépend d'eux en tout ou en partie. Les normes ou leurs clauses applicables sont énoncées dans le présent sous-appendice. En cas de conflit, les dispositions du présent sous-appendice prévalent.

Dans le présent sous-appendice, il est fait référence aux normes suivantes :

- **Bluetooth® – Version standard 5.0 ;**
- **ISO 16844-7 : Véhicules routiers − Systèmes tachygraphes − Partie 7 : paramètres ;**
- **ISO/CEI 7498-1:1994 Technologies de l'information − Interconnexion de systèmes ouverts (OSI) − Modèle de référence de base, le modèle de base.**

3. Principes de fonctionnement de l'interface STI

ITS_04 L'UEV est responsable de l'actualisation et du stockage des données tachygraphiques transmises par l'intermédiaire de l'interface STI, sans aucune intervention de l'interface STI.

3.1 Technologie de communication

ITS_05 La communication par l'intermédiaire de l'interface STI doit être effectuée au moyen d'une interface Bluetooth® et être compatible avec Bluetooth® Low Energy conformément à la version 5.0 de la norme Bluetooth® ou à une version plus récente.

ITS_06 La communication entre l'UEV et l'unité STI est établie après l'achèvement d'un processus de connexion Bluetooth®.

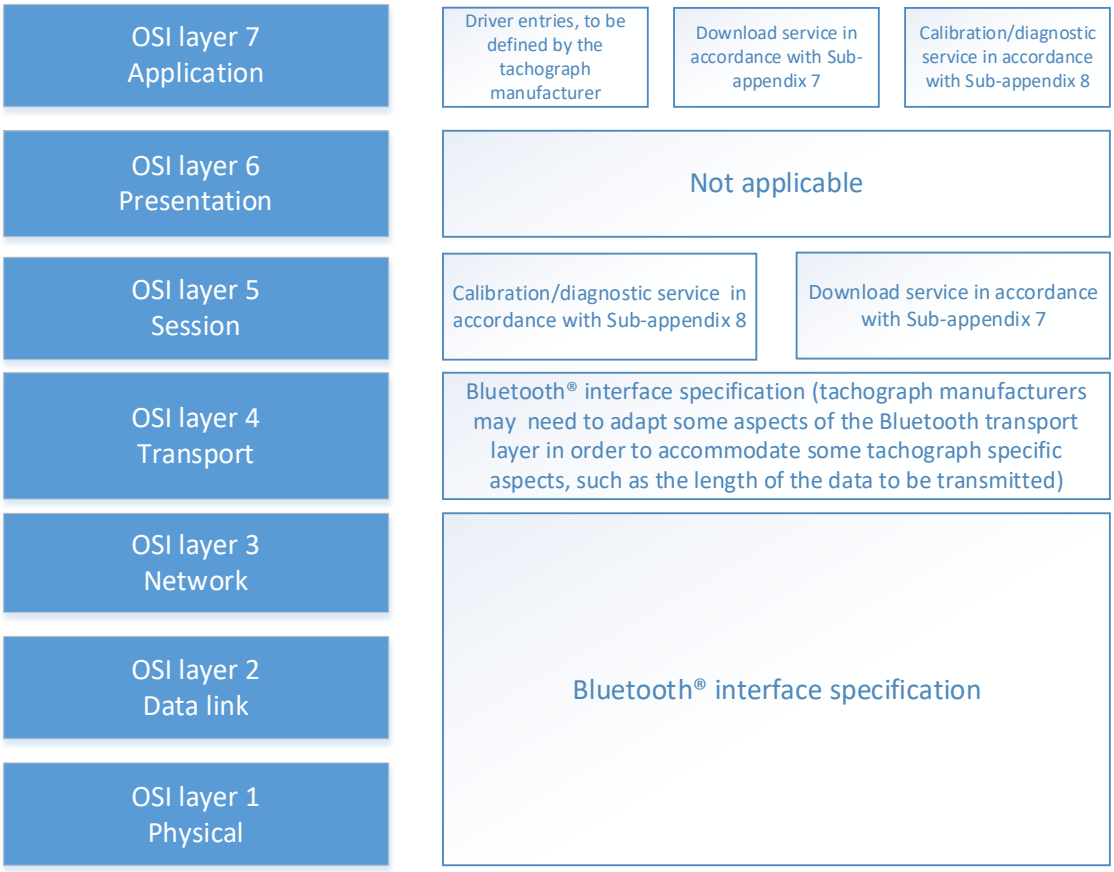
ITS_07 Une communication sécurisée et chiffrée est établie entre l'UEV et l'unité STI, conformément aux mécanismes de la spécification Bluetooth®. Le présent sous-appendice ne spécifie pas de mécanisme de chiffrement ou d'autres mécanismes de sécurité en plus de ceux prévus par Bluetooth®.

ITS_08 Bluetooth® utilise un modèle serveur/client pour contrôler la transmission de données entre appareils, dans lequel l'UEV fait office de serveur et l'unité STI de client.

3.2 Services disponibles

ITS_09 Les données à transmettre par l'intermédiaire de l'interface STI conformément au point 4 sont mises à disposition par l'intermédiaire des services spécifiés aux sous-appendice 7 et 8. En outre, l'UEV met à la disposition de l'unité STI les services nécessaires à la saisie manuelle de données prévue à l'exigence 61 de l'appendice 1C, et, éventuellement, à la saisie d'autres données en temps réel.

Figure 1
Cloisonnement de la communication via l'interface STI en fonction des couches du modèle OSI



ITS_10 Lorsque l'interface de téléchargement est utilisée par l'intermédiaire du connecteur frontal, l'UEV ne fournit pas les services de téléchargement spécifiés au sous-appendice 7 par l'intermédiaire de la connexion STI Bluetooth®.

ITS_11 Lorsque l'interface d'étalonnage est utilisée par l'intermédiaire du connecteur frontal, l'UEV ne fournit pas les services d'étalonnage spécifiés au sous-appendice 8 par l'intermédiaire de la connexion STI Bluetooth®.

3.3 Accès par l'intermédiaire de l'interface STI

ITS_12 L'interface STI fournit un accès sans fil à tous les services spécifiés aux sous-appendices 7 et 8, en remplacement de la connexion par câble au connecteur frontal à des fins d'étalonnage et de téléchargement spécifiées au sous-appendice 6.

ITS_13 L'UEV met l'interface STI à la disposition de l'utilisateur en fonction de la combinaison de cartes tachygraphiques valables insérées dans l'UEV, comme indiqué dans le tableau 1.

Disponibilité de l'interface STI		Lecteur « conducteur »				
		Pas de carte	Carte de conducteur	Carte de contrôleur	Carte d'atelier	Carte d'entreprise
Lecteur « co-conducteur »	Pas de carte	Non disponible	Disponible	Disponible	Disponible	Disponible
	Carte de conducteur	Disponible	Disponible	Disponible	Disponible	Disponible
	Carte de contrôleur	Disponible	Disponible	Disponible	Non disponible	Non disponible
	Carte d'atelier	Disponible	Disponible	Non disponible	Disponible	Non disponible
	Carte d'entreprise	Disponible	Disponible	Non disponible	Non disponible	Disponible

Tableau 1 − Disponibilité de l'interface STI en fonction du type de carte insérée dans le tachygraphe

ITS_14 Après un couplage STI Bluetooth® réussi, l'UEV attribue la connexion STI Bluetooth® à la carte tachygraphique insérée correspondante conformément au tableau 2.

Attribution de la connexion STI Bluetooth®		Lecteur « conducteur »				
		Pas de carte	Carte de conducteur	Carte de contrôleur	Carte d'atelier	Carte d'entreprise
Lecteur « co-conducteur »	Pas de carte	Non disponible	Carte de conducteur	Carte de contrôleur	Carte d'atelier	Carte d'entreprise
	Carte de conducteur	Carte de conducteur	Carte de conducteur (**)	Carte de contrôleur	Carte d'atelier	Carte d'entreprise
	Carte de contrôleur	Carte de contrôleur	Carte de contrôleur	Carte de contrôleur (*)	Non disponible	Non disponible
	Carte d'atelier	Carte d'atelier	Carte d'atelier	Non disponible	Carte d'atelier (*)	Non disponible
	Carte d'entreprise	Carte d'entreprise	Carte d'entreprise	Non disponible	Non disponible	Carte d'entreprise (*)

Tableau 2 − Attribution de la connexion STI en fonction du type de carte insérée dans le tachygraphe

(*) La connexion STI Bluetooth® est attribuée à la carte tachygraphique insérée dans le lecteur « conducteur » de l'UEV.
(**) L'utilisateur sélectionne la carte (insérée dans le lecteur « conducteur » ou « co-conducteur ») à laquelle la connexion STI Bluetooth® doit être attribuée.

ITS_15 Lorsqu'une carte tachygraphique est retirée, l'UEV met fin à la connexion STI Bluetooth® attribuée à cette carte.

ITS_16 L'UEV doit prendre en charge la connexion STI avec au moins une unité STI et peut prendre en charge les connexions avec plusieurs unités STI en même temps.

ITS_17 Les droits d'accès aux données et services disponibles par l'intermédiaire de l'interface STI doivent satisfaire aux exigences 12 et 13 de l'appendice 1C, ainsi qu'à l'exigence relative au consentement du conducteur définie au point 3.4 du présent sous-appendice.

3.4 Données disponibles et nécessité d'obtenir le consentement du conducteur

ITS_18 Toutes les données tachygraphiques disponibles par l'intermédiaire des services visés au point 3.3 sont classées comme étant soit à caractère personnel soit sans caractère personnel pour le conducteur, le co-conducteur ou les deux.

ITS_19 Au minimum, la liste des données classées comme étant obligatoires au chapitre 4 doit être accessibles par l'intermédiaire de l'interface STI.

ITS_20 Les données qui sont classées au chapitre 4 comme étant « à caractère personnel » ne sont accessibles que sous réserve du consentement du conducteur, lequel accepte que ses données à caractère personnel puissent quitter le réseau du véhicule, sauf dans le cas prévu à l'exigence ITS_25, pour lequel le consentement du conducteur n'est pas nécessaire.

ITS_21 Des données autres que celles visées au point 4 et considérées comme obligatoires peuvent être mises à disposition par l'intermédiaire de l'interface STI. Les données supplémentaires qui ne sont pas mentionnées au point 4 sont classées comme étant soit à caractère personnel soit sans caractère personnel par le fabricant de l'UEV, le consentement du conducteur étant requis pour les données qui ont été classées comme étant à caractère personnel, sauf dans le cas prévu par l'exigence ITS_25, pour lequel le consentement du conducteur n'est pas nécessaire.

ITS_22 En cas d'insertion d'une carte de conducteur inconnue de l'unité embarquée, le détenteur de la carte doit être invité par le tachygraphe à donner son consentement pour la transmission de données à caractère personnel par l'intermédiaire de l'interface STI, conformément à l'exigence 61 de l'appendice 1C.

ITS_23 Le statut de consentement (activé/désactivé) est enregistré dans la mémoire du tachygraphe de l'UEV.

ITS_24 Dans le cas de conducteurs multiples, seules les données à caractère personnel concernant les conducteurs qui ont donné leur consentement sont accessibles par l'intermédiaire de l'interface STI. Par exemple, dans le cas d'un équipage, si seul le conducteur a donné son consentement, les données à caractère personnel relatives au co-conducteur ne sont pas accessibles.

ITS_25 Lorsque l'UEV est en mode contrôle, entreprise ou étalonnage, les droits d'accès aux données par l'intermédiaire de l'interface STI sont gérés conformément aux exigences 12 et 13 de l'appendice 1C, de sorte que le consentement du conducteur n'est pas nécessaire.

4. Liste des données disponibles par l'intermédiaire de l'interface STI et classification des données à caractère personnel/sans caractère personnel

Nom des données	Structure des données	Source	Classification des données (à caractère personnel/ sans caractère personnel)		Consentement à la mise à disposition des données	Mise à disposition
			Conducteur	Co-conducteur		
VehicleIdentificationNumber	Appendice 8	UEV	sans caractère personnel	sans caractère personnel	consentement non requis	obligatoire
CalibrationDate	ISO 16844-7	UEV	sans caractère personnel	sans caractère personnel	Consentement non requis	obligatoire
TachographVehicleSpeed	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	obligatoire
Driver1WorkingState	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	obligatoire
Driver2WorkingState	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	obligatoire

Nom des données	Structure des données	Source	Classification des données (à caractère personnel/ sans caractère personnel)		Consentement à la mise à disposition des données	Mise à disposition
			Conducteur	Co-conducteur		
DriveRecognize	ISO 16844-7	UEV	sans caractère personnel	sans caractère personnel	consentement non requis	obligatoire
Driver1TimeRelatedStates	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	obligatoire
Driver2TimeRelatedStates	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	obligatoire
DriverCardDriver1	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	obligatoire
DriverCardDriver2	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	obligatoire
OverSpeed	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	obligatoire
TimeDate	Sous-appendice 8	UEV	sans caractère personnel	sans caractère personnel	consentement non requis	obligatoire
HighResolutionTotalVehicleDistance	ISO 16844-7	UEV	sans caractère personnel	sans caractère personnel	consentement non requis	obligatoire
HighResolutionTripDistance	ISO 16844-7	UEV	sans caractère personnel	sans caractère personnel	consentement non requis	obligatoire
ServiceComponentIdentification	ISO 16844-7	UEV	sans caractère personnel	sans caractère personnel	consentement non requis	obligatoire
ServiceDelayCalendarTimeBased	ISO 16844-7	UEV	sans caractère personnel	sans caractère personnel	consentement non requis	obligatoire
Driver1Identification	ISO 16844-7	Driver Card	à caractère personnel	sans objet	consentement du conducteur	obligatoire
Driver2Identification	ISO 16844-7	Driver Card	sans objet	à caractère personnel	consentement du co-conducteur	obligatoire
NextCalibrationDate	Sous-appendice 8	UEV	sans caractère personnel	sans caractère personnel	consentement non requis	obligatoire
Driver1ContinuousDrivingTime	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	obligatoire
Driver2ContinuousDrivingTime	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	obligatoire
Driver1CumulativeBreakTime	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	obligatoire
Driver2CumulativeBreakTime	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	obligatoire
Driver1CurrentDurationOfSelectedActivity	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	obligatoire
Driver2CurrentDurationOfSelectedActivity	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	obligatoire
SpeedAuthorised	Sous-appendice 8	UEV	sans caractère personnel	sans caractère personnel	consentement non requis	obligatoire
TachographCardSlot1	ISO 16844-7	UEV	sans caractère personnel	sans objet	consentement non requis	obligatoire
TachographCardSlot2	ISO 16844-7	UEV	sans objet	sans caractère personnel	consentement non requis	obligatoire
Driver1Name	ISO 16844-7	Driver Card	à caractère personnel	sans objet	consentement du conducteur	obligatoire
Driver2Name	ISO 16844-7	Driver Card	sans objet	à caractère personnel	consentement du co-conducteur	obligatoire
OutOfScopeCondition	ISO 16844-7	UEV	sans caractère personnel	sans caractère personnel	consentement non requis	obligatoire
ModeOfOperation	ISO 16844-7	UEV	sans caractère personnel	sans caractère personnel	consentement non requis	obligatoire

Nom des données	Structure des données	Source	Classification des données (à caractère personnel/ sans caractère personnel)		Consentement à la mise à disposition des données	Mise à disposition
			Conducteur	Co-conducteur		
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	obligatoire
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	obligatoire
EngineSpeed	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
RegisteringMemberState	Sous-appendice 8	UEV	sans caractère personnel	sans caractère personnel	consentement non requis	obligatoire
VehicleRegistrationNumber	Sous-appendice 8	UEV	sans caractère personnel	sans caractère personnel	consentement non requis	obligatoire
Driver1EndOfLastDailyRestPeriod	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2EndOfLastDailyRestPeriod	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
Driver1EndOfLastWeeklyRestPeriod	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2EndOfLastWeeklyRestPeriod	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
Driver1EndOfSecondLastWeeklyRestPeriod	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2EndOfSecondLastWeeklyRestPeriod	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
Driver1TimeLastLoadUnloadOperation	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2TimeLastLoadUnloadOperation	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
Driver1CurrentDailyDrivingTime	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2CurrentDailyDrivingTime	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
Driver1CurrentWeeklyDrivingTime	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2CurrentWeeklyDrivingTime	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
Driver1TimeLeftUntilNewDailyRestPeriod	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2TimeLeftUntilNewDailyRestPeriod	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
Driver1CardExpiryDate	ISO 16844-7	Driver Card	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2CardExpiryDate	ISO 16844-7	Driver Card	sans objet	à caractère personnel	consentement du co-conducteur	facultative
Driver1CardNextMandatoryDownloadDate	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2CardNextMandatoryDownloadDate	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
TachographNextMandatoryDownloadDate	ISO 16844-7	UEV	sans caractère personnel	sans caractère personnel	consentement non requis	facultative
Driver1TimeLeftUntilNewWeeklyRestPeriod	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2TimeLeftUntilNewWeeklyRestPeriod	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement non requis	facultative

Nom des données	Structure des données	Source	Classification des données (à caractère personnel/ sans caractère personnel)		Consentement à la mise à disposition des données	Mise à disposition
			Conducteur	Co-conducteur		
Driver2NumberOfTimes9hDailyDrivingTimesExceeded	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
Driver1CumulativeUninterruptedRestTime	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2CumulativeUninterruptedRestTime	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
Driver1MinimumDailyRest	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2MinimumDailyRest	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
Driver1MinimumWeeklyRest	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2MinimumWeeklyRest	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
Driver1MaximumDailyPeriod	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2MaximumDailyPeriod	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
Driver1MaximumDailyDrivingTime	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2MaximumDailyDrivingTime	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
Driver1NumberOfUsedReducedDailyRestPeriods	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2NumberOfUsedReducedDailyRestPeriods	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
Driver1RemainingCurrentDrivingTime	ISO 16844-7	UEV	à caractère personnel	sans objet	consentement du conducteur	facultative
Driver2RemainingCurrentDrivingTime	ISO 16844-7	UEV	sans objet	à caractère personnel	consentement du co-conducteur	facultative
VehiclePosition	Sous-appendice 8	UEV	à caractère personnel	à caractère personnel	consentement du conducteur et du co-conducteur	mandatory
ByDefaultLoadType	Sous-appendice 8	UEV	à caractère personnel	à caractère personnel	consentement du conducteur et du co-conducteur	obligatoire

~~Le règlement précise que les tachygraphes des véhicules peuvent être équipés d'interfaces normalisées permettant l'utilisation en mode opérationnel, par un dispositif extérieur, des données enregistrées ou produites par le tachygraphe, pour autant que les conditions suivantes soient remplies :~~

~~a) l'interface n'affecte pas l'authenticité ou l'intégrité des données du tachygraphe ;~~

~~b) l'interface est conforme aux dispositions détaillées énoncées à l'article 11 du règlement **dans le présent sous-appendice** ;~~

~~c) le dispositif extérieur connecté à l'interface n'a accès aux données à caractère personnel, y compris celles relatives à la géolocalisation, qu'après obtention du consentement vérifiable du conducteur auquel les données se rapportent.~~

2. Champ d'application

Le champ d'application du présent **sous** appendice consiste à préciser comment les applications hébergées sur des dispositifs externes obtiennent les *données* émanant d'un tachygraphe par connexion Bluetooth®.

Les données disponibles au moyen de cette interface sont décrites à l'annexe 1 du présent document. Cette interface n'empêche pas de mettre en œuvre d'autres interfaces (p. ex. au moyen d'un bus CAN) afin de transmettre les données de l'UEV à d'autres unités de traitement sur véhicule.

Le présent **sous** appendice précise :

- Les *données* disponibles grâce à l'interface ITS
- Le profil Bluetooth® utilisé pour transférer les données
- Les procédures de demande et de téléchargement et la séquence des opérations
- Le mécanisme de couplage entre le tachygraphe et le dispositif externe
- Le mécanisme d'accord accessible au conducteur

À titre d'éclaircissement, la **le** présente annexe **sous-appendice** ne précise pas :

- la collecte de l'opération et de la gestion des *données* au sein de l'UEV (qui sera spécifiée ailleurs dans le Règlement **l'Accord** ou constituera autrement une fonction de la conception du produit) ;
- La forme de la présentation des données collectées pour l'application hébergée sur le dispositif externe ;
- Les dispositions de protection des données au delà de ce que prévoit Bluetooth® (comme le codage) concernant le contenu des *données* (qui sera précisé ailleurs dans le règlement [**sous** appendice 10 – Mécanismes de sécurité communs]) ;
- Les protocoles Bluetooth® qu'utilise l'interface STI.

2.1 Abréviations, définitions et notations

Les abréviations et définitions qui suivent apparaissent dans le présent **sous** appendice :

la communication échange d'informations ou de données entre une unité maîtresse (comme les tachygraphes) et une unité externe à l'aide de l'interface ITS et de Bluetooth®.

les données telles que définies à l'annexe 1.

le règlement Règlement (UE) n° 165/2014 du Parlement européen et du Conseil du 4 février 2014 relatif aux tachygraphes dans les transports routiers, abrogeant le règlement (CEE) n° 3821/85 du Conseil concernant l'appareil de contrôle dans le domaine des transports par route et modifiant le règlement (CE) n° 561/2006 du Parlement européen et du Conseil relatif à l'harmonisation de certaines dispositions de la législation sociale dans le domaine des transports par route

BR Débit de base

EDR Débit de données amélioré

GNSS Global Navigation Satellite System (système mondial de radionavigation par satellite)

IRK Clé de résolution d'identité

ITS (ITS) Système de transport intelligent

LE Faible valeur énergétique

PIN Numéro d'identification personnel

PUC Code de déverrouillage personnel

SID Identifiant de diagnostic

SPP Profil de port série

SSP Couplage simple et sécurisé

PDT Paramètre de demande du transfert

PRT Paramètre de réponse du transfert

UEV Unité embarquée sur le véhicule

3. Règlement et normes de référence

La spécification définie au présent **sous** appendice se réfère et dépend en tout ou en partie des règlements et normes suivants. Les normes ou leurs clauses concernées figurent au fil des clauses du présent **sous** appendice. En cas de conflit, les clauses du présent **sous** appendice prévalent.

Les règlements et normes mentionnés au présent **sous** appendice sont les suivants :

Règlement (UE) n° 165/2014 du Parlement Européen et du Conseil du 4 février 2014 relatif aux tachygraphes dans les transports routiers, abrogeant le règlement (CEE) n° 3821/85 du Conseil concernant l'appareil de contrôle dans le domaine des transports par route et modifiant le règlement (CE) n° 561/2006 du Parlement européen et du Conseil relatif à l'harmonisation de certaines dispositions de la législation sociale dans le domaine des transports par route.

Règlement (CE) n° 561/2006 du Parlement européen et du Conseil du 15 mars 2006 relatif à l'harmonisation de certaines dispositions de la législation sociale dans le domaine des transports par route, modifiant les règlements (CEE) n° 3821/85 et (CE) n° 2135/98 du Conseil et abrogeant le règlement (CEE) n° 3820/85 du Conseil.

- ISO 16844-4: Véhicules routiers – Systèmes tachygraphes – Partie 4: Interface CAN
- ISO 16844-7: Véhicules routiers – Systèmes tachygraphes – Partie 7: Paramètres
- Bluetooth® – Profil de port série – V1.2
- Bluetooth® – Version standard 4.2
- Protocole NMEA 0183 V4.1

4. Principes de fonctionnement de l'interface

4.1 Conditions préalables au transfert de données au moyen de l'interface STI

L'UEV est responsable de l'actualisation et de la mémorisation des données dans l'UEV sans impliquer l'interface STI. Les moyens pour y parvenir sont internes à l'UEV. Ils sont précisés ailleurs dans le règlement **l'Accord** et pas au présent **sous** appendice.

4.1.1 Données fournies grâce à l'interface STI

L'UEV est responsable de l'actualisation des données qui seront disponibles grâce à l'interface STI selon une fréquence déterminée par les procédures de l'UEV, sans impliquer l'interface STI. Les données de l'UEV sont utilisées comme base d'alimentation et d'actualisation des *données*. Les moyens pour y parvenir sont précisés ailleurs dans le règlement **l'Accord**. En l'absence de précision, il s'agit d'une fonction liée à la conception du produit non spécifiée dans le présent **sous** appendice.

~~**4.1.2 Contenu des données**~~

~~Le contenu des *données* est spécifié en annexe 1 du présent **sous**-appendice.~~

~~**4.1.3 Applications STI**~~

~~Les applications STI utilisent les données mises à disposition par l'interface STI, par exemple, dans le but d'optimiser la gestion des activités du conducteur tout en respectant le Règlement **les dispositions de l'Accord** et pour détecter les éventuelles anomalies du tachygraphe ou utiliser les données du dispositif GNSS. Les spécifications des applications sortent du champ d'application du présent **sous**-appendice.~~

~~**Les parties contractantes peuvent mettre en place des restrictions à la transmission de données par les applications STI ; ces restrictions n'affectent pas les données fournies par l'interface STI conformément au point 4.1.1. Les Parties contractantes respectent la législation sur la protection des données en vigueur sur leurs territoires respectifs, en ce qui concerne la collecte, le stockage, le traitement et l'utilisation des données personnelles au moyen des STI.**~~

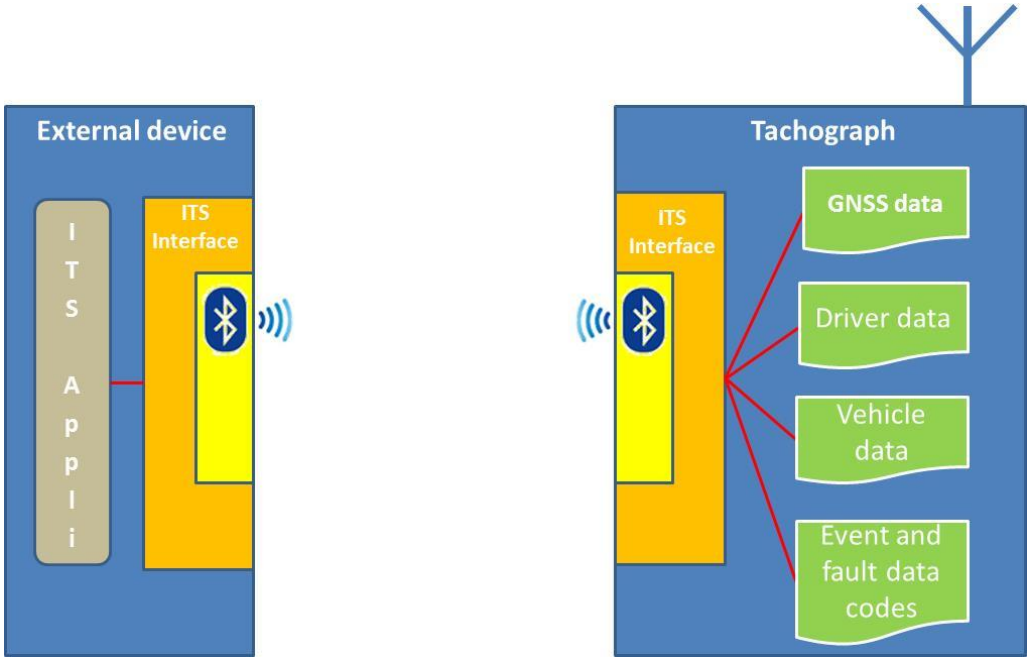
~~4.2 Technologie de communication~~

~~L'échange de *données* à l'aide de l'interface STI se fait par une interface Bluetooth® compatible de version 4.2 ou ultérieure. Bluetooth® opère sur la bande de fréquence industrielle, scientifique et médicale (ISM) sans licence entre 2,4 GHZ et 2,485 GHz. Bluetooth® 4.2 comprend des mécanismes de sécurité et de confidentialité renforcés et accroît la vitesse et la fiabilité des transferts de données. Aux fins de la présente spécification, on utilise la portée radio Bluetooth® classe 2 pouvant atteindre 10 m. Pour tout complément d'information sur Bluetooth® 4.2, consulter www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).~~

~~*La communication* est établie avec l'équipement de communication après avoir procédé au couplage à l'aide d'un dispositif homologué. Le concept Bluetooth® utilisant un modèle maître/esclave pour contrôler quand et où les dispositifs peuvent envoyer des données, le tachygraphe joue le rôle d'unité maitresse et le dispositif externe, celui d'esclave.~~

~~Lorsqu'un dispositif externe entre dans le champ de portée de l'UEV pour la première fois, la procédure de couplage Bluetooth® peut être démarrée (cf. Annexe 2). Les dispositifs partagent leur adresse, nom, profil et clé secrète commune. Cela leur permet de se connecter dès qu'ils se retrouvent à proximité l'un de l'autre à nouveau. Après cette étape, le dispositif externe est sécurisé et en mesure d'effectuer des demandes de téléchargement de données émanant du tachygraphe. Il n'est pas prévu d'ajouter des mécanismes de codage supplémentaires au-delà de ceux assurés par Bluetooth®. Cependant, si des mécanismes de sécurité additionnels se révélaient nécessaires, ils seraient ajoutés conformément à l'appendice **au sous-appendice** 10 (Mécanismes de sécurité communs).~~

~~Les principes de communication globaux sont décrits par la figure suivante.~~



~~Le profil SPP (Serial Port Profile) de Bluetooth® sert à transférer des données émanant de l'UEV à destination du dispositif externe.~~

~~4.3 Autorisation du PIN~~

~~Pour des raisons de sécurité, l'UEV exécute un système d'autorisation de code PIN distinct du couplage Bluetooth®. Chaque UEV est en mesure de générer des codes PIN à des fins d'authentification, composés d'au moins quatre chiffres. Chaque fois qu'un dispositif externe se couple avec l'UEV, il doit fournir le code PIN correct avant de recevoir des données, quelles qu'elles soient.~~

~~Renseigner le PIN place le dispositif sur la liste autorisée. La liste autorisée mémorise au moins 64 dispositifs couplés avec l'UEV considérée.~~

~~Trois tentatives infructueuses de renseignement du code PIN placent temporairement le dispositif sur la liste noire, ce qui le verrouille. Tant qu'il est exclu, toute nouvelle tentative du dispositif est vouée à l'échec. Toute nouvelle série de trois tentatives infructueuses successives à fournir le code PIN allonge la durée du verrouillage (cf. tableau 1). Renseigner le code PIN correct réinitialise la durée du verrouillage et le nombre de tentatives. La figure 1 de l'annexe 2 représente le déroulement chronologique d'une tentative de validation du PIN.~~

~~Tableau 150~~
~~**Durée du verrouillage selon le nombre d'échecs successifs à renseigner le code PIN correct**~~

~~*Nombre d'échecs successifs*~~	~~*Durée du verrouillage*~~
~~3~~	~~30 secondes~~
~~6~~	~~5 minutes~~
~~9~~	~~1 heure~~
~~12~~	~~24 heures~~
~~15~~	~~Permanents~~

~~Après quinze tentatives infructueuses successives (5 x 3) à renseigner le code PIN, l'unité ITS est définitivement verrouillée. La seule solution pour déverrouiller le système consiste à renseigner le code PUC correct.~~

Le code PUC est composé de huit chiffres. Il est communiqué par le fabricant avec l'UE. Après dix tentatives infructueuses successives à fournir le code PUC, l'unité STI est définitivement verrouillée et placée en liste noire.

Il arrive que le fabricant permette à titre facultatif de modifier le code PIN directement sur l'UEV ; toutefois, le code PUC n'est pas modifiable. La modification du code PIN, le cas échéant, requiert de renseigner le code PIN directement sur l'UEV.

De plus, tous les dispositifs placés en liste autorisée y demeurent jusqu'à leur retrait manuel par l'utilisateur (p. ex. à l'aide de l'interface homme-machine de l'UEV ou par d'autres moyens). Procéder de la sorte permet de supprimer les unités STI perdues ou volées de la liste autorisée. De même, toutes les unités STI sortant de la portée de connexion Bluetooth® plus de vingt-quatre heures doivent être automatiquement supprimées de la liste autorisée de l'UEV, et l'on doit renseigner le code PIN exact une nouvelle fois lorsque la connexion est rétablie.

La structure des messages entre l'interface de l'UEV et l'UEV n'est pas imposée, mais laissée à la discrétion du fabricant. Ledit fabricant doit toutefois s'assurer que la structure des messages échangés entre l'unité STI et l'interface de l'UEV est respectée (cf. spécifications ASN.1).

Toute demande de données doit donc satisfaire à la vérification correcte des identifiants de l'expéditeur préalablement à toute autre forme de traitement. La figure 2 de l'annexe 2 représente le schéma du déroulement chronologique de cette procédure. Tout dispositif verrouillé reçoit un refus automatique. Tout dispositif ni verrouillé ni autorisé reçoit une demande de PIN à renseigner avant de faire suivre sa demande de données.

4.4 Structure des messages

Tous les messages échangés entre l'unité STI et l'UEV se caractérisent par une structure à trois éléments: en-tête composé d'un octet cible (TGT), d'un octet source (SRC) et d'un octet de longueur (LEN).

La zone de données composée d'un octet d'identification de diagnostic (SID) et d'un nombre variable d'octets d'information (maximum 255).

L'octet total de contrôle correspond à une série de sommes d'1 octet modulo 256 représentant tous les octets du message à l'exclusion du CS lui-même.

Le message correspond au Big Endian.

Tableau 251
Structure générale des messages

En-tête			*Zone de données*					*Total de contrôle*
TGT	SRC	LEN	SID	PDT	CC	CM	données	CS
3 octets			255 octets max.					1 octet

En-tête

TGT et SRC: ID des dispositifs cible (TGT) et source (SRC) du message. L'interface UEV porte par défaut l'ID «EE». Cet ID n'est pas modifiable. L'unité STI utilise l'ID «A0» par défaut pour son premier message de session de communication. L'interface de l'UEV assigne alors un ID unique à l'unité STI et l'informe de cet ID pour les futurs messages de la session.

L'octet LEN tient compte uniquement de la partie «données» de la zone de données (cf. Tableau 2), car les quatre premiers octets sont implicites.

L'interface UEV confirme l'authenticité de l'expéditeur du message en contre-vérifiant sa propre liste d'ID avec les données Bluetooth® et en vérifiant que l'unité STI correspondant à l'ID fourni est bien à portée de la connexion Bluetooth®.

Zone de données

Outre le SID, la zone de données doit également comporter les paramètres suivants: un paramètre de demande du transfert (PDT) et des octets de compteur.

Si les données à transférer dépassent l'espace disponible dans un message, elles seront partagées en plusieurs sous-messages. Chaque sous-message présente le même en-tête et le même SID, mais contient un compteur sur deux octets, un compteur courant (CC) et un compteur max (CM) pour indiquer le numéro du sous-message. Afin de permettre le contrôle d'erreur et l'abandon éventuel d'un échange de données, le dispositif récepteur accuse réception de chaque sous-message. Le dispositif récepteur est à même d'accepter le sous-message, d'en demander la réémission et de demander au dispositif émetteur d'en reprendre ou d'en abandonner la transmission.

Non utilisés, CC et CM présentent la valeur 0xFF.

Par exemple: le message suivant

EN-TÊTE	*SID*	*PDT*	*CC*	*CM*	*Données*	*CS*
3 octets	Longueur supérieure à 255 octets					1 octet

est transmis ainsi:

EN-TÊTE	*SID*	*PDT*	*01*	*n*	*Données*	*CS*
3 octets	255 octets					1 octet

EN-TÊTE	*SID*	*PDT*	*02*	*n*	*Données*	*CS*
3 octets	255 octets					1 octet

…

EN-TÊTE	*SID*	*PDT*	*N*	*N*	*données*	*CS*
3 octets	255 octets max.					1 octet

Le tableau 3 présente les messages que l'UEV et l'unité STI seront en mesure d'échanger. Le contenu de chaque paramètre est fourni en code hexadécimal. Le tableau n'inclut pas CC et CM. Voir ci-dessus pour la structure complète.

Tableau 3 52
Contenu détaillé des messages

	En-tête			*Données*			*Total de contrôle*
Message	TGT	SRC	LEN	SID		DATA	
RequestPIN	*ITSID*	EE	00	01	FF		
SendITSID	*ITSID*	EE	01	02	FF	*ITSID*	
SendPIN	EE	*ITSID*	04	03	FF	4*INTEGER (0..9)	
PairingResult	*ITSID*	EE	01	04	FF	BOOLEAN (T/F)	
SendPUC	EE	*ITSID*	08	05	FF	8*INTEGER (0..9)	
BanLiftingResult	*ITSID*	EE	01	06	FF	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FF	Time	
RequestData							

	En-tête			*Données*			*Total de contrôle*
Message	TGT	SRC	LEN	SID		DATA	
standardTachData	EE	*ITSID*	01	08	01		
personalTachData	EE	*ITSID*	01	08	02		
gnssData	EE	*ITSID*	01	08	03		
standardEventData	EE	*ITSID*	01	08	04		
personalEventData	EE	*ITSID*	01	08	05		
standardFaultData	EE	*ITSID*	01	08	06		
manufacturerData	EE	*ITSID*	01	08	07		
ResquestAccepted	*ITSID*	EE	Len	09	PRT	Data	
DataUnavailable							
No data available	*ITSID*	EE	02	0A	PRT	10	
Personal data not shared	*ITSID*	EE	02	0A	PRT	11	
NegativeAnswer							
General reject	*ITSID*	EE	02	0B	SID dem	10	
Service not supported	*ITSID*	EE	02	0B	SID dem	11	
Sub function not supported	*ITSID*	EE	02	0B	SID dem	12	
Incorrect message length	*ITSID*	EE	02	0B	SID dem	13	
Conditions not correct or request sequence error	*ITSID*	EE	02	0B	SID dem	22	
Request out of range	*ITSID*	EE	02	0B	SID dem	31	
Response pending	*ITSID*	EE	02	0B	SID dem	78	
ITSID Mismatch	*ITSID*	EE	02	0B	SID dem	FC	
ITSID Not Found	*ITSID*	EE	02	0B	SID dem	FB	

RequestPIN (SID 01)

Ce message est émis par l'interface de l'UEV si une unité STI ni verrouillée ni autorisée lui adresse une demande de données.

SendITSID (SID 02)

Ce message est émis par l'interface de l'UEV dès qu'un nouveau dispositif lui adresse une demande. Ce dispositif utilise l'ID par défaut «A0» avant de se voir assigner un ID unique pour la session de communication.

SendPIN (SID 03)

Ce message est émis par l'unité STI pour que l'UEV la place en liste autorisée. Le contenu de ce message est un code constitué d'un nombre ENTIER de 4 chiffres compris entre 0 et 9.

PairingResult (SID 04)

~~Ce message est émis par l'interface de l'UEV pour informer l'unité du STI si le code PIN envoyé est correct. Le contenu de ce message est une valeur BOOLÉENNE d'une valeur «Vrai» si le code PIN est correct et «Faux» dans le cas contraire.~~

~~*SendPUC (SID 05)*~~

~~Ce message est émis par l'unité STI pour que l'UEV la supprime de la liste noire. Le contenu de ce message est un code constitué d'un nombre ENTIER de 8 chiffres compris entre 0 et 9.~~

~~*BanLiftingResult (SID 06)*~~

~~Ce message est émis par l'interface de l'UEV pour informer l'unité du STI si le code PUC envoyé est correct. Le contenu de ce message est une valeur BOOLÉENNE «vraie» si le code PUC est correct et «fausse» dans le cas contraire.~~

~~*RequestRejected (SID 07)*~~

~~Ce message est émis par l'interface de l'UEV en réponse à tout message émis par une unité STI verrouillée hormis «SendPUC». Ce message comporte la durée restante de verrouillage de l'unité STI, selon la structure séquentielle «chronologique» définie à l'annexe 3.~~

~~*RequestData* (SID 08)~~

~~Ce message d'accès aux données est émis par l'unité STI. Un paramètre de demande de transfert (PDT) d'un octet indique de quelle catégorie de données il s'agit. Il existe plusieurs catégories de données:~~

- ~~standardTachData (PDT 01): données disponibles en provenance du tachygraphe classées non personnelles.~~
- ~~personalTachData (PDT 02): données disponibles en provenance du tachygraphe classées personnelles.~~
- ~~gnssData (PDT 03): données du dispositif GNSS, toujours personnelles.~~
- ~~standardEventData (PDT 04): données relatives aux événements mémorisés classées non personnelles.~~
- ~~personalEventData (PDT 05): données relatives aux événements mémorisés classées personnelles.~~
- ~~standardFaultData (PDT 06): anomalies mémorisées classées non personnelles.~~
- ~~manufacturerData (PDT 07): données mises à disposition par le fabricant.~~

~~Voir annexe 3 du présent **sous**-appendice pour toute information complémentaire relative à chaque catégorie de données.~~

~~Voir **sous**-appendice 12 pour tout complément d'information à propos de la structure et du contenu des données du dispositif GNSS.~~

~~Voir annexes **appendices 1B** et **1C** pour tout complément d'information à propos du code et des anomalies relatifs aux données liées aux événements.~~

~~*ResquestAccepted* (SID 09)~~

~~Ce message est émis par l'interface de l'UEV si un message «RequestData» émanant d'une unité STI a été accepté. Ce message comporte un octet PRT, qui correspond à l'octet PDT du message RequestData associé et toutes les données de la catégorie demandée.~~

~~*DataUnavailable* (SID 0A)~~

~~Ce message est émis par l'interface de l'UEV si, pour une raison quelconque, il est impossible d'envoyer les données demandées à une unité STI autorisée. Ce message comporte un octet PRT, qui correspond au PDT des données demandées et un octet de code d'erreur spécifié au Tableau 3. Les codes suivants sont disponibles:~~

- ~~Aucune donnée disponible (10): l'interface de l'UEV ne parvient pas à accéder aux données de l'UEV pour des raisons non précisées.~~

- Données à caractère personnel non partagées (11): L'unité STI tente d'extraire des données à caractère personnel non partagées.

NegativeAnswer (SID 0B)

Ces messages sont émis par l'interface de l'UEV si une demande ne peut aboutir pour toute autre raison que l'indisponibilité des données. Ces messages résultent généralement d'une mauvaise formulation de la structure de la demande (longueur, SID, STIID...), sans s'y limiter. Le PDT dans la zone de données comporte le SID de la demande. La zone de données comporte un code identifiant la raison de la réponse négative. Les codes suivants sont d'application:

- Rejet général (code: 10)

L'action ne peut aboutir pour une raison non spécifiée, ni ci dessous ni dans la section (Renseigner le numéro de section *DataUnavailable*).

- Service non pris en charge (code: 11)

Le SID de la demande n'est pas compris.

- Sous-fonction non prise en charge (code: 12)

Le PDT de la demande n'est pas compris. Il peut par exemple être manquant ou en dehors de la plage de valeurs acceptée.

- Longueur du message incorrecte (code: 13)

La longueur du message reçu est erronée (décalage entre l'octet LEN et la longueur réelle du message).

- Conditions non correctes ou erreur affectant la séquence d'interrogation (code: 22)

Le service demandé n'est pas disponible ou la séquence des messages de demande est incorrecte.

- Demande excessive (code: 33)

Le relevé (champ de données) du paramètre de la demande n'est pas valable.

- Réponse en suspens (code: 78)

L'action réclamée ne peut être achevée dans le temps imparti et l'UEV n'est pas prête à accepter une autre demande.

- Décalage *ITSID* (code: FB)

L'*ITSID* du SRC ne correspond pas au dispositif associé après comparaison avec les informations émanant de Bluetooth®.

- *ITSID* introuvable (code: FC)

L'ITSID SRC n'est pas associé à un dispositif.

Les lignes 1 à 72 (FormatMessageModule) du code ASN.1 dans l'annexe 3 spécifient la structure des messages telle que décrite au tableau 3. Davantage d'informations suivent à propos du contenu des messages.

4.5 Consentement du conducteur

Toutes les données disponibles sont classées comme standard ou à caractère personnel. Les données à caractère personnel sont uniquement accessibles si le conducteur a donné son accord et accepter que ses données à caractère personnel liées au tachygraphe quittent le réseau du véhicule à destination d'applications tierces.

Le conducteur donne son accord lorsqu'à la première insertion d'une carte de conducteur ou d'atelier qui est encore inconnue de l'unité embarquée sur le véhicule, le détenteur est invité à donner son accord pour que les données à caractère personnel en lien avec le tachygraphe

puissent être extraites via l'interface STI facultative. (voir également annexe **appendice 1C**, paragraphe 3.6.2).

L'état de l'accord (activé/désactivé) est mémorisé par le tachygraphe.

Dans le cas de conducteurs multiples, seules les données à caractère personnel concernant les conducteurs qui ont donné leur accord sont partagées avec l'interface STI. Par exemple, si deux conducteurs occupent le véhicule et que seulement l'un d'entre eux accepte de partager ses données à caractère personnel, celles de l'autre conducteur ne sont pas partagées.

4.6 Récupération de données standard

La figure 3 de l'annexe 2 représente le schéma de la séquence d'une demande valable adressée par l'unité STI pour accéder aux données standard. L'unité STI est placée en liste autorisée et ne demande aucune donnée à caractère personnel. Aucune autre vérification n'est requise. Les schémas illustrent le respect de la procédure adéquate sur la Figure 2 de l'annexe 2. Cela correspond à la case grisée *REQUEST TREATMENT* de la Figure 2.

Parmi les données disponibles, les données suivantes sont considérées comme référence :

- standardTachData (PDT 01)
- standardEventData (PDT 04)
- standardFaultData (PDT 06)

4.7 Récupération de données à caractère personnel

La figure 4 de l'annexe 2 représente le schéma de la séquence de traitement d'une demande de données à caractère personnel. Comme précédemment expliqué, l'interface de l'UEV adresse des données à caractère personnel uniquement si le conducteur a donné son accord explicite (voir aussi 4.5). Dans le cas contraire, la demande doit être automatiquement rejetée.

Parmi les données disponibles, les données suivantes sont considérées comme personnelles :

- personalTachData (PDT 02)
- gnssData (PDT 03)
- personalEventData (PDT 05)
- manufacturerData (PDT 07)

4.8 Récupération de données relatives aux événements et aux anomalies

Les unités STI sont en mesure de demander des données associées aux événements comportant la liste de tous les événements imprévus. Ces données sont considérées comme étant des données standard ou personnelles (voir annexe 3). Le contenu de chaque événement varie selon la documentation fournie en annexe 1 du présent **sous** appendice.

~~ANNEXE 1~~

~~**1) LISTE DES DONNÉES DISPONIBLE PAR L'INTERMÉDIAIRE DE L'INTERFACE STI**~~

~~**2) DONNÉES ÉMANANT DU DISPOSITIF GNSS CONTINU DISPONIBLES AVEC LE CONSENTEMENT DU CONDUCTEUR**~~

~~Voir sous-appendice 12 (GNSS).~~

~~3) CODES ASSOCIÉS AUX ÉVÉNEMENTS DISPONIBLES SANS LE CONSENTEMENT DU CONDUCTEUR~~

Data	Source	Data classification (personal/not personal)
VehicleIdentificationNumber	Vehicle Unit	**not personal**
CalibrationDate	Vehicle Unit	**not personal**
TachographVehicleSpeed speed instant t	Vehicle Unit	personal
Driver1WorkingState Selector driver	Vehicle Unit	personal
Driver2WorkingState	Vehicle Unit	personal
DriveRecognize Speed Threshold detected	Vehicle Unit	**not personal**
Driver1TimeRelatedStates Weekly day time	Driver Card	personal
Driver2TimeRelatedStates	Driver Card	personal
DriverCardDriver1	Vehicle Unit	**not personal**
DriverCardDriver2	Vehicle unit	**not personal**
OverSpeed	Vehicle Unit	personal
TimeDate	Vehicle Unit	**not personal**
HighResolutionTotalVehicleDistance	Vehicle Unit	**not personal**
ServiceComponentIdentification	Vehicle Unit	**not personal**
ServiceDelayCalendarTimeBased	Vehicle Unit	**not personal**
Driver1Identification	Driver Card	personal
Driver2Identification	Driver Card	personal
NextCalibrationDate	Vehicle Unit	**not personal**
Driver1ContinuousDrivingTime	Driver Card	personal
Driver2ContinuousDrivingTime	Driver Card	personal
Driver1CumulativeBreakTime	Driver Card	personal
Driver2CumulativeBreakTime	Driver Card	personal
Driver1CurrentDurationOfSelectedActivity	Driver Card	personal
Driver2CurrentDurationOfSelectedActivity	Driver Card	personal
SpeedAuthorised	Vehicle Unit	**not personal**
TachographCardSlot1	Driver Card	**not personal**
TachographCardSlot2	Driver Card	**not personal**
Driver1Name	Driver Card	personal
Driver2Name	Driver Card	personal
OutOfScopeCondition	Vehicle Unit	**not personal**
ModeOfOperation	Vehicle Unit	**not personal**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Driver Card	personal
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Driver Card	personal
EngineSpeed	Vehicle Unit	personal
RegisteringMemberState	Vehicle Unit	**not personal**
VehicleRegistrationNumber	Vehicle Unit	**not personal**
Driver1EndOfLastDailyRestPeriod	Driver Card	personal
Driver2EndOfLastDailyRestPeriod	Driver Card	personal
Driver1EndOfLastWeeklyRestPeriod	Driver Card	personal
Driver2EndOfLastWeeklyRestPeriod	Driver Card	personal
Driver1EndOfSecondLastWeeklyRestPeriod	Driver Card	personal
Driver2EndOfSecondLastWeeklyRestPeriod	Driver Card	personal
Driver1CurrentDailyDrivingTime	Driver Card	personal
Driver2CurrentDailyDrivingTime	Driver Card	personal
Driver1CurrentWeeklyDrivingTime	Driver Card	personal
Driver2CurrentWeeklyDrivingTime	Driver Card	personal
Driver1TimeLeftUntilNewDailyRestPeriod	Driver Card	personal
Driver2TimeLeftUntilNewDailyRestPeriod	Driver Card	personal
Driver1CardExpiryDate	Driver Card	personal
Driver2CardExpiryDate	Driver Card	personal
Driver1CardNextMandatoryDownloadDate	Driver Card	personal
Driver2CardNextMandatoryDownloadDate	Driver Card	personal
TachographNextMandatoryDownloadDate	Vehicle Unit	**not personal**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Driver Card	personal
Driver2TimeLeftUntilNewWeeklyRestPeriod	Driver Card	personal
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Driver Card	personal
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Driver Card	personal
Driver1CumulativeUninterruptedRestTime	Driver Card	personal
Driver2CumulativeUninterruptedRestTime	Driver Card	personal
Driver1MinimumDailyRest	Driver Card	personal
Driver2MinimumDailyRest	Driver Card	personal
Driver1MinimumWeeklyRest	Driver Card	personal
Driver2MinimumWeeklyRest	Driver Card	personal
Driver1MaximumDailyPeriod	Driver Card	personal
Driver2MaximumDailyPeriod	Driver Card	personal
Driver1MaximumDailyDrivingTime	Driver Card	personal
Driver2MaximumDailyDrivingTime	Driver Card	personal
Driver1NumberOfUsedReducedDailyRestPeriods	Driver Card	personal
Driver2NumberOfUsedReducedDailyRestPeriods	Driver Card	personal
Driver1RemainingCurrentDrivingTime	Driver Card	personal
Driver2RemainingCurrentDrivingTime	Driver Card	personal
GnssPosition	Vehicle Unit	personal

Événement	*Règles de stockage*	*Données à enregistrer pour chaque événement*
Insertion d'une carte non valable	– les 10 événements les plus récents	– date et heure de l'événement – type, numéro et génération de la carte ou des cartes à l'origine de l'événement et État membre **Partie contractante** l'ayant délivrée – nombre d'événements semblables survenus le même jour
Conflit de carte	– les 10 événements les plus récents	– date et heure de début de l'événement – date et heure de fin de l'événement – type, numéro et génération de chacune des deux cartes à l'origine du conflit et État membre **Partie contractante** les ayant délivrées
Clôture incorrecte de la dernière session	– les 10 événements les plus récents	– date et heure de l'insertion – type, numéro et génération de la carte et État membre **Partie contractante** l'ayant délivrée – données relatives à la dernière session telles qu'elles figurent sur la carte : – date et heure de l'insertion – le numéro d'immatriculation, la Partie contractante d'immatriculation et la génération de l'UEV .
Interruption de l'alimentation électrique (2)	– l'événement le plus long pour chacun des 10 derniers jours d'occurrence – les 5 événements les plus longs enregistrés au cours des 365 derniers jours	– date et heure de début de l'événement – date et heure de fin de l'événement – type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et État membre **Partie contractante** l'ayant délivrée – nombre d'événements semblables survenus le même jour
Erreur de communication avec le dispositif de communication à distance	**– l'événement le plus long pour chacun des 10 derniers jours d'occurrence** **– les 5 événements les plus longs enregistrés au cours des 365 derniers jours**	**– date et heure de début de l'événement** **– date et heure de fin de l'événement** **– type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et État membre Partie contractante l'ayant délivrée** **– nombre d'événements semblables survenus le même jour**

Événement	*Règles de stockage*	*Données à enregistrer pour chaque événement*
Absence d'informations sur la position en provenance du récepteur GNSS	– l'événement le plus long pour chacun des 10 derniers jours d'occurrence – les 5 événements les plus longs enregistrés au cours des 365 derniers jours	– date et heure de début de l'événement – date et heure de fin de l'événement – type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et Partie contractante l'ayant délivrée – nombre d'événements semblables survenus le même jour
Erreur sur les données de mouvement	– l'événement le plus long pour chacun des 10 derniers jours d'occurrence – les 5 événements les plus longs enregistrés au cours des 365 derniers jours	– date et heure de début de l'événement – date et heure de fin de l'événement – type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et État membre **Partie contractante** l'ayant délivrée – nombre d'événements semblables survenus le même jour
Conflit concernant le mouvement du véhicule	– l'événement le plus long pour chacun des 10 derniers jours d'occurrence – les 5 événements les plus longs enregistrés au cours des 365 derniers jours	– date et heure de début de l'événement – date et heure de fin de l'événement – type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et État membre **Partie contractante** l'ayant délivrée – nombre d'événements semblables survenus le même jour
Tentative d'atteinte à la sécurité	– les 10 événements les plus récents pour chaque type d'événement	– date et heure de début de l'événement – date et heure de fin de l'événement (le cas échéant) – type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et État membre **Partie contractante** l'ayant délivrée – type d'événement
Conflit temporel	– l'événement le plus long pour chacun des 10 derniers jours d'occurrence – les 5 événements les plus longs enregistrés au cours des 365 derniers jours	– date et heure de l'appareil de contrôle – date et heure GNSS – type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et État membre **Partie contractante** l'ayant délivrée – nombre d'événements semblables survenus le même jour

4) CODES ASSOCIÉS AUX ÉVÉNEMENTS DISPONIBLES AVEC LE CONSENTEMENT DU CONDUCTEUR

Événement	*Règles de stockage*	*Données à enregistrer pour chaque événement*
Conduite sans carte appropriée	- l'événement le plus long pour chacun des 10 derniers jours d'occurrence - les 5 événements les plus longs enregistrés au cours des 365 derniers jours	- date et heure de début de l'événement - date et heure de fin de l'événement - type, numéro et génération de toute carte insérée au début et/ou à la fin de l'événement et État membre **Partie contractante** l'ayant délivrée - nombre d'événements semblables survenus le même jour
Insertion d'une carte en cours de conduite	- le dernier événement pour chacun des 10 derniers jours d'occurrence	- date et heure de l'événement - type, numéro et génération de la carte et État membre **Partie contractante** l'ayant délivrée - nombre d'événements semblables survenus le même jour
Excès de vitesse (1)	- l'événement le plus grave (c'est à dire celui présentant la vitesse moyenne la plus élevée) pour chacun des 10 derniers jours d'occurrence - les 5 événements les plus graves enregistrés au cours des 365 derniers jours - le premier événement survenu après le dernier étalonnage	- date et heure de début de l'événement - date et heure de fin de l'événement - vitesse maximale mesurée au cours de l'événement - vitesse moyenne arithmétique mesurée au cours de l'événement - type, numéro et génération de la carte de conducteur (le cas échéant) et État membre **Partie contractante** l'ayant délivrée - nombre d'événements semblables survenus le même jour

5) CODES ASSOCIÉS AUX DONNÉES CONCERNANT LES ANOMALIES DISPONIBLES SANS LE CONSENTEMENT DU CONDUCTEUR

Anomalie	*Règles de stockage*	*Données à enregistrer pour chaque anomalie*
Anomalie de la carte	- les 10 dernières anomalies de la carte de conducteur	- date et heure de début de l'anomalie - date et heure de fin de l'anomalie - type, numéro et génération de la carte et État membre **Partie contractante** l'ayant délivrée

Anomalie	*Règles de stockage*	*Données à enregistrer pour chaque anomalie*
Anomalies de l'appareil de contrôle	— les 10 anomalies les plus récentes pour chaque type d'anomalie — la première anomalie survenue après le dernier étalonnage	- date et heure de début de l'anomalie - date et heure de fin de l'anomalie - type d'anomalie - type, numéro et génération de toute carte insérée au début et/ou à la fin de l'anomalie et État membre **Partie contractante** l'ayant délivrée

Cette anomalie est déclenchée dans le cas des anomalies suivantes, en mode autre qu'étalonnage :

– anomalie interne de l'UEV ;

– anomalie de l'imprimante ;

– anomalie de l'affichage ;

– anomalie de téléchargement ;

– anomalie du capteur ;

– anomalie du récepteur GNSS ou du dispositif GNSS externe ;

– anomalie du dispositif de communication à distance ;

– anomalie **de l'interface STI (le cas échéant).**

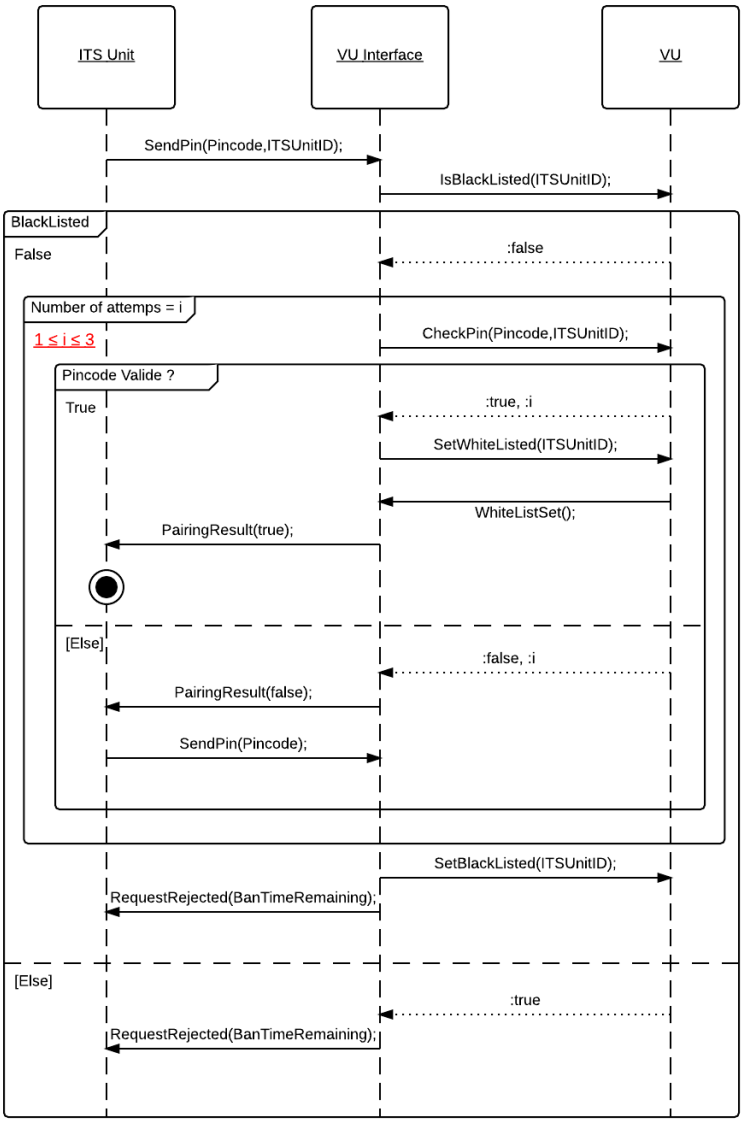
6) ÉVÉNEMENTS ET ANOMALIES PROPRES AU FABRICANT SANS LE CONSENTEMENT DU CONDUCTEUR

Événement ou anomalie	*Règles de stockage*	*Données à enregistrer pour chaque événement*
À définir par le fabricant	À définir par le fabricant	À définir par le fabricant

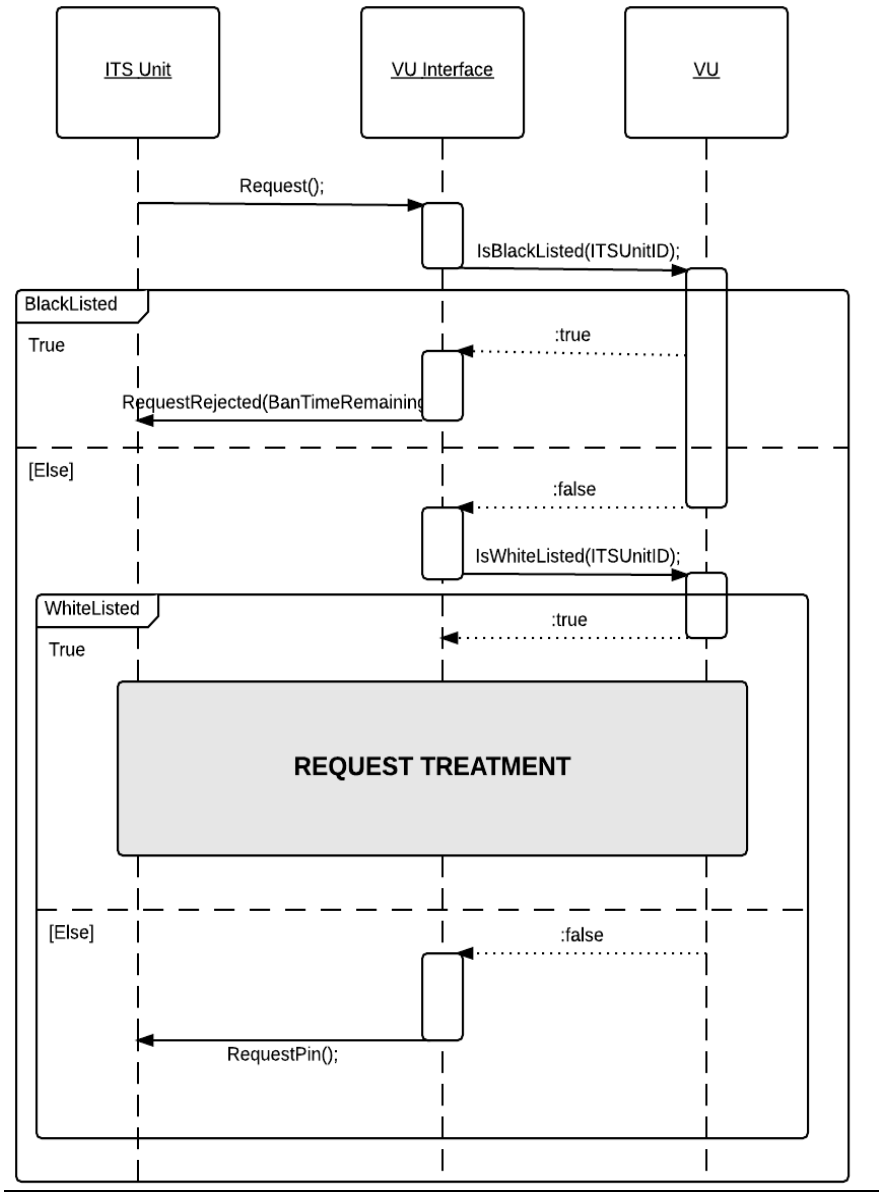
~~ANNEXE 2~~

~~SCHÉMAS DES SÉQUENCES D'ÉCHANGES DE MESSAGES AVEC L'UNITÉ STI~~

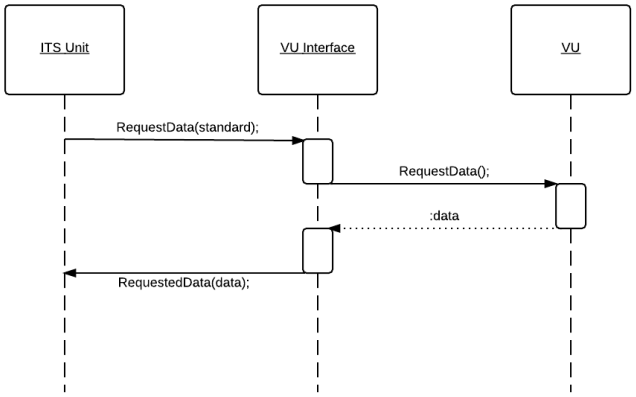
~~Figure 1~~ ~~18~~
~~Schéma de la séquence pour la tentative de validation du PIN~~



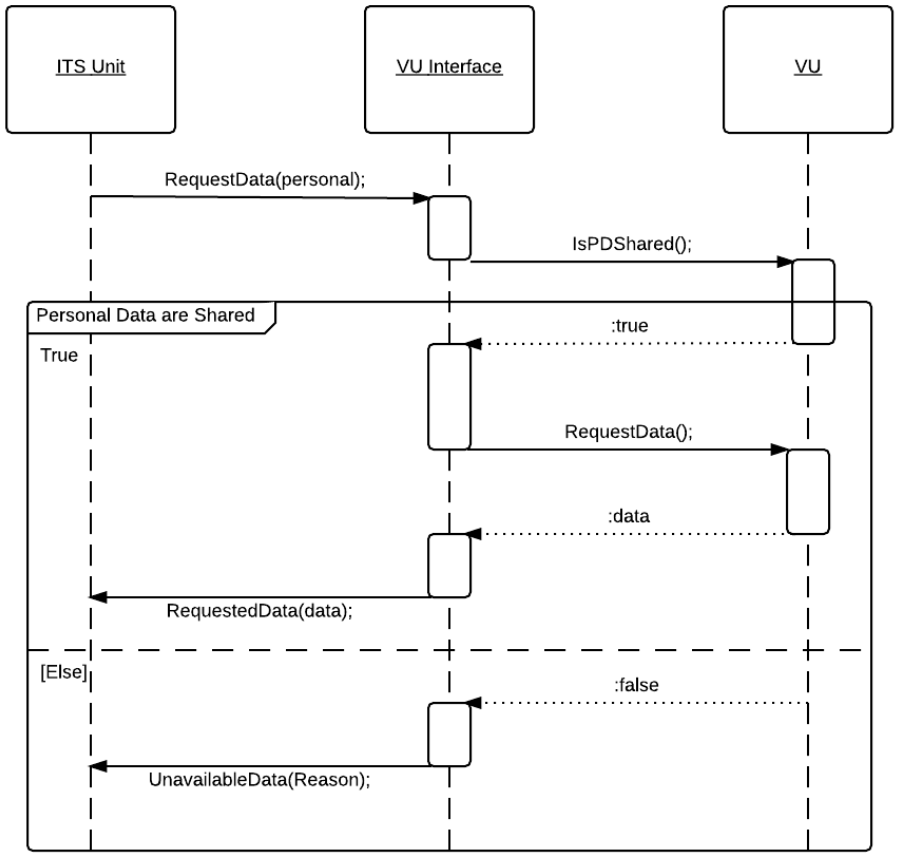
~~Figure 2~~ ~~19~~
~~Schéma de la séquence de vérification de l'autorisation par l'unité STI~~



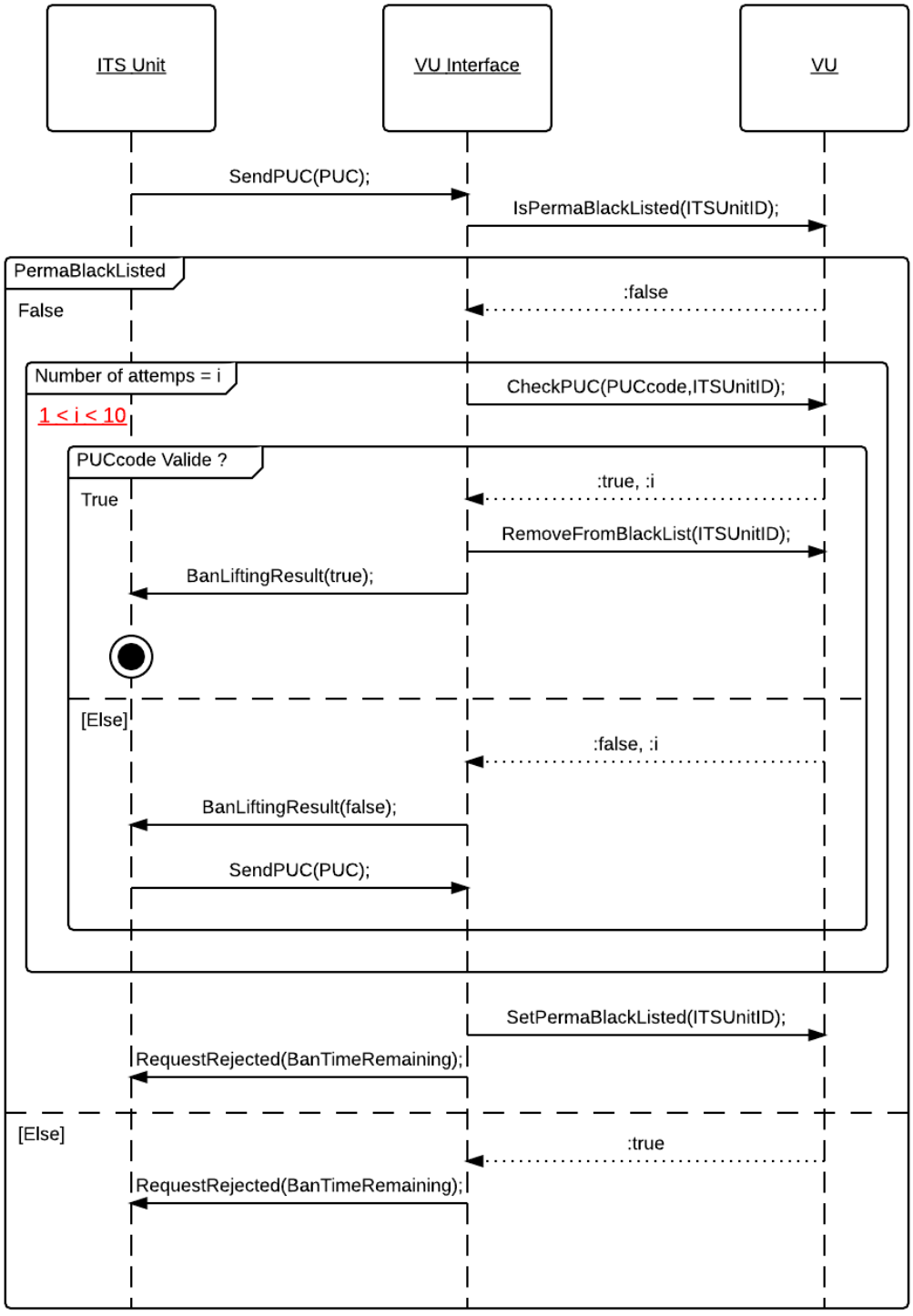
~~Figure 3~~ ~~20~~
~~Schéma de la séquence de traitement d'une demande de données sans caractère personnel (après accès PIN validé)~~



~~Figure 4~~ ~~21~~
~~Schéma de la séquence de traitement d'une demande de données à caractère personnel (après accès PIN validé)~~



~~Figure 5~~ ~~22~~
~~Schéma de la séquence pour la tentative de validation du PUC~~



ANNEXE 3

SPÉCIFICATIONS ASN.1

```
FormatMessageModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ;
IMPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
        BanLiftingResult FROM PINPUCDataFieldsModule
        RequestAccepted,RequestData, DataUnavailable FROM
        RequestDataFieldsModule
        SendITSID, NegativeAnswer FROM OtherDataFieldsModule ;
___________
    CompleteMessage ::=SEQUENCE{
          header Header,
          data DataField,
          checksum Checksum
    }
_______________
_____ _____________
      HEADER TYPES
_____ _____________
_____
_____
    Header::=SEQUENCE{
          tgt IDList,
          src IDList,
          len BIT STRING (1..255)
    }
___________
    vuID BIT STRING ::= 'EE'H
    IDList ::=CHOICE{
          vu BIT STRING (vuID),
          itsUnits SEQUENCE OF BIT STRING,
                  --Default hex Value:A0, redefined after first message exchange--
                --Each ID will be linked to the Bluetooth ID of the device--
___________
          ...
    }
_____
    ____________________
    --DATAFIELDS TYPES--
    ____________________
    DataField ::=SEQUENCE{
          sid BIT STRING,
          PDT BIT STRING,
          subMBytes SubMessageBytes,
          dataField Content,
___________
          ...
    }
_____
    SubMessageBytes ::= SEQUENCE{
          currentSubM BIT STRING,
          totalSubM BIT STRING
    }
_____
    Content ::= CHOICE{
          requestPIN RequestPIN,
          sendITSID SendITSID,
          sendPin SendPIN,
          pairRslt PairingResult,
          sendPUC SendPUC,
```

```
            banlift BanLiftingResult,
            requestRejected RequestRejected,
            requestData RequestData,
            requestOK RequestAccepted,
            dataUnavailable DataUnavailable,
            negAns NegativeAnswer
    }

    -------------------
    --CHECKSUM TYPES--
    -------------------

    Checksum ::= SEQUENCE{
            --SHA2 checksum
    }
END
```

```
PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult ;
IMPORTS ;
-----------
---Utils--
-----------

    PUC ::= SEQUENCE (SIZE(8)) OF
    INTEGER (SIZE(0..9))

    PIN ::=   SEQUENCE (SIZE(4)) OF
          INTEGER (SIZE(0..9))

-------------------------
--Messages From ITS Unit--
-------------------------

    SendPIN {PIN:pin} ::= SEQUENCE {
          sid BIT STRING ('03'H),
          pin PIN (pin)
    }

    SendPUC {PUC:puc} ::= SEQUENCE {
          sid BIT STRING ('05'H),
          puc PUC (puc)
    }
--------------------
--Messages From VU--
--------------------

    PairingResult ::= SEQUENCE{
          sid BIT STRING ('04'H),
          result BOOLEAN
    }

    RequestPIN {MType:receivedRequest}::= SEQUENCE{
          sid BIT STRING ('01'H)
    }

    RequestRejected ::= SEQUENCE{
          sid BIT STRING ('07'H),
          banTimeRemaining GeneralizedTime, --PermaBan == 1k years--    }

    BanLiftingResult ::= SEQUENCE{
          sid BIT STRING ('06'H),
          result BOOLEAN
    }
END
```

```
RequestDataFields DEFINITIONS AUTOMATIC TAGS ::= BEGIN
    EXPORTS RequestAccepted,RequestData, DataUnavailable ;
    IMPORTS StandardEvent, PersonalEvent, StandardFault FROM EventsModule ;
    ------------------------
    ---From ITS Unit--
    ------------------
    RequestData ::= SEQUENCE{
        sid BIT STRING (‘08’H),
        requestedData DataTypeCode,
        ...
    }
    -----------
    --From VU--
    -----------
    RequestAccepted ::=SEQUENCE{
        sid BIT STRING (‘09’H),
        trtp DataTypeCode,
        dataSheet CHOICE{
            standardData StandardTachDataContent,
            personalData PersonalTachDataContent,
            gnss GNSSDataContent,
            standardEvent StandardEventContent,
            personalEvent PersonalEventContent,
            standardFault StandardFaultContent,
            manufacturerdata ManufacturerDataContent,
            ...
        }
    }
    DataTypeCode ::=CHOICE{
        standardTachData BIT STRING (‘01’H),
        personalTachData BIT STRING (‘02’H),
        gnssData BIT STRING (‘03’H),
        standardEventData BIT STRING (‘04’H),
        personalEventData BIT STRING (‘05’H),
        standardFaultData BIT STRING (‘06’H),
        manufacturerData BIT STRING (‘07’H),
        ...
    }
    DataUnavailable ::=SEQUENCE{
        sid BIT STRING (‘0A’H),
        trtp DataTypeCode,
        reason UnavailableDataCodes
    }
    UnavailableDataCodes ::= CHOICE{
        noDataAvailable BIT STRING (‘10’H),
        personalDataNotShared BIT STRING (‘11’H),
        ...
    }
    ----------------------------
    --Complete Tachograph Data--
    ----------------------------
    --The format of the data was taken from the ISO16844-7 norm, more information
available in this ISO document--
    Time ::= SEQUENCE{
        seconds INTEGER (0..59.75), --increment: 0.25s--
```

```
            minutes INTEGER (0..59), --increment: 1min--
            hours INTEGER (0..23), --increment: 1h--
            day INTEGER (0.25.. 31.75), --increment: 0.25d--
            month INTEGER (1..12), --increment: 1month--
            year INTEGER (1985..2235), --increment: 1year--
            locMinOffset INTEGER (-59..59), --increment: 1min--
            locHouroffset INTEGER (-23..23)--increment: 1h--
      }

      Date ::= SEQUENCE{
            month INTEGER (1..12), --increment: 1month--
            day INTEGER (0.25.. 31.75), --increment: 0.25d--
            year INTEGER (1985..2235) --increment: 1year--
      }
      DriverName ::=SEQUENCE{
            codePageSurname UTF8String, --See ISO/CEI 8859--
            surname UTF8String,
            codePageFirstname UTF8String, --See ISO/CEI 8859--
            firstname UTF8String,
      }

      -- Message Content --

      StandardTachDataContent ::= SEQUENCE{
            trtp DataTypeCode (DataTypeCode.&standardTachData),
            personal BOOLEAN (FALSE),
            data StandardTachyDataSheet,
      }

      PersonalTachDataContent ::= SEQUENCE{
            trtp DataTypeCode (DataTypeCode.&personalTachData),
            personal BOOLEAN (TRUE),
            data PersonalTachyDataSheet
      }

      GNSSDataContent ::= SEQUENCE{
            trtp DataTypeCode (DataTypeCode.&gnssData),
            personal BOOLEAN (TRUE),
            data GNSSDataSheet
      }

      StandardEventContent ::= SEQUENCE{
            trtp DataTypeCode (DataTypeCode.&standardEventData),
            personal BOOLEAN (FALSE),
            data StandardEventDataSheet
      }

      PersonalEventContent ::= SEQUENCE{
            trtp DataTypeCode (DataTypeCode.&personalEventData),
            personal BOOLEAN (TRUE),
            data PersonalEventDataSheet
      }

      StandardFaultContent ::= SEQUENCE{
            trtp DataTypeCode (DataTypeCode.&standardFaultData),
            personal BOOLEAN (FALSE),
            data StandardFault
```

```
    }

    ManufacturerDataContent ::= SEQUENCE{
        trtp DataTypeCode (DataTypeCode.&manufacturerData),
        personal BOOLEAN (TRUE),
        ...
    }

    ----------------
    --DATA SHEETS--
    ----------------

    --Data sheet format follows ISO 16844-7.--
    StandardTachyDataSheet ::= SEQUENCE{
        vin UTF8String (SIZE(17)),
        calibrationDate Date,
        driveRecognize INTEGER (2 UNION 12),
        driverCardDriver1 INTEGER (2 UNION 12),
        driverCardDriver2 INTEGER (2 UNION 12),
        timeDate Time,
        highResolutionTotalVehicleDistance INTEGER (0..21055406),  --increment: 5m--
        serviceComponentIdentification INTEGER (0..255),
        serviceDelayCalendarTimeBased INTEGER ( 125..125),  --increment: 1week--
        nextCalibrationDate Date,
        speedAuthorised INTEGER (0..250.996), --increment 1/256km/h--
        tachographCardSlot1 INTEGER (0..4...), --Maximum 250--
        tachographCardSlot2 INTEGER (0..4...), --Maximum 250--
        outOfScopeCondition INTEGER(2 UNION 12),
        modeOfOperation INTEGER (0..4...), --Maximum 250--
        registeringMemberState UTF8String,      vehicleRegistrationNumber SEQUENCE {
            codePageVRN INTEGER (0..255),
            vrn OCTET STRING (SIZE(13)),
        },
        tachographNextMandatoryDownloadDate Date,
        ...
    }
    PersonalTachyDataSheet ::= SEQUENCE{
        tachographVehicleSpeed INTEGER (0..250.996), --increment 1/256km/h--
        driver1WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002 UNION
1012...),
        driver2WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002 UNION
1012...),

        driver1TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION 1002
UNION
                                         1012 UNION 1102 UNION 1112 UNION 10002 UNION
10012 UNION
                                         10102 UNION 10112 UNION 11002 UNION
11012...),
        driver2TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION 1002
UNION
                                         1012 UNION 1102 UNION 1112 UNION 10002 UNION
10012 UNION
                                         10102 UNION 10112 UNION 11002 UNION
11012...),
        overSpeed INTEGER (2 UNION 12),
        driver1Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS FROM TACHO
REGULATION--
```

~~driver2Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS FROM TACHO REGULATION--~~
~~driver1ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--~~
~~driver2ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--~~
~~driver1CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --increment: 1min--~~
~~driver2CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --increment: 1min--~~
~~driver1Name DriverName,~~
~~driver2Name DriverName,~~
~~driver1CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255), --increment: 1min--~~
~~driver2CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255), --increment: 1min--~~
~~engineSpeed INTEGER(0..8031.875), --increment: 0,125r/min--~~
~~driver1EndOfLastDailyRestPeriod Time,~~
~~driver2EndOfLastDailyRestPeriod Time,~~
~~driver1EndOfLastWeeklyRestPeriod Time,~~
~~driver2EndOfLastWeeklyRestPeriod Time,~~
~~driver1EndOfSecondLastWeeklyRestPeriod Time,~~
~~driver2EndOfSecondLastWeeklyRestPeriod Time,~~
~~driver1CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min--~~
~~driver2CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min--~~
~~driver1CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment: 1min--~~
~~driver2CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment: 1min--~~
~~driver1TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --increment: 1min--~~
~~driver2TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --increment: 1min--~~
~~driver1CardExpiryDate Date,~~
~~driver2CardExpiryDate Date,~~
~~driver1CardNextMandatoryDownloadDate Date,~~
~~driver2CardNextMandatoryDownloadDate Date,~~
~~driver1TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --increment: 1min--~~
~~driver2TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --increment: 1min--~~
~~driver1NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),~~
~~driver2NumberOfTimes9hDailyDrivingTimesExceeced INTEGER (0..13),~~
~~driver1CumulativeUninterruptedRestTime INTEGER (0.. 64255), --increment: 1min--~~
~~driver2CumulativeUninterruptedRestTime INTEGER (0.. 64255), --increment: 1min--~~
~~driver1MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--~~
~~driver2MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--~~
~~driver1MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--~~
~~driver2MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--~~
~~driver1MaximumDailyPeriod INTEGER (0..250), --increment: 1h--~~
~~driver2MaximumDailyPeriod INTEGER (0..250), --increment: 1h--~~
~~driver1MaximumDailyDrivingTime INTEGER (910 UNION 1010),~~
~~driver2MaximumDailyDrivingTime INTEGER (910 UNION 1010),~~
~~driver1NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),~~
~~driver2NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),~~
~~driver1RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment: 1min--~~
~~driver2RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment: 1min--~~
~~...~~
~~}~~
~~GNSSDataSheet ::= **SEQUENCE** {~~
~~gnssPosition GeoCoordinates~~

```
        --See Appendix 1 for definition of GeoCoordinates--
    }

    StandardEventDataSheet ::= SEQUENCE{
        events SEQUENCE OF StandardEvent
    }

    PersonalEventDataSheet ::= SEQUENCE{
        events SEQUENCE OF PersonalEvent
    }
END
EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
    EXPORTS ALL ;
    IMPORTS NationAlpha FROM Annex Appendix1 ; --See Annex Appendix 1 for more
information about NationAlpha--

        SecurityBreachEvent ::=SEQUENCE{
            See Appendix 1B for more information --
        }

        RecordingEquipmentFaultType ::= SEQUENCE{
            See Appendix 1B for more information --
        }

        StandardEvent::= CHOICE{
            insertionInvalidCard InsertionOfANonValidCard,
            cardConflict CardConflict,
            timeOverlap TimeOverlap,
            previousSessionNotClosed LastCardSessionNotCorrectlyClosed,
            overSpeeding OverSpeeding,
            powerSupplyInterruption PowerSupplyInterruption,
            comErrorWithRemoteFacility
CommunicationErrorWithTheRemoteCommunicationFacility,
            absenceGNSSPosition AbsenceOfPositionInformationFromGNSSReceiver,
            positionDataError PositionDataError,
            motionDataError MotionDataError,
            vehicleMotionConflict VehicleMotionConflict,
            securityBreachAttempt SecurityBreachAttempt,
            timeConflict TimeConflict,
            ...
        }

        PersonalEvent ::= CHOICE{
            lackOfAppropriateCard DrivingWithoutAnAppropriateCard,
            cardInsertionWhileDriving CardInsertionWhileDriving,
            overSpeeding OverSpeeding,
            ...
        }

        StandardFault ::= CHOICE{
            cardFault CardFault,
            recordingEquipementFault RecordingEquipmentFault,
        ...
        }

        ----------------
        --EVENTS LIST--
        ----------------
        InsertionOfANonValidCard::=SEQUENCE{
```

```
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER
          }

          CardConflict ::= SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER
          }

          TimeOverlap ::=SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
                numberSimilarEvent INTEGER
          }

          DrivingWithoutAnAppropriateCard ::= SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
                numberOfSimilarEvent INTEGER
          }

          CardInsertionWhileDriving ::= SEQUENCE{
                date GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                numberOfSimilarEvents INTEGER
          }

          LastCardSessionNotCorrectlyClosed ::=SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
                oldSession SEQUENCE{
                      beginDate GeneralizedTime,
                      endDate GeneralizedTime,
                      vrn UTF8String,
                      issuingMemberState NationAlpha,
                      cardsGeneration INTEGER,
                }
```

```
        }

        OverSpeeding ::=SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                maximumSpeed INTEGER,
                averageSpeed INTEGER,
                cardType UTF8String,
                cardNumber INTEGER,
                issuingMemberState NationAlpha,
                cardGeneration INTEGER,
                numberOfSimilarEvents INTEGER
        }

        PowerSupplyInterruption ::=SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
                numberOfSimilarEvent INTEGER
        }

        CommunicationErrorWithTheRemoteCommunicationFacility ::=SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
                numberOfSimilarEvent INTEGER
        }

        AbsenceOfPositionInformationFromGNSSReceiver ::= SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
                numberOfSimilarEvent INTEGER
        }

        PositionDataError ::= SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
                numberOfSimilarEvent INTEGER
        }

        MotionDataError ::= SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
```

```
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
                numberOfSimilarEvent INTEGER
        }

        VehicleMotionConflict ::= SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
                numberOfSimilarEvent INTEGER
        }

        SecurityBreachAttempt ::= SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
                numberOfSimilarEvent INTEGER,

SecurityBreachAttempt ::= SEQUENCE{
beginDate GeneralizedTime,
                endDate GeneralizedTime OPTIONAL,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                numberOfSimilarEvent INTEGER,
                typeOfEvent SecurityBreachEvent
                }

        TimeConflict ::= SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
                numberOfSimilarEvent INTEGER
        }

        ---------------
        --FAULTS LIST--
        ---------------

        CardFault ::= SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
        }

        RecordingEquipmentFault ::= SEQUENCE{
                beginDate GeneralizedTime,
```

```
                endDate GeneralizedTime,
                faultType RecordingEquipmentFaultType,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
        }
END
```

Sous-appendice 14

Fonction de communication à distance

Table des matières

1. Introduction

Le présent **sous-**appendice spécifie la conception et les procédures à suivre pour mettre en œuvre la fonction de communication à distance (ci-après la *communication*) ~~conformément aux dispositions de l'article 9 du règlement (UE) nº 165/2014 (le règlement)~~.

DSC_1 ~~Le règlement (UE) n° 165/2014 détermine que l~~**L**e tachygraphe est équipé d'une fonction de communication à distance qui permet aux agents des autorités de contrôle compétentes de lire les informations du tachygraphe embarqué sur les véhicules en circulation à l'aide d'un dispositif d'interrogation à distance (lecteur de communication à distance à des fins de détection précoce [LCDDP]). Il s'agit d'un dispositif d'interrogation à connexion sans fil utilisant des interfaces de communication spécialisée à courte portée (DSRC) dans la bande de fréquences CEN 5,8 GHz.

Il est important de comprendre que cette fonction est conçue uniquement pour servir de filtre afin de sélectionner les véhicules qui feront l'objet d'un contrôle plus approfondi. Cette fonction ne remplace pas la procédure d'inspection formelle ~~définie par les dispositions du règlement (UE) n° 165/2014. Voir le considérant 9 du préambule de ce règlement qui énonce que~~**. La** communication à distance entre le tachygraphe et les autorités chargées des contrôles routiers facilite les contrôles routiers ciblés.

DSC_2 Les *données* sont échangées au moyen de la *communication*, c'est-à-dire l'échange de données sans fil par l'intermédiaire de dispositifs DSRC dans la bande de fréquences 5,8 GHz, conforme au présent **sous-**appendice et testée par rapport aux paramètres pertinents de la norme EN 300 674-1 {Electromagnetic compatibility and Radio spectrum Matters (ERM) ; Road Transport and Traffic Telematics (RTTT) ; Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band ; Part 1: General characteristics and test methods for Road Side Units (RSU) and On -Board Units (OBU)}.

DSC_3 La *communication* est établie avec le dispositif de communication uniquement lorsque l'équipement de l'autorité de contrôle compétente en fait la demande en utilisant des moyens de radiocommunication compatibles (lecteur de communication à distance à des fins de détection précoce [LCDDP]).

DSC_4 Les *données* doivent être sécurisées de manière à garantir leur intégrité.

DSC_5 L'accès aux *données* communiquées est restreint aux autorités de contrôle compétentes ~~autorisées à contrôler les infractions au règlement (CE) n° 561/2006, au règlement (UE) n° 165/2014~~ et aux ateliers dans la mesure où cela s'avère nécessaire pour vérifier le bon fonctionnement du tachygraphe.

DSC_6 Les *données* échangées durant la *communication* sont limitées à celles qui sont nécessaires aux fins des contrôles routiers ciblant les véhicules dont le tachygraphe a pu être manipulé ou faire l'objet d'une utilisation abusive.

DSC_7 L'intégrité et la sécurité des *données* sont assurées par la sécurisation des *données* au sein de l'unité embarquée sur le véhicule (UEV) et par l'utilisation exclusive du dispositif de communication à distance sans fil DSRC dans la bande de fréquence 5,8 GHz pour transférer les données utiles sécurisées et les données relatives à la sécurité (voir ~~4.4.4~~**5.4.4**). Cela signifie que seul le personnel autorisé des autorités de contrôle compétentes dispose des moyens d'interpréter les données reçues par le canal de *communication* et de vérifier leur authenticité (voir **sous-**appendice 11, Mécanismes de sécurité communs).

DSC_8 Les *données* doivent contenir un horodatage indiquant l'heure de leur dernière mise à jour.

DSC_9 Le contenu des données relatives à la sécurité est connu uniquement des autorités de contrôle compétentes et des parties avec lesquelles elles partagent ces informations et ne relève pas de la *communication*, visée au présent **sous-**appendice, si ce n'est que la *communication* prévoit le transfert d'un paquet de données relatives à la sécurité avec chaque paquet de données utiles.

DSC_10 L'architecture et l'équipement spécifiés dans le présent sous-appendice doivent permettre d'extraire d'autres types de données (par exemple, concernant le poids à bord).

DSC_11 ~~Par souci de précision, conformément aux dispositions du règlement (UE) n° 165/2014 (article 7),~~ **Les** données concernant l'identité du conducteur ne sont pas transmises par la *communication*.

2. Champ d'application

Le présent **sous-**appendice vise à préciser la manière dont les agents des autorités de contrôle compétentes utilisent la communication sans fil DSRC 5,8 GHz spécifiée pour obtenir à distance des données (les *données*) d'un véhicule ciblé, ces données devant servir à déterminer si ce véhicule est en infraction avec le ~~règlement (UE) n° 165/2014~~ **présent Accord** et s'il faut envisager de l'arrêter afin de procéder à un contrôle plus poussé.

~~Le règlement (UE) n° 165/2014 exige que~~ **Les** données collectées se limitent à celles qui permettent de détecter une infraction éventuelle ou qui s'y rapportent~~, conformément à l'article 9 du règlement (UE) n° 165/2014~~.

Dans un tel cas de figure, la durée de communication est limitée parce que la *communication* est ciblée et qu'elle se fait à courte portée. Par ailleurs, les autorités de contrôle compétentes peuvent utiliser les moyens de communication servant au contrôle à distance des tachygraphes (RTM) pour d'autres applications, comme le contrôle du poids maximal et des dimensions maximales des poids lourds ~~définis dans la directive (UE) 2015/719~~. Ces opérations peuvent être distinctes du contrôle à distance des tachygraphes ou consécutives à celui-ci, à la discrétion des autorités de contrôle compétentes.

Le présent **sous-**appendice spécifie :

- L'équipement, les procédures et les protocoles de communication à utiliser pour la *communication* ;
- Les normes et les règlements auxquels l'équipement radio doit satisfaire ;
- La présentation des *données* à l'équipement de *communication* ;
- Les procédures de demande et de téléchargement et la séquence des opérations ;
- Les *données* à transférer ;
- L'interprétation possible des *données* transmises via *la communication* ;
- Les dispositions relatives aux données de sécurité liées à la *communication* ;
- La mise à disposition des *données* aux autorités de contrôle compétentes ;
- La façon dont le *lecteur de communication à distance à des fins de détection précoce* (LCDDP) peut demander plusieurs types de données relatifs au fret et à la flotte.

Il convient de préciser que le présent **sous-**appendice ne spécifie pas :

- La collecte et la gestion des *données* dans l'UEV ~~(qui dépendent de la conception du produit sauf mention contraire dans le règlement (UE) n° 165/2014)~~ ;
- La forme de présentation des données collectées à l'agent des autorités de contrôle compétentes ou les critères utilisés par celles-ci pour décider quel véhicule arrêter ~~(qui dépendent de la conception du produit, sauf s'il y est fait mention ailleurs dans le règlement (UE) n° 165/2014 ou dans une décision des autorités de contrôle compétentes)~~. Précision : la *communication* met uniquement les *données* à la disposition des autorités de contrôle compétentes afin qu'elles puissent prendre des décisions éclairées ;
- Les dispositions relatives à la sécurité des données (telles que le chiffrement) et de leur contenu (qui sont énoncées ~~à l'appendice~~ **au sous-appendice** 11, Mécanismes de sécurité communs) ;

- Le détail de tous les types de données autres que les données RTM pouvant être obtenus à l'aide de la même architecture et du même équipement ;
- Le détail du fonctionnement et de la gestion des relations entre l'UEV et le DSRC-UEV ou du fonctionnement au sein du DSRC-UEV (autre que dans le but de fournir les *données* en réponse à la demande d'un LCDDP).

3. Abréviations, définitions et notations

Dans le présent **sous-**appendice, les abréviations et définitions suivantes sont utilisées :

Antenne Dispositif électrique qui convertit l'énergie électrique en ondes radio et inversement, utilisé avec un émetteur ou un récepteur radio. En fonctionnement, un émetteur radio fournit un courant électrique oscillant à une fréquence radio aux bornes de l'antenne. L'antenne rayonne et émet l'énergie du courant électrique sous forme d'ondes électromagnétiques (ondes radio). En mode réception, une antenne capte une part de l'énergie émise par une onde électromagnétique pour produire une tension très faible à ses bornes, qui est amplifiée par un récepteur.

Communication Échange d'informations et de données entre un DSRC-LCDDP et un DSRC-UEV conformément au chapitre 5 et selon une relation maître-esclave en vue d'obtenir les données.

Données Données sécurisées adoptant une structure définie (voir **5.4.4**) demandées par le DSRC-LCDDP et fournies par le DSRC-UEV à l'aide d'une liaison DSRC dans la bande 5,8 GHz, comme prévu au chapitre 5.

~~Règlement (UE) n° 165/2014~~ ~~Règlement (UE) n° 165/2014 du Parlement Européen et du Conseil du 4 février 2014 relatif aux tachygraphes dans les transports routiers, abrogeant le règlement (CEE) n° 3821/85 du Conseil concernant l'appareil de contrôle dans le domaine des transports par route et modifiant le règlement (CE) n° 561/2006 du Parlement européen et du Conseil relatif à l'harmonisation de certaines dispositions de la législation sociale dans le domaine des transports par route.~~

AID Identificateur d'application

BLE Bluetooth Low Energy

BST Tableau de service de balise *(Beacon Service Table)*

CRC Contrôle de redondance cyclique

DSRC Communication spécialisée à courte portée

DSRC-LCDDP Dispositif DSRC du lecteur de communication à distance à des fins de détection précoce

DSRC-UEV Dispositif DSRC de l'unité embarquée sur le véhicule. Il s'agit du « dispositif de détection précoce à distance » défini à ~~l'annexe~~ **l'appendice** 1C.

EID Identificateur d'élément

LLC Contrôle de liaison logique (*Logical Link Control*)

LPDU Unité de données de protocole LLC (*LLC Protocol Data Unit*)

OBU Dispositif installé à bord du véhicule *(On-Board Unit)*

PDU Unité de données de protocole (*Protocol Data Uni*)

LCDDP	Lecteur de communication à distance à des fins de détection précoce. Il s'agit du « lecteur de communication à distance à des fins de détection précoce » défini à ~~l'annexe~~ **l'appendice** 1C.
RSU	Dispositif installé en bord de route (*Roadside Unit*)
RTM	Contrôle à distance des tachygraphes *(Remote Tachograph Monitoring)*
LCDDP-MS	Module de sécurité du lecteur de communication à distance à des fins de détection précoce
TARV	Applications télématiques collaboratives pour véhicules de fret commercial réglementé (série de normes ISO 15638)
UEV	Unité embarquée sur le véhicule *(VU, en anglais)*
UEV-MU	Mémoire utile de l'UEV
UEV-MS	Module de sécurité de l'UEV
VST	Tableau de service de véhicule *(Vehicle Service Table)*

La spécification définie au présent **sous-**appendice renvoie aux règlements et normes suivants, et dépend d'eux en tout ou en partie. Les normes ou leurs clauses applicables sont énoncées dans le présent **sous-**appendice. En cas de conflit, les dispositions du présent **sous-**appendice prévalent. En cas de conflit qu'aucune spécification du présent **sous-**appendice ne résout, le fonctionnement conformément à la recommandation ERC 70-03 (et testé par rapport aux paramètres pertinents de la norme EN 300 674-1)[15] prévaut, suivi, dans l'ordre, par[16] les normes EN 12795, EN 12253 EN 12834 et EN 13372, 6.2, 6.3, 6.4 et 7.1.

Dans le présent **sous-**appendice, les ~~règlements et~~ normes suivantes sont mentionnées :

~~Règlement (UE) n° 165/2014 du Parlement européen et du Conseil du 4 février 2014 relatif aux tachygraphes dans les transports routiers, abrogeant le règlement (CEE) n° 3821/85 du Conseil concernant l'appareil de contrôle dans le domaine des transports par route et modifiant le règlement (CE) n° 561/2006 du Parlement européen et du Conseil relatif à l'harmonisation de certaines dispositions de la législation sociale dans le domaine des transports par route.~~

~~Règlement (UE) n° 561/2006 du Parlement européen et du Conseil du 15 mars 2006 relatif à l'harmonisation de certaines dispositions de la législation sociale dans le domaine des transports par route, modifiant les règlements (CEE) n° 3821/85 et (CE) n° 2135/98 du Conseil et abrogeant le règlement (CEE) n° 3820/85 du Conseil (Texte présentant de l'intérêt pour l'EEE).~~

1. ERC 70-03 CEPT : Recommandation CCE 70-03 relative à l'utilisation des dispositifs à courte portée (DCP) ;

2. ISO 15638 Systèmes intelligents de transport − Cadre pour applications télématiques collaboratives pour véhicules de fret commercial réglementé (TARV) ;

3. EN 300 674-1 Electromagnetic compatibility and Radio spectrum Matters (ERM) ; Road Transport and Traffic Telematics (RTTT) ; Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band ; Part 1: General characteristics and test methods for Road Side Units (RSU) and On-Board Units (OBU).

[15] **Compte tenu des avancées scientifiques et technologiques, dans les cas où aucune norme ISO n'est spécifiée, mais qu'une norme régionale est indiquée, les autorités compétentes des Parties contractantes peuvent appliquer d'autres règles techniques, à condition que celles-ci ne soient pas moins strictes à celles prévues dans les normes applicables.**

[16] **Conversion en norme ISO prévue sur une période de cinq ans.**

4. EN 12253 Road transport and traffic telematics − Dedicated short-range communication − Physical layer using microwave at 5.8 GHz ;

5. EN 12795 Road transport and traffic telematics − Dedicated short-range communication − Data link layer: medium access and logical link control ;

6. EN 12834 Road transport and traffic telematics − Dedicated short-range communication − Application layer ;

7. EN 13372 Road transport and traffic telematics − Dedicated short-range communication − Profiles for RTTT applications ;

8. ISO 14906 Perception du télépéage − Définition de l'interface d'application relative aux communications dédiées à courte portée.

4. Cas de figure opérationnels

4.1 Vue d'ensemble

~~Le règlement (UE) n° 165/2014 prévoit des cas de figure spécifiques et contrôlés encadrant *la communication*.~~ Les cas de figure dans le cadre desquels la *communication* doit être utilisée sont les suivants :

« Profil de communication 1 : contrôle routier à l'aide d'un lecteur de communication à distance à des fins de détection précoce, sans fil et à courte portée, qui entraîne un contrôle routier physique (maître-:-esclave) ;

Profil de lecteur 1a : à l'aide d'un lecteur de communication à distance à des fins de détection précoce qui est dirigé manuellement ou installé et dirigé temporairement en bord de route ;

Profil de lecteur 1b : à l'aide d'un lecteur de communication à distance à des fins de détection précoce qui est installé et dirigé à bord d'un véhicule ».

4.1.1 Conditions préalables au transfert de données par l'intermédiaire de l'interface DSRC dans la bande de fréquence 5,8 GHz

Remarque : pour comprendre le contexte dans lequel s'inscrivent ces conditions préalables, le lecteur est invité à consulter la figure 14.3 ci-dessous.

4.1.1.1 Données stockées dans l'UEV

DSC_12 L'UEV est chargée de sauvegarder et d'actualiser toutes les 60 secondes les données qu'elle est tenue de stocker, sans recourir à la fonction de communication DSRC. Les moyens pour y parvenir sont internes à l'UEV. Ils sont définis ~~par le règlement (UE) n° 165/2014, annexe~~ **à la** section 3.19 **de l'appendice 1C** ~~« communication à distance pour les contrôles routiers ciblés »~~ et ne sont pas spécifiés dans le présent **sous-**appendice.

4.1.1.2 Données communiquées au dispositif DSRC-UEV

DSC_13 L'UEV est chargée d'actualiser les données tachygraphiques DSRC (les *données*) chaque fois qu'elle actualise les données qu'elle stocke, selon la fréquence définie à la section 4.1.1.1 (DSC_12), sans recourir à la fonction de communication DSRC.

DSC_14 Les données de l'UEV servent de base à l'alimentation et à l'actualisation des *données*. Les moyens pour y parvenir sont définis à ~~l'annexe~~ **l'appendice** 1C, section 3.19 (Communication à distance pour les contrôles routiers ciblés). En l'absence de précision, ces moyens dépendent de la conception du produit et ne sont pas décrits dans le présent **sous-**appendice. En ce qui concerne la conception de la connexion entre le dispositif DSRC-UEV et l'UEV, il convient de consulter la section 5.6.

4.1.1.3 Contenu des données

DSC_15 Le contenu et la structure des *données* sont tels qu'une fois déchiffrées, celles-ci sont structurées et mises à disposition sous la forme et selon la structure spécifiées à la section 5.4.4 du présent **sous-**appendice (Structures des données).

4.1.1.4 Présentation des données

DSC_16 Les *données*, régulièrement actualisées conformément aux procédures définies à la section 4.1.1.1, doivent être sécurisées avant d'être présentées au *DSRC-UEV* et doivent être présentées avec une valeur de concept de données sécurisées en vue de leur stockage temporaire dans le *DSRC-UEV* en tant que version actuelle des *données*. Ces données sont transférées de l'*UEV-MS* au à l'*UEV-MU* de la fonction DSRC. L'*UEV-MS* et l'*UEV-MU* sont des fonctions et ne sont pas nécessairement des entités physiques. La forme des instances physiques exécutant ces fonctions relève de la conception du produit, sauf indication contraire ailleurs dans ~~le règlement UE n° 165/2014~~ **l'appendice 1C.**

4.1.1.5 Données de sécurité

DSC_17 Les données de sécurité (***DSRC****securityData*), comprenant les données requises par le *LCDDP* pour déchiffrer les *données*, sont communiquées conformément aux dispositions ~~de l'appendice~~ **du sous-appendice** 11 (Mécanismes de sécurité communs) ~~et sont présentées comme une valeur de concept de données~~ en vue de leur stockage temporaire dans le DSRC-UEV en tant que version actuelle des ***DSRC****securityData*, sous la forme définie **à la section 5.4.4** du présent **sous-**appendice~~, section 5.4.4~~.

4.1.1.6 Données de l'UEV-MU disponibles pour le transfert par l'intermédiaire de l'interface DSRC

DSC_18 Le concept de données qui doit toujours être disponible dans l'UEV-MU de la fonction DSRC en vue de son transfert immédiat sur demande du *LCDDP* est défini à la section 5.4.4, qui contient les spécifications complètes du module ASN.1.

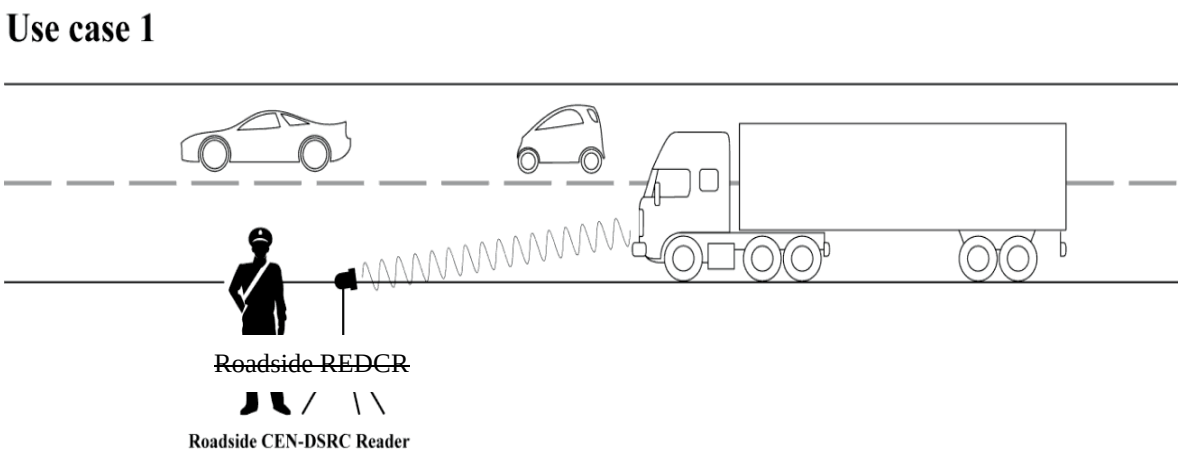
Présentation générale du profil de communication n° 1

Ce profil couvre le cas de figure dans lequel un agent des autorités de contrôle compétentes utilise un lecteur de communication à distance à des fins de détection précoce à courte portée (interfaces DSRC 5,8 GHz fonctionnant conformément à la recommandation ERC 70-03 et testées par rapport aux paramètres pertinents de la norme EN 300 674-1 comme décrit au chapitre 0) (le *LCDDP*) pour identifier à distance un véhicule ~~en infraction potentielle au règlement (UE) n° 165/2014~~. Une fois le véhicule identifié, l'agent décide si le véhicule doit être intercepté.

4.1.2 Profil 1a : à l'aide d'un lecteur de communication à distance à des fins de détection précoce dirigé manuellement ou installé et dirigé temporairement en bord de route

Dans ce cas de figure, l'agent des autorités de contrôle compétentes est placé sur le bord de la voie et utilise un *LCDDP* manuel, posé sur un tripode ou sur une structure portable similaire positionné au bord de la voie et orienté vers le centre du pare-brise du véhicule ciblé. L'interrogation est effectuée au moyen d'interfaces DSRC 5,8 GHz fonctionnant conformément à la recommandation ERC 70-03 et testée par rapport aux paramètres pertinents de la norme EN 300 674-1, comme décrit au chapitre 5 (voir fig. 14.1, cas de figure n° 1).

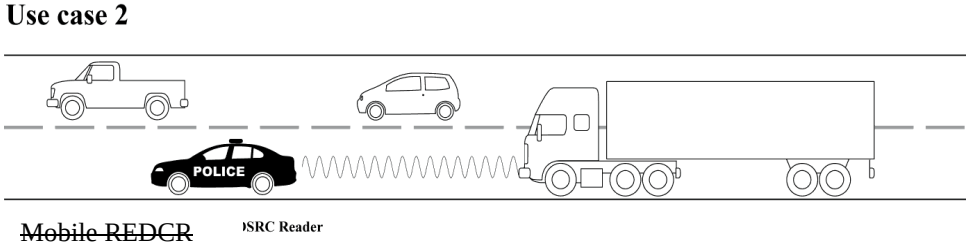
Figure 14.1
Interrogation en bord de route au moyen d'une interface DSRC 5,8 GHz



4.1.3 Profil 1b : à l'aide d'un lecteur de communication à distance à des fins de détection précoce (LCDDP) installé et dirigé à bord d'un véhicule

Dans ce cas, l'agent des autorités de contrôle compétentes se trouve à l'intérieur d'un véhicule en circulation et soit il utilise un *LCDDP* manuel et portable depuis le véhicule en le pointant vers le centre du pare-brise du véhicule ciblé, soit le *LCDDP* est installé dans ou sur le véhicule de manière à être dirigé vers le centre du pare-brise du véhicule ciblé lorsque le véhicule à bord duquel se trouve le LCDDP est dans une position particulière par rapport au véhicule ciblé (par exemple directement devant celui-ci dans un flux de circulation). L'interrogation est effectuée au moyen d'interfaces DSRC 5,8 GHz fonctionnant conformément à la recommandation ERC 70-03 et testée par rapport aux paramètres pertinents de la norme EN 300 674-1, comme décrit au chapitre 0 (voir fig. 14.2, cas de figure nº 2).

Figure 14.2
Interrogation depuis un véhicule au moyen d'une interface DSRC 5,8 GHz



4.2 Sécurité et intégrité

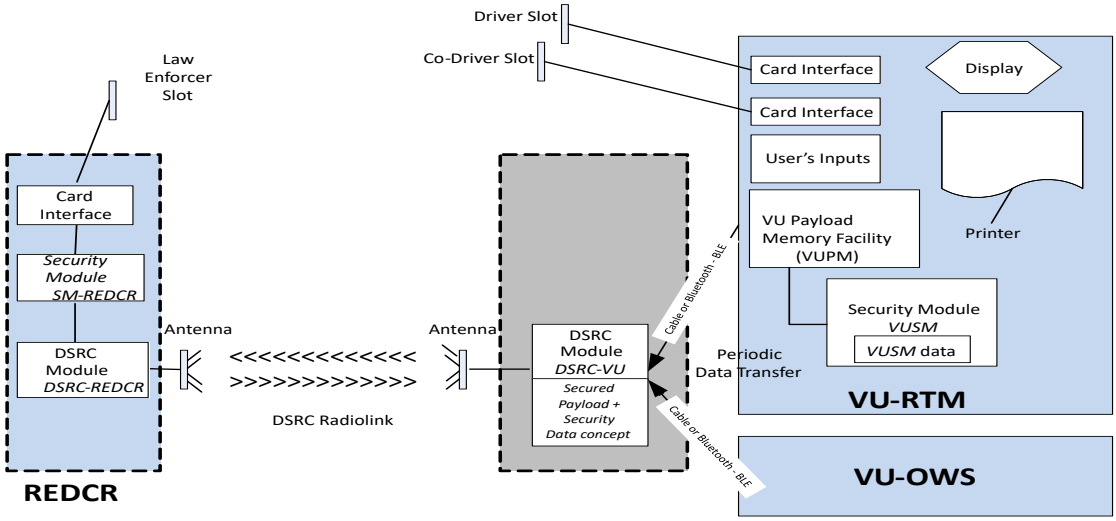
Afin de permettre la vérification de l'authenticité et de l'intégrité des données téléchargées dans le cadre de la procédure de communication à distance, les *données* sécurisées font l'objet d'une vérification et d'un déchiffrement conformément ~~à l'appendice~~ **au sous-appendice** 11 (Mécanismes de sécurité communs).

5. Conception et protocoles de la communication à distance

5.1 Conception

La conception de la fonction de communication à distance du tachygraphe intelligent est illustrée à la figure 14.3.

Figure 14.3
Conception de la fonction de communication à distance



DSC_19 Les fonctions suivantes sont situées dans l'UEV :

- Module de sécurité (*UEV-MS*). Cette fonction présente dans l'UEV est responsable de la sécurisation des *données* à transmettre depuis le *DSRC-UEV* à l'agent des autorités de contrôle compétentes par communication à distance ;
- Les données sécurisées sont stockées dans la mémoire de l'UEV-MS. La section 4.1.1.1 (DSC_12) prévoit la fréquence à laquelle l'UEV chiffre et renouvelle le concept RTMdata (qui comprend les valeurs de concept des données utiles et des données de sécurité déterminées dans le présent **sous-**appendice) stocké dans la mémoire du DSRC-UEV. Le fonctionnement du module de sécurité est défini ~~à l'appendice~~ **au sous-appendice** 11 (Mécanismes de sécurité communs) et n'entre pas dans le champ d'application du présent **sous-**appendice, si ce n'est que toute modification des données de l'UEV-MS doit entraîner la mise à jour du dispositif de communication de l'UEV ;
- La communication entre l'UEV et le DSRC-UEV peut être filaire ou de type Bluetooth Low Energy (BLE). LE DSRC-UEV peut être intégré physiquement à l'antenne sur le pare-brise du véhicule, interne à l'UEV ou situé à un point intermédiaire ;
- Le DSRC-UEV doit disposer d'une source d'alimentation électrique fiable à tout moment. Les moyens d'alimentation relèvent d'un choix de conception ;
- La mémoire du DSRC-UEV est non volatile, afin de préserver les données stockées dans le DSRC-UEV, y compris lorsque le contact du véhicule est coupé ;
- Si la communication entre l'UEV et le DSRC-UEV s'établit via BLE et que l'alimentation provient d'une batterie non rechargeable, l'alimentation du DSRC-UEV doit être remplacée à chaque inspection périodique. En outre, le fabricant du DSRC-UEV est tenu de veiller à ce que l'alimentation électrique perdure d'une inspection périodique à l'autre et garantisse un accès normal aux données au moyen d'un LCDDP durant toute la période sans anomalie ni interruption ;
- Mémoire utile RTM de l'UEV (*UEV-MU*). Cette fonction présente dans l'UEV est chargée de fournir et d'actualiser les *données.* Le contenu des *données* (TachographPayload) est défini aux sections 5.4.4 et 5.4.5 ci-après et mis à jour à la fréquence indiquée à la section 4.1.1.1 (DSC_12) ;
- DSRC-UEV. Il s'agit de la fonction intégrée à l'antenne ou connectée à celle-ci, qui communique avec l'UEV grâce à une connexion filaire ou sans fil (BLE), qui détient les données actuelles (*données* de l'*UEV-MU*) et qui gère la réponse à une interrogation par l'intermédiaire de l'interface DSRC 5,8 GHz. Toute déconnexion du

dispositif DSRC ou interférence avec le fonctionnement de celui-ci pendant l'exploitation normale du véhicule constitue une infraction au ~~règlement (UE) n° 165/2014~~ **présent Accord** ;

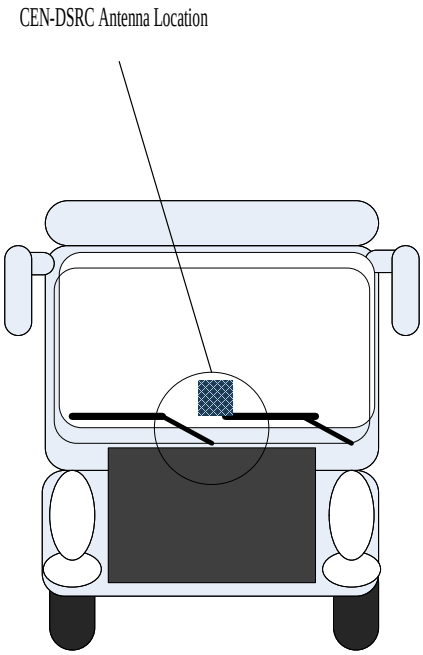
- Le module de sécurité du LCDDP (*LCDDP-MS*) est la fonction servant à déchiffrer les données en provenance de l'UEV et à en vérifier l'intégrité. Les moyens pour y parvenir sont définis ~~à l'appendice~~ **au sous-appendice** 11 (Mécanismes de sécurité communs). Ils ne sont pas définis dans le présent **sous-**appendice ;
- Le dispositif DSRC du LCDDP (*DSRC-LCDDP*) comprend un émetteur-récepteur de 5,8 GHz ainsi que le micrologiciel et le logiciel associés qui gèrent la *communication* avec le *DSRC-UEV* conformément au présent **sous-**appendice ;
- Le *DSRC-LCDDP* interroge le *DSRC-UEV* du véhicule ciblé et obtient les *données* (les *données* actuelles de l'*UEV-MU* du véhicule ciblé) grâce à la liaison DSRC, puis traite et stocke les données reçues dans son *LCDDP-MS* ;
- L'antenne DSRC-UEV est placée de manière à optimiser la communication DSRC entre le véhicule et l'antenne **du lecteur installé** en bord de route ~~(en général, au centre ou à proximité du centre du pare-brise du véhicule)~~ **lorsque le lecteur est installé à 15 mètres de distance en amont du véhicule et à 2 mètres de hauteur, et vise le centre horizontal et vertical du pare-brise.** Pour les véhicules légers, une installation **correspondante** sur la partie supérieure du pare-brise convient. **Pour tous les autres véhicules, l'antenne DSRC est installée soit au niveau de la partie inférieure, soit au niveau de la partie supérieure du pare-brise ;**
    - Aucun objet métallique (par exemple, badges, autocollants, bandes (teintées) anti-reflets, pare-soleil, essuie-glace au repos) ne doit se trouver à proximité ou devant l'antenne, car il pourrait interférer avec la communication ;
    - L'antenne est installée de sorte que son axe de visée soit à peu près parallèle avec la surface de la route.

DSC_20 L'antenne et la *communication* fonctionnent conformément à la recommandation ERC 70-03 et sont testées par rapport aux paramètres pertinents de la norme EN 300 674-1, comme prévu au chapitre **45**. L'antenne et la *communication* peuvent mettre en œuvre des techniques d'atténuation contre le risque d'interférence sans fil comme décrit dans le rapport ECC 228, en utilisant notamment des filtres dans la communication CEN DSRC 5,8 GHz.

DSC_21 L'antenne DSRC est connectée au DSRC-UEV soit directement à l'intérieur du module installé sur le pare-brise ou à proximité du pare-brise, soit par un câble spécialement conçu pour rendre difficile toute déconnexion illégale. Toute déconnexion de l'antenne ou interférence avec son fonctionnement constitue une infraction ~~au règlement (UE) n° 165/2014~~ **au présent Accord**. Le masquage délibéré ou tout autre agissement qui nuit à la performance opérationnelle de l'antenne constitue également une infraction ~~au règlement (UE) n° 165/2014~~ **au présent Accord**.

DSC_22 Le facteur de forme de l'antenne n'est pas défini et relève d'une décision commerciale, pour autant que le DSRC-UEV installé satisfasse aux exigences de conformité énoncées au chapitre 5 ci-après. L'antenne doit être positionnée comme défini au point DSC_19 et ~~comme illustré à la figure 14.4 (ligne ovale) et~~ doit **assurer** efficacement les fonctions prévues dans les cas de figure décrits aux sections ~~3.1.2 et 3.1.3~~ **4.1.2 et 4.1.3**.

Figure 14.4
Exemple de positionnement de l'antenne DSRC 5,8 GHz sur le pare-brise de véhicules réglementés



Le facteur de forme du *LCDDP* et de son antenne varie en fonction des caractéristiques du lecteur (installé sur un tripode, tenu à la main, installé dans un véhicule, etc.) et du mode opératoire adopté par l'agent des autorités de contrôle compétentes.

Une fonction d'affichage et/ou de notification permet de présenter les résultats obtenus à l'aide de la fonction de communication à distance avec l'agent des autorités de contrôle compétentes. Il peut s'agir d'un affichage sur écran, d'une sortie imprimée, d'un signal audio ou d'une combinaison de ces notifications. La forme de cet affichage et/ou de cette notification dépend des exigences des agents des autorités de contrôle compétentes et de la conception de l'équipement. Elle n'est pas spécifiée dans le présent **sous-**appendice.

DSC_23 La conception et le facteur de forme du *LCDDP* dépendent de la conception commerciale, compte tenu de la recommandation ERC 70-03 et des spécifications en matière de conception et de performance définies dans le présent **sous-**appendice (sect. 5.3.2). Le marché dispose de fait d'une souplesse optimale pour concevoir et fournir des équipements permettant de répondre aux diverses situations d'interrogation auxquelles est confrontée toute autorité de contrôle compétente.

DSC_24 La conception et le facteur de forme du *DSRC-UEV* ainsi que son positionnement à l'intérieur ou à l'extérieur de l'UEV dépendent de la conception commerciale, compte tenu de la recommandation ERC 70-03 et des spécifications en matière de conception et de performance définies dans le présent **sous-**appendice (sect. 5.3.2) et dans la présente clause (5.1).

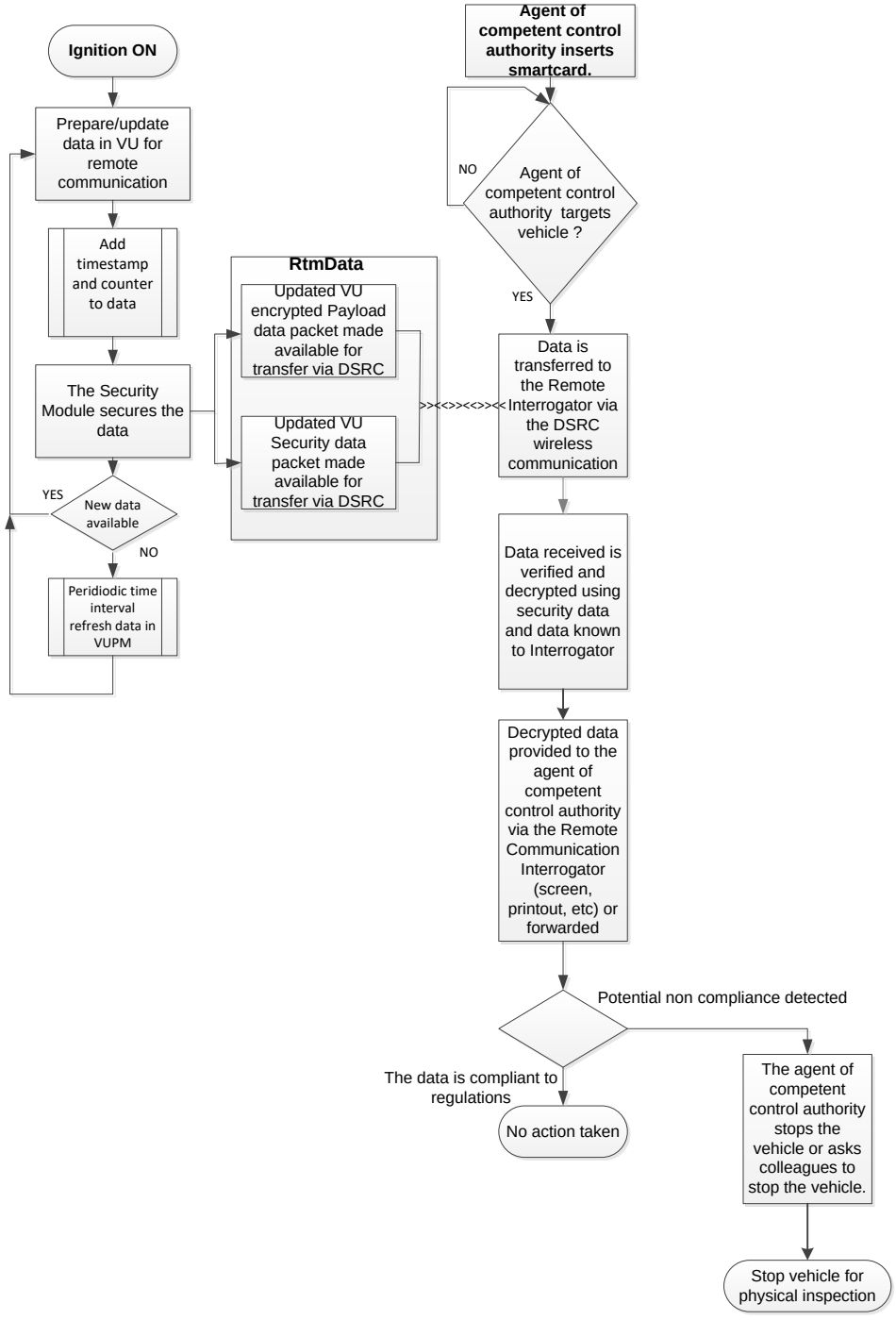
DSC_25 Toutefois, le *DSRC-UEV* doit être en mesure d'accepter des valeurs de concept de données provenant d'autres équipements de véhicule intelligents (par exemple, un système de pesage embarqué) et transmises au moyen d'une connexion et de protocoles ouverts et normalisés, pourvu que de tels concepts de données soient identifiés par des identificateurs d'application et des noms de fichiers connus et uniques, et à condition que les instructions d'utilisation desdits protocoles soient mises à la disposition ~~de la Commission européenne~~ **du laboratoire compétent pour les essais d'interopérabilité** et disponibles sans frais pour les fabricants des équipements pertinents.

5.24.2 Déroulement des opérations

5.2.15.1 Opérations

Le déroulement des opérations est illustré dans la figure 14.5.

Figure 14.5
Déroulement des opérations de la fonction de communication à distance



Les étapes sont décrites ci-après :

a) Lorsque le véhicule est en marche (contact enclenché), le tachygraphe fournit des données à l'UEV. La fonction de l'UEV prépare les *données* pour la fonction de communication à distance (chiffrée) et actualise l'UEV-MU au sein de la mémoire du DSRC-UEV (tel que spécifié aux sections 4.1.1.1 et 4.1.1.2). Les *données* collectées sont formatées comme défini aux sections 5.4.4 et 5.4.5 ci-dessous ;

b) Chaque fois que les *données* sont actualisées, l'horodatage indiqué dans le concept de données de sécurité doit être actualisé ;

c) La fonction *UEV-MS* sécurise les données en appliquant les procédures prévues ~~à l'appendice~~ **au sous-appendice** 11 ;

d) À chaque mise à jour (voir sect. 4.1.1.1 et 4.1.1.2), les *données* sont transférées au DSRC-UEV où elles remplacent toutes les données antérieures afin que les données actualisées (les *données*) soient toujours disponibles en cas d'interrogation par un *LCDDP*. Lorsqu'elles sont fournies par l'UEV au DSRC-UEV, les données doivent pouvoir être identifiées par le nom de fichier RtmData ou par des identificateurs d'application et d'attribut ;

e) Si un agent des autorités de contrôle compétentes souhaite cibler un véhicule et recueillir les *données* de ce véhicule, il commence par insérer sa carte à puce dans le *LCDDP* pour établir la *communication* et permettre au *LCDDP-MS* de vérifier son authenticité et de déchiffrer les données ;

f) L'agent de l'autorité de contrôle compétente vise ensuite un véhicule et procède à la demande de données par l'intermédiaire de la communication à distance. Le *LCDDP* ouvre une session d'interface DSRC 5,8 GHz avec le DSRC-UEV du véhicule ciblé et demande les *données*. Les *données* sont transférées vers le *LCDDP* grâce au système de communication sans fil en tant qu'attribut DSRC à l'aide du service d'application GET, comme défini à la section 5.4. L'attribut contient les valeurs des données utiles chiffrées et les données relatives à la sécurité DSRC ;

g) Le *LCDDP* analyse les données qui sont ensuite communiquées à l'agent de l'autorité de contrôle compétente ;

h) L'agent de l'autorité de contrôle compétente utilise les données pour prendre la décision d'arrêter ou non le véhicule en vue d'une inspection approfondie ou pour demander à un autre agent de l'autorité de contrôle compétente d'arrêter le véhicule.

5.2.2 Interprétation des données reçues via la communication DSRC

DSC_26 Les données reçues par l'intermédiaire de l'interface 5,8 GHz ont la signification et la portée indiquées aux sections 5.4.4 et 5.4.5 ci-dessous et uniquement celles-là, et doivent être interprétées au regard des objectifs qui y sont définis. Conformément aux dispositions ~~du règlement (UE) n° 165/2014~~ **de la législation en vigueur dans chaque Partie contractante**, les *données* servent uniquement à fournir les informations pertinentes à une autorité de contrôle compétente afin de l'aider à déterminer quel véhicule intercepter pour une inspection physique et doivent ensuite être détruites conformément ~~à l'article 9 du règlement (UE) n° 165/2014~~ **à la législation en vigueur dans chaque Partie contractante**.

5.3 Paramètres de l'interface DSRC physique pour la communication à distance

5.3.1 Contraintes d'emplacement

DSC_27 L'interrogation à distance de véhicules à l'aide d'une interface DSRC 5,8 GHz ne doit pas se faire dans un rayon de 200 mètres autour d'un portique DSRC 5,8 GHz opérationnel.

5.3.2 Paramètres de liaisons descendante et montante

DSC_28 L'équipement servant au contrôle à distance des tachygraphes doit être conforme à la recommandation ERC 70-03 et fonctionner selon celle-ci. Il doit également respecter les paramètres définis aux tableaux 14.1 et 14.2 ci-dessous.

DSC_29 En outre, pour garantir la compatibilité avec les paramètres opérationnels d'autres systèmes DSRC 5,8 GHz normalisés, l'équipement utilisé pour le contrôle à distance des tachygraphes doit être conforme aux paramètres définis dans les normes EN 12253 et EN 13372.

À savoir :

Tableau 14.1
Paramètres de liaison descendante

Point	*Paramètre*	*Valeur(s)*	*Remarque*
D1	Fréquences porteuses descendantes	Le LCDDP dispose de quatre possibilités : 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	Dans le cadre de la norme ERC 70-03. Les fréquences porteuses peuvent être sélectionnées par le responsable de la mise en œuvre du système de contrôle routier et ne doivent pas nécessairement être connues au niveau du DSRC-UEV (conformément aux normes EN 12253 et EN 13372)
D1a(*)	Tolérance pour la fréquence porteuse	±5 ppm	**(**conformément à la norme EN 12253**)**
D2(*)	Masque spectral d'émission du RSU (LCDDP)	Dans le cadre de la norme ERC 70-03. Le LCDDP doit correspondre à la classe B,C telle que définie dans la norme EN 12253. Aucune autre exigence spécifique prévue dans ~~la présente annexe~~ **le présent appendice**	Paramètre utilisé pour maîtriser les interférences entre interrogateurs à proximité (comme défini dans les normes EN 12253 et EN 13372).
D3	Gamme de fréquences minimale de l'OBU (DSRC-UEV)	5,795 − 5,815 GHz	(conformément à la norme EN 12253)
D4(*)(**)	P.I.R.E. maximale	Dans le cadre de la norme ERC 70-03 (sans autorisation) et de la réglementation nationale Maximum +33 dBm	(conformément à la norme EN 12253)
D4a	Masque angulaire P.I.R.E.	Conformément à la spécification déclarée et publiée du concepteur de l'interrogateur	**(**conformément à la norme EN 12253**)**
D5	Polarisation	Circulaire antihoraire	**(**conformément à la norme EN 12253**)**
D5a	Polarisation croisée	XPD : Dans la ligne de visée : (LCDDP) RSU t ≥15 dB (DSRC-UEV) OBU r ≥10 dB Dans la zone -3 dB : (LCDDP) RSU t ≥10 dB (DSRC-UEV) OBU r ≥ 6 dB	**(**conformément à la norme EN 12253**)**
D6(*)	Modulation	Modulation d'amplitude à deux niveaux	**(**conformément à la norme EN 12253**)**
D6a(*)	Indice de modulation	0,5 ... 0,9	**(**conformément à la norme EN 12253**)**

Point	*Paramètre*	*Valeur(s)*	*Remarque*
D6b	Diagramme de l'œil	≥90 % (temps)/≥85 % (amplitude)	
D7(*)	Codage de données	FM0 Le bit « 1 » ne présente de transitions qu'au début et à la fin de l'intervalle de bits. Le bit « 0 » présente une transition supplémentaire au milieu de l'intervalle de bits par rapport au bit « 1 ».	**(**conformément à la norme EN 12253**)**
D8(*)	Débit binaire	500 kBit/s	**(**conformément à la norme EN 12253**)**
D8a	Tolérance de l'horloge bit	Mieux que ±100 ppm	(conformément à la norme EN 12253)
D9(*)	Taux d'erreur binaire pour la communication	$\leq 10^{-6}$ si la puissance incidente au niveau de l'OBU (DSRC-UEV) se situe dans la plage donnée par [D11a à D11b].	**(**conformément à la norme EN 12253**)**
D10	Signal déclenchant l'activation de l'OBU (DSRC-UEV)	L'OBU (DSRC-UEV) est activé à la réception d'une trame comportant 11 octets ou plus (préambule inclus)	Aucune structure particulière n'est nécessaire pour le signal d'activation. Le DSRC-UEV peut être activé à la réception d'une trame comportant moins de 11 octets. (conformément à la norme EN 12253)
D10a	Temps de démarrage maximal	≤5 ms	**(**conformément à la norme EN 12253**)**
D11	Zone de communication	Espace dans lequel un taux d'erreur binaire conforme à D9a est atteint	**(**conformément à la norme EN 12253**)**
D11a(*)	Limite de puissance (supérieure) pour la communication.	-24 dBm	**(**conformément à la norme EN 12253**)**
D11b(*)	Limite de puissance (inférieure) pour la communication.	Puissance incidente : -43 dBm (ligne de visée) -41 dBm (dans la plage -45° à +45° correspondant au plan parallèle à la surface de la route, lorsque le DSRC-UEV est installé ultérieurement dans le véhicule (azimut))	**(**conformément à la norme EN 12253**)** Exigence étendue pour des angles horizontaux jusqu'à ±45°, compte tenu des cas de figure définis dans ~~la présente annexe~~ **le présent sous-appendice**.
D12(*)	Niveau de puissance de coupure (DSRC-UEV)	-60 dBm	(conformément à la norme EN 12253)
D13	Préambule	Préambule obligatoire.	**(**conformément à la norme EN 12253**)**
D13a	Longueur et structure du préambule	16 bits ± 1 bit « 1 » codé en FM0	**(**conformément à la norme EN 12253**)**

Point	*Paramètre*	*Valeur(s)*	*Remarque*
D13b	Forme d'onde du préambule	Séquence alternant les niveaux bas et haut, avec une durée d'impulsion de 2 µs. La tolérance est donnée par D8a.	**(**conformément à la norme EN 12253**)**
D13c	Bits délimiteurs de fin (trailers)	Le RSU (LCDDP) peut émettre au maximum 8 bits après le drapeau de fin. Un OBU (DSRC-UEV) n'est pas tenu de prendre en compte ces bits supplémentaires.	**(**conformément à la norme EN 12253**)**

(*) Paramètres de liaison descendante soumis à des essais de conformité selon l'essai de paramétrage pertinent prévu par la norme EN 300 674-1.

(**) La valeur maximale de la puissance isotrope rayonnée efficace (P.I.R.E.) de l'équipement utilisé pour le contrôle à distance du tachygraphe doit être conforme aux exigences appliquées sur le territoire de la Partie contractante.**

Tableau 14.2
Paramètres de liaison montante

Point	*Paramètre*	*Valeur(s)*	*Remarque*
U1(*)	Fréquences sous-porteuses	Une OBU (DSRC-UEV) prend en charge les fréquences 1,5 MHz et 2,0 MHz Une RSU (LCDDP) prend en charge les fréquences 1,5 MHz ou 2,0 MHz ou les deux. U1-0 : 1,5 MHz U1-1 : 2,0 MHz	La sélection de la fréquence sous-porteuse (1,5 MHz ou 2,0 MHz) dépend du profil EN 13372 choisi.
U1a(*)	Tolérance pour la fréquence sous-porteuse	±0,1 %	(conformément à la norme EN 12253)
U1b	Utilisation de bandes latérales	Mêmes données des deux côtés	(conformément à la norme EN 12253)
U2(*)	Masque spectral d'émission de l'OBU (DSRC-UEV)	Conformément à la norme EN12253. 1) Puissance hors bande : voir ETSI EN 300674-1 2) Puissance dans la bande : [U4a] dBm à 500 kHz 3) Émission dans tout autre canal montant : U2(3)-1 = -35 dBm à 500 kHz	(conformément à la norme EN 12253)
U4a(*)	P.I.R.E. maximale − bande latérale unique (ligne de visée)	Deux options : U4a-0 : -14 dBm U4a-1 : -21 dBm	Conformément à la spécification déclarée et publiée du concepteur de l'équipement
U4b(*)	P.I.R.E. maximale − bande latérale unique (35^0)	Deux options : – Non applicable – -17 dBm	Conformément à la spécification déclarée et publiée du concepteur de l'équipement

Point	*Paramètre*	*Valeur(s)*	*Remarque*
U5	Polarisation	Circulaire antihoraire	(conformément à la norme EN 12253)
U5a	Polarisation croisée	XPD : Dans la ligne de visée : (LCDDP) RSU r **≥15dB** (DSRC-UEV)) OBU t ≥10 dB Dans la zone -3dB : (LCDDP) RSU r ≥ **0 dB** (DSRC-UEV) OBU t ≥ 6 dB	(conformément à la norme EN 12253)
U6	Modulation de sous-porteuse	2-PSK Données codées synchronisées avec la sous-porteuse : les transitions des données codées coïncident avec les transitions de la sous-porteuse.	(conformément à la norme EN 12253)
U6b	Cycle de fonctionnement	Cycle de fonctionnement : 50 % ± α, α ≤ 5 %	(conformément à la norme EN 12253)
U6c	Modulation sur porteuse	Multiplication de la sous-porteuse modulée par la porteuse.	(conformément à la norme EN 12253)
U7(*)	Codage de données	NRZI (pas de transition au début du bit « 1 », transition au début du bit « 0 », pas de transition à l'intérieur du bit)	(conformément à la norme EN 12253)
U8(*)	Débit binaire	250 kbit/s	(conformément à la norme EN 12253)
U8a	Tolérance de l'horloge bit	±1 000 ppm	(conformément à la norme EN 12253)
U9	Taux d'erreur binaire pour la communication	$\leq 10^{-6}$	(conformément à la norme EN 12253)
U11	Zone de communication	Espace dans lequel se situe le DSRC-UEV, de telle sorte que ses émissions soient reçues par le LCDDP avec un taux d'erreur binaire inférieur à celui indiqué à U9a.	(conformément à la norme EN 12253)
U12a(*)	Gain de conversion (limite inférieure)	1 dB pour chaque bande latérale Plage angulaire : circulairement symétrique entre la ligne de visée et ±35°	
		et dans la plage -45° à +45° correspondant au plan parallèle à la surface de la route, lorsque le DSRC-UEV est installé ultérieurement dans le véhicule (azimut)	Supérieur à la plage de valeurs spécifiée pour des angles horizontaux jusqu'à ±45°, compte tenu des cas de figure définis dans la présente annexe.
U12b(*)	Gain de conversion (limite supérieure)	10 dB pour chaque bande latérale	Inférieur à la plage de valeurs spécifiée pour chaque bande latérale à l'intérieur d'un cône circulaire autour de la ligne de visée de 45° d'angle d'ouverture

Point	*Paramètre*	*Valeur(s)*	*Remarque*
U13	Préambule	Préambule obligatoire	(conformément à la norme EN 12253)
U13a	Préambule Longueur et structure	32 à 36 µs, modulé avec sous-porteuse uniquement, puis 8 bits « 0 » en codage NRZI.	(conformément à la norme EN 12253)
U13b	Bits délimiteurs de fin (trailers)	Le DSRC-UEV peut émettre au maximum 8 bits après le drapeau de fin. Un RSU (LCDDP) n'est pas tenu de prendre en compte ces bits supplémentaires.	(conformément à la norme EN 12253)

(*) Paramètres de liaison montante soumis à des essais de conformité selon l'essai de paramétrage pertinent prévu par la norme EN 300 674-1

5.3.3~~4.3.3~~ Conception de l'antenne

5.3.3.1~~4.3.3.1~~ Antenne LCDDP

DSC_30 La conception de l'antenne du *LCDDP* dépend de la conception commerciale, dans les limites définies à la section 5.3.2, et est adaptée de manière à optimiser la performance de lecture du *DSRC-LCDDP* aux fins spécifiques et aux circonstances de lecture pour lesquelles le *LCDDP* a été conçu.

5.3.3.2~~4.3.3.2~~ Antenne UEV

DSC_31 La conception de l'antenne du *DSRC-UEV* dépend de la conception commerciale, dans les limites définies à la section 5.3.2, et est adaptée de manière à optimiser la performance de lecture du *DSRC-LCDDP* aux fins spécifiques et aux circonstances de lecture pour lesquelles le *LCDDP* a été conçu.

DSC_32 L'antenne de l'UEV est fixée sur le pare-brise du véhicule ou à proximité de celui-ci, comme spécifié à la section 5.1.

DSC_33 Dans l'environnement d'essai en atelier (voir sect. 6.3), l'antenne d'un DSRC-UEV, installée conformément à la section 5.1, doit pouvoir se connecter au moyen d'une communication d'essai standard et effectuer une transaction RTM telle que définie dans le présent **sous-**appendice, à une distance située entre 2 et 10 mètres, plus de 99 % du temps en moyenne, sur plus de 1 000 interrogations de lecture.

5.4~~4.4~~ Exigences du protocole DSRC pour le contrôle à distance des tachygraphes (RTM)

5.4.1~~4.4.1~~ Vue d'ensemble

DSC_34 Le protocole de transaction relatif au téléchargement des *données* par la liaison avec l'interface DSRC 5,8 GHz doit se dérouler selon les étapes suivantes. La présente section décrit le flux de transaction dans des conditions idéales sans retransmission ou interruption de la communication.

Remarque : l'objectif de la phase d'initialisation (Étape 1) est d'établir la communication entre le *LCDDP* et les *DSRC-UEV* présents dans la zone de transaction DSRC 5,8 GHz (relation maître-esclave), mais qui n'ont pas encore établi de communication avec le *LCDDP*, puis de notifier les processus d'application.

↳ **Étape 1** Initialisation. Le *LCDDP* envoie une trame contenant un « tableau de service de balises » (BST) qui comprend les identificateurs d'application (AID) dans la liste des services pris en charge. Dans l'application RTM, cela correspondra simplement au service de valeur AID = 2 (Freight&Fleet). Le *DSRC-UEV* évalue le BST reçu et répond (voir ci-dessous) en envoyant la liste des applications prises en charge dans le domaine

Freight&Fleet ou ne répond pas si aucune application n'est prise en charge. Si le *LCDDP* ne propose pas AID = 2, le DSRC-UEV ne répond pas.

↳ **Étape 2** Le *DSRC-UEV* envoie une trame contenant une demande d'allocation de fenêtre privée.

↳ **Étape 3** Le *LCDDP* envoie une trame contenant une allocation de fenêtre privée.

↳ **Étape 4** Le *DSRC-UEV* utilise cette fenêtre privée pour envoyer une trame contenant son tableau de service de véhicules (VST). Ce VST comprend la liste de toutes les différentes instances d'applications prises en charge par ce *DSRC-UEV* dans le cadre d'un AID = 2. Les différentes instances sont identifiées au moyen d'EID générés de manière unique, chaque EID étant associé à une valeur de paramètre « marque de contexte d'application » (Application Context Mark) qui indique la norme et l'application prises en charge.

↳ **Étape 5** Ensuite, le *LCDDP* analyse le VST proposé et décide soit de mettre fin à la connexion (RELEASE) car il n'est pas intéressé par l'offre du VST (c'est-à-dire qu'il reçoit un VST d'un *DSRC-UEV* qui ne prend pas en charge la transaction RTM), soit de lancer une instance d'application, s'il reçoit un VST approprié.

↳ **Étape 6** Pour ce faire, le *LCDDP* envoie une trame contenant une commande d'extraction des données RTM en identifiant l'instance de l'application RTM concernée par son identificateur (tel qu'indiqué par le *DSRC-UEV* dans le VST), puis alloue une fenêtre privée.

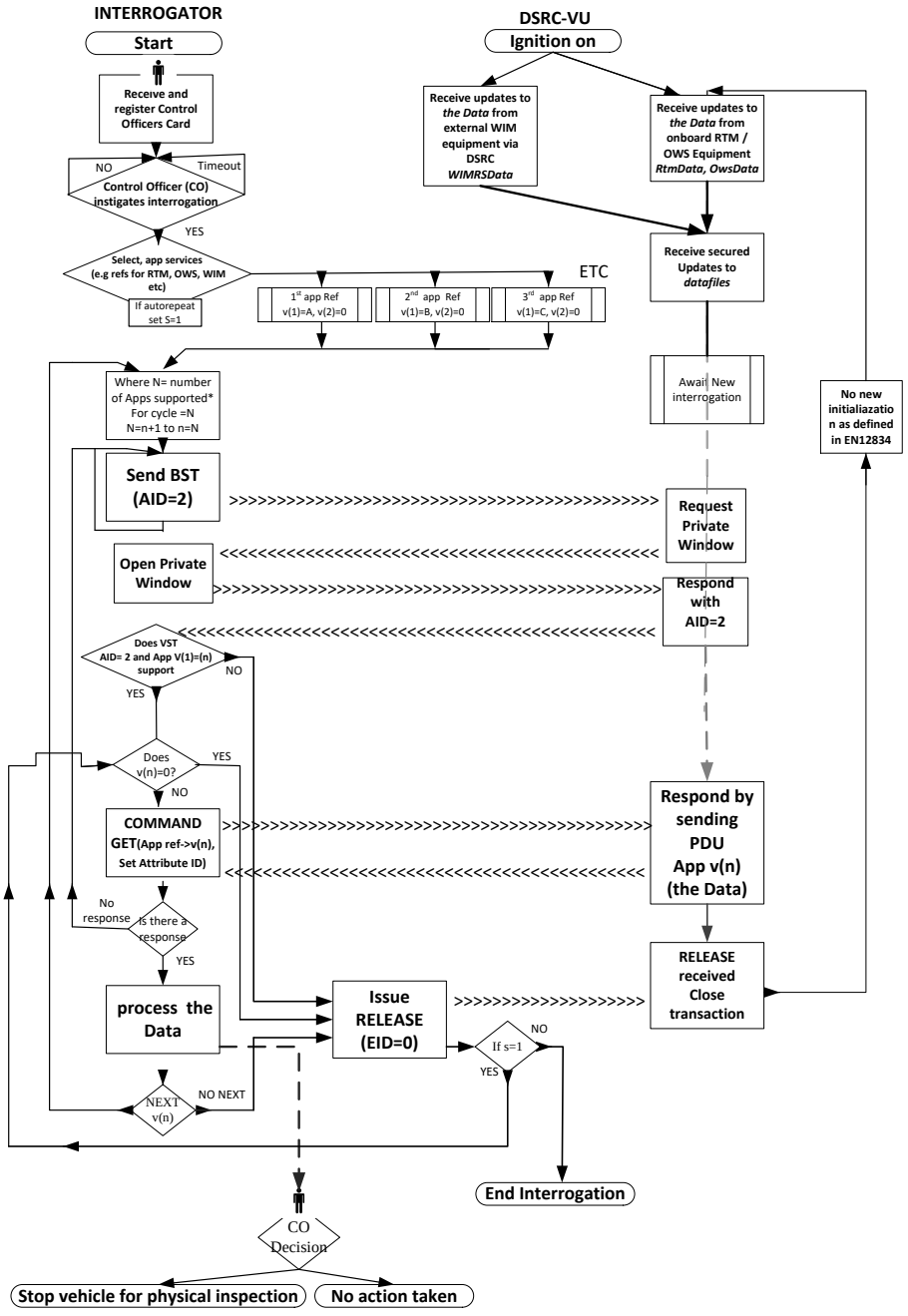
↳ **Étape 7** Le *DSRC-UEV* utilise la fenêtre privée qui vient d'être allouée pour envoyer une trame qui contient l'identificateur adressé correspondant à l'instance d'application RTM tel que fourni dans le VST, suivi de l'attribut *RtmData* (élément de données utiles + élément de sécurité).

↳ **Étape 8** Si plusieurs services sont requis, la valeur 'n' est remplacée par le numéro de référence du service suivant et la procédure est répétée.

↳ **Étape 9** Le *LCDDP* confirme la réception des données en envoyant une trame contenant une commande RELEASE au *DSRC-UEV* pour mettre fin à la session ou, en cas d'échec de la validation d'un accusé de réception de la LDPU, il revient à l'étape 6.

Voir la figure 14.6 pour une illustration du protocole de transaction.

Figure 14.6
Déroulement d'une procédure RTM via une interface DSRC 5,8 GHz



5.4.2~~4.4.2~~ Commandes

DSC_35 Les commandes suivantes sont les seules utilisées dans une phase de transaction RTM.

- **INITIALISATION.request :** commande émise par le LCDDP sous la forme d'une diffusion avec définition des applications qu'il prend en charge ;
- **INITIALISATION.response :** réponse émise par le DSRC-UEV confirmant la connexion et contenant la liste des instances d'applications prises en charge, avec leurs caractéristiques et les informations relatives à la façon de les adresser (EID) ;
- **GET.request :** commande envoyée par le *LCDDP* au *DSRC-UEV* qui spécifie l'instance d'application à adresser au moyen d'un EID défini, tel que reçu dans le VST, et qui donne l'instruction au *DSRC-UEV* d'envoyer l'attribut ou les attributs sélectionnés avec les *données*. L'objectif de la commande GET est de permettre au *LCDDP* d'obtenir les *données* du *DSRC-UEV* ;

- **GET.response :** réponse du *DSRC-UEV* contenant les *données* demandées ;
- **ACTION.request ECHO :** commande donnant l'instruction au *DSRC-UEV* de renvoyer des données au *LCDDP*. L'objectif de la commande ECHO est de permettre aux ateliers ou aux structures chargées des essais d'homologation de vérifier que la liaison DSRC fonctionne sans avoir besoin d'accéder aux éléments d'authentification de sécurité ;
- **ACTION.response ECHO** : réponse du *DSRC-UEV* à la commande ECHO ;
- **EVENT_REPORT.request RELEASE** : commande informant le *DSRC-UEV* que la transaction est terminée. L'objectif de la commande RELEASE est de mettre fin à la session avec le *DSRC-UEV*. Dès réception de la commande RELEASE, le *DSRC-UEV* ne répond plus à aucune interrogation relevant de la connexion en cours. Remarque : la norme EN 12834 prévoit qu'un *DSRC-UEV* ne se connecte pas deux fois au même interrogateur, à moins qu'il ait quitté la zone de communication pendant 255 secondes ou que l'identificateur de la balise de l'interrogateur ait changé.

5.4.3~~4.4.3~~ Séquence de commande d'interrogation

DSC_36 Du point de vue de la séquence commande-réponse, la transaction se décrit comme suit :

Séquence	*Émetteur*		*Récepteur*	*Description*	*Action*
1	LCDDP	>	DSRC-UEV	Initialisation de la liaison de communication − Demande	LCDDP transmet le BST
2	*DSRC-UEV*	*>*	*LCDDP*	*Initialisation de la liaison de communication − Réponse*	*Si le BST contient AID = 2 alors le DSRC-UEV demande l'allocation d'une fenêtre privée*
3	LCDDP	>	DSRC-UEV	Alloue une fenêtre privée	Envoie une trame contenant une allocation de fenêtre privée
4	*DSRC-UEV*	*>*	*LCDDP*	*Envoie un VST*	*Envoie une trame contenant un VST*
5	LCDDP	>	DSRC-UEV	Envoie une commande GET.request concernant les données d'un attribut pour un EID spécifique	
6	*DSRC-UEV*	*>*	*LCDDP*	*Envoie une commande GET.response avec l'attribut demandé pour l'EID spécifique*	*Envoie l'attribut (RtmData, OWSData….) avec les données pour l'EID spécifique*
7	LCDDP	>	DSRC-UEV	Envoie une commande GET.request concernant les données **d'un** autre attribut ~~(le cas échéant)~~	
8	*DSRC-UEV*	*>*	*LCDDP*	*Envoie une commande GET.response avec l'attribut demandé*	*Envoie l'attribut avec les données pour l'EID spécifique*
9	LCDDP	>	DSRC-UEV	Accuse réception des données	Envoie la commande RELEASE qui met fin à la transaction
10	*DSRC-UEV*			*Met fin à la transaction*	

Un exemple de la séquence de transaction et du contenu des trames échangées est présenté aux sections 5.4.7 et 5.4.8.

5.4.4~~4.4.4~~ Structures des données

DSC_37 La structure sémantique des *données* lorsque celles-ci sont transmises via l'interface DSRC 5,8 GHz doit être conforme à la description faite dans le présent **sous-**appendice. La présente section spécifie la manière dont ces données sont structurées.

DSC_38 Les données utiles (données RTM) consistent en la concaténation des :

1. Données EncryptedTachographPayload, qui résultent du chiffrement des données de type TachographPayload définies en ASN.1 à la section 5.4.5. La méthode de chiffrement est décrite ~~à l'appendice~~ **au sous-appendice** 11 ;

2. Données DSRCSecurityData spécifiées ~~à l'appendice~~ **au sous-appendice** 11.

DSC_39 Les données RTM sont adressées comme attribut RTM = 1 et transférées dans le conteneur RTM = 10.

DSC_40 La marque de contexte RTM doit identifier la partie de la norme prise en charge parmi la série de normes TARV (RTM correspond à la partie 9).

Le module ASN.1 concernant les données DSRC dans l'application RTM est défini comme suit :

```
TarvRtm  {iso(1)  standard(0)  15638  part9(9)
version1(1)} DEFINITIONS AUTOMATIC TAGS
::= BEGIN
IMPORTS
-- Importation des attributs et des éléments de données de l'EFC servant au RTM
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}
-- Importation des paramètres des fonctions à partir de la définition de l'interface d'application EFC
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}
-- Importation des données du module L7 DSRCData à partir de la définition de l'interface d'application
EFC
Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
Attributes,
BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)} ;
-- Définitions des fonctions RTM :
RTM-InitialiseComm-Request ::= BST
RTM-InitialiseComm-Response::= VST
RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials
ABSENT,iid ABSENT,  attrIdList})
RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
eventType (0)})
RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
(15), accessCredentials ABSENT, iid ABSENT})
RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
(0), iid ABSENT})
-- Définitions des attributs RTM :
RtmData ::= SEQUENCE {
encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calcul du chiffrement de
TachographPayload conformément ~~à l'appendice~~ au sous-appendice 11  --}),
DSRCSecurityData OCTET STRING
}
TachographPayload ::= SEQUENCE {
          tp15638VehicleRegistrationPlate LPN - Plaque d'immatriculation des véhicules utilisant la
                                          structure de données de la norme ISO 14906, mais pour
                                          l'application RTM, la LPN est fixée à 17 octets (pas de
                                          facteur de longueur)~~conformément à la norme EN 15509~~[17].
          tp15638SpeedingEvent            BOOLEAN,  -- 1= irrégularités de vitesse (voir appendice
1C)
          tp15638DrivingWithoutValidCard  BOOLEAN,    -- 1= utilisation d'une carte non valable
(voir ~~annexe~~ appendice 1C)
          tp15638DriverCard               BOOLEAN,-- 0= désigne une carte de conducteur non valable
(voir ~~annexe~~ appendice 1C)
          tp15638CardInsertion            BOOLEAN, -- 1= insertion d'une carte en cours de conduite
(voir ~~annexe~~ appendice 1C)
          tp15638MotionDataError          BOOLEAN, -- 1= erreur sur les données de mouvement (voir
~~annexe~~ appendice 1C)
          tp15638VehicleMotionConflict    BOOLEAN,  -- 1= conflit concernant le mouvement du
véhicule (voir ~~annexe~~ appendice 1C)
```

[17] ~~Si un LPN contient un AlphabetIndicator LatinAlphabetNo2 ou LatinCyrillicAlphabet, les caractères spéciaux sont adaptés au niveau de l'interrogateur routier selon des règles spéciales définies à l'annexe E de la norme ISO/DIS 14906.2.~~

```
          tp156382ndDriverCard            BOOLEAN,  --  1=  insertion  d'une  deuxième  carte  de
 conducteur (voir annexe appendice 1C)
          tp15638CurrentActivityDriving   BOOLEAN, -- 1= autre activité sélectionnée ;
                                                   -- 0= conduite sélectionnée ;
          tp15638LastSessionClosed        BOOLEAN, -- 1= clôture incorrecte d'une session, 0= clôture
 correcte d'une session
          tp15638PowerSupplyInterruption  INTEGER  (0..127),  --  interruption  de  l'alimentation
 électrique au cours des 10 derniers jours
          tp15638SensorFault              INTEGER  (0..255),--  eventFaultType  conformément  au
 dictionnaire des données
 -- Tous les autres types de données liés à l'heure tels que définis à l'annexe appendice 1C.
          tp15638TimeAdjustment           INTEGER(0..4294967295), -- Heure de la dernière remise à
 l'heure
          tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Heure de la dernière tentative
 d'atteinte à la sécurité
          tp15638LastCalibrationData      INTEGER(0..4294967295), -- Heure associée aux données du
 dernier étalonnage
          tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Heure associée aux données de
 l'étalonnage précédent
                    tp15638DateTachoConnected  INTEGER(0..4294967295),  --  Date  de  connexion  du
 tachygraphe

          tp15638CurrentSpeed             INTEGER  (0..255),  --  Dernière  vitesse  instantanée
 enregistrée
          tp15638Timestamp                INTEGER(0..4294967295) - Horodatage de l'enregistrement
 actif2
          tp15638LatestAuthenticatedPosition     INTEGER(0..4294967295), – Heure correspondant à la
                                                  dernière position authentifiée
          tp15638ContinuousDrivingTime    INTEGER  (0..255),  --  Temps  de  conduite  continue  du
 conducteur
          tp15638DailyDrivingTimeShift    INTEGER  (0..255),  --  Temps  de  conduite  journalier  du
                                            conducteur pour la période de travail RTM en cours et la
                                            précédente
          tp15638DailyDrivingTimeWeek     INTEGER (0..255), -- Temps de conduite journalier le plus
                                            long du conducteur pour la semaine en cours
          tp15638WeeklyDrivingTime        INTEGER  (0..255),  --  Temps  de  conduite  hebdomadaire  du
 conducteur
          tp15638FortnightlyDrivingTime   INTEGER (0..255) – Temps de conduite du conducteur pour
 deux semaines
          }
Rtm-ContextMark ::= SEQUENCE {
 standardIdentifier    StandardIdentifier, -- identificateur de la composante TARV et de sa version
 RtmCommProfile             INTEGER {
                    C1 (1),
                    C2 (2)
                    } (0..255) DEFAULT 1
 }
RtmTransferAck ::= INTEGER {
        Ok (1),
        NoK (2)
        } SIZE(1..255)
StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
        integer                      [0]    INTEGER,
        bitstring                    [1]    BIT STRING,
        octetstring                  [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString              [3]    UniversalString,
        beaconId                     [4]    BeaconID,
        t-apdu                       [5]    T-APDUs,
        dsrcApplicationEntityId      [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                  [7]    Dsrc-EID,
        attrIdList                   [8]    AttributeIdList,
        attrList                     [9]    AttributeList{RtmContainer},
        rtmData                      [10]   RtmData,
        rtmContextmark               [11]   Rtm-ContextMark,
        reserved12                   [12]   NULL,
        reserved13                    [13]   NULL,
        reserved14                   [14]   NULL,
        time                         [15]   Time,
 -- valeurs de 16 à 255 réservées à une utilisation conforme aux normes ISO/CEN
        }}
```

5.4.5~~4.4.101~~ Éléments de données RTM ~~RtmData~~, actions effectuées et définitions

DSC_41 Les valeurs de données à calculer par l'UEV et utilisées pour actualiser les données sécurisées dans le DSRC-UEV sont calculées selon les règles prévues au tableau 14.3 :

Tableau 14.3
Éléments RtmData, actions effectuées et définitions

(1) *Élément de données RTM*	*(2)* *Action effectuée par l'UEV*		*(3)* *Définition des données ASN.1*
RTM1 **Plaque d'immatriculation du véhicule**	L'UEV définit la valeur de l'élément de données RTM1 tp15638VehicleRegistrationPlate provenant de la valeur enregistrée du type de données VehicleRegistrationIdentification tel que défini ~~à l'appendice~~ **au sous-appendice** 1 VehicleRegistrationIdentification	Plaque d'immatriculation du véhicule exprimée par une chaîne de caractères	tp15638VehicleRegstrationPlate LPN, --Plaque d'immatriculation du véhicule importée de la norme ISO 14906 avec les limitations spécifiées dans la norme EN 15509 ; il s'agit d'une SEQUENCE commençant par le code pays, suivi d'un indicateur alphabétique puis du numéro d'immatriculation lui-même, qui comprend toujours 14 octets (complétés par des zéros de remplissage), de sorte que la longueur du type LPN conformément à la norme EN 15509 est toujours de 17 octets, dont 14 correspondent au numéro « réel » de la plaque d'immatriculation.
RTM2 **Excès de vitesse**	L'UEV génère une valeur booléenne pour l'élément de données RTM2 tp15638SpeedingEvent. La valeur tp15638SpeedingEvent est calculée par l'UEV d'après le**s** ~~nombre d'~~événements de type « excès de vitesse » (tel que défini à l'~~annexe~~**appendice** 1C) enregistrés dans l'UEV au cours des 10 derniers jours d'occurrence. ~~S'il existe au moins un tp15638SpeedingEvent dans les 10 derniers jours d'occurrence, tp15638SpeedingEvent prend la valeur TRUE (vrai).~~ ~~AUTREMENT, si aucun événement n'est survenu au cours des 10 derniers jours d'occurrence, tp15638SpeedingEvent prend la valeur FALSE (faux).~~	1 (TRUE) : **si l'événement de type « excès de vitesse » le plus récent s'est terminé au cours des 10 derniers jours ou est toujours en cours ;** ~~Indique des irrégularités de vitesse au cours des 10 derniers jours d'occurrence~~ **0 (FALSE) : dans tout autre cas.**	tp15638speedingEvent BOOLEAN,

(1) *Élément de données RTM*	*(2)* *Action effectuée par l'UEV*		*(3)* *Définition des données ASN.1*
RTM3 **Conduite sans carte valable**	L'UEV génère une valeur booléenne pour l'élément de données RTM3 tp15638DrivingWithoutValidCard. L'UEV attribue la valeur TRUE à la variable tp15638DrivingWithoutValidCard si ~~les données de l'UEV ont enregistré~~ au moins un événement de type « conduite sans carte appropriée » (tel que défini à ~~l'annexe~~ **l'appendice** 1C) **a été enregistré dans l'UEV au cours des 10 derniers jours** ~~d'occurrence~~. ~~AUTREMENT, si aucun événement n'est survenu au cours des 10 derniers jours d'occurrence, la variable tp15638DrivingWithoutValidCard prend la valeur FALSE.~~	1 (TRUE) : **si l'événement de type « conduite sans carte appropriée » le plus récent s'est terminé au cours des 10 derniers jours ou est toujours en cours ;** **0 (FALSE) : dans tout autre cas.** ~~Indique l'utilisation d'une carte invalide~~	tp15638DrivingWithoutValidCard BOOLEAN,
RTM4 **Carte de conducteur valable**	L'UEV génère une valeur booléenne pour l'élément de données RTM4 tp15638DriverCard sur la base **de la carte de conducteur en cours de validité insérée dans le lecteur « conducteur »** ~~des données enregistrées dans l'UEV et conformément à l'appendice **au sous-appendice** 1~~. ~~Si aucune carte de conducteur valide n'est présente, l'UEV attribue la valeur TRUE à la variable.~~ ~~AUTREMENT, si une carte de conducteur valide est présente, l'UEV attribue la valeur FALSE à la variable.~~	**1 (TRUE) : si aucune carte de conducteur en cours de validité n'est présente dans le lecteur « conducteur » de l'UEV ;** 0 (FALSE) : ~~indique~~ **si** une carte de conducteur valable **est présente dans le lecteur « conducteur » de l'UEV**.	tp15638DriverCard BOOLEAN,
RTM5 **Insertion d'une carte en cours de conduite**	L'UEV génère une valeur booléenne pour l'élément de données RTM5 **tp15638CardInsertion**. L'UEV attribue la valeur TRUE à la variable tp15638CardInsertion si ~~les données de l'UEV ont enregistré~~ au moins un événement de type « insertion d'une carte en cours de conduite » (tel que défini à ~~l'annexe~~ l'**appendice** 1C) **a été enregistré dans l'UEV au cours des 10 derniers jours** ~~d'occurrence~~. ~~AUTREMENT si aucun événement de ce type n'est survenu au cours des 10 derniers jours d'occurrence, la variable tp15638CardInsertion prend la valeur FALSE.~~	1 (TRUE) : ~~Indique l'~~ **si l'événement de type** « insertion d'une carte en cours de conduite » **le plus récent s'est produit** au cours des 10 derniers jours~~d'occurrence~~ ; **0 (FALSE) : dans tout autre cas.**	tp15638CardInsertion BOOLEAN,

(1) *Élément de données RTM*	*(2)* *Action effectuée par l'UEV*		*(3)* *Définition des données ASN.1*
RTM6 **Erreur sur les données de mouvement**	L'UEV génère une valeur booléenne pour l'élément de données RTM6. L'UEV attribue la valeur TRUE à la variable tp15638MotionDataError si ~~les données de l'UEV ont enregistré~~ au moins un événement de type « erreur sur les données de mouvement » (tel que défini à ~~l'annexe~~ **l'appendice** 1C) **a été enregistré dans l'UEV au cours des 10 derniers jours** ~~d'occurrence~~. ~~AUTREMENT, si aucun événement de ce type n'est survenu au cours des 10 derniers jours d'occurrence, la variable tp15638MotionDataError prend la valeur FALSE.~~	1 (TRUE) : ~~Indique une~~ **si l'événement de type** « erreur sur les données de mouvement » **le plus récent s'est terminé** au cours des 10 derniers jours ~~d'occurrence~~ **ou est toujours en cours ;** **0 (FALSE) : dans tout autre cas.**	tp15638**M**~~m~~otionDataError BOOLEAN,
RTM7 **Conflit concernant le mouvement du véhicule**	L'UEV génère une valeur booléenne pour l'élément de données RTM7. L'UEV assigne la valeur TRUE à la variable tp15638~~v~~**V**ehicleMotionConflict si ~~les données de l'UEV ont enregistré~~ au moins un événement de type « conflit concernant le mouvement du véhicule » ~~(valeur '0A'H)~~ **a été enregistré dans l'UEV au cours des 10 derniers jours** ~~d'occurrence~~. ~~AUTREMENT, si aucun événement de ce type n'est survenu au cours des 10 derniers jours d'occurrence, la variable tp15638vehicleMotionConflict prend la valeur FALSE.~~	1 (TRUE) : ~~Indique un~~ **si l'événement de type** « conflit concernant le mouvement du véhicule » **le plus récent s'est terminé** au cours des 10 derniers jours ~~d'occurrence~~ **ou est toujours en cours ;** **0 (FALSE) : dans tout autre cas.**	tp15638**V**~~v~~ehicleMotionConflict BOOLEAN,
RTM8 **Deuxième carte de conducteur**	L'UEV génère une valeur booléenne pour l'élément de données RTM8 sur la base de ~~l'annexe~~ **l'appendice** 1C (« Données relatives à l'activité du conducteur » ÉQUIPAGE et CO-CONDUCTEUR). Si une ~~deuxième~~ carte de **co-**conducteur valable est présente, l'UEV attribue la valeur TRUE à ~~la variable~~ **l'élément RTM8**. ~~AUTREMENT, en l'absence d'une deuxième carte de conducteur valide, l'UEV attribue la valeur FALSE à la variable.~~	1 (TRUE) : **si** ~~Indique qu'~~une ~~deuxième~~ carte de **co-**conducteur **valable est présente dans l'UEV** ~~a été insérée~~ ; **2 (FALSE) : si aucune carte de co-conducteur valable n'est présente dans l'UEV**	tp156382ndDriverCard BOOLEAN,

(1) *Élément de données RTM*	*(2)* *Action effectuée par l'UEV*		*(3)* *Définition des données ASN.1*
RTM9 **Activité en cours**	L'UEV génère une valeur booléenne pour l'élément de données RTM9. Si l'activité en cours est enregistrée dans l'UEV en tant qu'activité autre que « CONDUITE » (telle que définie à ~~l'annexe~~ **l'appendice** 1C), l'UEV attribue la valeur TRUE à ~~la variable~~ **l'élément RTM9**. ~~AUTREMENT, si l'activité en cours est enregistrée dans l'UEV comme « CONDUITE », l'UEV attribue la valeur FALSE à la variable.~~	1 (TRUE) :~~=~~ autre activité sélectionnée ; 0 (FALSE) :~~=~~ conduite sélectionnée	tp15638~~c~~**C**urrentActivityDriving BOOLEAN
RTM10 **Clôture de la dernière session**	L'UEV génère une valeur booléenne pour l'élément de données RTM10. Si la dernière session d'une carte n'a pas été clôturée correctement comme le prévoit ~~l'annexe~~ **l'appendice** 1C, l'UEV attribue la valeur TRUE à ~~la variable~~ **l'élément RTM10**. ~~AUTREMENT, si la dernière session d'une carte a été correctement clôturée, l'UEV attribue la valeur FALSE à la variable.~~	1 (TRUE) : **au moins une des cartes insérées a ouvert une dernière session qui n'a pas été clôturée correctement** ~~= la clôture de session a échoué~~ 0 (FALSE) : **aucune des cartes insérées n'a ouvert de dernière session n'ayant pas été clôturée correctement** ~~= la clôture de session a abouti~~	tp15638**L**~~l~~astSessionClosed BOOLEAN
RTM11 **Interruption de l'alimentation électrique**	L'UEV génère une valeur exprimée par un nombre entier pour l'élément de données RTM11. L'UEV attribue à la variable tp15638PowerSupplyInterruption une valeur égale ~~à la~~ **au nombre d'événements de type «** interruption de l'alimentation électrique » ~~journée la plus longue~~ (~~conformément aux dispositions de l'article 9 du règlement (UE) n° 165/2014~~ **tel que défini à l'appendice 1C**) **enregistrés dans l'UEV au cours des 10 derniers jours**. ~~électrique» (tel que défini à l'annexe 1C).~~ **Si aucun événement de type « interruption de l'alimentation électrique » n'a été enregistré dans l'UEV au cours des 10 derniers jours, l'UEV attribue la valeur 0 à RTM11.** ~~AUTREMENT, si aucun événement de type « interruption de l'alimentation électrique » n'est survenu au cours des 10 derniers jours d'occurrence, la variable du nombre entier est 0.~~	-- Nombre ~~d'interruptions~~ **d'événements de type** « interruption de l'alimentation électrique » **enregistrés** au cours des 10 derniers jours ~~d'occurrence~~	tp15638**P**~~p~~owerSupplyInterruption INTEGER (0..127),

(1) *Élément de données RTM*	*(2)* *Action effectuée par l'UEV*		*(3)* *Définition des données ASN.1*
RTM12 **Anomalie du capteur**	L'UEV génère une valeur exprimée par un nombre entier pour l'élément de données RTM12. L'UEV attribue à la variable sensorFault une valeur de : - 1 si un événement de type **'35'H** « anomalie du capteur » **est survenu et a pris fin** ~~a été enregistré~~ au cours des 10 derniers jours **ou est toujours en cours** ; - 2 si un événement de type « anomalie du récepteur GNSS » (interne ou externe, avec les valeurs enum ~~'51'H~~ **'36'H** ou ~~'52'H~~ **'37'H**) **est survenu et a pris fin** ~~a été enregistré~~ au cours des 10 derniers jours **ou est toujours en cours** ; - 3 si un événement de type ~~'53'H~~ '**0E'H** « erreur de communication ~~du~~ **avec le** dispositif GNSS **externe** » **est survenu et a pris fin** ~~a été enregistré~~ au cours des 10 derniers jours **ou est toujours en cours** ~~d'occurrence~~ ; - 4 si à la fois des anomalies du capteur et du récepteur GNSS **sont survenues et ont pris fin** ~~ont été enregistrées~~ au cours des 10 derniers jours **ou sont toujours en cours** ~~d'occurrence~~ ; - 5 si à la fois des anomalies du capteur et des erreurs de communication ~~du~~ **avec le** dispositif GNSS externe **sont survenus et ont pris fin** ~~ont été enregistrés~~ cours des 10 derniers jours **ou sont toujours en cours** ~~d'occurrence~~ ; - 6 si à la fois des anomalies du récepteur GNSS et des erreurs de communication ~~du~~ **avec le** dispositif GNSS externe **sont survenues et ont pris fin** ~~ont été enregistrées~~ au cours des 10 derniers jours ~~d'occurrence~~**ou sont toujours en cours ;** - 7 si les trois types d'anomalies sont survenus et ont pris fin ~~ont été enregistrés~~ au cours des 10 derniers jours **ou sont toujours en cours** ~~d'occurrence~~ . ~~AUTREMENT, une valeur de 0 est attribuée si~~ **S**i aucun événement n'a été enregistré au cours des 10 derniers jours ou n'est toujours en cours, **l'UEV attribue la valeur 0 à RTM12** ~~d'occurrence~~**.**	--anomalie du capteur codé sur un octet conformément au dictionnaire des données	tp15638SensorFault INTEGER (0..255),

(1) *Élément de données RTM*	*(2)* *Action effectuée par l'UEV*		*(3)* *Définition des données ASN.1*
RTM13 **Remise à l'heure**	L'UEV génère une valeur exprimée par un nombre entier (timeReal ~~de l'appendice~~ **du sous-appendice** 1) pour l'élément de données RTM13, en fonction de la présence de données concernant la remise à l'heure (telle que définie à ~~l'annexe~~**l'appendice** 1C). L'UEV ~~attribue~~ **fixe** la valeur **de RTM13 à** l'heure correspondant au dernier événement de type « remise à l'heure ». ~~AUTREMENT, s~~**S**i aucun événement de type « remise à l'heure » (tel que défini à ~~l'annexe~~ **l'appendice** 1C) n'est enregistré dans l'UEV, la valeur 0 est attribuée **à RTM13**.	~~Heure~~ **oldTimeValue** de la ~~dernière~~ remise à l'heure **la plus récente**	tp15638TimeAdjustment INTEGER(0..4294967295),
RTM14 **Tentative d'atteinte à la sécurité**	L'UEV génère une valeur exprimée par un nombre entier (timeReal ~~de l'appendice~~ **du sous-appendice** 1) pour l'élément de données RTM14, en fonction de la présence d'un événement de type « tentative d'atteinte à la sécurité » (tel que défini à ~~l'annexe~~ **l'appendice** 1C). L'UEV attribue la valeur horaire correspondant au dernier événement de type « tentative d'atteinte à la sécurité » enregistré par l'UEV. ~~AUTREMENT, s~~**S**i aucun événement de type « tentative d'atteinte à la sécurité » (tel que défini à ~~l'annexe~~ **l'appendice** 1C) n'est présent dans les données de l'UEV, la valeur 0 ~~0x00FF~~ est attribuée **à RMT14**.	Heure de **début du dernier événement de type** ~~la dernière~~ **«** tentative d'atteinte **à la sécurité » enregistré** ~~– Valeur par défaut = 0x00FF~~	tp15638LatestBreachAttempt INTEGER(0..4294967295),
RTM15 **Dernier étalonnage**	L'UEV génère une valeur exprimée par un nombre entier (timeReal ~~de l'appendice~~ **du sous-appendice** 1) pour l'élément de données RTM15, en fonction de la présence de données relatives au dernier étalonnage (tel que défini à ~~l'annexe~~ **l'appendice** 1C). L'UEV attribue à RTM15 la valeur **oldTimeValue de l'enregistrement d'étalonnage le plus récent** ~~des deux derniers étalonnages (RTM15 et RTM16), fixée dans VuCalibrationData comme le précise l'appendice le sous-appendice 1~~. **Si aucun étalonnage n'a été effectué,** ~~Ll~~'UEV ~~attribue~~ **fixe** la valeur ~~pour~~ **de** RTM15 **à 0** ~~au timeReal du plus récent enregistrement d'étalonnage~~.	~~Heure~~ **oldTimeValue** ~~du des données de dernier~~ **de l'enregistrement d'**étalonnage **le plus récent**	tp15638PrevCalibrationData INTEGER(0..4294967295),

(1) *Élément de données RTM*	*(2)* *Action effectuée par l'UEV*		*(3)* *Définition des données ASN.1*
RTM16 **Étalonnage précédent**	L'UEV génère une valeur exprimée par un nombre entier (timeReal ~~de l'appendice~~ **du sous-appendice** 1) pour l'élément de données RTM16, **en fonction de** l'enregistrement de l'étalonnage précédant ~~celui du~~ **le** dernier étalonnage. ~~AUTREMENT, si aucun étalonnage n'a été effectué précédemment,~~ ~~l~~**L**'UEV attribue ~~la valeur 0~~ à RTM16 **la valeur oldTimeValue de l'enregistrement de l'étalonnage précédent le dernier étalonnage**. **Si aucun étalonnage n'a été effectué précédemment, l'UEV attribue la valeur 0 à RTM16.**	~~Heure~~ **oldTimeValue** ~~des données de l'~~ **de l'enregistrement d'**étalonnage précédent **celui de l'étalonnage le plus récent**	tp15638PrevCalibrationData INTEGER(0..4294967295),
RTM17 **Date de connexion du tachygraphe**	~~Pour l'élément de données RTM17,~~ ~~l~~**L**'UEV ~~attribue~~ **génère** une valeur exprimée par un nombre entier (timeReal ~~de l'appendice~~ **du sous-appendice** 1) **pour l'élément de données RMT17**. L'UEV attribue **à RMT17** la valeur ~~temporelle~~ **de la date du premier étalonnage de l'unité embarquée sur le véhicule considéré.** ~~de l'installation initiale de l'UEV.~~ L'UEV extrait ces données de VuCalibrationData (~~appendice~~ **sous-appendice** 1) dans le vuCalibrationRecords avec CalibrationPurpose égal à : '03'H. **Si aucun étalonnage n'a été effectué précédemment, l'UEV attribue la valeur 0 à RTM17.**	Date **du premier étalonnage de l'unité embarquée sur le véhicule considéré** ~~de connexion du tachygraphe~~	tp15638DateTachoConnected INTEGER(0..4294967295),
RTM18 **Vitesse instantanée**	L'UEV génère une valeur exprimée par un nombre entier pour l'élément de données RTM18. L'UEV attribue comme valeur à l'élément RTM1**8**~~6~~ la dernière vitesse instantanée enregistrée au moment de la dernière mise à jour de RtmData.	Dernière vitesse instantanée enregistrée	tp15638CurrentSpeed INTEGER (0..255),
RTM19 **Horodatage**	~~Pour l'élément de données RTM19,~~ ~~l~~**L**'UEV ~~attribue~~ **génère** une valeur exprimée par un nombre entier (timeReal ~~de l'appendice~~ **du sous-appendice** 1) **pour l'élément de données RTM19**. L'UEV attribue comme valeur à l'élément RTM19 l'heure de la dernière mise à jour de RtmData.	Horodatage de l'enregistrement TachographPayload actuel	tp15638Timestamp INTEGER(0..4294967295),

(1) *Élément de données RTM*	*(2)* *Action effectuée par l'UEV*		*(3)* *Définition des données ASN.1*
RTM20 **Heure à laquelle la dernière position authentifiée du véhicule était disponible**	**L'UEV génère une valeur exprimée par un nombre entier (timeReal du sous-appendice 1) pour l'élément de données RTM20.** **L'UEV attribue comme valeur à l'élément RTM20 l'heure à laquelle la dernière position authentifiée du véhicule était disponible auprès du récepteur GNSS.** **Si aucune position authentifiée du véhicule n'était disponible auprès du récepteur GNSS, l'UEV attribue la valeur 0 à RTM20.**	**Horodatage de la dernière position authentifiée du véhicule**	**tp15638LatestAuthenticatedPosition** **INTEGER(0..4294967295),**
RMT21 **Temps de conduite continue**	**L'UEV génère une valeur exprimée par un nombre entier pour l'élément de données RTM21.** **L'UEV attribue comme valeur à l'élément RTM21 le temps de conduite continue actuel du conducteur.**	**Temps de conduite continue du conducteur, exprimé par un nombre entier.** **Longueur : 1 octet** **Résolution : 2 minutes/bit** **Décalage 0** **Étendue des données : 0 à 250** **Une valeur de 250 indique que le temps de conduite continue du conducteur est égal ou supérieur à 500 minutes. Les valeurs 251 à 254 ne sont pas utilisées.** **La valeur 255 indique que les informations ne sont pas disponibles.**	**tp15638ContinuousDrivingTime** **INTEGER (0..255),**
RTM22 **Temps de conduite journalier le plus long pour la période de travail RTM en cours et pour la période précédente, calculé conformément à l'annexe du sous-appendice 14**	**L'UEV génère une valeur exprimée par un nombre entier pour l'élément de données RTM22.** **L'UEV attribue comme valeur à l'élément RTM22 la plus longue des deux périodes de conduite journalières du conducteur, soit celle de la période de travail RTM en cours, soit celle de la période précédente.**	**Temps de conduite journalier du conducteur, exprimé par un nombre entier.** **Longueur : 1 octet** **Résolution : 4 minutes/bit** **Décalage 0** **Étendue des données : 0 à 250** **Une valeur de 250 indique que le temps de conduite journalier du conducteur est égal ou supérieur à 1 000 minutes. Les valeurs 251 à 254 ne sont pas utilisées.** **La valeur 255 indique que les informations ne sont pas disponibles.**	**tp15638DailyDrivingTimeShift** **INTEGER (0..255),**

(1) *Élément de données RTM*	*(2)* *Action effectuée par l'UEV*		*(3)* *Définition des données ASN.1*
RTM23 **Temps de conduite journalier le plus long pour la semaine en cours, calculé conformément à l'annexe du sous-appendice 14**	**L'UEV génère une valeur exprimée par un nombre entier pour l'élément de données RTM23.** **L'UEV attribue comme valeur à l'élément RTM23 la période de conduite journalière la plus longue qu'il s'agisse de la période de travail RTM en cours ou d'une période de travail RTM achevée ou commencée pendant la semaine en cours.**	**Temps de conduite journalier du conducteur, exprimé par un nombre entier.** **Longueur : 1 octet** **Résolution : 4 minutes/bit** **Décalage 0** **Étendue des données : 0 à 250** **Une valeur de 250 indique que le temps de conduite journalier du conducteur est égal ou supérieur à 1 000 minutes. Les valeurs 251 à 254 ne sont pas utilisées.** **La valeur 255 indique que les informations ne sont pas disponibles.**	**tp15638DailyDrivingTimeWeek INTEGER (0..255),**
RTM24 **Temps de conduite hebdomadaire, calculé conformément à l'annexe du sous-appendice 14**	**L'UEV génère une valeur exprimée par un nombre entier pour l'élément de données RTM24.** **L'UEV attribue comme valeur à l'élément RTM24 le temps de conduite hebdomadaire du conducteur.**	**Temps de conduite hebdomadaire du conducteur, exprimé par un nombre entier.** **Longueur : 1 octet** **Résolution : 20 minutes/bit** **Décalage 0** **Étendue des données : 0 à 250** **Une valeur de 250 indique que le temps de conduite hebdomadaire du conducteur est égal ou supérieur à 5 000 minutes. Les valeurs 251 à 254 ne sont pas utilisées.** **La valeur 255 indique que les informations ne sont pas disponibles.**	**tp15638WeeklyDrivingTime INTEGER (0..255),**

(1) *Élément de données RTM*	*(2)* *Action effectuée par l'UEV*		*(3)* *Définition des données ASN.1*
RTM25 **Temps de conduite pour deux semaines, calculé conformément à l'annexe du sous-appendice 14**	**L'UEV génère une valeur exprimée par un nombre entier pour l'élément de données RTM25.** **L'UEV attribue comme valeur à l'élément RTM25 le temps de conduite pour deux semaines du conducteur.**	**Temps de conduite pour deux semaines du conducteur, exprimé par un nombre entier.** **Longueur : 1 octet** **Résolution : 30 minutes/bit** **Décalage 0** **Étendue des données : 0 à 250** **Une valeur de 250 indique que le temps de conduite pour deux semaines du conducteur est égal ou supérieur à 7 500 minutes. Les valeurs 251 à 254 ne sont pas utilisées.** **La valeur 255 indique que les informations ne sont pas disponibles.**	**tp15638FortnightlyDrivingTime INTEGER (0..255),**

Remarque : les éléments de données RTM22, RTM23, RTM24 et RTM25 sont calculés conformément à l'annexe du présent sous-appendice.

5.4.6~~4.4.102~~ Mécanisme de transfert de données

DSC_42 Les données utiles définies précédemment sont demandées par le LCDDP après la phase d'initialisation, puis sont transmises par le DSRC-UEV dans la fenêtre allouée. Le LCDDP utilise la commande GET pour extraire les données.

DSC_43 Pour tous les échanges DSRC, les données sont codées à l'aide des règles de codage compact PER (Packed Encoding Rules) UNALIGNED**, à l'exception des éléments de données TachographPayload et OwsPayload, qui doivent être codés à l'aide des règles de codage des octets OER (Octet Encoding Rules) définies dans la norme ISO/CEI 8825-7 et dans la recommandation Rec. ITU-T X.696**

5.4.7~~4.4.103~~ Description détaillée de la transaction DSRC

DSC_44 L'initialisation est effectuée conformément aux dispositions DSC_44 à DSC_48 et aux tableaux 14.4 à 14.9. Durant la phase d'initialisation, le LCDDP commence par envoyer une trame contenant un BST (tableau de service de balise) selon les normes EN 12834 et EN 13372, sections 6.2, 6.3, 6.4 et 7.1, avec le paramétrage défini au tableau 14.4 ci-dessous.

Tableau 14.4
Initialisation − paramétrage de la trame BST

Champ	*Paramétrage*
Link Identifier	Adresse de diffusion
BeaconId	Conformément à EN 12834
Time	Conformément à EN 12834
Profile	Pas d'extension, utiliser 0 or 1

Champ	*Paramétrage*
MandApplications	Pas d'extension, EID non présent, paramètre non présent, AID = 2 Freight&Fleet
NonMandApplications	Non présent
ProfileList	Pas d'extension, nombre de profils dans la liste = 0
Fragmentation header	Pas de fragmentation
Layer 2 settings	PDU de commande, commande UI

Un exemple pratique du paramétrage indiqué au tableau 14.4 est fourni dans le tableau 14.5 ci-dessous, avec un exemple de codage binaire.

Tableau 14.5
Initialisation − Exemple de contenu de la trame BST

Octet #	Attribut/Champ	Bits dans l'octet	Description
1	FLAG	0111 1110	Drapeau de début
2	Broadcast ID	1111 1111	Adresse de diffusion
3	MAC Control Field	1010 0000	PDU de commande
4	LLC Control field	0000 0011	Commande UI
5	Fragmentation header	1xxx x001	Pas de fragmentation
6	BST	1000	Demande d'initialisation
	SEQUENCE {		
	OPTION indicator	0	Applications NonMand non présentes
	BeaconID SEQUENCE {		
	ManufacturerId INTEGER (0..65535)		
		xxx	Identificateur du fabricant
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	ID de 27 bits disponible pour le fabricant
9		xxxx xxxx	
10		xxxx xxxx	
11		xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	Temps réel UNIX 32 bits
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,...)	0000 0000	Pas d'extension. Profil d'exemple 0
17	MandApplications SEQUENCE (SIZE(0..127,...)) OF {	0000 0001	Pas d'extension, nombre mandApplications = 1
18	SEQUENCE {		
	OPTION indicator	0	EID non présent
	OPTION indicator	0	Paramètre non présent
	AID DSRCApplicationEntityID } }	00 0010	Pas d'extension. AID= 2
19	ProfileList SEQUENCE (0..127,...) OF Profile }	0000 0000	Pas d'extension, nombre de profils dans la liste = 0

Octet #	Attribut/Champ	Bits dans l'octet	Description
20	**FCS**	**xxxx xxxx**	**Séquence de contrôle de trame**
21		**xxxx xxxx**	
22	**Flag**	**0111 1110**	**Drapeau de fin**

DSC_45 Lorsqu'un DSRC-UEV reçoit un BST, il demande l'allocation d'une fenêtre privée selon les normes EN 12795 et EN 13372, section 7.1.1, sans paramétrage RTM particulier. Le tableau 14.6 fournit un exemple de codage binaire.

Tableau 14.6
Initialisation − Contenu de la trame d'une demande d'allocation de fenêtre privée

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
1	FLAG	0111 1110	Drapeau de début
2	Private LID	xxxx xxxx	Adresse de liaison du DSRC-UEV spécifique
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0110 0000	Demande d'allocation de fenêtre privée
7	FCS	xxxx xxxx	Séquence de contrôle de trame
8		xxxx xxxx	
9	Flag	0111 1110	Drapeau de fin

DSC_46 Le LCDDP répond en allouant une fenêtre privée, comme spécifié dans les normes EN 12795 et EN 13372, section 7.1.1, sans paramétrage RTM particulier.

Le tableau 14.7 donne un exemple de codage binaire.

Tableau 14.7
Initialisation − Contenu de la trame d'allocation de fenêtre privée

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
1	FLAG	0111 1110	Drapeau de début
2	Private LID	xxxx xxxx	Adresse de liaison du DSRC-UEV spécifique
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0010 s000	Allocation de fenêtre privée
7	FCS	xxxx xxxx	Séquence de contrôle de trame
8		xxxx xxxx	
9	Flag	0111 1110	Drapeau de fin

DSC_47 Lorsque le DSRC-UEV reçoit l'allocation de fenêtre privée, il envoie son VST (tableau de service de véhicule) tel que défini dans les normes EN 12834 et EN 13372, sections 6.2., 6,3, 6.4. et 7.1, avec le paramétrage spécifié au tableau 14.8, en utilisant la fenêtre de diffusion allouée.

Tableau 14.8
Initialisation − Paramétrage de la trame VST

Champ	*Paramétrage*
Private LID	Conformément à EN 12834
VST parameters	Fill = 0, puis pour chaque application prise en charge : EID présent, paramètre présent, AID = 2, EID tel que généré par l'OBU
Parameter	Pas d'extension, contient la marque de contexte RTM
ObeConfiguration	Le champ optionnel ObeStatus peut être présent, mais n'est pas utilisé par le LCDDP
Fragmentation header	Pas de fragmentation
Layer 2 settings	PDU de commande, commande UI

DSC_48 Le DSRC-UEV prend en charge l'application « Freight and Fleet », désignée par l'identificateur d'application '2'. D'autres identificateurs d'application peuvent être pris en charge, mais ne doivent pas être présents dans ce VST, car le BST exige uniquement AID = 2. Le champ « Applications » contient une liste des instances d'application prises en charge dans le DSRC-UEV. Pour chaque instance d'application prise en charge, une référence à la norme appropriée est indiquée. Cette référence est constituée d'une marque de contexte RTM, elle-même composée d'un identificateur d'objet qui désigne la norme correspondante, sa partie (9 pour RTM) et éventuellement sa version, ainsi qu'un EID généré par le DSRC-UEV et associé à cette instance d'application.

Un exemple pratique du paramétrage indiqué au tableau 14.8 est fourni dans le tableau 14.9, avec une indication du codage binaire.

Tableau 14.9
Initialisation − Exemple de contenu de la trame VST

Octet #	Attribut/Champ	Bits dans l'octet	Description
1	FLAG	0111 1110	Drapeau de début
2	Private LID	xxxx xxxx	Adresse de liaison du DSRC-UEV spécifique
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1100 0000	PDU de commande
7	LLC Control field	0000 0011	Commande UI
8	Fragmentation header	1xxx x001	Pas de fragmentation
9	VST SEQUENCE { Fill BIT STRING (SIZE(4))	1001 0000	Réponse d'initialisation Inutilisé, prend la valeur 0
10	Profile INTEGER (0..127,...)	0000 0000	Pas d'extension. Profil d'exemple 0
11		0000 0001	Pas d'extension, 1 application

12	**SEQUENCE {** **OPTION indicator** **OPTION indicator** **AID DSRCApplicationEntityID**	 **1** **1** **00 0010**	 **EID présent** **Paramètre présent** **Pas d'extension. AID= 2 Freight&Fleet**
13	**EID Dsrc-EID**	**xxxx xxxx**	**Défini pour l'OBU et identifie l'instance d'application**
14	**Parameter Container {**	**0000 0010**	**Pas d'extension, choix de conteneur = 02, Chaîne d'octets**
15		**0000 0110**	**Pas d'extension, longueur de la marque de contexte RTM = 6**
16	**Rtm-ContextMark ::= SEQUENCE {**	**0000 0101**	**Le premier octet est 05H, qui correspond à la longueur.** **Les 5 octets suivants codent l'identificateur d'objet de la norme prise en charge, y compris sa partie et sa version.** **{ISO (1) Standard (0) TARV (15638) part9(9) Version2 (2)}**
17	**standardIdentifier**	**0010 1000**	
18		**1111 1010**	
19		**0001 0110**	
20		**0000 1001**	
21		**0000 0010**	
22	**ObeConfiguration Sequence {** **OPTION indicator**	 **0**	 **ObeStatus non présent.**
23	**EquipmentClass INTEGER (0..32767)**	**xxx xxxx** **xxxx xxxx**	**Ce champ doit contenir les indications du fabricant concernant la version du logiciel et du matériel de l'interface DSRC.**
24	**ManufacturerId INTEGER (0..65535)**	**xxxx xxxx**	**Identificateur du fabricant pour le DSRC-UEV tel qu'il figure dans le registre ISO 14816.**
25		**xxxx xxxx**	
26	**FCS**	**xxxx xxxx**	**Séquence de contrôle de trame**
27		**xxxx xxxx**	
28	**Flag**	**0111 1110**	**Drapeau de fin**

~~Octet #~~	~~*Attribut/Champ*~~	~~*Bits dans l'octet*~~	~~*Description*~~
~~1~~	~~FLAG~~	~~0111 1110~~	~~Drapeau de début~~
~~2~~	~~Private LID~~	~~xxxx xxxx~~	
~~3~~		~~xxxx xxxx~~	
~~4~~		~~xxxx xxxx~~	~~Adresse de liaison du DSRC UEV~~
~~5~~		~~xxxx xxxx~~	~~spécifique~~
~~6~~	~~MAC Control field~~	~~1100 0000~~	~~PDU de commande~~

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
7	LLC Control field	0000 0011	Commande UI
8	Fragmentation header	1xxx x001	Pas de fragmentation
9	VST	1001	Réponse d'initialisation
	SEQUENCE {		
	Fill BIT STRING (SIZE(4))	0000	Inutilisé, prend la valeur 0
10	Profile INTEGER (0..127,...)		
	Applications SEQUENCE OF {	0000 0000	Pas d'extension. Profil d'exemple 0
11		0000 0001	Pas d'extension, 1 application
12	SEQUENCE {		
	OPTION indicator	1	EID présent
	OPTION indicator	1	Paramètre présent
	AID		Pas d'extension. AID= 2
	DSRCApplicationEntityID	00 0010	Freight&Fleet
13			Défini pour l'OBU et identifie
	EID Dsrc EID	xxxx xxxx	l'instance d'application.
14			Pas d'extension, choix de conteneur = 02,
	Parameter Container {	0000 0010	chaîne d'octet
15		0000 1000	Pas d'extension, longueur de marque de contexte RTM = 8
16	Rtm ContextMark ::= SEQUENCE {		Identificateur d'objet de la norme, partie et version prise en charge.
	StandardIdentifier	0000 0110	Exemple: ISO (1) Standard (0)
17	standardIdentifier	0000 0110	TARV (15638) part9(9) Version1 (1).
18	———	0010 1000	Le premier octet est 06H, qui est
19	———	1000 0000	l'identificateur d'objet. Le
20		1111 1010	deuxième octet est 06H, qui est sa
21		0001 0110	longueur. Les 6 octets suivants
22		0000 1001	codent l'identificateur d'objet de l'exemple.
23			Remarque: un seul élément de la séquence est présent (l'élément optionnel RtmCommProfile est
		0000 0001	omis).
24	ObeConfiguration Sequence {		
	OPTION indicator	0	ObeStatus non présent
	EquipmentClass INTEGER	xxx xxxx	
25	(0..32767)	xxxx xxxx	
26			
	ManufacturerId INTEGER	xxxx xxxx	Identificateur du fabricant pour le
27	(0..65535)	xxxx xxxx	DSRC UEV tel qu'il figure au registre ISO 14816
28		xxxx xxxx	
29	FCS	xxxx xxxx	Séquence de contrôle de trame
30	Flag	0111 1110	Drapeau de fin

DCS_49 Le LCDDP extrait ensuite les données en émettant une commande GET, conforme à la commande GET définie dans les normes EN 13372, sections 6.2, 6.3 et 6.4, et EN 12834, avec le paramétrage spécifié dans le tableau 14.10.

Tableau 14.10
Présentation − Paramétrage de la trame de la demande GET

Champ	*Paramétrage*
Invoker Identifier (IID)	Non présent
Link Identifier (LID)	Adresse de liaison du DSRC-UEV spécifique
Chaining	Non
Element Identifier (EID)	Comme spécifié dans le VST. Pas d'extension
Access Credentials	Non
AttributeIdList	Pas d'extension, 1 attribut, AttributeID = 1 (RtmData)
Fragmentation	Non
Layer2 settings	PDU de commande, commande ACn d'interrogation

Le tableau 14.11 montre un exemple de lecture des données RTM.

Tableau 14.11
Présentation − Exemple de trame de demande GET

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
1	FLAG	0111 1110	Drapeau de début
2	Private LID	xxxx xxxx	Adresse de liaison du DSRC-UEV spécifique
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	PDU de commande
7	LLC Control field	n111 0111	Commande ACn d, bit n
8	Fragmentation header	1xxx x001	Pas de fragmentation
9	Get.request	0110	Demande GET
	SEQUENCE {		
	OPTION indicator	0	Éléments d'authentification d'accès non présents
	OPTION indicator		
	OPTION indicator	0	IID non présent
	Fill BIT STRING(SIZE(1))		
		1	AttributeIdList présent
		0	Mis à 0.
10	EID INTEGER(0..127,…)	xxxx xxxx	L'EID de l'instance d'application RTM, tel que spécifié dans le VST. Pas d'extension
11	AttributeIdList SEQUENCE OF { AttributeId	0000 0001	Pas d'extension, nombre d'attributs = 1
12		0000 0001	AttributeId=1, RtmData. Pas d'extension

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
13	FCS	xxxx xxxx	Séquence de contrôle de trame
14		xxxx xxxx	
15	Flag	0111 1110	Drapeau de fin

DSC_50 Lorsque le DSRC-UEV reçoit la demande GET, il envoie une réponse GET avec les données demandées conformes à la réponse GET définie par la norme EN 13372, sections 6.2, 6.3 et 6.4, et la norme EN 12834, avec le paramétrage spécifié au tableau 14.12.

Tableau 14.12
Présentation − Paramétrage de la trame de réponse GET

Champ	*Paramétrage*
Invoker Identifier (IID)	Non présent
Link Identifier (LID)	Conformément à EN 12834
Chaining	Non
Element Identifier (EID)	Comme indiqué dans le VST
Access Credentials	Non
Fragmentation	Non
Layer2 settings	PDU de réponse, réponse disponible et commande acceptée, commande ACn

Le tableau 14.13 donne un exemple d'extraction de données RTM.

Tableau 14.13
Présentation − Exemple de contenu de trame de réponse

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
1	FLAG	0111 1110	Drapeau de début
2	Private LID	xxxx xxxx	Adresse de liaison du DSRC-UEV spécifique
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	PDU de réponse
7	LLC Control field	n111 0111	Réponse disponible, commande ACn bit n
8	LLC Status field	0000 0000	Réponse disponible et commande acceptée
9	Fragmentation header	1xxx x001	Pas de fragmentation
10	Get.response	0111	Réponse GET
	SEQUENCE {		
	OPTION indicator	0	IID non présent
	OPTION indicator	1	Liste d'attributs présente

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
	OPTION indicator	0	Statut de retour non présent
	Fill BIT STRING(SIZE(1))	0	Non utilisé
11	EID INTEGER(0..127,…)	xxxx xxxx	Réponse provenant de l'instance d'application RTM. Pas d'extension.
12	AttributeList SEQUENCE OF {	0000 0001	Pas d'extension, nombre d'attributs = 1
13	Attributes SEQUENCE {	0000 0001	Pas d'extension, AttributeId=1 (RtmData)
	AttributeId		
14	AttributeValue CONTAINER {	0000 1010	Pas d'extension, choix de conteneur = 1010.
15		kkkk kkkk	RtmData
16	}}}}	kkkk kkkk	
17		kkkk kkkk	
…		…	
n		kkkk kkkk	
n + 1	FCS	xxxx xxxx	Séquence de contrôle de trame
n + 2		xxxx xxxx	
n + 3	Flag	0111 1110	Drapeau de fin

DSC_51 Le LCDDP met alors fin à la connexion en émettant une commande EVENT_REPORT RELEASE conforme aux normes EN 13372, sections 6.2, 6.3 et 6.4, et EN 12834, section 7.3.8, sans paramétrage RTM particulier. Le tableau 14.14 donne un exemple de codage binaire de la commande RELEASE.

Tableau 14.14
Fin de connexion − Contenu de trame de fin de connexion EVENT_REPORT

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
1	FLAG	0111 1110	Drapeau de début
2	Private LID	xxxx xxxx	Adresse de liaison DSRC-UEV spécifique
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1000 s000	La trame contient une LPDU de commande
7	LLC Control field	0000 0011	Commande UI
8	Fragmentation header	1xxx x001	Pas de fragmentation

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
9	EVENT_REPORT.request	0010	EVENT_REPORT (Release)
	SEQUENCE {		
	OPTION indicator	0	Éléments d'authentification d'accès non présents
	OPTION indicator		
	OPTION indicator	0	Paramètre d'événement non présent
	Mode BOOLEAN		
		0	IID non présent
		0	Pas de réponse attendue
10	EID INTEGER (0..127,…)	0000 0000	Pas d'extension, EID = 0 (System)
11	EventType INTEGER (0..127,…) }	0000 0000	Type d'événement 0 = Release
12	FCS	xxxx xxxx	Séquence de contrôle de trame
13		xxxx xxxx	
14	Flag	0111 1110	Drapeau de fin

DSC_52 Le DSRC-UEV n'est pas censé répondre à la commande RELEASE. Il est alors mis fin à la communication.

5.4.8~~4.4.104~~ Description de la transaction d'essai DSRC

DSC_53 Les essais complets, qui comprennent la sécurisation des données, doivent être effectués conformément aux dispositions ~~de l'appendice~~ **du sous-appendice** 11 (Mécanismes de sécurité communs), par des personnes autorisées ayant accès aux procédures de sécurité, à l'aide de la commande GET normale définie ci-dessus.

DSC_54 Les essais de mise en service et d'inspection périodique qui nécessitent le déchiffrement et la compréhension du contenu des données déchiffrées doivent être effectués conformément aux dispositions ~~de l'appendice~~ **du sous-appendice** 11 (Mécanismes de sécurité communs) et ~~de l'appendice~~ **du sous-appendice** 9 (Homologation − Liste des essais minimaux requis).

Cependant, il est possible de tester la communication DSRC de base à l'aide de la commande ECHO. De tels essais peuvent être requis lors de la mise en service, lors des inspections périodiques ou sur demande des autorités de contrôle compétentes ~~ou conformément aux dispositions du règlement (UE) n° 165/2014 (cf. 6 ci-dessous)~~.

DSC_55 Afin d'effectuer un essai de communication de base, le LCDDP émet la commande ECHO pendant une session, c'est-à-dire après une phase d'initialisation réussie. La séquence des interactions est donc similaire à celle d'une interrogation :

↳ Étape 1 Le LCDDP envoie un « tableau de service de balise » (BST) qui comprend les identificateurs d'application (AID) dans la liste des services pris en charge. Dans les applications RTM, cela correspond simplement au service de valeur AID = 2.

Le DSRC-UEV évalue le BST reçu et répond lorsqu'il détecte que le BST demande le service Freight&Fleet (AID = 2). Si le LCDDP ne propose pas AID = 2, le DSRC-UEV met fin à la transaction avec le LCDDP.

↳ Étape 2 Le DSRC-UEV envoie une demande d'allocation de fenêtre privée.

↳ Étape 3 Le LCDDP envoie une allocation de fenêtre privée.

↳ Étape 4 Le DSRC-UEV utilise cette fenêtre privée pour envoyer son tableau de service de véhicule (VST). Ce VST comprend la liste de toutes les différentes instances d'application prises en charge par ce DSRC-UEV dans le cadre de AID = 2. Les différentes instances sont

identifiées au moyen d'EID uniques, chacun étant associé à une valeur de paramètre indiquant l'instance de l'application prise en charge.

↳ Étape 5 Ensuite, le LCDDP analyse le VST proposé et décide soit de mettre fin à la connexion (RELEASE) car il n'est pas intéressé par l'offre du VST (c'est-à-dire qu'il reçoit un VST d'un DSRC-UEV qui ne prend pas en charge la transaction RTM), soit de lancer une instance d'application, s'il reçoit un VST approprié.

↳ Étape 6 Le LCDDP émet une commande (ECHO) à l'intention du DSRC-UEV et alloue une fenêtre privée.

↳ Étape 7 Le DSRC-UEV utilise la fenêtre privée qui vient d'être allouée pour envoyer une trame de réponse ECHO.

Les tableaux suivants donnent un exemple pratique d'une session d'échange ECHO.

DSC_56 L'initialisation est effectuée conformément aux dispositions de la section 5.4.7 (DSC_44 à DSC_48) et des tableaux 14.4 à 14.9.

DSC_57 Le LCDDP émet alors une commande ACTION, ECHO conforme à la norme ISO 14906, contenant 100 octets de données et sans paramétrage RTM particulier. Le tableau 14.15 présente le contenu de la trame envoyée par le LCDDP.

Tableau 14.15
Exemple de trame de demande ACTION, ECHO

Octet #	*Attribut/Champ*		*Bits dans l'octet*	*Description*
1	FLAG		0111 1110	Drapeau de début
2	Private LID		xxxx xxxx	Adresse de liaison du DSRC-UEV spécifique
3			xxxx xxxx	
4			xxxx xxxx	
5			xxxx xxxx	
6	MAC Control field		1010 s000	PDU de commande
7	LLC Control field		n111 0111	Commande ACn d'interrogation, bit n
8	Fragmentation header		1xxx x001	Pas de fragmentation
9	ACTION.request		0000	Demande d'action (ECHO)
	SEQUENCE {			
	OPTION indicator		0	Éléments d'authentification d'accès non présents
	OPTION indicator		1	Paramètre d'action présent
	OPTION indicator		0	IID non présent
	Mode	BOOLEAN	1	Réponse attendue
10	EID (0..127,…)	INTEGER	0000 0000	Pas d'extension, EID = 0 (System)
11	ActionType (0..127,…)	INTEGER	0000 1111	Pas d'extension, type d'action demande ECHO
12	ActionParameter CONTAINER {		0000 0010	Pas d'extension, choix de conteneur = 2
13			0110 0100	Pas d'extension. Longueur de chaîne = 100 octets

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
14		xxxx xxxx	Données à renvoyer
…	}}	…	
113		xxxx xxxx	
114	FCS	xxxx xxxx	Séquence de contrôle de trame
115		xxxx xxxx	
116	Flag	0111 1110	Drapeau de fin

DSC_58 Lorsque le DSRC-UEV reçoit la demande ECHO, il envoie une réponse ECHO de 100 octets de données en reprenant la commande reçue, conformément aux dispositions de la norme ISO 14906, sans paramétrage RTM particulier. Le tableau 14.16 donne un exemple de codage binaire.

Tableau 14.16
Exemple de trame de réponse ACTION, ECHO

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
1	FLAG	0111 1110	Drapeau de début
2	Private LID	xxxx xxxx	Adresse de liaison de l'UEV spécifique
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	PDU de réponse
7	LLC Control field	n111 0111	Commande ACn, bit n
8	LLC status field	0000 0000	Réponse disponible
9	Fragmentation header	1xxx x001	Pas de fragmentation
10	ACTION.response	0001	Réponse ACTION (ECHO)
	SEQUENCE {		
	OPTION indicator	0	IID non présent
	OPTION indicator	1	Paramètre de réponse présent
	OPTION indicator	0	Statut de retour non présent
	Fill BIT STRING (SIZE (1))	0	Inutilisé
11	EID INTEGER (0..127,…)	0000 0000	Pas d'extension, EID = 0 (System)
12	ResponseParameter CONTAINER {	0000 0010	Pas d'extension, choix de conteneur = 2
13		0110 0100	Pas d'extension. Longueur de chaîne = 100 octets
14		xxxx xxxx	Données renvoyées
…		….	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Séquence de contrôle de trame

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
115		xxxx xxxx	
116	Flag	0111 1110	Drapeau de fin

5.5~~4.5 Conformité à la directive 2015/71/CE~~ Réservé pour une utilisation future

5.6 ~~4.5.7 Mécanismes de t~~Transfert de données entre le DSRC-UEV et l'UEV

~~DSC_64 Le mécanisme de transfert de données OWS entre l'interrogateur et le dispositif DSRC dans le véhicule est identique à celui utilisé pour les données RTM (voir 4.4.102).~~

~~DSC_65 Le transfert de données entre la plateforme qui recueille les données de poids maximaux et le dispositif DSRC dans le véhicule repose sur la connexion physique et les interfaces et le protocole définis à la section 4.6.~~

~~4.6 Transfert de données entre le DSRC-UEV et l'UEV~~

5.6.1~~4.6.1~~ Connexion physique et interfaces

DSC_66 La connexion entre l'UEV et le DSRC-UEV peut être établie soit par un câble physique, soit au moyen d'une communication sans fil à courte portée reposant sur le protocole Bluetooth v4.0 BLE.

DSC_67 Quel que soit le choix de la connexion et de l'interface physiques, les exigences suivantes doivent être satisfaites :

DSC_68 a) Afin que plusieurs fournisseurs puissent être engagés pour fournir l'UEV et le DSRC-UEV, voire différents lots de DSRC-UEV, la connexion reliant l'UEV et le DSRC-UEV, lorsque celui-ci n'est pas interne à l'UEV, doit être une connexion ouverte normalisée. L'UEV doit être connectée au DSRC-UEV :

i) Au moyen d'un câble fixe de 2 mètres au minimum avec un connecteur mâle homologué à 11 broches Straight DIN 41612 H11 sur le DSRC-UEV, s'emboîtant dans un connecteur femelle homologué DIN/ISO correspondant sur l'UEV ;

ii) Au moyen d'une connexion Bluetooth Low Energy (BLE) ;

iii) Au moyen d'une connexion normalisée ISO 11898 ou SAE J1939 ;

DSC_69 b) la définition des interfaces et de la connexion entre l'UEV et le DSRC-UEV doit être compatible avec les commandes du protocole d'application définies à la section 5.6.2 ;

DSC_70 c) l'UEV et le DSRC-UEV doivent assurer le bon déroulement du transfert de données via la connexion en ce qui concerne les performances et l'alimentation électrique.

5.6.2~~4.6.2~~ Protocole d'application

DSC_71 Le protocole d'application entre le dispositif de communication à distance de l'UEV et le DSRC-UEV gère le transfert régulier des données de communication à distance de l'UEV vers le DSRC.

DSC_72 Les commandes principales sont les suivantes :

1. Initialisation de la liaison de communication − Demande
2. Initialisation de la liaison de communication − Réponse

3. Envoi de données avec l'identificateur de l'application RTM et les données utiles définies par RTMData

4. Accusé de réception des données

5. Fin de la liaison de communication − Demande

6. Fin de la liaison de communication − Réponse

DSC_73 En ASN1.0, les commandes précédentes peuvent être définies comme suit :

```
Remote Communication DT Protocol DEFINITIONS ::= BEGIN

 RCDT-Communication Link Initialization - Request ::= SEQUENCE { LinkIdentifier INTEGER

        }

 RCDT-Communication Link Initialization - Response::= SEQUENCE { LinkIdentifier INTEGER,

        answer        BOOLEAN

        }

        RCDT- Send Data ::= SEQUENCE {
        LinkIdentifier INTEGER, DataTransactionId
        INTEGER,                RCDTData
        SignedTachographPayload

        }

        RCDT Data Acknowledgment :: SEQUENCE {
        LinkIdentifier INTEGER, DataTransactionId INTEGER,

        answer        BOOLEAN

        }

       RCDT-Communication Link Termination - Request ::= SEQUENCE { LinkIdentifier INTEGER

        }

       RCDT-Communication Link Termination - Response::= SEQUENCE { LinkIdentifier INTEGER,

        answer        BOOLEAN

        }

End
```

DSC_74 La description des commandes et des paramètres est la suivante :

`RCDT-Communication Link Initialization - Request` sert à initialiser la liaison de communication. La commande est envoyée par l'UEV au DSRC-UEV. Le LinkIdentifier est défini par l'UEV et communiqué au DSRC-UEV afin de suivre une liaison de communication spécifique.

(Remarque : cela permet d'assurer la prise en charge des liaisons ultérieures et d'autres applications ou d'autres modules comme le système de pesage embarqué).

`RCDT-Communication Link Initialization - Response` est utilisée par le DSRC-UEV pour répondre à la demande d'initialisation de la liaison de communication. La commande est envoyée par le DSRC-UEV à l'UEV. La commande transmet le résultat de l'initialisation sous la forme d'une réponse = 1 (réussite) ou =0 (échec).

DSC_75 L'initialisation de la liaison de communication ne doit avoir lieu qu'après l'installation, l'étalonnage et le démarrage du moteur ou de l'UEV.

`RCDT - Send Data` est utilisée par l'UEV pour envoyer les RCDTData signées (c'est-à-dire les *données de communication à distance*) au DSRC-UEV. Les données sont envoyées toutes les 60 secondes. Le paramètre DataTransactionId identifie la transmission de données spécifique. En outre, le LinkIdentifier sert à garantir que la liaison concernée est adaptée.

`RCDT - Data Acknowledgment` est envoyée par le DSRC-UEV pour fournir un retour à l'UEV quant à la réception des données d'une commande RCDT- Send Data identifiée par le paramètre DataTransactionId. Le paramètre de réponse est 1 (réussite) ou 0 (échec). Si une UEV reçoit plus de trois réponses égales à 0 ou si elle ne reçoit pas de RCDT Data

Acknowledgment pour une commande RCDT- Send Data envoyée précédemment avec un DataTransactionId spécifique, l'UEV génère et enregistre un événement.

`RCDT-Communication Link Termination request` est envoyée par l'UEV au DSRC-UEV pour mettre fin à une liaison correspondant à un LinkIdentifier spécifique.

DSC_76 Au redémarrage du DSRC-UEV ou d'une UEV, il convient de supprimer toutes les liaisons de communication existantes, car il pourrait subsister des liaisons en suspens du fait de l'arrêt soudain d'une UEV.

`RCDT-Communication Link Termination - Response` est envoyée par le DSRC-UEV à l'UEV pour confirmer sa demande d'interruption de la liaison correspondant à un LinkIdentifier spécifique.

5.7~~4.7~~ Traitement des erreurs

5.7.1~~4.7.1~~ Enregistrement et communication des données au sein du DSRC-UEV

DSC_77 Les *données* doivent être fournies déjà sécurisées par la fonction UEV-MS au DSRC-UEV. L' UEV-MS vérifie que les données enregistrées dans le DSRC-UEV **ont été transmises avec succès** ~~le sont de manière satisfaisante~~. L'enregistrement et le signalement de toute erreur survenue pendant le transfert de données de l'UEV vers la mémoire du DSRC-UEV doivent être consignés avec le type EventFaultType et la valeur enum ~~d'erreur de communication~~ ~~'62'H~~ **'0C'H** *Erreur de communication avec le dispositif de communication à distanc*e, ainsi que l'horodatage correspondant. **L'UEV-MS doit vérifier que les données ont été transmises au DSRC-UEV avec succès.**

DSC_78 **Réservé pour une utilisation future** ~~L'UEV tient à jour un fichier désigné par un intitulé unique aisément identifiable par les inspecteurs aux fins de l'enregistrement des « anomalies de communication internes à l'UEV ».~~

DSC_79 Si l'UEV-MU tente d'obtenir les données de l'UEV auprès du module de sécurité (pour les transférer au DSRC-UEV), mais échoue, elle doit enregistrer cet échec avec le type EventFaultType et la valeur enum *'62'H Erreur de communication du dispositif de communication à distance*, ainsi que l'horodatage correspondant. L'erreur de communication est détectée lorsqu'aucun message `RCDT Data Acknowledgment` n'est reçu pour le `RCDT Send Data` correspondant (c'est-à-dire doté du même DataTransactionId dans les messages `Send Data` et `Acknowledgment`) plus de trois fois consécutives.

5.7.2~~4.7.2~~ Erreurs de communication sans fil

DSC_80 Le traitement des erreurs de communication doit être conforme aux dispositions des normes DSRC correspondantes, à savoir EN 300 674-1, EN 12253, EN 12795 et EN 12834, et aux paramètres appropriés de la norme EN 13372.

5.7.2.1~~4.7.2.1~~ Erreurs de chiffrement et de signature

DSC_81 Les erreurs de chiffrement et de signature doivent être traitées conformément aux dispositions ~~de l'appendice~~ **du sous-appendice** 11 (Mécanismes de sécurité communs) et ne figurent pas dans les messages d'erreur associés au transfert de données DSRC.

5.7.2.2~~4.7.2.2~~ Enregistrement des erreurs

La technologie DSRC est une communication sans fil dynamique dans un environnement marqué par des conditions atmosphériques et des interférences incertaines, en particulier dans les cas où un LCDDP portable et un véhicule en circulation sont impliqués dans cette application. Il est donc nécessaire de distinguer un « échec de lecture » d'une condition d'« erreur ». Dans une transaction avec une interface sans fil, l'échec de lecture est courant et entraîne habituellement une nouvelle tentative, c'est-à-dire la rediffusion du BST et une nouvelle tentative d'envoi de la séquence, qui, dans la plupart des cas, aboutiront à une connexion de communication réussie et au transfert des données, sauf si le véhicule ciblé se déplace hors portée pendant le temps nécessaire à la retransmission. (La « réussite » d'une « lecture » peut requérir plusieurs tentatives).

L'échec de lecture peut être dû au fait que les antennes ne sont pas couplées correctement (anomalie de « visée ») ; au fait que l'une des antennes est masquée − de manière délibérée ou à cause de la présence physique d'un autre véhicule ; à des interférences radio, en particulier à proximité de communications WIFI d'environ 5,8 GHz ou d'autres types de communications sans fil d'accès public, ou à des interférences causées par des radars ; à des conditions atmosphériques (par exemple, pendant un orage), ou simplement à un déplacement hors de portée de la communication DSRC. Les cas particuliers d'échec de lecture, par leur nature, ne peuvent pas être enregistrés, car la communication n'a tout simplement pas eu lieu.

Cependant, si l'agent de l'autorité de contrôle compétente cible un véhicule et tente d'interroger son DSRC-UEV, mais qu'aucun transfert de données n'aboutit, cet échec pourrait s'expliquer par une manipulation délibérée. Par conséquent, l'agent de l'autorité de contrôle compétente doit disposer d'un moyen d'enregistrer l'échec et d'alerter ses collègues en aval d'un risque d'infraction. Les collègues peuvent alors intercepter le véhicule et procéder à une inspection physique. Toutefois, aucune communication n'ayant abouti, le DSRC-UEV ne peut fournir de données concernant cette anomalie. Ce type de rapport doit donc être une fonction intégrée dans la conception de l'équipement LCDDP.

L'« échec de lecture » est techniquement différent d'une « erreur ». Dans ce contexte, une « erreur » désigne l'acquisition d'une valeur erronée.

Les données transférées au DSRC-UEV sont fournies déjà sécurisées et doivent donc faire l'objet d'une vérification par le fournisseur des données (voir 5.4).

Les données transférées ultérieurement par l'intermédiaire de l'interface aérienne sont soumises à des contrôles de redondance cyclique au niveau des communications. Si le CRC les valide, les données sont correctes. Si le CRC ne les valide pas, les données sont retransmises. Statistiquement, la probabilité que des données erronées passent à travers un contrôle CRC est tellement faible qu'elle peut être écartée.

Si le CRC ne valide pas les données et que le temps manque pour procéder à une retransmission et à une réception des données correctes, il ne s'agira pas d'une erreur, mais d'un type particulier d'échec de lecture.

Les seules données significatives concernant les échecs qui peuvent être enregistrées sont le nombre d'initiations de transactions réussies, qui n'aboutissent pas à un transfert des données vers le LCDDP.

DSC_82 Le LCDDP doit donc enregistrer, avec horodatage, le nombre de transactions pour lesquelles la phase d'« initialisation » d'une interrogation DSRC a abouti, mais qui ont été interrompues avant que les *données* n'aient pu être extraites par le LCDDP. Ces données doivent être mises à la disposition des agents de l'autorité de contrôle compétente et stockées dans la mémoire de l'équipement LCDDP. Les moyens pour y parvenir relèvent de la conception du produit ou des spécifications de l'autorité de contrôle compétente.

Les seules données significatives concernant les « erreurs » qui peuvent être enregistrées sont le nombre d'occasions où le LCDDP ne parvient pas à déchiffrer les *données* reçues. Cependant, il faut noter que cela ne concerne que l'efficacité du logiciel du LCDDP. Les données peuvent être déchiffrées techniquement, mais ne pas avoir de sens du point de vue sémantique.

DSC_83 Le LCDDP enregistre et horodate par conséquent le nombre de tentatives infructueuses de déchiffrement des données reçues par l'intermédiaire de l'interface DSRC.

6.~~5.~~ Mise en service et essais d'inspection périodique relatifs à la fonction de communication à distance

6.1~~5.1~~ Généralités

DSC_84 Deux types d'essais sont prévus pour la fonction de communication à distance :

1) Un essai ECHO pour valider le canal de communication sans fil *DSRC-LCDDP* >>-:-< *DSRC-UEV* ;

2) Un essai de sécurité de bout en bout pour s'assurer qu'une carte d'atelier est en mesure d'accéder au contenu des données signées et chiffrées créé par l'UEV et transmis sur le canal de communication sans fil.

6.2~~5.2~~ ECHO

La présente section contient des dispositions spécifiques permettant uniquement de vérifier que la liaison *DSRC-LCDDP* >>-:-<*DSRC-UEV* est fonctionnelle.

L'objectif de la commande ECHO est de permettre aux ateliers ou aux structures chargées des essais d'homologation de vérifier que la liaison DSRC fonctionne sans avoir besoin d'accéder aux éléments d'authentification de sécurité. L'équipement d'essai doit donc seulement être en mesure d'initialiser une communication DSRC (envoi d'un BST avec AID = 2), d'envoyer la commande ECHO et, si la communication DSRC fonctionne, de recevoir la réponse ECHO. Pour de plus amples informations, voir la section 5.4.8. Dans l'hypothèse où cette réponse est bien reçue, la liaison DSRC (*DSRC-LCDDP* >>-:-< *DSRC-UEV*) peut être considérée comme fonctionnant correctement et validée.

6.3~~5.3~~ Essais de validation du contenu des données sécurisées

DSC_85 Cet essai permet de vérifier que le flux de données est sécurisé de bout en bout. Il est nécessaire de disposer d'un lecteur d'essai DSRC pour procéder à cet essai. Le lecteur d'essai DSRC assure les mêmes fonctions et est utilisé selon les mêmes spécifications que le lecteur utilisé par les agents des forces de l'ordre, à la différence qu'une carte d'atelier est utilisée pour authentifier l'utilisateur du lecteur plutôt qu'une carte de contrôleur. Cet essai peut être exécuté après l'activation initiale d'un tachygraphe intelligent ou à la fin de la procédure d'étalonnage. Après son activation, l'unité embarquée sur le véhicule génère et communique au DSRC-UEV les données sécurisées de détection précoce.

DSC_86 Le personnel de l'atelier doit placer le lecteur d'essai DSRC à une distance située entre 2 et 10 mètres devant le véhicule.

DSC_87 Le personnel de l'atelier doit ensuite insérer une carte d'atelier dans le lecteur d'essai DSRC pour envoyer une interrogation portant sur les données de détection précoce à l'unité embarquée sur le véhicule. Après une interrogation réussie, le personnel de l'atelier accède aux données reçues pour vérifier que leur intégrité a été validée et qu'elles ont été déchiffrées.

Annexe

Règles pour le calcul des temps de conduite journaliers, hebdomadaires et pour deux semaines

1. Règles de calcul de base

L'UEV calcule les temps de conduite journaliers, hebdomadaires et pour deux semaines sur la base des données pertinentes stockées sur une carte de conducteur (ou d'atelier) insérée dans le lecteur « conducteur » (lecteur 1, lecteur de carte #1) de l'unité embarquée sur le véhicule, ainsi que des activités du conducteur sélectionnées pendant que cette carte est insérée dans l'UEV.

Les temps de conduite ne sont pas calculés tant qu'aucune carte de conducteur (ou d'atelier) n'est insérée.

La ou les périodes INCONNUES constatées au cours de la période nécessaire aux calculs sont assimilées à des périodes INTERRUPTION/REPOS.

Les périodes et activités INCONNUES dont la durée est négative (c'est-à-dire que le début de l'activité intervient après la fin de l'activité) en raison de chevauchements temporels entre deux UEV différentes ou en raison d'une remise à l'heure ne sont pas prises en compte.

Les activités enregistrées sur la carte de conducteur correspondant à des périodes HORS CHAMP conformément à la définition gg) de l'appendice 1C sont interprétées de la manière suivante :

- **INTERRUPTION/REPOS est calculé comme REPOS ou INTERRUPTION ;**
- **TRAVAIL et CONDUITE sont considérés comme TRAVAIL ;**
- **DISPONIBILITÉ est considérée comme DISPONIBILITÉ.**

Dans le cadre de la présente annexe, l'UEV présume un temps de repos journalier au début des enregistrements d'activité sur la carte.

2. Définitions

Les concepts suivants s'appliquent exclusivement au présent appendice et visent à préciser le calcul des temps de conduite par l'UEV et leur transmission ultérieure par le dispositif de communication à distance.

a) « période de travail RTM », la période comprise entre les fins respectives de deux temps de repos journaliers consécutifs.

L'UEV entame une nouvelle période de travail RTM à la fin de chaque temps de repos journalier.

La période de travail RTM en cours est la période écoulée depuis la fin du dernier temps de repos journalier ;

b) « temps de conduite accumulé », la somme de la durée de toutes les activités de CONDUITE du conducteur au cours d'une période où il n'est pas HORS CHAMP ;

c) « temps de conduite journalier », le temps de conduite accumulé au cours d'une période de travail RTM ;

d) « temps de conduite hebdomadaire », le temps de conduite accumulé pour la semaine en cours ;

e) « temps repos continu », toute période ininterrompue d'INTERRUPTION/REPOS ;

f) « temps de conduite pour deux semaines », le temps de conduite accumulé pour la semaine en cours et la semaine précédente ;

g) « temps de repos journalier », une période d'INTERRUPTION/REPOS, qui peut être :

- **Un temps de repos journalier normal ;**
- **Un temps de repos journalier fractionné ;**
- **Un temps de repos journalier réduit.**

Dans le contexte du sous-appendice 14, lorsqu'une UEV calcule les temps de repos hebdomadaires, ceux-ci sont considérés comme des temps de repos journaliers ;

h) « temps de repos journalier normal », une période de repos ininterrompue d'au moins 11 heures.

À titre exceptionnel, lorsqu'une condition TRAJET EN FERRY/TRAIN est active, le temps de repos journalier normal peut être interrompu au maximum deux fois par des activités autres que le repos, avec une durée cumulée maximale d'une heure, de telle sorte que le temps de repos journalier normal comportant une ou plusieurs périodes de trajets en ferry/train peut être scindé en deux ou trois parties. L'UEV calcule ensuite un temps de repos journalier normal lorsque le temps de repos accumulé calculé conformément au point 3 est d'au moins 11 heures.

Lorsqu'un temps de repos journalier normal a été interrompu, l'UEV :

- **N'inclut pas l'activité de conduite détectée pendant ces interruptions dans le calcul du temps de conduite journalier ; et**
- **Commence une nouvelle période de travail RTM à la fin du temps de repos journalier normal qui a été interrompu.**

A	B	C	D	E	F	G
⊙/✕/⊠	⊢	⊙/✕/⊠	⊢	⊙/✕/⊠	⊢	⊙/✕/⊠
Working Period	2 h	30 min	8 h	30 min	2 h	New Day

Figure 1. Exemple de temps de repos journalier interrompu en raison d'un trajet en ferry/train

i) « temps de repos journalier réduit », une période de repos ininterrompue d'au moins 9 heures et de moins de 11 heures ;

j) « temps de repos journalier fractionné », un temps de repos journalier pris en deux parties :

- **La première partie est une période de repos ininterrompue d'au moins 3 heures et de moins de 9 heures ;**
- **La seconde partie est une période de repos ininterrompue d'au moins 9 heures.**

À titre exceptionnel, lorsqu'une condition TRAJET EN FERRY/TRAIN est active pendant l'une ou les deux parties d'un temps de repos journalier fractionné, le temps de repos journalier fractionné peut être interrompu au maximum deux fois par d'autres activités d'une durée cumulée maximale d'une heure, c'est-à-dire que :

- **La première partie du temps de repos journalier fractionné peut être interrompue une ou deux fois ; ou**
- **La seconde partie du temps de repos journalier fractionné peut être interrompue une ou deux fois ; ou**
- **La première partie du temps de repos journalier fractionné peut être interrompue une fois et la seconde partie du temps de repos journalier fractionné peut être interrompue une fois.**

L'UEV calcule ensuite un temps de repos journalier fractionné lorsque le temps de repos accumulé calculé conformément au point 3 est :

- **D'au moins 3 heures et de moins de 11 heures pour la première période de repos et d'au moins 9 heures pour la seconde période de repos, lorsque la première période de repos a été interrompue par un TRAJET EN FERRY/TRAIN ;**
- **D'au moins 3 heures et de moins de 9 heures pour la première période de repos et d'au moins 9 heures pour la deuxième période de repos, lorsque la première période de repos n'a pas été interrompue par un TRAJET EN FERRY/TRAIN.**

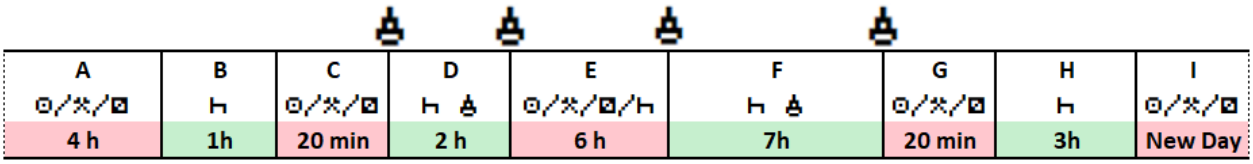


Figure 2. Exemple de temps de repos journalier fractionné en raison d'un trajet en ferry/train

Lorsqu'un temps de repos journalier fractionné est interrompu, l'UEV :

- **N'inclut pas l'activité de conduite détectée pendant ces interruptions dans le calcul du temps de conduite journalier ; et**
- **Commence une nouvelle période de travail RTM à la fin du temps de repos journalier fractionné qui a été interrompu ;**

k) « semaine », la période comprise entre 00 h 00 le lundi et 24 h 00 le dimanche (heure UTC).

3. Calcul d'un temps repos interrompu en raison d'un trajet en ferry/train

Pour le calcul du temps de repos lorsque celui-ci a été interrompu en raison d'un trajet en ferry/train, l'UEV calcule le temps de repos accumulé selon les étapes suivantes :

a) Étape 1

L'UEV détecte les interruptions du temps de repos intervenues avant l'activation du drapeau TRAJET EN FERRY/TRAIN (début) comme indiqué à la figure 3 et, le cas échéant, à la figure 4, et évalue pour chaque interruption détectée si les conditions suivantes sont remplies :

- **L'interruption fait que la durée totale des interruptions détectées, y compris, le cas échéant, des interruptions survenues pendant la première partie d'un temps de repos journalier fractionné en raison d'un trajet en ferry/train, dépasse une heure au total ;**
- **L'interruption fait que le nombre total d'interruptions détectées, y compris, le cas échéant, des interruptions survenues pendant la première partie d'un temps de repos journalier fractionné en raison d'un trajet en ferry/train, est supérieur à deux ;**
- **Une « saisie du lieu de fin de la période de travail journalière » a été enregistrée après la fin de l'interruption.**

Si aucune des conditions ci-dessus n'est remplie, le temps de repos continu précédant immédiatement l'interruption est ajouté au temps de repos accumulé.

Si au moins l'une des conditions ci-dessus est remplie, l'UEV doit soit interrompre le calcul du temps de repos accumulé comme prévu à l'étape 2, soit détecter les interruptions du temps de repos survenues après l'activation du drapeau TRAJET EN FERRY/TRAIN (début) comme prévu à l'étape 3.

b) Étape 2

Pour chaque interruption détectée à l'étape 1, l'UEV doit déterminer si le calcul du temps de repos accumulé doit être arrêté. L'UEV met fin au processus de calcul lorsque deux temps de repos continus survenus avant l'activation du drapeau TRAJET EN

FERRY/TRAIN (début) ont été ajoutés au temps de repos accumulé, y compris, le cas échéant, les temps de repos ajoutés dans la première partie d'un temps de repos journalier fractionné également interrompu par un trajet en ferry/train. Si ce n'est pas le cas, l'UEV procède conformément à l'étape 3.

c) Étape 3

Si, après la réalisation de l'étape 2, l'UEV poursuit le calcul du temps de repos accumulé, elle doit détecter les interruptions survenues après la désactivation de la condition TRAJET EN FERRY/TRAIN comme indiqué à la figure 3 et, le cas échéant, à la figure 4.

Pour chaque interruption constatée, l'UEV doit déterminer si l'interruption fait que le temps accumulé de toutes les interruptions détectées dépasse une heure au total, auquel cas le calcul du temps de repos accumulé se termine à la fin du temps de repos continu précédant l'interruption. Dans le cas contraire, les temps de repos continus postérieurs aux interruptions correspondantes doivent être ajoutés au calcul du temps de repos journalier jusqu'à ce que la condition de l'étape 4 soit remplie.

d) Étape 4

Le calcul du temps de repos accumulé s'arrête lorsque l'UEV a ajouté, à la suite des étapes 1 et 3, un maximum de deux temps de repos continus à la période de repos pour laquelle la condition TRAJET EN FERRY/TRAIN a été activée, y compris, le cas échéant, les interruptions survenues au cours de la première partie d'un temps de repos journalier fractionné en raison d'un trajet en ferry/train.

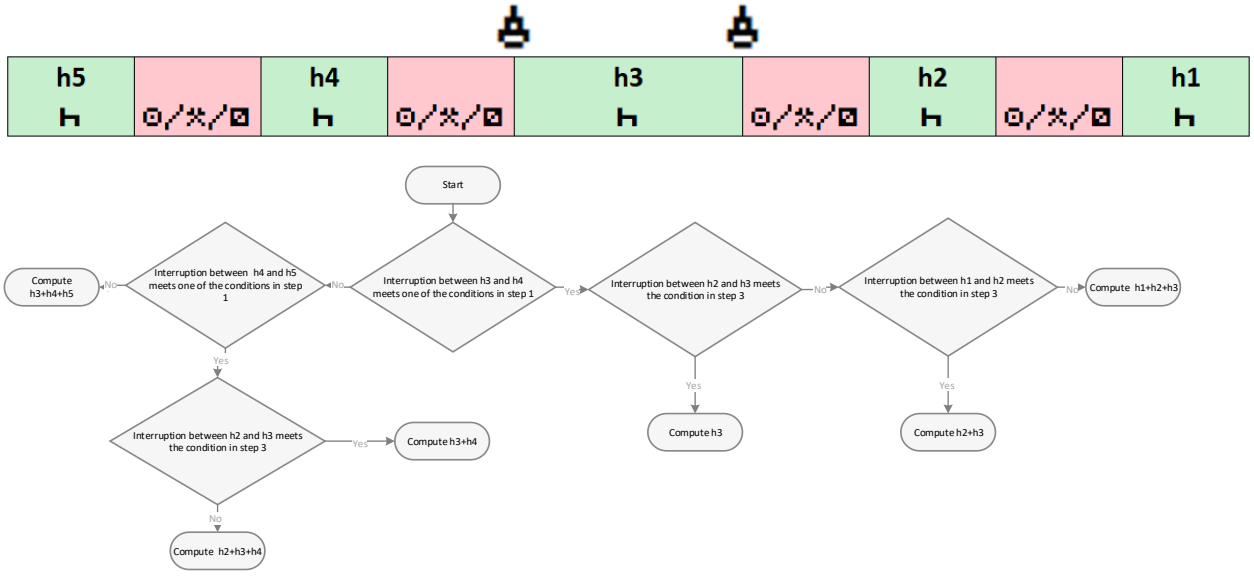


Figure 3. Traitement des temps de repos par l'UEV afin de déterminer si un temps de repos interrompu doit être calculé comme un temps de repos journalier normal ou comme la première partie d'un temps de repos journalier fractionné

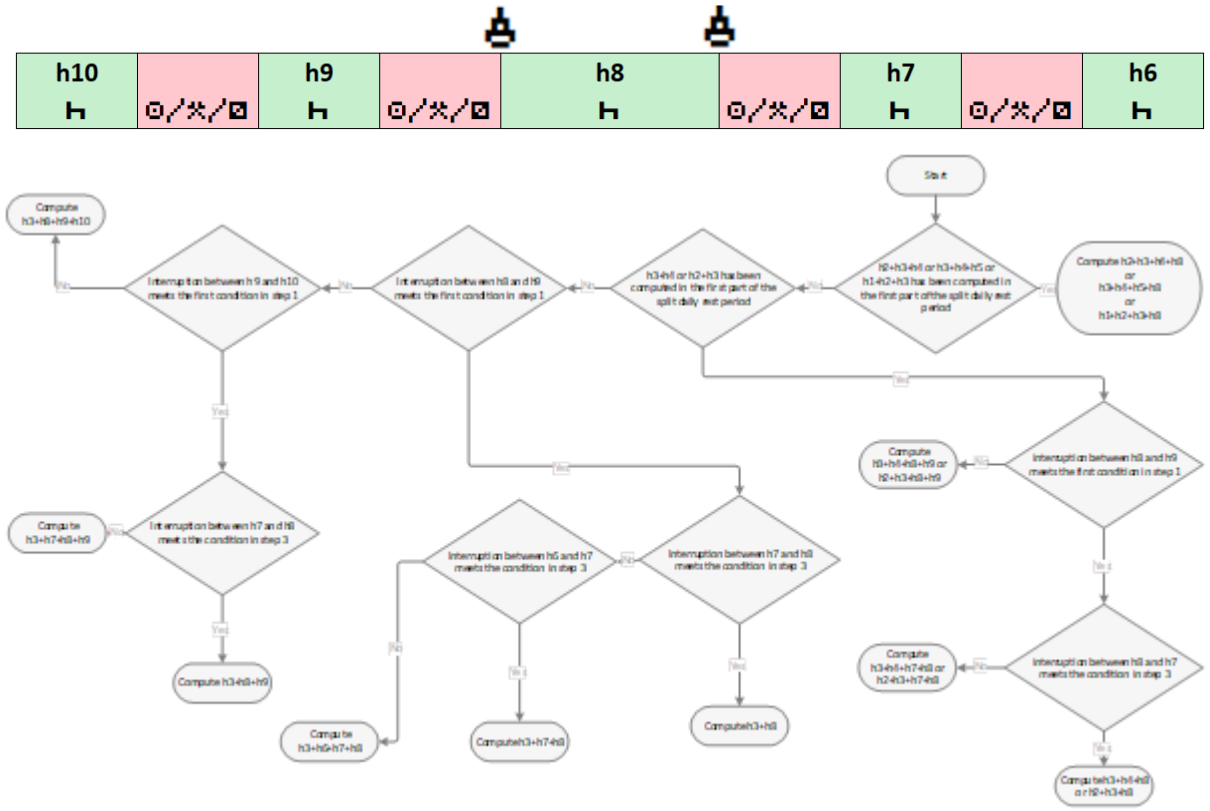


Figure 4. **Traitement des temps de repos par l'UEV afin de déterminer si un temps de repos interrompu doit être calculé comme la deuxième partie d'un temps de repos journalier fractionné**

A	B	C	D	E	F	G	H	I
4,5h	2h	20 min	1h	20 min	8h	20 min	2h	
Working	Rest	Movement	Rest	Embarking	Rest on Ferry	Disembark	Rest	
						Start of new shift due to three interruptions		Manually selected Start of new work period

Figure 5. **Exemple de temps de repos journalier interrompu plus de deux fois entraînant la non-inclusion du temps de repos H dans le calcul**

A	B	C	D	E	F	G	H	I
4,5h	2h	20 min	1h	20 min	8h	20 min	2h	
Working	Rest	Movement	Rest	Embarking	Rest on Ferry	Disembark	Rest	
			Manually selected End of work period					Manually selected Start of new work period

Start of New Shift

Figure 6. **Exemple de temps de repos journalier où la période de calcul des trajets en ferry/train commence à la fin de la période de travail**

A	B	C	D	E	F	G	H	I
4,5h	1h	10 min	1h	10 min	1h	10 min	9h	
Working	Rest	Movement	Rest	Movement	Rest	Embarking	Rest on ferry	
								Start of New Shift

Figure 7. **Exemple de temps de repos journalier interrompu plus de deux fois entraînant la non-inclusion du temps de repos B dans le calcul**

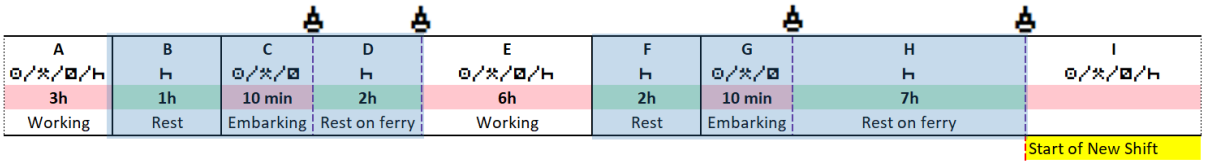


Figure 8. **Exemple de temps de repos journalier fractionné interrompu une fois pendant le premier temps de repos et une fois pendant le deuxième temps de repos**

4. Calcul des temps de conduite journalier, hebdomadaire et pour deux semaines

L'UEV calcule le ou les temps de conduite journaliers pour les périodes de travail RTM en cours et antérieures. Le temps de conduite survenu pendant les interruptions des temps de repos journaliers n'est pas ajouté au calcul du temps de conduite journalier, lorsque ces interruptions sont dues à des trajets en ferry/train et que les exigences énoncées aux points 2 h) et 2 j) ainsi qu'au point 3 sont remplies. Néanmoins, dans la mesure où un temps de repos journalier normal ou fractionné n'a pas été calculé par l'UEV conformément au point 3, les temps de conduite survenus pendant les interruptions doivent être ajoutés au temps de conduite journalier pour la période de travail RTM en cours.

L'UEV calcule également les temps de conduite hebdomadaires et les temps de conduite pour deux semaines. Le temps de conduite survenu pendant les interruptions des temps de repos journaliers en raison de trajets en ferry/train est ajouté au calcul des temps de conduite hebdomadaires et des temps de conduite pour deux semaines.

~~Appendice~~ Sous-appendice 15

Migration : gérer la coexistence de plusieurs générations d'équipements

Table des matières

1. Définitions

Aux fins du présent **sous-**appendice, les définitions suivantes sont appliquées :

Tachygraphe intelligent : tel que défini par ~~la présente annexe~~ **le présent appendice** (chap. 1 : définition bbb)) ;

Tachygraphe de première génération : tel que défini ~~par le présent règlement~~ **dans l'introduction du présent appendice** ~~(article 2 : définition 1)~~ ;

Tachygraphe de deuxième génération : tel que défini ~~par le présent règlement~~ **dans l'introduction du présent appendice** ~~(article 2 : définition 7)~~ ;

Date de lancement : telle que définie par ~~la présente annexe~~ **le présent appendice** (chap. 1 : définition ccc)) ;

Équipement spécialisé intelligent (IDE) : équipement servant à télécharger des données, tel que défini ~~à l'appendice~~**au sous-appendice** 7 ~~de la présente annexe~~ **du présent appendice**.

2. Dispositions générales

2.1 Présentation de la transition

~~Le préambule~~ **L'introduction** ~~de la présente annexe~~ **du présent sous-appendice** donne un aperçu de la transition de la première à la deuxième génération de tachygraphes, **et du lancement de la deuxième version d'appareils de contrôle et de cartes tachygraphiques de deuxième génération.**

Outre les dispositions de la présente **introduction, il convient de rappeler les informations suivantes** ~~préambule~~ :

- La première génération de capteurs de mouvement **n'est** ~~ne sera~~ pas interopérable avec la deuxième génération d'unités embarquées**, indépendamment de leur version** ;
- **Seuls des** ~~L'installation de la deuxième génération des~~ capteurs de mouvement **de deuxième génération peuvent être installés** dans les véhicules **équipés** ~~commencera en même temps que celle de la deuxième génération~~ d'unités embarquées **de deuxième génération, indépendamment de leur version** ;
- Les équipements destinés au téléchargement des données et à l'étalonnage **doivent** ~~devront évoluer pour~~ être compatibles avec les deux générations **ou versions** ~~d'équipement d'enregistrement~~ **d'appareils de contrôle** et de cartes tachygraphiques.

2.2 Interopérabilité entre les unités embarquées et les cartes

Il est entendu que la première génération de cartes tachygraphiques est interopérable avec la première génération d'unités embarquées ~~(~~conformément à ~~l'annexe 1B de la présente directive)~~ **l'appendice 1B**, ~~alors~~ **et** que la deuxième génération de cartes tachygraphiques est interopérable avec la deuxième génération d'unités embarquées, indépendamment de la version, ~~(~~conformément à ~~l'annexe~~ **l'appendice** 1C ~~de la présente directive)~~ **du présent Accord**. En outre, les exigences ci-dessous s'appliquent.

MIG_001 Sous réserve des dispositions prévues aux exigences MIG_004 et MIG_005, les cartes tachygraphiques de première génération peuvent continuer à être utilisées dans les unités embarquées de deuxième génération**, indépendamment de leur version,** jusqu'à leur date d'expiration. Leurs détenteurs peuvent toutefois demander leur replacement par des cartes tachygraphiques de deuxième génération dès que ces dernières sont disponibles.

MIG_002 Toutes les versions d'unités embarquées de deuxième génération pourront utiliser toute carte de conducteur, de contrôleur et d'entreprise de première génération valide qui aura été insérée.

MIG_003 Les ateliers peuvent supprimer définitivement cette possibilité dans lesdites unités embarquées, de sorte que la première génération de cartes tachygraphiques ne soit plus acceptée. Cela ne pourra avoir lieu qu'après ~~que la Commission européenne aura lancé~~ **le lancement** une procédure visant à demander aux ateliers de procéder ainsi, notamment à chaque inspection périodique du tachygraphe.

MIG_004 Les unités embarquées de deuxième génération ne peuvent utiliser que des cartes d'ateliers de deuxième génération.

MIG_005 Afin de déterminer le mode de fonctionnement des unités embarquées de deuxième génération**, quelle que soit leur version**, il suffira d'examiner les types de cartes valides insérées, indépendamment de leur génération **ou de leur version**.

MIG_006 Toute carte tachygraphique de deuxième génération valide**, indépendamment de sa version,** peut être utilisée sur des unités embarquées de première génération exactement de la même manière qu'une carte tachygraphique de première génération de même type.

2.3 Interopérabilité entre les unités embarquées et les capteurs de mouvement

Il est entendu que la première génération de capteurs de mouvement est interopérable avec la première génération d'unités embarquées, et que la deuxième génération de capteurs de mouvement est interopérable avec la deuxième génération d'unités embarquées sur les véhicules**, indépendamment de la version**. En outre, les exigences ci-dessous s'appliquent.

MIG_007 Les unités embarquées de deuxième génération**, indépendamment de leur version,** ne ~~pourront~~ **peuvent** pas être couplées et utilisées avec des capteurs de mouvement de première génération.

MIG_008 Les capteurs de mouvement de deuxième génération peuvent être couplés et utilisés soit uniquement avec des unités embarquées de deuxième génération, **indépendamment de leur version,** soit avec les deux générations d'unités embarquées.

2.4 Interopérabilité entre les unités embarquées, les cartes tachygraphiques et l'équipement de téléchargement de données

MIG_009 L'équipement de téléchargement de données peut être **compatible** ~~utilisé~~ avec ~~une seule~~ **toutes les** générations **et toutes les versions** d'unités embarquées et de cartes tachygraphiques ~~ou avec les deux~~.

2.4.1 Téléchargement direct de carte par l'ESI

MIG_010 Les données sont téléchargées par l'ESI à partir des cartes tachygraphiques d'une génération particulière qui ont été insérées dans les lecteurs de cartes, selon les mécanismes de sécurité et les protocoles de téléchargement de données applicables à cette génération, et les données téléchargées sont au format défini pour la génération **et la version** correspondante**.**

MIG_011 Pour permettre aux autorités de contrôles autres que celles de l'UE de contrôler les conducteurs, il doit également être possible de télécharger des cartes de conducteurs (et d'ateliers) de deuxième génération**, quelle que soit leur version,** de la même manière que les cartes de conducteurs (et d'ateliers) de première génération. Ce type de téléchargement comprend :

- Les EF IC et ICC non signés **(facultatif)** ;
- Les EF (de première génération) Card_Certificate et CA_Certificate non signés ;

- Les autres EF de données d'application (dans le DF **Tachograph**) requis par le protocole de téléchargement des cartes de première génération. Ces informations doivent être protégées par une signature numérique, conformément aux mécanismes de sécurité de première génération.

Ce type de téléchargement ne comprend pas les EF de données d'application présents uniquement sur les cartes de conducteurs (et d'ateliers) de deuxième génération, **versions 1 et 2** (c'est-à-dire les EF de données d'application figurant dans le **DF Tachograph**_G2).

2.4.2 Téléchargement de carte par l'intermédiaire d'une unité embarquée

MIG_012 Les données sont téléchargées à partir d'une carte de deuxième génération**, indépendamment de sa version,** insérée dans une unité embarquée de première génération selon le protocole de téléchargement de données de première génération. La carte réagit aux commandes de l'unité embarquée exactement de la même manière qu'une carte de première génération. Les données téléchargées ont le même format que les données téléchargées à partir d'une carte de première génération.

MIG_013 Les données sont téléchargées à partir d'une carte de première génération insérée dans une unité embarquée de deuxième génération selon le protocole de téléchargement de données défini ~~à l'appendice~~**au sous-appendice** 7 ~~de la présente annexe~~ **du présent appendice**. L'unité embarquée adresse des commandes à la carte exactement de la même manière qu'une unité embarquée de première génération. Les données téléchargées ont la structure définie pour les cartes de première génération.

2.4.3 Téléchargement à partir d'une unité embarquée

MIG_014 ~~Les~~ **Hors du cadre du contrôle des conducteurs par des autorités de contrôles autres que celles de l'UE, les** données sont téléchargées à partir d'une unité embarquée de deuxième génération selon les mécanismes de sécurité de deuxième génération et le protocole de téléchargement de données défini ~~à l'appendice~~**au sous-appendice** 7 ~~de la présente annexe~~ **du présent appendice**.

MIG_015 Pour permettre le contrôle des conducteurs par des autorités de contrôles autres que celles de l'UE, il peut également être rendu possible de télécharger des données à partir d'unités embarquées de deuxième génération**, quelle que soit leur version,** en appliquant les mécanismes de sécurité de première génération et le protocole de téléchargement de données de première génération. Les données téléchargées ont **alors** le même format que les données téléchargées depuis une unité embarquée de première génération. Cette fonctionnalité peut être sélectionnée à l'aide des commandes se trouvant dans le menu.

2.5 Interopérabilité entre les unités embarquées et l'équipement d'étalonnage

MIG_016 L'équipement d'étalonnage doit permettre l'étalonnage de chaque génération **ou version** de tachygraphe en appliquant le protocole d'étalonnage de la génération correspondante. L'équipement d'étalonnage peut être ~~utilisé~~ **compatible** avec ~~une seule~~ **toutes les** génération**s et versions** de tachygraphe ~~ou avec les deux~~.

3. Principales étapes précédant le lancement

MIG_017 Les clés et les certificats d'essai seront à la disposition des fabricants ~~au moins **30 mois** avant~~ **à** la date ~~d'introduction~~ **de publication du présent appendice**.

MIG_018 Les essais d'interopérabilité **concernant la version 2 des unités embarquées et des cartes tachygraphiques** seront prêts à commencer sur demande des fabricants au plus tard **15 mois** avant la date de lancement.

MIG_019 **Pour la version 2 de la deuxième génération de tachygraphes, de cartes tachygraphiques et de capteurs de mouvement,** ~~L~~l**es mêmes** clés et ~~les~~ certificats ~~officiels~~ seront **utilisés que pour la version 1 de la deuxième génération d'équipements** ~~à la disposition des fabricants au moins **12 mois** avant la date de lancement~~.

MIG_020 Les ~~États membres~~ **Parties contractantes** pourront émettre des cartes d'ateliers de deuxième génération**, version 2,** au plus tard ~~3~~**1** mois avant la date de lancement.

MIG_021 Les ~~États membres~~ **Parties contractantes** pourront émettre tous les **autres** types de cartes tachygraphiques de deuxième génération**, version 2,** au plus tard **1 mois avant la date de lancement**.

4. Dispositions relatives à la période suivant le lancement

MIG_022 **À compter de** ~~Après~~ la date de lancement, les ~~États membres~~ **Parties contractantes** n'émettront que des cartes tachygraphiques de deuxième génération**, version 2**.

MIG_023 Les fabricants d'unités embarquées ou de capteurs de mouvement seront autorisés à produire des unités embarquées ou des capteurs de mouvement de première génération tant que ceux-ci resteront utilisés sur le terrain, de façon à pouvoir remplacer les composants qui dysfonctionneraient.

MIG_024 À compter de la date de lancement, les unités embarquées ou les dispositifs GNSS externes de deuxième génération, version 1, qui ne fonctionnent pas correctement seront remplacés par des unités embarquées ou des dispositifs GNSS externes de deuxième génération, version 2.

MIG_025~~4~~ ~~—~~Les fabricants d'unités embarquées ou de capteurs de mouvement seront autorisés à demander et à obtenir le maintien de l'homologation pour des unités embarquées ou des capteurs de mouvement de première génération, **ou pour des unités embarquées de deuxième génération, version 1,** ayant déjà été homologués.

~~Appendice~~ Sous-appendice 16

Adaptateur pour les véhicules des catégories M1 et N1

Table des matières

1. Abréviations et documents de référence

1.1 Abréviations

UEV Unité embarquée sur le véhicule *(VU, en anglais)*

1.2 Normes de référence

ISO 16844-3 Véhicules routiers − Systèmes tachygraphes − Partie 3 : interface de capteur de mouvement

2. Caractéristiques générales et fonctions de l'adaptateur

2.1 Description générale de l'adaptateur

ADA_001 L'adaptateur fournit en permanence à une UEV connectée des données de mouvement sécurisées représentatives de la vitesse du véhicule et de la distance parcourue.

L'adaptateur est conçu uniquement pour les véhicules qui doivent être équipés d'un appareil de contrôle conformément au présent ~~règlement~~ **Accord**.

Il est installé et utilisé uniquement dans les types de véhicules spécifiés dans la définition yy) « adaptateur » **de l'appendice 1C**, lorsqu'il n'est pas mécaniquement possible d'installer un autre type de capteur de mouvement existant par ailleurs conforme aux dispositions ~~de la présente annexe~~ **du présent appendice** et de ses **sous-**appendices 1 à 16.

L'adaptateur n'est pas relié mécaniquement à un élément mobile du véhicule, mais il est connecté aux impulsions de vitesse/distance produites par des capteurs intégrés ou d'autres interfaces.

ADA_002 Un capteur de mouvement homologué (conformément aux dispositions ~~de la présente annexe~~ **du présent appendice** 1C, chapitre 8, Homologation de l'appareil de contrôle et des cartes tachygraphiques) est installé dans le boîtier de l'adaptateur, qui comporte également un convertisseur d'impulsions orientant les impulsions entrantes vers le capteur de mouvement intégré. Le capteur de mouvement intégré est lui-même connecté à l'UEV, si bien que l'interface entre l'UEV et l'adaptateur est conforme aux exigences de la norme ISO 16844-3.

2.2 Fonctions

ADA_003 L'adaptateur comporte les fonctions suivantes :

- Interfaçage et adaptation des impulsions de vitesse entrantes ;
- Orientation des impulsions entrantes vers le capteur de mouvement intégré ;
- Toutes les fonctions du capteur de mouvement intégré, fournissant des données de mouvement sécurisées à l'UEV.

2.3 Sécurité

ADA_004 La sécurité de l'adaptateur n'est pas certifiée conformément aux objectifs de sécurité générique du capteur de mouvement définis ~~à l'appendice~~ **au sous-appendice** 10 ~~de la présente annexe~~ **du présent appendice**, mais conformément aux exigences de sécurité spécifiées à la section 4.4 du présent **sous-**appendice.

3. Exigences relatives à l'appareil de contrôle lorsqu'un adaptateur est installé

Les exigences figurant dans les chapitres qui suivent indiquent comment les exigences énoncées dans ~~la présente annexe~~ **le présent sous-appendice** doivent être comprises lorsqu'un adaptateur est utilisé. Les numéros des exigences **de l'appendice 1C** concernées sont indiqués entre parenthèses.

ADA_005 L'appareil de contrôle de tout véhicule équipé d'un adaptateur doit être conforme à toutes les dispositions ~~de la présente annexe~~ **du présent sous-appendice**, sauf indications contraires dans le présent **sous-**appendice.

ADA_006 Lorsqu'un adaptateur est installé, l'appareil de contrôle comporte des câbles, l'adaptateur (comprenant un capteur de mouvement) et une UEV [01].

ADA_007 La fonction de détection d'événements et/ou d'anomalies de l'appareil de contrôle est modifiée comme suit :

- L'événement « interruption de l'alimentation électrique » est déclenché par l'UEV, en mode autre qu'étalonnage, en cas d'interruption pendant plus de 200 millisecondes (ms) de l'alimentation électrique du capteur de mouvement intégré [79] ;
- L'événement « erreur sur les données de mouvement » est déclenché par l'UEV en cas d'interruption du flux normal de données entre le capteur de mouvement intégré et l'UEV et/ou en cas d'erreur d'intégrité ou d'authentification des données au cours de l'échange de données entre le capteur de mouvement intégré et l'UEV [83] ;
- L'événement « tentative d'atteinte à la sécurité » est déclenché par l'UEV pour tout autre événement affectant la sécurité du capteur de mouvement intégré, dans les modes autres qu'étalonnage [85] ;
- L'anomalie « appareil de contrôle » est déclenchée par l'UEV, en mode autre qu'étalonnage, pour toute anomalie du capteur de mouvement intégré [88].

ADA_008 Les anomalies de l'adaptateur détectables par l'appareil de contrôle sont celles liées au capteur de mouvement intégré [88].

ADA_009 La fonction d'étalonnage de l'UEV permet de coupler automatiquement le capteur de mouvement intégré à l'UEV [202, 204].

4. Exigences de construction et de fonctionnement de l'adaptateur

4.1 Interfaçage et adaptation des impulsions de vitesse entrantes

ADA_011 L'interface d'entrée de l'adaptateur accepte les impulsions de fréquence représentatives de la vitesse du véhicule et de la distance parcourue. Les caractéristiques électriques des impulsions entrantes sont à définir par le fabricant. Les ajustements réalisables uniquement par le fabricant de l'adaptateur et l'atelier agréé qui procède à l'installation de l'adaptateur permettent le bon interfaçage de l'adaptateur au véhicule, le cas échéant.

ADA_012 L'interface d'entrée de l'adaptateur peut, le cas échéant, multiplier ou diviser les impulsions de fréquence des impulsions de vitesse entrantes par un facteur fixe pour adapter le signal à l'intervalle de valeurs du facteur k défini dans ~~la présente annexe~~ **le présent appendice** (**2** 400~~0~~ à 25 000 impulsions/km). Ce facteur fixe ne peut être programmé que par le fabricant de l'adaptateur et l'atelier agréé qui effectue l'installation de l'adaptateur.

4.2 Orientation des impulsions entrantes vers le capteur de mouvement intégré

ADA_013 Les impulsions entrantes, éventuellement adaptées comme indiqué ci-dessus, sont orientées vers le capteur de mouvement intégré de sorte que chaque impulsion entrante soit détectée par le capteur de mouvement.

4.3 Capteur de mouvement intégré

ADA_014 Le capteur de mouvement intégré est stimulé par les impulsions, ce qui lui permet de générer des données de mouvement représentant exactement les mouvements du véhicule, comme s'il était mécaniquement couplé à un élément mobile du véhicule.

ADA_015 Les données d'identification du capteur de mouvement intégré sont utilisées par l'UEV pour identifier l'adaptateur [95].

ADA_016 Les données d'installation stockées dans le capteur de mouvement intégré sont considérées comme représentant les données d'installation de l'adaptateur [122].

4.4 Exigences de sécurité

ADA_017 Le boîtier de l'adaptateur ne doit pas pouvoir être ouvert. Il est scellé de telle manière que toute tentative de manipulation soit aisément décelable (par exemple, par une inspection visuelle, voir ADA_035). Les scellements doivent satisfaire aux mêmes exigences que les scellements des capteurs de mouvement (398 à 406).

ADA_018 Il doit être impossible de retirer le capteur de mouvement intégré de l'adaptateur sans rompre le(s) scellement(s) du boîtier de l'adaptateur ou le scellement entre le capteur et le boîtier de l'adaptateur (voir ADA_034).

ADA_019 L'adaptateur garantit que les données de mouvement ne peuvent être traitées et dérivées qu'à partir des données entrantes de l'adaptateur.

4.5 Caractéristiques de performance

ADA_020 L'adaptateur doit fonctionner correctement dans la gamme de températures définie par le fabricant.

ADA_021 L'adaptateur doit fonctionner correctement dans une plage d'humidité comprise entre 10 % et 90 % [214].

ADA_022 L'adaptateur doit être protégé contre les surtensions, l'inversion de polarité et les courts-circuits [216].

ADA_023 L'adaptateur doit :

- Soit réagir à un champ magnétique qui perturbe la détection des mouvements du véhicule. Dans de telles circonstances, l'unité embarquée enregistrera et stockera une anomalie du capteur [88] ;
- Soit posséder un élément de détection protégé des champs magnétiques ou insensible à ceux-ci [217].

ADA_024 L'adaptateur doit être conforme au Règlement ONU n° 10, relatif à la compatibilité électromagnétique, et être protégé contre les décharges électrostatiques et transitoires [218].

4.6 Matériaux

ADA_025 L'adaptateur doit satisfaire au niveau de protection (à définir par le fabricant, en fonction de l'emplacement de l'installation [220, 221].

ADA_026 Le boîtier de l'adaptateur doit être jaune.

4.7 Inscriptions

ADA_027 Une plaque signalétique doit être fixée sur l'adaptateur et comporter les indications suivantes :

- Nom et adresse du fabricant de l'adaptateur ;
- Numéro de pièce du fabricant et année de fabrication de l'adaptateur ;
- Marque d'homologation du type d'adaptateur ou du type d'appareil de contrôle incluant l'adaptateur ;
- Date d'installation de l'adaptateur ;
- Numéro d'identification du véhicule sur lequel il est installé.

ADA_028 La plaque signalétique doit aussi comporter les indications suivantes (si elles ne sont pas directement visibles de l'extérieur du capteur de mouvement intégré) :

- Nom du fabricant du capteur de mouvement intégré ;
- Numéro de pièce du fabricant et année de fabrication du capteur de mouvement intégré ;
- Marque d'homologation du capteur de mouvement intégré.

5. Installation de l'appareil de contrôle lorsqu'un adaptateur est utilisé

5.1 Installation

ADA_029 Les adaptateurs à installer dans les véhicules le sont uniquement par des constructeurs de véhicules ou par des ateliers agréés autorisés à installer, activer et étalonner les tachygraphes numériques et intelligents.

ADA_030 L'atelier agréé qui installe l'adaptateur règle l'interface d'entrée et choisit le taux de division du signal d'entrée (le cas échéant).

ADA_031 L'atelier agréé qui installe l'adaptateur scelle le boîtier de l'adaptateur.

ADA_032 L'adaptateur doit être monté aussi près que possible de la partie du véhicule qui lui fournit ses impulsions d'entrée.

ADA_033 Les câbles fournissant l'alimentation de l'adaptateur sont rouges (courant positif) et noirs (câbles de terre).

5.2 Scellement

ADA_034 Les exigences suivantes en matière de scellement doivent être respectées :

- Le boîtier de l'adaptateur doit être scellé (voir ADA_017) ;
- Le boîtier du capteur intégré doit être scellé au boîtier de l'adaptateur, à moins qu'il ne soit pas possible de retirer le capteur intégré sans rompre le(s) scellement(s) du boîtier de l'adaptateur (voir ADA_018) ;
- Le boîtier de l'adaptateur doit être scellé au véhicule ;
- La connexion entre l'adaptateur et l'équipement qui lui fournit ses impulsions d'entrée doit être scellée aux deux extrémités (dans la mesure où cela est raisonnablement possible).

6. Contrôles, inspections et réparations

6.1 Inspections périodiques

ADA_035 Lorsqu'un adaptateur est utilisé, chaque inspection périodique (conformément aux exigences 409 à 413 de ~~l'annexe~~ **l'appendice** 1C) de l'appareil de contrôle comprend les vérifications suivantes :

- L'adaptateur porte les marques d'homologation appropriées ;
- Les scellements placés sur l'adaptateur et ses connexions sont intacts ;
- L'adaptateur est installé comme indiqué sur la plaquette d'installation ;
- L'adaptateur est installé comme spécifié par le fabricant de l'adaptateur et/ou du véhicule ;
- Le montage d'un adaptateur est autorisé pour le véhicule inspecté.

ADA_036 Ces inspections comprennent également un étalonnage et un remplacement de tous les scellements, quel que soit leur état.

7. Homologation de l'appareil de contrôle lorsqu'un adaptateur est utilisé

7.1 Points généraux

ADA_037 L'appareil de contrôle doit être présenté pour homologation dans son intégralité, avec l'adaptateur [425].

ADA_038 Tout adaptateur peut être présenté pour homologation en tant que tel ou en tant que composant d'un appareil de contrôle.

ADA_039 Une telle homologation doit comprendre des essais de fonctionnement portant sur l'adaptateur. Les résultats positifs à chacun de ces essais sont attestés par un certificat approprié [426].

7.2 Certificat de fonctionnement

ADA_040 Le certificat de fonctionnement d'un adaptateur ou d'un appareil de contrôle comportant un adaptateur n'est délivré au fabricant de l'adaptateur que si les essais de fonctionnement minimaux suivants ont été passés avec succès.

Nº	*Essai*	*Description*	*Exigences connexes*
1.	**Examen administratif**		
1.1	Documentation	Exactitude de la documentation de l'adaptateur	
2.	**Inspection visuelle**		
2.1	Conformité de l'adaptateur à la documentation		
2.2	Identification/marquage de l'adaptateur		ADA_027, ADA_028
2.3	Matériaux de l'adaptateur		[219] à [223] ADA_026
2.4	Scellement		ADA_017, ADA_018, ADA_034
3.	**Essais de fonctionnement**		
3.1	Orientation des impulsions de vitesse vers le capteur de mouvement intégré		ADA_013
3.2	Interfaçage et adaptation des impulsions de vitesse entrantes		ADA_011, ADA_012
3.3	Précision de la mesure des mouvements		[30] à [35], [217]
4.	**Essais environnementaux**		
4.1	Résultats des essais effectués par le fabricant	Résultats des essais environnementaux effectués par le fabricant	ADA_020, ADA_021, ADA_022, ADA_024
5.	**Essais de compatibilité électromagnétique**		
5.1	Émissions rayonnées et susceptibilité	Vérifier la conformité avec ~~la Directive 2006/28/EC~~ **le Règlement ONU nº 10**	ADA_024
5.2	Résultats des essais effectués par le fabricant	Résultats des essais environnementaux effectués par le fabricant	ADA_024