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

Conseil économique et social

Distr.: générale
17 janvier 2018
Français
Original: anglais, français et russe

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)

Dix-septième session
Genève, 19 février 2018
Point 2 b) de l'ordre du jour provisoire
Programme de travail

Appendice 1C

Soumis par l'Estonie *

Ce document contient l'annexe IC du règlement (UE) 2016/799. Le document devrait être utilisé avec les propositions d'amendement figurant dans le document ECE/TRANS/SC.1/GE.21/2018/1.

* Le document est reproduit tel que soumis.

FR

ANNEXE I C
Exigences de construction, d'essai, d'installation et de contrôle

INTRODUCTION

Le tachygraphe numérique de première génération est déployé depuis le 1er mai 2006. 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.

La présente annexe contient les exigences relatives aux appareils de contrôle et cartes tachygraphiques de deuxième génération.
À partir de sa date de mise en œuvre, l'appareil de contrôle de deuxième génération devra être installé dans les véhicules immatriculés pour la première fois et des cartes tachygraphiques de deuxième génération devront être délivrées.
Afin de favoriser une mise œuvre sans heurts du tachygraphe de deuxième génération:

- les cartes tachygraphiques de deuxième génération doivent être conçues pour être également utilisées dans les unités embarquées de première génération,
- le remplacement des cartes tachygraphiques de première génération en cours de validité à la date de mise œuvre ne sera pas exigé.

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

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

La présente annexe contient toutes les exigences liées à l'interopérabilité entre les tachygraphes de première et de deuxième générations.

L'appendice 15 contient des détails supplémentaires sur la façon dont la coexistence des deux systèmes doit être gérée.

Liste des 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 DE DONNÉES

App 8: PROTOCOLE D'ÉTALONNAGE

App 9: HOMOLOGATION ET LISTE DES ESSAIS MINIMAUX REQUIS

App 10: EXIGENCES EN MATIÈRE DE SÉCURITÉ

App 11: MÉCANISMES DE SÉCURITÉ COMMUNS

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

App 13: INTERFACE ITS

App 14: FONCTION DE COMMUNICATION À DISTANCE

1 Définitions

Dans la présente annexe, 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 allant de minuit à minuit (24 heures). Tous les jours civils sont liés à l'heure universelle coordonnée (UTC);

f) «étalonnage» d'un tachygraphe intelligent signifie:
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 (VIN), numéro d'immatriculation (VRN) et État membre d'immatriculation] et les caractéristiques du véhicule [w, k, l, taille des pneumatiques, réglage du limiteur de vitesse (le cas échéant), heure UTC, kilométrage]; pendant l'étalonnage d'un appareil de contrôle, les types et les identifiants des scellements pertinents pour l'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; ce numéro comporte un indice séquentiel de la carte (le cas échéant), un indice de remplacement de la carte et un indice de renouvellement de la carte;
chaque carte est ainsi identifiable par le code de l'État membre qui l'a délivrée et par le numéro de carte;

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(e) 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 du tachygraphe;

j) «indice de remplacement de la carte»:
le 15e caractère alphanumérique du numéro de carte, incrémenté à chaque remplacement de la carte tachygraphique;

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 boîte de vitesses ou essieu) pendant que le véhicule se déplace sur une distance d'un kilomètre dans les conditions d'essai standard telles que définies dans 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 État membre 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 données ont été verrouillées par cette même entreprise;

m) «constante de l'appareil de contrôle»:
la caractéristique numérique 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», le temps de conduite continue calculé par l'appareil de contrôle comme étant[1]:
la somme des temps de conduite accumulés par un conducteur donné depuis la fin de sa dernière période de DISPONIBILITÉ ou de PAUSE/REPOS ou INCONNUE[2] de 45 minutes ou plus [cette période peut avoir été divisée conformément au règlement (CE) n° 561/2006]. 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 correspondant au lecteur pertinent;

o) «carte de contrôleur»:
une carte tachygraphique délivrée par les autorités d'un État membre à une autorité nationale de contrôle compétente, ladite carte permettant l'identification de l'organisme de contrôle et, facultativement, de l'agent de contrôle, ainsi que l'accès aux données stockées dans la mémoire ou sur les cartes de conducteur et, facultativement, sur les cartes d'atelier, pour lecture, impression et/ou téléchargement;
elle donne également accès à la fonction de contrôle de l'étalonnage routier et aux données se trouvant sur le lecteur de communication de détection précoce à distance.

p) «temps de pause cumulé», », le temps de pause cumulé calculé par l'appareil de contrôle comme étant[1]:
la somme des périodes de DISPONIBILITÉ ou de PAUSE/REPOS ou INCONNUES[2] de 15 minutes ou plus accumulées par un conducteur donné, depuis la fin de sa dernière période de DISPONIBILITÉ ou PAUSE/REPOS ou INCONNUE[2] de 45 minutes ou plus [cette période peut avoir été divisée conformément au règlement (CE) n° 561/2006.]
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 pour la période en cours où aucune carte n'a été insérée et correspondant au lecteur pertinent;

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, qui permettent à son destinataire d'avoir la preuve de son authenticité et de son intégrité;

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

[2] Les périodes INCONNUES 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.

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 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 prennent toutes les dispositions appropriées, dans la mesure du raisonnable, pour que les entreprises de transport ou les conducteurs puissent effectuer le téléchargement de ces données dans les meilleurs délais. Il se peut que le téléchargement du fichier de relevés détaillés de la vitesse ne soit pas nécessaire pour établir la conformité avec le règlement (CE) n° 561/2006, 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 État membre à un conducteur. La carte tachygraphique permet l'identification du conducteur et le stockage des données relatives à son activité;

u) «circonférence effective des roues»:
la moyenne des distances parcourues par chacune des roues entraînant le véhicule (roues motrices) lors d'une rotation complète. La mesure de ces distances doit se faire dans les conditions normales d'essai telles que définies dans 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 et en ordre de marche[3]. Les méthodes suivies pour effectuer ce calcul théorique devront être approuvées par une autorité compétente de l'État membre et ne pourront 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 sur le véhicule;

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 en anglais) afin de déterminer la position, la vitesse et l'heure;

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 mécanisme mis en place entre les systèmes, qui leur permet de communiquer et d'interagir;

cc) «position»

[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.

les coordonnées géographiques du véhicule à un moment donné;

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

ee) «carte non valable»:
une carte détectée comme présentant un défaut, ou dont l'authentification initiale a échoué, ou dont la date de début de validité n'a pas encore été atteinte, ou dont la date d'expiration est passée;

ff) «norme ouverte»:
une norme définie dans une spécification de norme librement accessible ou disponible contre une somme symbolique et 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 n'est pas requise, conformément au règlement (CE) n° 561/2006;

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 de limitation 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;

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 la détection précoce à distance»:
la communication entre le dispositif de communication de la détection précoce à distance et le lecteur de communication de la détection précoce à distance lors de 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»:
l'équipement de l'unité embarquée sur le véhicule utilisé pour les contrôles routiers ciblés;

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

nn) «renouvellement»:
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;

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

pp) «remplacement de la carte»:
la délivrance d'une carte tachygraphique en remplacement d'une carte existante qui a été déclarée perdue, volée ou ne fonctionnant pas correctement, 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 consistant à certifier, par un organisme de certification «critères communs», que l'appareil de contrôle (ou le composant de cet appareil) ou la carte tachygraphique satisfait aux exigences de sécurité définies dans les profils de protection correspondants;

rr) «autotest»:
les 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 à intervalles réguliers et dans la limite d'une tolérance maximale d'une minute, ou un réglage effectué pendant l'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;

vv) «identification du véhicule»:
les numéros permettant d'identifier le véhicule: numéro d'immatriculation (VRN) avec indication de l'État membre d'immatriculation, et numéro d'identification du véhicule (VIN)[6];

ww) «semaine», aux fins du calcul dans l'appareil de contrôle:
une période comprise entre 00.00 heure UTC le lundi et 24.00 heures UTC le dimanche;

xx) «carte d'atelier»:
une carte tachygraphique délivrée par les autorités d'un État membre 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 État membre. La carte d'atelier permet l'identification du détenteur ainsi que l'essai, l'étalonnage et l'activation de tachygraphes et/ou le téléchargement à partir de ceux-ci;

yy) «adaptateur»:
un dispositif émettant un signal permanent représentatif de la vitesse et/ou de la distance parcourue par le véhicule, autre que celui qui est utilisé pour la détection de mouvement indépendante, et qui est:

- installé et utilisé uniquement sur les types de véhicules 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,
- installé lorsqu'il n'est pas mécaniquement possible d'installer un autre type de capteur de mouvement par ailleurs conforme aux dispositions de la présente annexe et de ses 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 fournies par des capteurs intégrés ou des interfaces de remplacement;
- vu d'une unité embarquée, le comportement de l'adaptateur est le même que si un capteur de mouvement, conforme aux dispositions de la présente annexe et de ses appendices 1 à 16, était connecté à l'unité embarquée sur le véhicule;

[5] JO L 129 du 14.5.1992, p. 95.
[6] Directive 76/114/CEE du 18.12.1975; JO L 24 du 30.1.1976, p. 1.

l'utilisation d'un tel adaptateur dans les véhicules décrits ci-dessus doit permettre l'installation et l'utilisation correcte d'une unité embarquée conforme à toutes les exigences de la présente annexe;
pour ces véhicules, le tachygraphe intelligent comprend des câbles, un adaptateur et une unité embarquée sur le véhicule;

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 endommagées lors des processus d'écriture et de lecture vers et à partir d'une carte tachygraphique, d'un équipement dédié 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;

bbb) «tachygraphe intelligent»:
l'appareil de contrôle, les cartes tachygraphiques et l'ensemble des équipements qui interagissent directement ou indirectement au cours de leur construction, 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 de données, à l'analyse des données, à l'étalonnage, à la génération, à la gestion ou à l'introduction d'éléments de sécurité, etc.;

ccc) date de mise en œuvre:
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 la date après laquelle les véhicules immatriculés pour la première fois:

- *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 de sécurité en matière de garantie de l'information;

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

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 présente annexe doit comporter un indicateur de vitesse et un compteur kilométrique. Ces fonctions peuvent être incluses dans l'appareil de contrôle.

01) L'appareil de contrôle comprend des câbles, un capteur de mouvement et une unité embarquée sur le véhicule.

02) L'interface entre les capteurs de mouvement et les unités embarquées se conforme aux dispositions de l'appendice 11.

03) L'unité embarquée sur le véhicule doit être connectée à un ou plusieurs systèmes mondiaux de navigation par satellite, comme indiqué à l'appendice 12.

04) L'unité embarquée sur le véhicule doit communiquer avec des lecteurs de communication et de détection précoces à distance conformément à l'appendice 14.

05) L'unité embarquée sur le véhicule peut comporter une interface ITS, qui est spécifiée à l'appendice 13.
L'appareil de contrôle peut être relié à d'autres équipements par le biais d'interfaces supplémentaires et/ou de l'interface ITS facultative.

06) Toute insertion ou connexion de toute fonction ou dispositif(s), homologué(s) 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.

Les utilisateurs de l'appareil de contrôle s'identifient dans l'appareil à l'aide de cartes tachygraphiques.

07) L'appareil de contrôle ouvre des droits d'accès sélectifs aux données et 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[7], 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[8] et en conformité avec l'article 7 du règlement (UE) n° 165/2014.

2.2 Fonctions

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

- surveillance des insertions et retraits de carte,
- 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,
- saisie manuelle de données par le conducteur:
    - lieu de début et/ou de fin des périodes journalières de travail,
    - saisie manuelle des activités du conducteur,
    - saisie des conditions particulières,
- gestion des verrouillages d'entreprise,
- suivi des activités de contrôle,
- détection des événements et/ou des anomalies,

[7] JO L 281 du 23.11.1995, p. 31.
8. JO L 201 du 31.7.2002, p. 37

- autotests intégrés,
- lecture de données stockées sur la mémoire,
- enregistrement et stockage de données sur la mémoire,
- lecture des cartes tachygraphiques,
- enregistrement et stockage de données sur les cartes tachygraphiques,
- affichage,
- impression,
- avertissement,
- téléchargement de données vers des médias externes,
- communication à distance pour les contrôles routiers ciblés,
- sortie de données vers des équipements additionnels,
- étalonnage,
- contrôle routier d'étalonnage,
- remise à l'heure.

2.3 Modes de fonctionnement

09) L'appareil de contrôle doit permettre 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 de carte. La génération à laquelle appartient la carte du tachygraphe n'est pas pertinente en vue de déterminer le mode de fonctionnement à condition 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 unité embarquée de deuxième génération.

Mode de fonctionnement		Lecteur «conducteur»				
		Pas de carte	Carte du conducteur	Carte de contrôleur	Carte d'atelier	Carte d'entreprise
Lecteur «convoyeur»	Pas de carte	Opérationnel	Opérationnel	Contrôle	Étalonnage	Entreprise
	Carte du 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 doit être possible.

12) Toutes les fonctions énumérées au point 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, non accessible en mode opérationnel (sauf dans les cas prévus à l'exigence 193), excepté le téléchargement d'une carte de conducteur lorsqu'aucun autre type de carte n'est inséré dans la VU.

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

- en mode opérationnel, toute identification personnelle [nom et prénom(s)] ne correspondant pas à la carte tachygraphique insérée sera masquée, et tout numéro de carte ne correspondant pas à la carte tachygraphique insérée sera partiellement masqué (un caractère sur deux, de gauche à droite),
- en mode entreprise, les données relatives au conducteur (exigences 102, 105 et 108) 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 provenant de la VU ne doivent pas être extraites via l'interface ITS de la VU à moins que le consentement du conducteur à qui se rapportent ces données soit vérifié,
- les unités embarquées ont une période de validité opérationnelle normale de 15 ans à partir de la date 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 et la manipulation de données, et à détecter les tentatives de manipulation, à préserver l'intégrité et l'authenticité des données échangées entre le capteur de mouvement et l'unité embarquée sur le véhicule ainsi qu'entre l'appareil de contrôle et les cartes tachygraphiques, à préserver l'intégrité et l'authenticité des données échangées entre l'appareil de contrôle et le dispositif GNSS externe, à préserver la confidentialité, l'intégrité et l'authenticité des données échangées via 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 d'assurer la sécurité du système, les composants suivants doivent satisfaire aux exigences spécifiées dans leur profil de protection, comme le requiert l'appendice 10:

- unité embarquée sur le véhicule,
- carte tachygraphique,
- capteur de mouvement,
- dispositif GNSS externe (ce profil n'est nécessaire et applicable que pour la variante du GNSS externe).

3 Exigences constructives et fonctionnelles applicables à l'appareil de contrôle

3.1 Suivi de l'insertion et du retrait des cartes

- L'appareil de contrôle doit assurer le suivi des insertions et retraits de carte.
-
- Lors de l'insertion d'une carte, l'appareil de contrôle vérifie la validité de la carte et identifie 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.

- 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, en conformité avec l'appendice 15 (exigence MIG003).
-
- Les cartes d'atelier de première génération qui sont insérées dans l'appareil de contrôle de deuxième génération doivent être considérées comme non valables.

15) L'appareil de contrôle doit être conçu de manière à ce que les cartes tachygraphiques soient verrouillées en position correcte dans l'interface.

16) 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 stockées sur la carte. Le retrait de la carte nécessite une intervention concrète de l'utilisateur.

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

17) Le capteur de mouvement (éventuellement intégré dans l'adaptateur) est la principale source de mesure de la vitesse et de la distance parcourue.

18) Cette fonction assure une mesure en continu et permet d'indiquer la valeur kilométrique correspondant à la distance totale parcourue par le véhicule en utilisant les impulsions envoyées par le capteur de mouvement.

19) Cette fonction assure une mesure en continu et permet d'indiquer la vitesse du véhicule en utilisant les impulsions envoyées par le capteur de mouvement.

20) La fonction de mesure de la vitesse doit également indiquer si le véhicule est en mouvement ou à l'arrêt. 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 à l'arrêt.

21) Les dispositifs indicateurs de vitesse et kilométriques installés sur tout véhicule muni d'un appareil de contrôle conforme au présent règlement doivent satisfaire aux exigences concernant les tolérances maximales (voir points 3.2.1 et 3.2.2) fixées dans la présente annexe.

22) Pour détecter la manipulation de données de mouvement, les informations provenant du capteur de mouvement sont corroborées par des informations relatives au mouvement du véhicule provenant du récepteur GNSS et éventuellement d'une ou plusieurs autres sources indépendantes du capteur de mouvement.

23) 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 convoyeur commencent leur période de travail journalière,
- des positions correspondant aux lieux où le temps de conduite continue du conducteur atteint un multiple de trois heures,
- des positions correspondant aux lieux où le conducteur et/ou le convoyeur terminent leur période de travail journalière.

3.2.1 Mesure de la distance parcourue

24) La distance parcourue peut être mesurée de manière à:
- soit cumuler les mouvements en marche avant et en marche arrière,
- soit prendre uniquement en compte les mouvements en marche avant.

25) L'appareil de contrôle doit mesurer la distance parcourue de 0 à 9 999 999,9 km.

26) La distance mesurée doit être dans 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.

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

3.2.2 Mesure de la vitesse

28) L'appareil de contrôle doit mesurer la vitesse de 0 à 220 km/h.

29) Afin de garantir une tolérance maximale sur la vitesse indiquée de ± 6 km/h en service, et en tenant compte:

– d'une tolérance de ± 2 km/h pour les variations du signal d'entrée (variations dues aux pneumatiques, etc.),
– 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 4 000 et 25 000 imp/km, mesurer la vitesse avec une tolérance de ± 1 km/h (à vitesse constante).
Remarque: la résolution du stockage des données entraîne une tolérance additionnelle de ± 0,5 km/h sur la vitesse stockée par l'appareil de contrôle.

30) La vitesse doit être mesurée correctement, dans les tolérances normales, 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.

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

3.2.3 Mesure de la position

32) L'appareil de contrôle doit mesurer la position absolue du véhicule à l'aide du récepteur GNSS.

33) La position absolue est 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

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

35) 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 4 «Tirages papier».

36) 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 autre décalage qu'un multiple positif ou négatif de la demi-heure n'est autorisé.

37) La dérive temporelle ne doit pas excéder ± 2 secondes par jour dans les conditions d'homologation, en l'absence de toute remise à l'heure.

38) Le temps mesuré doit avoir une résolution meilleure que ou égale à 1 seconde.

39) 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 Surveillance des activités du conducteur

40) Cette fonction doit assurer une surveillance permanente et séparée des activités d'un seul conducteur et d'un seul convoyeur.

41) L'activité du conducteur doit être la CONDUITE, le TRAVAIL, la DISPONIBILITÉ ou la PAUSE/REPOS.

42) Il doit être possible au conducteur et/ou au convoyeur de sélectionner manuellement l'activité TRAVAIL, DISPONIBILITÉ ou PAUSE/REPOS.

43) 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 convoyeur.

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

45) Le premier changement d'activité vers 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).

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

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

48) Étant donné une minute calendrier non considérée comme activité de CONDUITE en application de l'exigence 051, 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).

49) Cette fonction doit également permettre le suivi permanent du temps de travail continu et le temps de pause cumulé du conducteur.

3.5 Surveillance de l'état de conduite

50) Cette fonction doit assurer en permanence et automatiquement la surveillance de la situation de conduite.

51) 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

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

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

54) Lors du retrait d'une carte de conducteur, l'appareil de contrôle doit inviter le conducteur/convoyeur à saisir le «lieu où s'achève la période de travail journalière».

55) Le conducteur renseigne alors l'emplacement actuel du véhicule, ce qui est considéré comme la saisie temporaire.

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

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

57) 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 sur le véhicule, le détenteur est invité à donner son accord pour que les données personnelles en lien avec le tachygraphe puissent être extraites via l'interface ITS facultative.

L'accord 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 le TRAVAIL, la DISPONIBILITÉ ou la PAUSE/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 sélectionner un type, une heure de début et 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.

Au cours 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 (qui se substitue à la saisie effectuée lors du dernier retrait de la carte),
- un lieu où débute la période de travail journalière actuelle, associé à l'heure correspondante.

Si le détenteur de la carte ne renseigne aucun emplacement 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
- le véhicule est mis en mouvement alors que la carte se trouve dans le lecteur réservé au conducteur.

Des interruptions supplémentaires 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 pour la seconde carte.

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

- saisie manuelle des activités, 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. Le type d'activité et l'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 peut alors, à titre facultatif, permettre au détenteur de la carte de modifier toute activité saisie manuellement, jusqu'à la 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

58) 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 survenir lorsque la condition «HORS CHAMP» est ouverte.
Une condition «HORS CHAMP» ouverte doit impérativement être automatiquement fermée 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 début du TRAJET EN FERRY/TRAIN doit être pointé avant l'arrêt du moteur sur le ferry/train.

Un TRAJET EN FERRY/TRAIN ouvert doit se terminer lorsque l'une des possibilités suivantes se produit:

- le conducteur met fin au TRAJET EN FERRY/TRAIN manuellement,
- le conducteur éjecte sa carte,

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.

3.7 Gestion des dispositifs de verrouillage de l'entreprise

59) 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».

60) 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 carte d'entreprise (lors du verrouillage).

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

62) Le déverrouillage ne peut être effectué que par l'entreprise qui a verrouillé (telle qu'identifiée par les 13 premiers chiffres du numéro de la carte d'entreprise), ou

63) le déverrouillage est automatique lorsqu'une autre entreprise verrouille.

64) Dans le cas où une entreprise verrouille et où le verrouillage précédent a été effectué pour la 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

65) 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 de l'ÉTALONNAGE, toutes menées en mode «contrôle».

66) 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» un message «excès de vitesse» a été envoyé sur l'imprimante ou l'écran, ou lorsque des données «événements ou anomalies» ont été téléchargées depuis la mémoire de la VU.

3.9 Détection d'événements et/ou d'anomalies

67) Cette fonction détecte les événements et/ou anomalies suivants:

3.9.1 Événement «Insertion d'une carte non valable»

68) Cet événement est déclenché par l'insertion d'une carte non valable, par l'insertion d'une carte de conducteur déjà remplacée et/ou lorsque la validité d'une carte insérée vient à expiration.

3.9.2 Événement «Conflit de carte»

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

Conflit de carte		Lecteur «conducteur»				
		Pas de carte	Carte du conducteur	Carte de contrôleur	Carte d'atelier	Carte d'entreprise
Lecteur «convoyeur»	Pas de carte					
	Carte du 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»

70) Cet événement est déclenché lorsque la date/l'heure de dernier retrait d'une carte de conducteur, tel qu'elle apparaît sur la carte, est postérieure à la date/l'heure actuelle de l'appareil de contrôle dans lequel la carte est insérée.

3.9.4 Événement «Conduite sans carte appropriée»

71) Cet événement est déclenché pour toute combinaison de cartes tachygraphiques valables marquée d'une croix dans le tableau suivant, lorsque l'activité du conducteur devient «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 du conducteur	Carte de contrôleur	Carte d'atelier	Carte d'entreprise
Lecteur	Pas de carte (ou carte non valable)	X		X		X
	Carte du 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»

72) 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 «Dernière session incorrectement clôturée»

73) Cet événement est déclenché lorsque l'appareil de contrôle détecte lors de l'insertion de la carte que, malgré les dispositions du paragraphe 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»

74) Cet événement est déclenché lors de chaque excès de vitesse.

3.9.8 Événement «Interruption de l'alimentation électrique»

75) 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»

76) Cet événement est déclenché **en mode autre qu'«étalonnage»** et que 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»

77) Cet événement est déclenché lorsque la VU **n'est pas en mode étalonnage**, que le récepteur GNSS (interne ou externe) ne fournit aucune information de position pendant plus de trois heures de conduite consécutives.

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

78) Cet événement est déclenché **en mode autre qu'«étalonnage»**, que 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»

79) 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 sur l'intégrité des données ou l'authentification des données au cours de l'échange de données entre le capteur de mouvement et la VU.

3.9.13 Événement «Conflit concernant le mouvement du véhicule»

80) Cet 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 fournies par le récepteur GNSS interne ou par le dispositif GNSS externe, voire par d'autres sources indépendantes, conformément à l'appendice 12. Cet événement n'est pas déclenché lors d'un trajet en ferry/train, en condition HORS DE PORTÉE ou lorsque les informations de position fournies par le récepteur GNSS ne sont pas disponibles.

3.9.14 Événement «Tentative d'atteinte à la sécurité»

81) Cet événement est déclenché en cas de tout autre événement affectant la sécurité du capteur de mouvement et/ou de l'unité embarquée sur le véhicule et/ou du dispositif GNSS externe, comme prévu dans l'appendice 10, dans les modes autres qu'étalonnage.

3.9.15: Événement «Conflit temporel»

82) Cet événement est déclenché **en mode autre qu'«étalonnage»** lorsque la VU détecte un écart de plus d'une minute entre le temps fourni par sa fonction de mesure du temps et le temps fourni par le récepteur GNSS. Cet événement est enregistré conjointement 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», la VU 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. Cependant, lorsque les informations de position fournies par le récepteur GNSS sont à nouveau disponibles, la remise à l'heure automatique sera effectuée.

3.9.16 Anomalie «Carte»

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

3.9.17 Anomalie «Appareil de contrôle»

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

- anomalie interne de la VU
- 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.

3.10 Autotests intégrés

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

86)

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

3.11 Lecture de la mémoire

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

3.12 Enregistrement et stockage dans la mémoire

Aux fins du présent paragraphe,

- 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 convoyeurs, 6 cycles d'insertion/retrait de cartes et 256 changements d'activités. «365 jours» incluent donc au moins 2 190 conducteurs/convoyeurs, 2 190 cycles d'insertion/retrait de carte et 93 440 changements d'activité,
- le nombre moyen de positions par jour est défini comme au moins 6 positions correspondant aux lieux 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»,
- les heures sont enregistrées à la minute près, sauf indication contraire,
- les valeurs kilométriques sont enregistrées 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, en association avec la précision et le temps d'acquisition du GNSS.

88) 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 14, ne doivent pas être affectées par les coupures d'alimentation de moins de 28 jours.

89) 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'appareil

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

90) 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 des pièces,
- numéro de série,
- génération de la VU,
- possibilité d'utiliser des cartes tachygraphiques de première génération,
- numéro de la version du logiciel,
- date d'installation de la version du logiciel,
- année de construction de l'appareil,
- numéro d'homologation.

91) 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 sur le véhicule, sauf les données concernant le logiciel et le numéro d'homologation, qui peuvent être modifiés en cas d'évolution du logiciel, et la possibilité d'utiliser des cartes tachygraphiques de première génération.

3.12.1.2 Données d'identification du capteur de mouvement

92) 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 (par ex. numéro de série du microprocesseur interne),
- identificateur du système d'exploitation (par ex. numéro de la version du logiciel).

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

94) L'unité embarquée sur le véhicule enregistre et mémorise dans sa mémoire de données les données suivantes associées aux 20 appariements de capteurs de mouvement les plus récents (si plusieurs appariements ont eu lieu en un jour calendaire, seuls le premier et le dernier de la journée sont mémorisés):

Les données suivantes sont enregistrées pour chacun de ces appariements:

- données d'identification du capteur de mouvement:
  - numéro de série,
  - numéro d'homologation,
- données de couplage du capteur de mouvement:
  - date d'appariement.

3.12.1.3 Données d'identification des systèmes mondiaux de navigation par satellite (Global Navigation Satellite Systems)

95) 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 (par ex. numéro de série du microprocesseur interne),
- identificateur du système d'exploitation (par ex. numéro de la version du logiciel).

96) Les données d'identification sont enregistrées et stockées une fois pour toutes sur le dispositif GNSS externe par le fabricant de ce dernier.

97) L'unité embarquée sur le véhicule enregistre et mémorise dans sa mémoire de données les données suivantes associées aux 20 appariements de dispositifs GNSS externes les plus récents (si plusieurs appariements ont eu lieu en un jour calendaire, seuls le premier et le dernier de la journée sont mémorisés).

Les données suivantes sont enregistrées pour chacun de ces appariements:
- données d'identification du dispositif GNSS externe:
  - numéro de série,
  - numéro d'homologation.
- données de couplage du dispositif GNSS externe:
  - date d'appariement

3.12.2 Clés et certificats

98) L'appareil de contrôle doit être en mesure de stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié à l'appendice 11, parties A et B.

3.12.3 Données d'insertion et de retrait de la carte du conducteur ou de l'atelier

99) Pour chaque cycle 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 que stockés sur la carte,
- le numéro de la carte, l'État membre qui l'a délivrée et la date d'expiration tels que 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 relatives au dernier véhicule utilisé par le conducteur, telles que stockées sur la carte:
  - le numéro et l'État membre d'immatriculation,
  - la génération de la VU (si disponible),
  - la date et l'heure du retrait de la carte,
- un code indiquant si le détenteur de la carte a saisi manuellement des activités lors de l ' insertion de la carte ou non.

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

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

3.12.4 Données relatives à l'activité du conducteur

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

- situation de conduite (ÉQUIPAGE, SEUL),
- lecteur (CONDUCTEUR, CONVOYEUR),
- situation de la carte dans le lecteur (INSÉRÉE/NON INSÉRÉE),
- activité (CONDUITE, DISPONIBILITÉ, TRAVAIL, PAUSE/REPOS),
- date et heure du changement.

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 ex. une carte d'entreprise est insérée, ou aucune carte n'est insérée).

Les données relatives à l'activité saisies manuellement par un conducteur ne sont pas enregistrées dans la mémoire.

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

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

3.12.5 Lieux et positions des lieux où les périodes de travail journalières commencent et se terminent et/ou où les 3 heures de temps de conduite continue sont atteintes

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

- les lieux et positions des lieux où le conducteur et/ou le convoyeur commencent leur période de travail journalière,
- les positions des lieux où le temps de conduite continue du conducteur atteint un multiple de trois heures,
- les lieux et positions des lieux où le conducteur et/ou le convoyeur terminent leur période de travail journalière.

106) Lorsque le récepteur GNSS ne peut 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.

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

- le numéro de carte de conducteur/convoyeur et l'État membre qui a délivré la carte,
- la génération de la carte,
- la date et l'heure de la saisie,
- le type de saisie (début, fin ou 3 heures de conduite continue),
- la précision GNSS, la date et l'heure correspondantes, le cas échéant,
- kilométrage du véhicule.

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

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

3.12.6 Données relatives au kilométrage

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

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

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

3.12.7 Données détaillées relatives à la vitesse

113) L'appareil de contrôle enregistre et stocke dans sa mémoire la vitesse instantanée du véhicule et la date et l'heure correspondantes à chaque seconde d'au moins les 24 dernières heures au cours desquelles le véhicule était conduit.

3.12.8 Données relatives aux événements

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

114) L'appareil de contrôle enregistre et stocke dans sa mémoire les données suivantes pour chaque événement détecté, conformément aux 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,	- la date et l'heure de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de la carte à l'origine de l'événement, - le nombre d'événements semblables survenus le même jour.
Conflit de carte	- les 10 événements les plus récents,	- la date et l'heure du début de l'événement, - la date et l'heure de fin de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de chacune des deux cartes à l'origine du conflit.
Conduite sans carte appropriée	- l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence, - les 5 événements les plus longs enregistrés au cours des 365 derniers jours,	- la date et l'heure du début de l'événement, - la date et l'heure de fin de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, - le nombre d'événements semblables survenus le même jour.

Événement	*Règles de stockage*	*Données à enregistrer pour chaque événement*
Insertion d'une carte en cours de conduite	- le dernier événement pour chacun des 10 derniers jours d'occurrence,	- la date et l'heure de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération, - le nombre d'événements semblables survenus le même jour.
Clôture incorrecte de la dernière session	- les 10 événements les plus récents,	- la date et l'heure de l'insertion, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération, - les données relatives à la dernière session telles qu'elles figurent sur la carte: - la date et l'heure de l'insertion, - le numéro d'immatriculation, l'État membre d'immatriculation et la génération de la VU.
Excès de vitesse (1)	- l'événement le plus grave (c.-à-d. celui présentant la vitesse moyenne la plus élevée) des 10 derniers jours d'occurrence, - les 5 événements les plus graves au cours des 365 derniers jours, - le premier événement survenu après le dernier étalonnage,	- la date et l'heure du début de l'événement, - la date et l'heure de fin de l'événement, - la vitesse maximale mesurée au cours de l'événement, - la vitesse moyenne arithmétique mesurée au cours de l'événement, - le type, le numéro, la génération et l'État membre ayant délivré la carte de conducteur (le cas échéant), - le nombre d'événements semblables survenus le même jour.

Événement	*Règles de stockage*	*Données à enregistrer pour chaque événement*
Interruption de l'alimentation électrique (2)	- l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence, - les 5 événements les plus longs enregistrés au cours des 365 derniers jours,	- la date et l'heure du début de l'événement, - la date et l'heure de fin de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, - le nombre d'événements semblables survenus le même jour.
Erreur de communication avec le dispositif de communication à distance	- l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence, - les 5 événements les plus longs enregistrés au cours des 365 derniers jours,	- la date et l'heure du début de l'événement, - la date et l'heure de fin de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, - le nombre d'événements semblables survenus le même jour.
Absence d'informations de positionnement en provenance du récepteur GNSS	- l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence, - les 5 événements les plus longs enregistrés au cours des 365 derniers jours,	- la date et l'heure du début de l'événement, - la date et l'heure de fin de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, - le nombre d'événements semblables survenus le même jour.

Événement	*Règles de stockage*	*Données à enregistrer pour chaque événement*
Erreur sur les données de mouvement	- l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence, - les 5 événements les plus longs enregistrés au cours des 365 derniers jours,	- la date et l'heure du début de l'événement, - la date et l'heure de fin de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, - le nombre d'événements semblables survenus le même jour.
Conflit concernant le mouvement du véhicule	- l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence, - les 5 événements les plus longs enregistrés au cours des 365 derniers jours,	- la date et l'heure du début de l'événement, - la date et l'heure de fin de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, - le 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,	- la date et l'heure du début de l'événement, - la date et l'heure de la fin de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, - le type d'événement.

Événement	*Règles de stockage*	*Données à enregistrer pour chaque événement*
Conflit temporel	- l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence, - les 5 événements les plus longs enregistrés au cours des 365 derniers jours,	- la date et l'heure de l'appareil de contrôle, - la date et l'heure du GNSS, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, - le 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 après ce CONTRÔLE D'EXCÈS DE VITESSE,
- le nombre d'événements du 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.

115) L'appareil de contrôle doit essayer d'enregistrer et de stocker dans sa mémoire les données suivantes pour chaque anomalie détectée, conformément aux 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,	- la date et l'heure de début de l'anomalie, - la date et l'heure de fin de l'anomalie, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération.
Anomalies de l'appareil de contrôle	- les 10 anomalies les plus récentes pour chaque type d'anomalie, - la première anomalie après le dernier étalonnage,	- la date et l'heure de début de l'anomalie, - la date et l'heure de fin de l'anomalie, - le type d'anomalie, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'anomalie.

3.12.10 Données d'étalonnage

116) L'appareil de contrôle enregistre et stocke dans sa mémoire les données ayant trait:
- aux paramètres d'étalonnage connus au moment de l'activation,
- à son 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, ou VIN),
- les 20 étalonnages les plus récents (lorsque plusieurs étalonnages interviennent le même jour civil, seuls le premier et le dernier sont archivés).

117) Les données suivantes sont 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 ayant délivré la carte et la date d'expiration de la carte,
- identification du véhicule,
- les paramètres mis à jour ou confirmés: w, k, l, taille des pneumatiques, réglage du limiteur de vitesse, compteur kilométrique (ancienne et nouvelle valeurs), date et heure (ancienne et nouvelle valeurs),
- les types et les identifiants de tous les scellements en place.

118) En outre, l'appareil de contrôle enregistre et stocke dans sa mémoire sa capacité à utiliser les cartes tachygraphiques de première génération (encore activées ou non).

119) Le capteur de mouvement enregistre et stocke dans sa mémoire les données suivantes concernant son installation:
- première connexion à une VU (date, heure, numéro d'homologation de la VU, numéro de série de la VU),
- dernière connexion à une VU (date, heure, numéro d'homologation de la VU, numéro de série de la VU).

120) Le dispositif GNSS externe enregistre et stocke dans sa mémoire les données suivantes concernant son installation:
- premier couplage à une VU (date, heure, numéro d'homologation de la VU, numéro de série de la VU),
- dernier couplage à une VU (date, heure, numéro d'homologation de la VU, numéro de série de la VU).

3.12.11 Données de remise à l'heure

121) L'appareil de contrôle enregistre et stocke dans sa mémoire les données pertinentes relatives aux remises à l'heure exécutées en mode «étalonnage» hors du cadre d'un étalonnage périodique (déf. f):

- la plus récente remise à l'heure,
- les 5 remises à l'heure les plus importantes.

122) Les données suivantes sont enregistrées pour chacune de ces remises à l'heure:

- la date et l'heure, l'ancienne valeur,
- la date et l'heure, la nouvelle valeur,
- le nom et l'adresse de l'atelier,
- le numéro de la carte d'atelier, l'État membre ayant délivré la carte, la génération de la carte et la date d'expiration de la carte.

3.12.12 Données d'activité de contrôle

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

- date et heure du contrôle,
- le numéro de la carte de contrôleur, l'État membre qui a délivré la carte et la génération de la carte,
- le type de contrôle (affichage et/ou tirage papier et/ou téléchargement depuis la VU et/ou téléchargement depuis la carte et/ou contrôle d'étalonnage sur route).

124) 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

125) 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 de la carte d'entreprise, l'État membre qui a délivré la carte et la génération de la carte,
- le nom et l'adresse de l'entreprise.

Les données précédemment verrouillées par un verrouillage supprimé de la mémoire en raison de la limite précitée sont traitées comme étant non verrouillées.

3.12.14 Données relatives au téléchargement

126) L'appareil de contrôle enregistre et stocke dans sa mémoire les données suivantes ayant trait au dernier téléchargement depuis 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 ayant délivré la carte et la génération de la carte,
- le nom de l'entreprise ou de l'atelier.

3.12.15 Données concernant les conditions particulières

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

- la date et l'heure de la saisie,
- le type de condition particulière.

128) La mémoire doit pouvoir conserver les données relatives aux conditions particulières pendant au moins 365 jours (en supposant qu'en moyenne 1 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 à la carte tachygraphique

129) L'appareil de contrôle doit pouvoir stocker les données suivantes relatives aux différentes cartes tachygraphiques qui avaient été utilisées dans la VU:
- 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.

130) L'appareil de contrôle doit permettre le stockage d'au moins 88 enregistrements de ce type.

3.13 Lecture des cartes tachygraphiques

131) L'appareil de contrôle doit pouvoir lire sur les cartes tachygraphiques de première et deuxième générations, au besoin, 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 de pause cumulé et les temps de conduite cumulés pour la semaine précédente et la semaine en cours,
- imprimer les demandes d'impression de données enregistrées sur une carte de conducteur,
- télécharger une carte de conducteur sur un média externe.

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

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

3.14 Enregistrement et stockage sur cartes tachygraphiques

3.14.1 Enregistrement et stockage sur les cartes tachygraphiques de première génération

133) 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.

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

135) 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 en relation avec le détenteur de la carte. Les données enregistrées sur ces cartes sont spécifiées au chapitre 4.

136) L'appareil de contrôle met à jour les données concernant l'activité du conducteur et les lieux (telles que 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 au lieu saisies manuellement par le détenteur de la carte.

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

138) 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.

139) 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.

140) Avant la libération d'une carte de conducteur, et après que toutes les données pertinentes ont été stockées 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

141) Les cartes tachygraphiques de deuxième génération doivent contenir 2 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», comme spécifié dans le chapitre 4 et dans l'appendice 2.

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

143) L'appareil de contrôle met à jour les données stockées sur les 2 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 en relation avec le détenteur de la carte. Les données enregistrées sur ces cartes sont spécifiées au chapitre 4.

144) L'appareil de contrôle met à jour les données concernant les lieux et les positions d'activité du conducteur (telles que 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.

145) 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.

146) 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.

147) Avant la libération d'une carte de conducteur, et après que toutes les données pertinentes ont été stockées sur les 2 applications de la carte, l'appareil de contrôle remet à zéro les «données de session».

3.15 Affichage

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

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

150) Le dispositif d'affichage doit prendre en charge les caractères spécifiés au chapitre 4 «Jeux de caractères» de l'appendice 1. L'affichage peut utiliser des graphies simplifiées (par ex., les caractères accentués peuvent être affichés sans accent, ou les minuscules peuvent être affichées en majuscules).

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

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

153) L'appareil de contrôle doit pouvoir afficher:

- des données concernant les anomalies,
- des données d'avertissement,
- des données relatives à l'accès aux menus,

- d'autres données demandées par l'utilisateur.

Des informations additionnelles peuvent être affichées par l'appareil de contrôle, à condition d'être clairement distinctes des informations précitées.

154) L'affichage de l'appareil de contrôle doit utiliser les pictogrammes ou les combinaisons de pictogrammes énumérées à l'appendice 3. Des pictogrammes ou des combinaisons de pictogrammes additionnels peuvent également être utilisés, pour autant qu'ils soient clairement distincts des pictogrammes ou combinaisons de pictogrammes précités.

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

156) 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 indiqué à l'appendice 5.

3.15.1 Affichage par défaut

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

- heure locale (UTC + décalage fixé par le conducteur),
- mode de fonctionnement,
- activité en cours du conducteur et du convoyeur,
- informations sur le conducteur:
  - si son activité en cours est la CONDUITE, son temps de conduite continue et son temps de pause cumulé courants,
  - si son activité en cours n'est pas la CONDUITE, la durée de cette activité (depuis sa sélection) et le temps de pause cumulé courants.

158) L'affichage des données concernant chaque conducteur doit être clair, simple et dépourvu d'ambiguïté. Lorsque les informations relatives au conducteur et au convoyeur ne peuvent 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 sur le convoyeur.

159) 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.

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

161) Lorsqu'une condition «HORS CHAMP» ou « 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 d'avertissements

162) L'appareil de contrôle utilise principalement, pour les avertissements, les pictogrammes figurant à l'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

163) L'appareil de contrôle doit comporter les commandes nécessaires dans le cadre d'un menu approprié.

3.15.4 Autres affichages

164) Il doit être possible d'afficher au choix, sur demande:

- la date et l'heure UTC et le décalage de l'heure locale,
- le contenu d'un des six tirages papier correspondants, dans le même format que le tirage papier lui-même,
- le temps de conduite continue et le temps de pause cumulé du conducteur,
- le temps de conduite continue et le temps de pause cumulé du convoyeur,
- le temps de conduite cumulé du conducteur pour la semaine précédente et la semaine en cours,
- le temps de conduite cumulé du convoyeur pour la semaine précédente et pour la semaine en cours,

à titre facultatif:

- la durée actuelle de l'activité du convoyeur (depuis sa sélection),
- le temps de conduite cumulé du conducteur pour la semaine en cours,
- le temps de conduite cumulé du convoyeur pour la période de travail journalière en cours,
- le temps de conduite cumulé du conducteur pour la période de travail journalière en cours.

165) 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 de tirage papier prévues pour les informations manuscrites peuvent être omises.

3.16 Impression

166) 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:

- activités du conducteur stockées sur la carte,
- activités du conducteur stockées sur l'unité embarquée sur le véhicule,
- événements et anomalies stockés sur la carte,
- événements et anomalies stockés sur l'unité embarquée sur le véhicule,
- données techniques,
- excès de vitesse,
- historique des données de la carte tachygraphique pour une VU donnée (voir chapitre 3, point 12.16).

Le détail du format et du contenu à respecter pour ces tirages papier est spécifié à l'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.

167) Les tirages papier «activités du conducteur figurant sur la carte» et «événements et anomalies figurant sur la carte» ne peuvent être obtenus 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 en cause avant de lancer l'impression.

168) Afin d'imprimer les «activités du conducteur figurant sur la carte» ou les «événements et anomalies figurant 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.

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

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

171) L'imprimante doit prendre en charge les caractères spécifiés au chapitre 4 «Jeux de caractères» de l'appendice 1.

172) Les imprimantes doivent être conçues de telle manière que le degré de définition des sorties papier soit suffisant pour éviter toute ambiguïté à la lecture.

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

174) Le papier homologué utilisé par l'appareil de contrôle doit porter la marque d'homologation appropriée et une indication du ou des types d'appareil de contrôle avec lesquels il peut être utilisé.

175) Les tirages papier doivent rester facilement lisibles et identifiables dans les conditions normales de stockage, en termes d'intensité lumineuse, d'humidité et de température, pendant au moins deux ans.

176) Les tirages papier doivent être conformes au minimum aux spécifications d'essai définies à l'appendice 9.

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

178) 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

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

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

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

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

183) 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.

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

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

186) 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.

187) 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.

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

3.18 Téléchargement de données à destination de supports externes

189) L'appareil de contrôle doit permettre le téléchargement à la demande de données stockées sur sa mémoire ou sur une carte de conducteur vers des médias externes, par l'intermédiaire d'une connexion d'étalonnage/de téléchargement. L'appareil de contrôle met à jour les données stockées sur la carte en cause avant de lancer le téléchargement.

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

191) Le téléchargement ne doit ni modifier ni effacer aucune des données stockées.

192) L'interface électrique de connexion pour l'étalonnage et le téléchargement est spécifiée à l'appendice 6.

193) Les protocoles de téléchargement sont spécifiés à l'appendice 7.

3.19 Communication à distance pour les contrôles routiers ciblés

194) Lorsque le contact est mis, la VU stocke, toutes les 60 secondes, dans le dispositif de communication à distance, les données les plus récentes nécessaires aux fins de contrôles routiers ciblés. Ces données sont chiffrées et signées, conformément aux appendices 11 et 14.

195) Les données qui doivent être contrôlées à distance doivent être disponibles pour les lecteurs de communication à distance par communication sans fil, comme indiqué à l'appendice 14.

196) Les données nécessaires aux fins de contrôles routiers ciblés doivent être liées aux éléments suivants:

- dernière tentative d'infraction à la sécurité,
- interruption d'alimentation électrique la plus longue,
- anomalie du capteur,
- erreur sur les données de mouvement,
- conflit concernant le mouvement du véhicule,
- conduite sans carte en cours de validité,
- insertion de carte pendant la conduite,
- données concernant la remise à l'heure,
- données d'étalonnage, y compris les dates des deux derniers enregistrements d'étalonnage stockés,
- numéro d'immatriculation du véhicule,
- vitesse enregistrée par le tachygraphe.

3.20 Données transmises à des dispositifs externes supplémentaires

197) L'appareil de contrôle peut également être équipé d'interfaces normalisées permettant l'utilisation par un dispositif externe, en mode opérationnel ou «étalonnage», des données enregistrées ou produites par le tachygraphe.

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

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 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 la VU.

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 informer les autres dispositifs externes du consentement du conducteur.

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

198) L'interface de liaison série spécifiée dans l'annexe 1B du règlement (CEE) n° 3821/85, tel que modifié en dernier lieu, peut continuer à équiper les tachygraphes afin d'assurer leur compatibilité avec les équipements de première génération. Quoi qu'il en soit, le consentement du conducteur est toujours nécessaire lorsque des données personnelles sont transmises.

3.21 Étalonnage

199) La fonction d'étalonnage permet:

- le couplage automatique du capteur de mouvement avec la VU,
- le couplage automatique du dispositif GNSS externe avec la VU, le cas échéant,
- l'adaptation numérique de la constante de l'appareil de contrôle (k) au coefficient caractéristique du véhicule (w),
- la remise à l'heure au cours de 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 réglage du limiteur de vitesse le cas échéant.

200) En outre, la fonction d'étalonnage permet de rendre impossible l'utilisation de cartes tachygraphiques de première génération dans l'appareil de contrôle, pour autant que les conditions spécifiées à l'appendice 15 soient remplies.

201) Le couplage du capteur de mouvement à la VU consiste au moins en:

- la mise à jour des données d'installation du capteur de mouvement détenues par le capteur de mouvement (au besoin),
- la copie, dans la mémoire de la VU, des données d'identification nécessaires du capteur de mouvement.

202) Le couplage du dispositif GNSS externe avec la VU 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 vers la mémoire de la VU, à partir du dispositif GNSS externe, des données d'identification nécessaires du dispositif GNSS externe, y compris le numéro de série du dispositif GNSS externe,

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

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

3.22 Contrôles routiers d'étalonnage

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

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

206) La fonction de contrôle routier d'étalonnage doit également permettre le contrôle de la sélection du mode de la ligne de signalisation d'entrée/sortie d'étalonnage spécifié dans l'appendice 6, au moyen de l'interface avec la ligne K. Ceci doit être réalisé par le biais de la session de réglage «ECUAdjustmentSession», comme spécifié dans l'appendice 8, section 7, «Contrôle des impulsions d'essai – Unité fonctionnelle de contrôle des entrées/sorties».

3.23 Remise à l'heure

207) La fonction de remise à l'heure doit permettre de régler l'heure automatiquement. Deux sources temporelles sont utilisées par l'appareil de contrôle pour la remise à l'heure: 1) l'horloge interne de la VU et 2) le récepteur GNSS.

208) Le réglage de l'heure de l'horloge interne de la VU est automatiquement réajusté toutes les 12 heures au maximum. Lorsque ce délai a expiré et que le signal GNSS n'est pas disponible, le réglage de l'heure se fait dès que la VU est en mesure d'accéder à une heure valable fournie par le récepteur GNSS, selon les conditions d'allumage du véhicule. La base temps pour le réglage automatique de l'heure de l'horloge interne de la VU doit être 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.

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

3.24 Caractéristiques de performance

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

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

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

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

214) Le capteur de mouvement doit:

- 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 qui soit protégé des champs magnétiques ou immunisé contre ceux-ci.

215) L'appareil de contrôle et le dispositif GNSS externe doivent être conformes à la réglementation internationale R10 de l'ECE-ONU et être protégés contre les décharges électrostatiques et transitoires.

3.25 Matériaux

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

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

218) 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, aux termes de la norme IEC 60529:1989, y compris les annexes A1:1999 et A2:2013.

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

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

3.26 Inscriptions

221) 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».

222) 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 pièce du fabricant et année de fabrication de l'appareil,
- numéro de série de l'appareil,
- marque d'homologation de l'appareil.

223) 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 du composant de l'appareil.

4 Exigences de fabrication et exigences fonctionnelles applicables aux cartes tachygraphiques

4.1 Données visibles

Le recto de la carte doit comporter:

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

225) le nom de l'État membre qui a délivré la carte (facultatif);

226) le code de l'État membre qui a délivré la carte, imprimé en négatif dans un rectangle bleu et entouré de 12 étoiles jaunes. Les codes 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
F	France	S	Suède
HR	Croatie		
H	Hongrie		
IRL	Irlande	UK	Royaume-Uni
I	Italie		

227) des indications particulières concernant la carte délivrée, numérotées comme suit:

	Carte du 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		

	Carte du conducteur	*Carte de contrôleur*	*Carte d'entreprise ou d'atelier*
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 (mention facultative)		
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 de l'installateur (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

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

Le verso de la carte doit comporter:

229) une légende des numéros indiqués au recto;

230) 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.

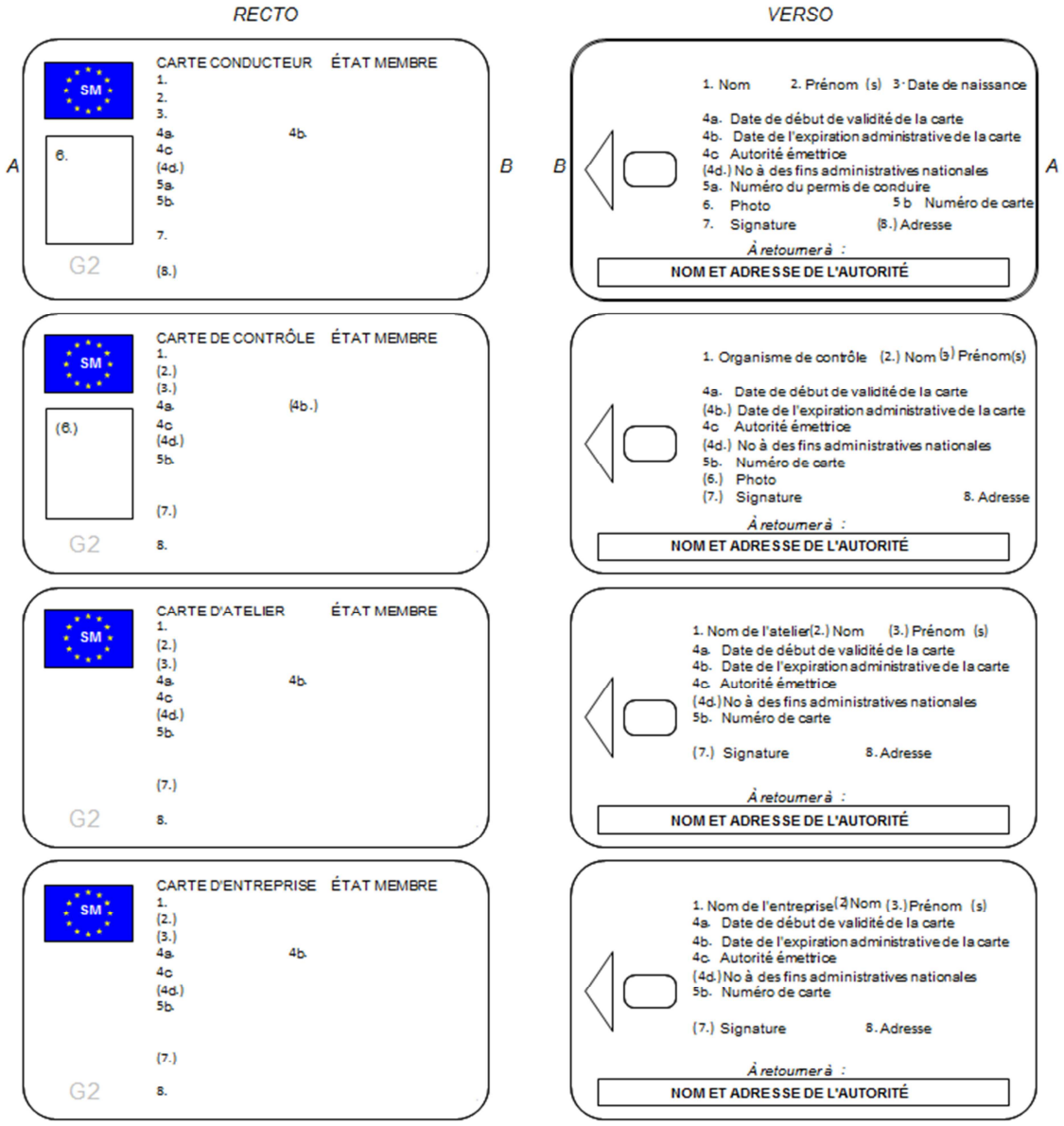
231) Les cartes tachygraphiques doivent être imprimées sur les fonds de couleur suivants:

- carte de conducteur: blanc,
- carte de contrôleur: bleu,
- carte d'atelier: rouge,
- carte d'entreprise: jaune.

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

- 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.

CARTES TACHYGRAPHIQUES DE MODÈLE COMMUNAUTAIRE



233) Après consultation de la Commission, les États membres 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.

234) 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.

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.

235) Afin d'assurer cette sécurité, les cartes tachygraphiques doivent satisfaire aux exigences de sécurité définies dans les appendices 10 et 11.

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

4.3 Normes

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

- ISO/IEC 7810 Cartes d'identification – Caractéristiques physiques,
- ISO/IEC 7816 Cartes d'identification – Cartes à circuit(s) intégré(s):
  - Partie 1: caractéristiques physiques,
  - Partie 2: dimensions et emplacement des contacts (ISO/IEC 7816-2:2007),
  - Partie 3: interface électrique et protocoles de transmission (ISO/IEC 7816-3:2006),
  - Partie 4: organisation, sécurité et commandes pour les échanges (ISO/IEC 7816-4:2013 + Cor 1:2014),
  - Partie 6: éléments de données intersectoriels pour les échanges (ISO/IEC 7816-6:2004 + Cor 1:2006),
  - Partie 8: commandes pour des opérations de sécurité (ISO/IEC 7816-8:2004).
- Les cartes tachygraphiques doivent être testées conformément à la norme ISO/IEC 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

238) Les cartes tachygraphiques doivent pouvoir fonctionner correctement dans toutes les conditions climatiques normalement observées sur le territoire communautaire, 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.

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

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

241) En fonctionnement, les cartes tachygraphiques doivent satisfaire à la réglementation R10 de l'ECE-ONU, relative 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 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 mémoire prévue pour les enregistrements concernés est épuisée.

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

243) Toutes les données supplémentaires qui peuvent être stockées sur des cartes tachygraphiques, 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 personnes physiques à l'égard du traitement 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.

244) 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 deux fichiers dédiés (DF):

- DF Tachograph, qui contient l'application accessible à la première génération de VU et qui est également présent sur les cartes tachygraphiques de première génération,
- DF Tachograph_G2, qui contient l'application accessible à la deuxième génération de VU et qui est seulement présent sur les cartes tachygraphiques de deuxième génération.

L'intégralité des détails relatifs à la structure des cartes tachygraphiques est spécifiée dans l'appendice 2.

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

4.5.2 Identification des cartes à circuit intégré

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

- arrêt d'horloge,
- 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,
- identificateur du circuit intégré.

4.5.2.1 Identification du microprocesseur

246) 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 (uniquement présent sur les cartes tachygraphiques de deuxième génération)

247) Les cartes tachygraphiques doivent pouvoir stocker les objets de données pour l'identification des applications spécifiés dans l'appendice 2.

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

248) Les cartes tachygraphiques doivent pouvoir stocker l'objet de données suivant relatif aux informations sur la période étendue:

- lorsque la carte de tachygraphe prend en charge les champs de période étendue, l'objet de données relatif aux informations sur la période étendue spécifié dans l'appendice 2.

4.5.2.4 Informations relatives à la période étendue (conditionnelles, présentes uniquement sur les cartes tachygraphiques de deuxième génération)

249) Les cartes tachygraphiques doivent pouvoir stocker les objets de données suivants relatifs aux informations sur la période étendue:

- lorsque la carte de tachygraphe prend en charge les champs de période étendue, les objets de données relatifs aux informations sur la période étendue spécifiés dans l'appendice 2.

[8] JO L 281 du 23.11.1995, p. 31.
[9] JO L 201 du 31.7.2002, p. 37

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

250) 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.

4.5.3.1.2 Clés et certificats

251) La carte de conducteur doit être en mesure de stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié dans l'appendice 11, partie A.

4.5.3.1.3 Identification de carte

252) La carte de conducteur doit pouvoir stocker les données suivantes pour l'identification de la carte:
- numéro de la carte,
- État membre qui a délivré la carte, autorité compétente pour la 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

253) 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.

4.5.3.1.5 Téléchargement (download) d'une carte

254) La carte de conducteur doit permettre le stockage des données suivantes concernant le téléchargement des cartes:
- date et heure du dernier téléchargement d'une carte (à d'autres fins que le contrôle).

255) La carte de conducteur doit permettre le stockage d'un de ces enregistrements.

4.5.3.1.6 Renseignements concernant le permis de conduire

256) La carte de conducteur doit pouvoir stocker les données suivantes concernant le permis de conduire:
- État membre qui a délivré le permis, nom de l'autorité compétente pour la 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.

257) 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 session précédente (lorsque cet événement concerne la carte),
- interruption de l'alimentation électrique,
- erreur sur les données de mouvement,
- tentatives d'atteinte à la sécurité.

258) La carte de conducteur doit permettre le stockage des données suivantes concernant ces événements:
- code d'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 si l'événement était en cours à ce moment-là),
- numéro et État membre 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 actuel où l'événement est apparu.

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

- 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.

259) La carte de conducteur doit permettre le stockage des données concernant les 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.

260) 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 à l'origine de l'événement),
- anomalie de l'appareil de contrôle.

261) 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 si l'anomalie était en cours à ce moment-là),
- numéro et État membre d'immatriculation du véhicule dans lequel l'anomalie est survenue.

262) La carte de conducteur doit permettre le stockage des données relatives aux douze dernières anomalies par type (soit 24 anomalies).

4.5.3.1.9 Données relatives aux activités du conducteur

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

- date,
- compteur de présence journalière (augmenté d'une unité pour chacun de ces jours civils),
- distance totale parcourue par le conducteur pendant cette journée,
- situation du conducteur à 00h00,
- les changements d'activité du conducteur et/ou les changements de situation de conduite et/ou l'insertion ou le retrait de la carte de conducteur:
  - situation de conduite (ÉQUIPAGE, SEUL),
  - lecteur (CONDUCTEUR, CONVOYEUR),
  - situation de la carte (INSÉRÉE, NON INSÉRÉE),
  - activité (CONDUITE, DISPONIBILITÉ, TRAVAIL, PAUSE/REPOS),

- heure du changement.

264) 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).

265) 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

266) 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 00h00 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 23h59 si la période d'utilisation est en cours à cette heure-là),
- kilométrage du véhicule à ce moment,
- numéro et État membre d'immatriculation du véhicule.

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

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

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

- date et heure de la saisie (ou date/heure liée 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.

269) La mémoire de la carte de conducteur doit permettre le stockage d'au moins 42 paires d'enregistrements de ce type.

4.5.3.1.12 Données concernant les sessions pour chaque carte

270) 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.-à-d. de l'insertion de la carte), à la seconde près,
- numéro et État membre d'immatriculation du véhicule.

4.5.3.1.13 Données relatives aux activités de contrôle

271) La carte de conducteur doit permettre le stockage des données suivantes concernant les activités de contrôle:

- date et heure du contrôle,
- numéro de la carte de contrôleur et État membre qui l'a délivrée,
- type de contrôle [affichage et/ou impression et/ou téléchargement à partir de la VU et/ou à partir de la carte (voir remarque)],
- période téléchargée, le cas échéant,
- numéro et État membre 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.

272) La carte de conducteur doit permettre le stockage d'un de ces enregistrements.

4.5.3.1.14 Données concernant les conditions particulières

273) 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):

- la date et l'heure de la saisie,

– le type de condition particulière.

274) 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 VU de première génération)

4.5.3.2.1 Identification des applications

275) 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.

4.5.3.2.2 Clés et certificats

276) La carte de conducteur doit être en mesure de stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié dans l'appendice 11, partie B.

4.5.3.2.3 Identification de carte

277) La carte de conducteur doit pouvoir stocker les données suivantes pour l'identification de la carte:
- numéro de la carte,
- État membre qui a délivré la carte, autorité compétente pour la 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

278) 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 (download) d'une carte

279) La carte de conducteur doit permettre le stockage des données suivantes concernant le téléchargement des cartes:
- date et heure du dernier téléchargement d'une carte (à d'autres fins que le contrôle).

280) La carte de conducteur doit permettre le stockage d'un de ces enregistrements.

4.5.3.2.6 Renseignements concernant le permis de conduire

281) La carte de conducteur doit pouvoir stocker les données suivantes concernant le permis de conduire:
- État membre qui a délivré le permis, nom de l'autorité compétente pour la délivrance,
- numéro du permis de conduire (au moment 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.

282) 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 session précédente (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.

283) La carte de conducteur doit permettre le stockage des données suivantes concernant ces événements:
- code d'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 si l'événement était en cours à ce moment-là),
- numéro et État membre 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 actuel où l'événement est apparu.

Remarque: concernant l'événement «clôture incorrecte de la session précédente»:
- 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.

284) La carte de conducteur doit permettre le stockage des données concernant les six derniers événements de chaque type (soit 66 événements).

4.5.3.2.8 Données relatives aux anomalies

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

285) 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 à l'origine de l'événement),
- anomalie de l'appareil de contrôle.

286) 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 si l'anomalie était en cours à ce moment-là),
- numéro et État membre d'immatriculation du véhicule dans lequel l'anomalie est survenue.

287) La carte de conducteur doit permettre le stockage des données relatives aux douze dernières anomalies par type (soit 24 anomalies).

4.5.3.2.9 Données relatives aux activités du conducteur

288) La carte de conducteur doit pouvoir stocker, pour chaque jour civil au cours duquel la carte a été utilisée ou le conducteur a saisi les activités manuellement, les données suivantes:
- date,
- compteur de présence journalière (augmenté d'une unité pour chacun de ces jours civils),
- distance totale parcourue par le conducteur pendant cette journée,
- situation du conducteur à 00h00,

- les changements d'activité du conducteur; et/ou les changements de situation de conduite, et/ou l'insertion ou le retrait de la carte de conducteur:
  - situation de conduite (ÉQUIPAGE, SEUL),
  - lecteur (CONDUCTEUR, CONVOYEUR),
  - situation de la carte (INSÉRÉE, NON INSÉRÉE),
  - activité (CONDUITE, DISPONIBILITÉ, TRAVAIL, PAUSE/REPOS),
  - heure du changement.

289) 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).

290) 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

291) 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 00h00 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 23h59 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 d'immatriculation du véhicule,
- numéro d'identification du véhicule.

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

4.5.3.2.11 Lieux et positions de début/fin des périodes journalières de travail

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

- date et heure de la saisie (ou date/heure liée 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,
- la précision GNSS, la date et l'heure de détermination de la position.

294) La mémoire de la carte de conducteur doit permettre le stockage d'au moins 84 paires d'enregistrements de ce type.

4.5.3.2.12 Données concernant les sessions pour chaque carte

295) 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.-à-d. de l'insertion de la carte), à la seconde près,
- numéro et État membre d'immatriculation du véhicule.

4.5.3.2.13 Données relatives aux activités de contrôle

296) La carte de conducteur doit permettre le stockage des données suivantes concernant les activités de contrôle:

- date et heure du contrôle,
- numéro de la carte de contrôleur et État membre qui l'a délivrée,
- type de contrôle [affichage et/ou impression et/ou téléchargement à partir de la VU et/ou à partir de la carte (voir remarque)],

- période téléchargée, le cas échéant,
- numéro et État membre d'immatriculation du véhicule dans lequel le contrôle a été effectué.

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

297) La carte de conducteur doit permettre le stockage d'un de ces enregistrements.

4.5.3.2.14 Données concernant les conditions particulières

298) 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):

- la date et l'heure de la saisie,
- le type de condition particulière.

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

4.5.3.2.15 Données concernant les unités embarquées sur véhicule qui ont été utilisées

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

- la date et l'heure du 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 l'unité embarquée sur véhicule pour cette période),
- le fabricant de l'unité embarquée sur véhicule,
- le type de VU,
- le numéro de version du logiciel de la VU.

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

4.5.3.2.16 Données relatives aux lieux où les trois heures de conduite continue ont été atteintes

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

- la date et l'heure où le temps de conduite continue du détenteur de la carte atteint un multiple de trois heures,
- la position du véhicule,
- la précision GNSS, la date et l'heure de détermination de la position.

303) La carte de conducteur doit pouvoir stocker au moins 252 enregistrements de ce type.

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

304) 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

305) La carte d'atelier doit être en mesure de stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié dans l'appendice 11, partie A.

306) La carte d'atelier doit permettre le stockage d'un numéro personnel d'identification (code PIN).

4.5.4.1.3 Identification de carte

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

- numéro de la carte,
- État membre qui a délivré la carte, autorité compétente pour la 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

308) 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 (download) d'une carte

309) La carte d'atelier doit permettre le stockage des enregistrements de données relatives au téléchargement d'une carte de la même manière qu'une carte de conducteur.

4.5.4.1.6 Données concernant l'étalonnage et la remise à l'heure

310) La carte d'atelier doit permettre le stockage des enregistrements de données relatives aux étalonnages et/ou aux remises à l'heure réalisés alors que la carte est insérée dans l'appareil.

311) Chaque enregistrement d'étalonnage doit pouvoir 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 (numéros des pièces et numéro de série de la VU, numéro de série du capteur de mouvement).

312) La carte d'atelier doit permettre le stockage d'au moins 88 enregistrements de ce type.

313) La carte d'atelier doit comporter un compteur indiquant le nombre total d'étalonnages réalisés avec la carte.

314) 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

315) La carte d'atelier doit permettre le stockage des enregistrements de données relatives aux événements et aux anomalies de la même manière qu'une carte de conducteur.

316) 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 aux activités du conducteur

317) La carte d'atelier doit permettre le stockage de données concernant l'activité du conducteur de la même manière que la carte de conducteur.

318) La carte d'atelier doit permettre le stockage de données concernant l'activité du conducteur pendant au moins 1 jour d'activité moyenne du conducteur.

4.5.4.1.9 Données concernant les véhicules utilisés

319) La carte d'atelier doit permettre le stockage des enregistrements de données relatives aux véhicules utilisés de la même manière que la carte de conducteur.

320) La carte d'atelier doit permettre le stockage d'au moins 4 enregistrements de ce type.

4.5.4.1.10 Données concernant le début et/ou la fin des périodes de travail journalières

321) La carte d'atelier doit permettre le stockage des enregistrements de données relatives au début et/ou à la fin des périodes de travail journalières de la même manière qu'une carte de conducteur.

322) La carte d'atelier doit permettre le stockage d'au moins 3 paires d'enregistrements de ce type.

4.5.4.1.11 Données concernant les sessions pour chaque carte

323) La carte d'atelier doit permettre le stockage des enregistrements de 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

324) La carte d'atelier doit permettre le stockage des enregistrements de données relatives aux activités de contrôle de la même manière qu'une carte de conducteur.

4.5.4.1.13 Données concernant les conditions particulières

325) La carte d'atelier doit permettre le stockage des données relatives aux conditions particulières de la même manière qu'une carte de conducteur.

326) La carte d'atelier doit permettre le stockage d'au moins 2 enregistrements de ce type.

4.5.4.2 Application tachygraphique de deuxième génération (non accessible aux VU de première génération)

4.5.4.2.1 Identification des applications

327) 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.

4.5.4.2.2 Clés et certificats

328) La carte d'atelier doit être en mesure de stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié dans l'appendice 11, partie B.

329) La carte d'atelier doit permettre le stockage d'un numéro personnel d'identification (code PIN).

4.5.4.2.3 Identification de carte

330) La carte d'atelier doit permettre le stockage des données suivantes pour l'identification de la carte:
- numéro de la carte,
- État membre qui a délivré la carte, autorité compétente pour la 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

331) 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 (download) d'une carte

332) La carte d'atelier doit permettre le stockage des enregistrements de données relatives au téléchargement d'une carte de la même manière qu'une carte de conducteur.

4.5.4.2.6 Données concernant l'étalonnage et la remise à l'heure

333) La carte d'atelier doit permettre le stockage des enregistrements de données relatives aux étalonnages et/ou aux remises à l'heure réalisés alors que la carte est insérée dans l'appareil.

334) Chaque enregistrement d'étalonnage doit pouvoir 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 (numéros des pièces de la VU, numéro de série de la VU, du capteur de mouvement, du dispositif de communication à distance et du dispositif GNSS externe, le cas échéant),
- type et identifiant de tous les scellements en place,
- possibilité pour la VU d'utiliser les cartes tachygraphiques de première génération (activées ou non).

335) La carte d'atelier doit permettre le stockage d'au moins 88 enregistrements de ce type.

336) La carte d'atelier doit comporter un compteur indiquant le nombre total d'étalonnages réalisés avec la carte.

337) 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

338) La carte d'atelier doit permettre le stockage des enregistrements de données relatives aux événements et aux anomalies de la même manière qu'une carte de conducteur.

339) 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 aux activités du conducteur

340) La carte d'atelier doit permettre le stockage de données concernant l'activité du conducteur de la même manière que la carte de conducteur.

341) La carte d'atelier doit permettre le stockage de données concernant l'activité du conducteur pendant au moins 1 jour d'activité moyenne du conducteur.

4.5.4.2.9 Données concernant les véhicules utilisés

342) La carte d'atelier doit permettre le stockage des enregistrements de données relatives aux véhicules utilisés de la même manière que la carte de conducteur.

343) La carte d'atelier doit permettre le stockage d'au moins 4 enregistrements de ce type.

4.5.4.2.10 Données concernant le début et/ou la fin des périodes de travail journalières

344) La carte d'atelier doit permettre le stockage des enregistrements de données relatives au début et/ou à la fin des périodes de travail journalières de la même manière qu'une carte de conducteur.

345) La carte d'atelier doit permettre le stockage d'au moins 3 paires d'enregistrements de ce type.

4.5.4.2.11 Données concernant les sessions pour chaque carte

346) La carte d'atelier doit permettre le stockage des enregistrements de 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

347) La carte d'atelier doit permettre le stockage des enregistrements de 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 sur véhicule qui ont été utilisées

348) La carte d'atelier doit permettre le stockage des données suivantes relatives aux différentes unités embarquées sur véhicule dans lesquelles la carte a été utilisée:
- la date et l'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 sur véhicule pour cette période),
- le fabricant de l'unité embarquée sur véhicule,
- le type de VU,
- le numéro de version du logiciel de la VU.

349) La carte d'atelier doit permettre le stockage d'au moins 4 enregistrements de ce type.

4.5.4.2.14 Données relatives aux lieux où les trois heures de conduite continue ont été atteintes

350) La carte d'atelier doit permettre le stockage des données suivantes relatives à la position du véhicule lorsque le temps de conduite continue du conducteur atteint un multiple de trois heures:
- la date et l'heure où le temps de conduite continue du détenteur de la carte atteint un multiple de trois heures,
- la position du véhicule,
- la précision GNSS, la date et l'heure de détermination de la position.

351) La carte d'atelier doit permettre le stockage d'au moins 18 enregistrements de ce type.

4.5.4.2.15 Données concernant les conditions particulières

352) La carte d'atelier doit permettre le stockage des données relatives aux conditions particulières de la même manière qu'une carte de conducteur.

353) La carte d'atelier doit permettre le stockage d'au moins 2 enregistrements de ce type.

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

354) 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

355) La carte de contrôleur doit être en mesure de stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié dans l'appendice 11, partie A.

4.5.5.1.3 Identification de carte

356) La carte de contrôleur doit permettre le stockage des données suivantes pour l'identification de la carte:
- numéro de la carte,
- État membre qui a délivré la carte, autorité compétente pour la délivrance, date de délivrance,
- date de début de validité de la carte, date d'expiration (le cas échéant).

4.5.5.1.4 Identification du détenteur de la carte

357) 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

358) La carte de contrôleur doit permettre le stockage des données suivantes relatives aux activités de contrôle:
- date et heure du contrôle,
- le type de contrôle (affichage et/ou tirage papier et/ou téléchargement depuis la VU et/ou téléchargement depuis la carte et/ou contrôle d'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 qui l'a délivrée.

359) La carte de contrôleur doit permettre le stockage d'au moins 230 enregistrements de ce type.

4.5.5.2 Application tachygraphique de deuxième génération (non accessible aux VU de première génération)

4.5.5.2.1 Identification des applications

360) 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.

4.5.5.2.2 Clés et certificats

361) La carte de contrôleur doit être en mesure de stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié dans l'appendice 11, partie B.

4.5.5.2.3 Identification de carte

362) La carte de contrôleur doit permettre le stockage des données suivantes pour l'identification de la carte:
- numéro de la carte,
- État membre qui a délivré la carte, autorité compétente pour la délivrance, date de délivrance,
- date de début de validité de la carte, date d'expiration (le cas échéant).

4.5.5.2.4 Identification du détenteur de la carte

363) 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

364) La carte de contrôleur doit permettre le stockage des données suivantes relatives aux activités de contrôle:
- date et heure du contrôle,
- type du contrôle (affichage et/ou impression et/ou téléchargement à partir de la VU et/ou à partir 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 qui l'a délivrée.

365) La carte de contrôleur doit permettre le stockage d'au moins 230 enregistrements de ce type.

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

366) 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

367) La carte d'entreprise doit être en mesure de stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié dans l'appendice 11, partie A.

4.5.6.1.3 Identification de carte

368) La carte d'entreprise doit permettre le stockage des données suivantes pour l'identification de la carte:
- numéro de la carte,
- État membre qui a délivré la carte, autorité compétente pour la délivrance, date de délivrance,
- date de début de validité de la carte, date d'expiration (le cas échéant).

4.5.6.1.4 Identification du détenteur de la carte

369) 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 concernant l'activité de l'entreprise

370) La carte d'entreprise doit permettre le stockage des données suivantes concernant les activités de l'entreprise:
- date et heure de l'activité,
- type de l'activité (verrouillage et/ou déverrouillage de la VU, téléchargement à partir de la VU 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 qui l'a délivrée (en cas de téléchargement à partir de la carte).

371) La carte d'entreprise doit permettre le stockage d'au moins 230 enregistrements de ce type.

4.5.6.2 Application tachygraphique de deuxième génération (non accessible aux VU de première génération)

4.5.6.2.1 Identification des applications

372) 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.

4.5.6.2.2 Clés et certificats

373) La carte d'entreprise doit être en mesure de stocker un certain nombre de certificats et de clés cryptographiques, comme spécifié dans l'appendice 11, partie B.

4.5.6.2.3 Identification de carte

374) La carte d'entreprise doit permettre le stockage des données suivantes pour l'identification de la carte:
- numéro de la carte,
- État membre qui a délivré la carte, autorité compétente pour la délivrance, date de délivrance,
- date de début de validité de la carte, date d'expiration (le cas échéant).

4.5.6.2.4 Identification du détenteur de la carte

375) 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 concernant l'activité de l'entreprise

376) La carte d'entreprise doit permettre le stockage des données suivantes concernant les activités de l'entreprise:
- date et heure de l'activité,
- type de l'activité (verrouillage et/ou déverrouillage de la VU, téléchargement à partir de la VU 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 qui l'a délivrée (en cas de téléchargement à partir de la carte).

377) La carte d'entreprise doit permettre le stockage d'au moins 230 enregistrements de ce type.

5 Installation de l'appareil de contrôle

5.1 Installation

378) L'appareil de contrôle neuf est livré non activé aux installateurs ou aux constructeurs de véhicules, avec tous les paramètres d'étalonnage figurant sur la liste du chapitre 3, paragraphe 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 au «0» pour les paramètres numériques. La fourniture de pièces de l'appareil de contrôle en rapport avec la sécurité peut être restreinte au besoin au cours de la certification de sécurité.

379) Avant son activation, l'appareil de contrôle doit donner accès à la fonction d'étalonnage même s'il n'est pas en mode étalonnage.

380) Avant son activation, l'appareil de contrôle ne doit ni enregistrer ni stocker les données visées au chapitre 3, points 12.3, 12.9 et 12.12 à 12.15 inclus.

381) Au cours de l'installation, les constructeurs du véhicule doivent prérégler tous les paramètres connus.

382) Les constructeurs de véhicules ou les installateurs doivent activer l'appareil de contrôle installé au plus tard avant que le véhicule soit utilisé conformément au règlement (CE) n° 561/2006.

383) 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 une quelconque des interfaces destinées aux cartes.

384) Les opérations particulières de couplage nécessaires entre le capteur de mouvement et l'unité embarquée sur le véhicule, le cas échéant, interviennent automatiquement avant ou pendant l'activation.

385) 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.

386) Après l'activation, l'appareil de contrôle applique pleinement le contrôle d'accès aux fonctions et aux données.

387) Après son activation, l'appareil de contrôle communique au dispositif de communication à distance les données sécurisées nécessaires aux fins de contrôles routiers ciblés.

388) Les fonctions d'enregistrement et de stockage de l'appareil de contrôle doivent être pleinement opérationnelles après l'activation.

389) L'installation doit être suivie d'un étalonnage. Le premier étalonnage ne comporte pas nécessairement la saisie du numéro d'immatriculation du véhicule (VRN) s'il n'est pas connu de l'atelier agréé qui doit procéder à cet étalonnage. Dans ces circonstances, il doit être possible pour le propriétaire du véhicule, uniquement à ce moment, de saisir le VRN à l'aide de sa carte d'entreprise avant l'utilisation du véhicule conformément au règlement (CE) n° 561/2006 (par

exemple à l'aide de commandes via une structure de menu appropriée 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.

390) L'installation d'un dispositif GNSS externe nécessite son couplage avec la VU et la vérification ultérieure des informations de position GNSS.

391) L'appareil de contrôle doit être positionné dans le véhicule de telle manière que le conducteur ait accès aux fonctions nécessaires depuis son siège.

5.2 Plaquette d'installation

392) Après la vérification de l'appareil de contrôle une fois 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 sur l'encadrement de la portière du côté conducteur, et être bien visible dans tous les cas.

Après chaque inspection par un atelier ou un installateur agréé, une nouvelle plaquette est fixée à la place de la précédente.

393) La plaquette doit comporter au moins les indications suivantes:

- le nom, l'adresse ou la raison sociale de l'installateur 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»,
- les circonférences effectives 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 (ou non) d'un dispositif GNSS externe,
- le numéro de série du dispositif GNSS externe,
- le numéro de série de l'appareil de communication à distance,
- le numéro de série de tous les scellements en place,
- la partie du véhicule où l'adaptateur, le cas échéant, est installé,
- 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 ses impulsions entrantes,
- le numéro de série du capteur de mouvement intégré de l'adaptateur.

394) Pour les véhicules des catégories M1 et N1 uniquement, équipés d'un adaptateur conformément au règlement (CE) n° 68/2009[11], 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, une plaque supplémentaire peut être utilisée. Dans ce cas, celle-ci 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 bénéficier du même niveau de protection. En outre, la plaquette supplémentaire doit aussi comporter le nom, l'adresse ou la raison sociale de l'installateur ou de l'atelier agréé qui a procédé à l'installation, ainsi que la date d'installation.

5.3 Scellement

395) Les éléments suivants doivent être scellés:

[10] JO L 102 du 11.4.2006, p. 1.
[11] JO L 21 du 24.1.2009, p. 3.

- toute connexion qui, si elle était interrompue, entraînerait des modifications indécelables ou des pertes de données indécelables (cela peut par exemple s'appliquer au montage du capteur de mouvement sur la boîte de vitesses, à l'adaptateur pour les véhicules des catégories M1/N1, à la connexion GNSS externe ou à la VU);
- 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.

396) Les scellements précités peuvent être retirés:
- en cas d'urgence,
- afin d'installer, d'ajuster ou de réparer un limiteur de vitesse ou tout autre dispositif contribuant à la sécurité routière, pour autant que l'appareil de contrôle continue à fonctionner de manière fiable et correcte, et qu'il soit scellé à nouveau par un installateur ou un atelier agréé (conformément 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 pour les autres cas.

397) À chaque bris de ces scellements, une déclaration écrite indiquant les raisons de cette action est rédigée et transmise à l'autorité compétente.

398) Les scellements doivent porter un numéro d'identification, alloué 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 est défini comme suit: MM NNNNNN, faisant l'objet d'un marquage indélébile, où MM est l'identifiant unique du fabricant (enregistrement dans une base de données qui sera gérée par la CE) et NNNNNN est le numéro alphanumérique du scellement, unique dans le domaine du fabricant.

399) Les scellements doivent présenter un espace libre où les installateurs, ateliers ou 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.

400) Les fabricants de scellements doivent être enregistrés dans une base de données dédiée et rendre publics leurs numéros d'identification de scellements par une procédure établie par la Commission européenne.

401) Les ateliers et constructeurs de véhicules agréés doivent, dans le cadre du règlement (UE) n° 165/2014, n'utiliser que des scellements issus des fabricants de scellements répertoriés dans la base de données mentionnée ci-dessus.

402) Les fabricants de scellements et leurs distributeurs doivent conserver des dossiers de traçabilité complète des scellements vendus pour une utilisation dans le cadre du règlement (UE) n° 165/2014 et doivent être prêts à les communiquer aux autorités nationales compétentes à chaque fois que c'est nécessaire.

403) Les numéros d'identification uniques des scellements doivent être visibles sur la plaquette d'installation.

6 Contrôles, inspections et réparations

Les prescriptions 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 au chapitre 5, point 3, de la présente annexe.

6.1 Agrément des installateurs, des ateliers et des constructeurs de véhicules

Les États membres agréent, contrôlent régulièrement et certifient les organismes chargés des tâches suivantes:
- installations,
- contrôles,
- inspections,
- réparations.

Les cartes d'atelier ne doivent être délivrées qu'aux installateurs et/ou aux ateliers agréés pour l'activation et/ou l'étalonnage d'appareils de contrôle, conformément à la présente annexe 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 requis dans l'appendice 10.

6.2 Vérification d'instruments neufs ou réparés

404) Chaque dispositif, neuf ou réparé, doit être vérifié pour s'assurer de son fonctionnement correct et de la précision de ses relevés et de ses enregistrements, dans les limites fixées au chapitre 3, points 2.1, 2.2, 2.3 et 3 par le scellement prévu au chapitre 5, point 3, et à l'étalonnage.

6.3 Inspection de l'installation

405) Lors de son montage sur un véhicule, l'ensemble de l'installation (y compris l'appareil de contrôle) doit respecter les dispositions en matière de tolérances maximales fixées au chapitre 3, points 2.1, 2.2, 2.3 et 3.

6.4 Inspections périodiques

406) 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 minutes, ou lorsque le numéro d'immatriculation a changé, et au moins une fois tous les deux ans (24 mois).

407) Ces inspections comprennent les vérifications suivantes:

- fonctionnement correct de l'appareil de contrôle, y compris la fonction de stockage de données sur les cartes tachygraphiques et la communication à l'aide de lecteurs de communication à distance,
- conformité aux dispositions du chapitre 3, points 2.1 et 2.2 concernant les tolérances maximales à l'installation,
- conformité aux dispositions du chapitre 3, points 2.3 et 3,
- présence de la marque d'homologation sur l'appareil de contrôle,
- présence de la 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 (le fabricant de scellements est référencé dans la base de données de la CE) et correspondance entre leurs numéros d'identification et les marquages des plaquettes d'installation (voir exigence 401).

408) S'il est constaté qu'un des événements figurant au chapitre 3, point 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 fait peser un risque potentiel sur la sécurité de l'équipement, l'atelier:

a. effectue une comparaison entre les données d'identification du capteur de mouvement connecté à la boîte de vitesse avec celles du capteur de mouvement couplé enregistrées dans l'unité embarquée;
b. vérifie si les informations inscrites sur la plaquette d'installation correspondent à celles enregistrées dans l'unité embarquée;
c. vérifie 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. compare les données d'identification inscrites sur la plaque signalétique du dispositif GNSS externe, le cas échéant, à celles stockées dans la mémoire de la VU.

409) 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 2 ans et les mettent à la disposition de l'autorité compétente sur toute demande.

410) Ces inspections comprennent un étalonnage et un remplacement préventif des scellements dont l'installation s'effectue sous la responsabilité d'ateliers .

6.5 Détermination des erreurs

411) La détermination des erreurs à l'installation et en service doit être effectuée dans les conditions suivantes, qui sont à considérer comme les conditions d'essai standard:

- véhicule à vide en ordre de marche,
- pression des pneumatiques conforme aux instructions du fabricant,
- usure des pneumatiques dans les limites autorisées en droit national,
- 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. La distance mesurée doit être d'au moins 1 000 m,
- pour autant qu'elles soient d'une précision comparable, d'autres méthodes, comme par exemple l'utilisation d'un banc approprié, peuvent également être mises en œuvre pour l'essai.

6.6 Réparations

412) Les ateliers doivent pouvoir télécharger des données à partir de l'appareil de contrôle afin de les restituer à l'entreprise de transport appropriée.

413) Les ateliers agréés délivrent aux entreprises de transport un certificat attestant que les données ne peuvent être téléchargées lorsqu'un dysfonctionnement de l'appareil de contrôle empêche de télécharger les données stockées, même après réparation à l'atelier même. 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 pour la délivrance des cartes sont conformes aux prescriptions suivantes:

414) Le numéro de carte pour la première délivrance d'une carte tachygraphique doit comporter un indice séquentiel (au besoin), un indice de remplacement et un indice de renouvellement fixé à «0».

415) Les numéros de carte de toutes les cartes tachygraphiques non nominatives délivrées au même organisme de contrôle ou au même atelier ou à la même entreprise de transport doivent comporter 13 chiffres identiques suivis d'un indice séquentiel.

416) 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).

417) Une carte tachygraphique délivrée en remplacement d'une carte tachygraphique existante doit avoir la même date d'expiration que cette dernière.

418) 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).

419) 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 même État membre, ou les règles applicables à une première délivrance s'il est effectué dans un autre État membre.

420) 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, de l'installateur ou de l'agent de contrôle selon ce que décident les États membres.

421) 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.

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 la VU, le dispositif GNSS externe à la VU ou le dispositif de communication à distance à la VU. Le papier utilisé pour l'appareil de contrôle est considéré comme un composant de l'appareil.

Tout fabricant peut demander l'homologation de ses composants avec tout type de capteur de mouvement, de dispositif GNSS externe et vice versa, à condition que chaque composant soit conforme aux exigences contenues dans la présente annexe. Les fabricants peuvent également demander l'homologation de l'appareil de contrôle.

422) L'appareil de contrôle doit être présenté pour homologation avec tous ses composants ainsi que tout dispositif additionnel éventuellement intégré.

423) L'homologation d'un appareil de contrôle et de 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 approprié.

424) Les autorités d'homologation des États membres n'accorderont pas de certificat d'homologation tant qu'elles ne sont pas en possession:

- d'un certificat de sécurité,
- d'un certificat de fonctionnement
- et d'un certificat d'interopérabilité

pour l'appareil de contrôle ou la carte tachygraphique faisant l'objet de la demande d'homologation.

425) Toute modification du logiciel ou du matériel, ou des matériaux utilisés dans la fabrication doit être notifiée au préalable à l'autorité qui a accordé l'homologation de l'appareil. Cette autorité doit confirmer au fabricant l'extension de l'homologation, ou bien elle peut demander une mise à jour ou une confirmation des certificats de fonctionnement, de sécurité et/ou d'interopérabilité.

426) Les procédures pour la mise à niveau 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 logicielle ne doit ni modifier ni supprimer aucune donnée relative à l'activité du conducteur stockée dans l'appareil de contrôle. Le logiciel ne peut être mis à niveau que sous la responsabilité du fabricant de l'appareil de contrôle.

427) L'homologation des modifications de logiciels visant à mettre à niveau un appareil de contrôle préalablement homologué ne peut être refusée si ces modifications ne s'appliquent qu'à des fonctions non spécifiées dans la présente annexe. 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

428) Le certificat de sécurité est délivré conformément aux dispositions de l'appendice 10 de la présente annexe. Les composants de l'appareil de contrôle qui doivent être certifiés sont: la VU, le capteur de mouvement, le dispositif GNSS externe et les cartes tachygraphiques.

429) Dans la circonstance exceptionnelle et spécifique où les autorités de 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.

430) Dans cette circonstance, l'État membre concerné informe sans retard la Commission européenne qui, dans les douze mois civils qui suivent l'octroi de l'homologation, lance une procédure pour s'assurer que le niveau de sécurité a été ramené à son niveau d'origine.

8.3 Certificat de fonctionnement

431) Chaque candidat à l'homologation doit fournir à l'autorité d'homologation de l'État membre tout le matériel et la documentation que cette autorité juge nécessaires.

432) Les fabricants fournissent les échantillons pertinents de produits en attente d'une 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.

433) 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 9.

434) 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.

435) 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.

436) 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

437) Les essais d'interopérabilité sont réalisés par un seul et même laboratoire sous l'autorité et la responsabilité de la Commission européenne.

438) Le laboratoire enregistre les demandes d'essais d'interopérabilité introduites par les fabricants dans l'ordre chronologique de leur arrivée.

439) Les demandes ne sont officiellement enregistrées que lorsque le laboratoire est en possession:

- de l'ensemble du matériel et des documents nécessaires pour les 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.

440) Aucun essai d'interopérabilité n'est réalisé par le laboratoire sur un appareil de contrôle ou une carte tachygraphique qui n'a pas reçu de certificat de sécurité et de certificat de fonctionnement, sauf dans les circonstances exceptionnelles décrites sous l'exigence 432.

441) 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.

442) Les essais d'interopérabilité sont effectués, conformément à l'appendice 9 de la présente annexe, 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 existe un certificat d'interopérabilité en cours de validité.

443) Les tests d'interopérabilité doivent couvrir toutes les générations d'appareils de contrôle ou de cartes tachygraphiques encore en usage.

444) Le certificat d'interopérabilité doit être délivré au fabricant par le laboratoire uniquement après que des résultats positifs ont été obtenus pour tous les essais d'interopérabilité.

445) En cas de résultat négatif des essais d'interopérabilité sur un ou plusieurs appareils de contrôle ou cartes tachygraphiques, le certificat d'interopérabilité n'est pas délivré tant que le fabricant concerné 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 l'origine du problème avec l'aide du fabricant concerné, et s'efforce d'assister ce fabricant 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.

446) 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 qui a délivré le certificat de fonctionnement.

447) 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

448) L'autorité d'homologation de l'État membre peut délivrer le certificat d'homologation dès qu'elle est en possession des trois certificats requis.

449) 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.

450) 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.

451) Le laboratoire compétent pour les essais d'interopérabilité doit mettre à jour, sur un site Internet 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.

8.6 Procédure exceptionnelle: les premiers certificats d'interopérabilité pour des unités de contrôle et des cartes tachygraphiques de deuxième génération

452) 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.

453) À l'issue de cette période, si tous les produits concernés sont interopérables, tous les certificats d'interopérabilité deviennent définitifs.

454) 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.

455) 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.

456) 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.

***

FR

ANNEXE II

MARQUE ET CERTIFICAT D'HOMOLOGATION

I. MARQUE D'HOMOLOGATION

1. La marque d'homologation est composée:

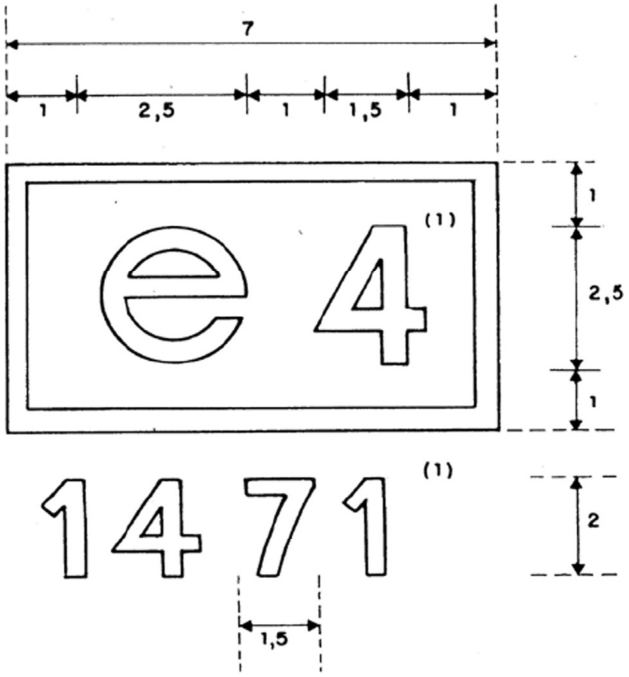
a) d'un rectangle à l'intérieur duquel est placée la lettre «e» minuscule suivie d'un numéro distinctif ou d'une lettre distinctive du pays ayant délivré l'homologation, conformément aux conventions suivantes:

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,
Royaume-Uni	11;

et

b) d'un numéro d'homologation correspondant au numéro du certificat d'homologation établi pour le prototype de l'appareil de contrôle ou de la feuille d'enregistrement ou correspondant au numéro d'une 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

L'État membre ayant procédé à l'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 des homologations délivrées ou, le cas échéant, retirées.

CERTIFICAT D'HOMOLOGATION

Nom de l'administration compétente .....

Communication concernant (1):

— l'homologation d'un modèle d'appareil de contrôle

— le retrait d'homologation d'un modèle d'appareil de contrôle

— l'homologation d'un modèle de feuille d'enregistrement

— le retrait d'homologation d'un modèle de feuille d'enregistrement

N° d'homologation: …….

1. Marque de fabrique ou de commerce .....
2. Dénomination du modèle .....
3. Nom du fabricant .....
4. Adresse du fabricant .....
5. Présenté à l'homologation le .....
6. Laboratoire(s) .....
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 ……

14. Remarques (notamment, le cas échéant, concernant l'emplacement des scellements)

(Signature)

([1]) Rayer les mentions inutiles.

III. CERTIFICAT D'HOMOLOGATION DES TACHYGRAPHES NUMÉRIQUES

Un État membre ayant 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 des homologations délivrées ou, le cas échéant, retirées.

CERTIFICAT D'HOMOLOGATION DES TACHYGRAPHES NUMÉRIQUES

Nom de l'administration compétente **……**

Communication concernant ([1]):

□ l'homologation de: □ le retrait de l'homologation de

□ un modèle d'appareil de contrôle

□ un composant d'appareil de contrôle ([2])

□ une carte de conducteur

□ une carte d'atelier

□ une carte d'entreprise

□ une carte d'agent de contrôle

N° d'homologation: …….

1. Marque de fabrique ou marque commerciale **……**
2. Nom du modèle **……**
3. Nom du fabricant **……**
4. Adresse du fabricant **……**
5. Présenté à l'homologation de **……**
6. Laboratoire(s) **……**
7. Date et numéro du procès-verbal 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 **……**
14. Remarques (notamment, le cas échéant, concernant l'emplacement des scellements)

(Signature)

(1) Cochez les cases pertinentes.
(2) Préciser le composant qui fait l'objet de la notification.

IV. CERTIFICAT D'HOMOLOGATION DES TACHYGRAPHES INTELLIGENTS

Un État membre ayant 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 des homologations délivrées ou, le cas échéant, retirées.

CERTIFICAT D'HOMOLOGATION DES TACHYGRAPHES INTELLIGENTS

Nom de l'administration compétente .....

Communication concernant ([1]):

□ l'homologation de:

□ un modèle d'appareil de contrôle

□ un composant d'appareil de contrôle ([2])

□ une carte de conducteur

□ une carte d'atelier

□ une carte d'entreprise

□ une carte d'agent de contrôle

□ le retrait de l'homologation de

N° d'homologation: …….

1. Marque de fabrique ou marque commerciale .....
2. Nom du modèle .....
3. Nom du fabricant .....
4. Adresse du fabricant .....
5. Présenté à l'homologation de .....
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 .....
14. Remarques (notamment, le cas échéant, concernant l'emplacement des scellements)

(Signature)

(1) Cochez les cases pertinentes.
(2) Préciser le composant qui fait l'objet de la notification.

FR

APPENDICE 1. DICTIONNAIRE DE DONNEES

TABLE DES MATIERES

1. Introduction

Le présent appendice fournit une série de précisions concernant les formats, éléments et structures de données utilisés au sein des appareils de contrôle et cartes tachygraphiques.

1.1. Méthode d'établissement des définitions de type de données

Le présent appendice a recours à la méthode Abstract Syntax Notation One (ASN.1) pour définir les différents types de données. Ce système autorise la définition de 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 du type ASN.1 sont établies en conformité avec la norme ISO/IEC 8824-1. Cela implique que:

- dans la mesure du possible, la signification d'un type de données est implicitement fournie par le nom qui leur est attribué,
- si un type de données se compose d'autres types de données, le nom de ce type de données se présente encore et toujours sous la forme d'une seule séquence de caractères alphabétiques commençant par une majuscule, quoique ce nom comporte un nombre indéterminé de majuscules qui en rappellent la signification,
- de manière générale, les noms de type 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 mémorisées 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 ASN.1 sera défini dans le présent appendice.

Afin d'autoriser l'application de plusieurs types de règles de codage, certains types ASN.1 évoqués dans le présent appendice sont soumis à des identificateurs de plage de valeurs. Ces identificateurs de plage de valeurs sont définis au paragraphe 3, appendice 2.

1.2. Références

Le présent appendice fait référence aux documents suivants:

ISO 639	Code de 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 du véhicule (VIN) - Contenu et structure. 2009
ISO/IEC 7816-5	Cartes d'identification - Cartes à circuit intégré - Partie 5: Enregistrement des fournisseurs d'application. Deuxième édition: 2004.
ISO/IEC 7816-6	Cartes d'identification - Cartes à circuit intégré - Partie 6: Éléments de données intersectoriels pour les échanges, 2004 + Rectificatif technique 1: 2006
ISO/IEC 8824-1	Technologies de l'information - Notation de syntaxe abstraite numéro un (ASN.1): Spécification de la notation de base. 2008 + Rectificatif technique 1: 2012 et Rectificatif technique 2: 2014.
ISO/IEC 8825-2	Technologies de l'information - Règles de codage ASN.1: Spécification des règles de codage compact (PER) 2008.
ISO/IEC 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/IEC 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 + 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, un contenu «inconnu» ou «sans objet» entraînera l'attribution d'une valeur par défaut résultant du remplissage de l'élément de données concerné au moyen d'octets ′FF′.

Tous les types de données servent aux applications de génération 1 et 2 sauf disposition contraire.

2.1. ActivityChangeInfo

Ce type de données autorise le codage, en mots de deux octets, d'un état du lecteur à 00h00 et/ou d'un état du conducteur à 00h00 et/ou de changements d'activité, d'état de conduite et/ou d'état de carte se rapportant à un conducteur ou un convoyeur. Ce type de données est lié aux exigences 105, 266, 291, 320, 321, 343 et 344 de l'annexe 1C.

ActivityChangeInfo ::= OCTET STRING (SIZE(2))

Assignation de valeur — Octet aligné: ‘scpaatttttttttt’B (16 bits)

Pour les enregistrements en mémoire de données (ou de l'état du lecteur):

‘s’B Lecteur:
‘0’B: CONDUCTEUR
‘1’B: CONVOYEUR

‘c’B État de conduite:
‘0’B: SEUL
‘1’B: ÉQUIPAGE

'p'B État de la carte de conducteur (ou d'atelier) insérée dans le lecteur approprié:
‘0’B: INSÉRÉE, la carte est insérée
‘1’B: NON INSÉRÉE, aucune carte n'est insérée (ou la carte est retirée)

‘aa’B Activité
‘00’B: PAUSE/REPOS
‘01’B: DISPONIBILITÉ
‘10’B: TRAVAIL
‘11’B: CONDUITE

‘ttttttttttt’B Heure du changement: nombre de minutes écoulées depuis 00h00 le jour considéré.

Pour les enregistrements (et l'état du conducteur) sur carte de conducteur (ou d'atelier):

's'B Lecteur (hors de propos si 'p' = 1 sauf remarque ci-après):
‘0’B: CONDUCTEUR
‘1’B: CONVOYEUR

‘c’B État de conduite (cas ‘p’=0) ou État d'activité suivant (cas ‘p’=1):
‘0’B: UNIQUE, ‘0’B: INCONNU
‘1’B: ÉQUIPAGE, ‘1’B: CONNU (= saisie manuelle)

‘p’B État 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 est retirée)

'aa'B Activité (hors de propos si 'p' = 1 et 'c' = 0 sauf remarque ci-après):
‘00’B: PAUSE/REPOS
‘01’B: DISPONIBILITÉ
‘10’B: TRAVAIL
‘11’B: CONDUITE

‘ttttttttttt’B Heure du changement: nombre de minutes écoulées depuis 00h00 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 au même moment.

Rien ne s'oppose à ce que les bits ′c′ et ′aa′ du mot (enregistré sur une carte) soient écrasés à la suite d'une saisie manuelle pour refléter l'entrée de données correspondante.

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 encodée 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: pas spécifiée davantage.

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 possède une valeur de 16.

2.5. AES192Key
Génération 2:

Une clé AES192.

```
AES192Key ::= SEQUENCE {
    longueur                    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 possède une valeur de 24.

2.6. AES256Key

Génération 2:

Une clé AES256.

```
AES256Key ::= SEQUENCE {
    longueur                                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 possède une valeur de 32.

2.7. BCDString

BCDString s'applique à la représentation de données en décimal codé binaire (DCB). Ce type de données s'utilise pour représenter un chiffre décimal par un quartet (4 bits). BCDString repose sur l'application de la norme ISO/IEC 8824-1 ′CharacterStringType′ (type de chaîne de caractères).

```
BCDString ::= CHARACTER  STRING (WITH COMPONENTS {
    identification ( WITH COMPONENTS {
    fixed PRESENT }) })
```

BCDString a recours à 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 le nombre approprié de quartets de droite nuls à partir de la position qu'occupe le quartet le plus significatif 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 1B et des exigences 119 de l'annexe 1C.

CalibrationPurpose ::= OCTET STRING (SIZE(1))

Attribution de valeur:

Génération 1:

′00′H valeur réservée
'01'H enregistrement de paramètres d'étalonnage connus, au moment de l'activation de la VU,
'02'H premier étalonnage de la VU après son activation,
'03'H premier étalonnage de l'unité embarquée sur le véhicule considéré,
′04′H inspection périodique,

Génération 2:

Outre la génération 1, les valeurs suivantes sont utilisées:

'05'H entrée des VRN par entreprise,

'06'H mise à l'heure sans étalonnage,

‘07’H à ‘7F’H RFU, ‘80’H à ‘FF’H propre au fabricant.

2.9. CardActivityDailyRecord

Informations enregistrées sur une carte et se rapportant aux activités auxquelles le conducteur s'est livré pendant un jour civil précis. Ce type de données est lié aux exigences 266, 291, 320 et 343 de l'annexe 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 relevé quotidien exprimée en octets. La valeur maximale correspond à la longueur de la CHAÎNE D'OCTETS contenant ces relevés (cf. CardActivityLengthRange, appendice 2, paragraphe 4) Lorsque ces données correspondent au relevé quotidien le plus ancien, la valeur de l'activityPreviousRecordLength doit être mise à 0.

activityRecordLength indique la longueur totale de ce relevé exprimée en octets. La valeur maximale correspond à la longueur de la CHAÎNE D'OCTETS contenant ces relevés.

activityRecordDate indique la date du relevé.

activityDailyPresenceCounter indique l'état du compteur de présence journalière pour la carte et le jour considérés.

activityDayDistance indique la distance totale parcourue le jour considéré.

activityChangeInfo indique le jeu de données ActivityChangeInfo se rapportant au conducteur et au jour considérés. Cette chaîne d'octets ne peut contenir plus de 1440 valeurs (un changement d'activité par minute). Ce jeu comprend toujours l'ActivityChangeInfo encodant l'état du conducteur à 00h00.

2.10. CardActivityLengthRange

Nombre d'octets qu'une carte de conducteur ou d'atelier est susceptible d'affecter à l'enregistrement de relevés d'activité d'un conducteur.

```
CardActivityLengthRange ::= INTEGER(0..216-1)
```

Attribution de valeur: cf. appendice 2.

2.11. CardApprovalNumber

Numéro d'homologation de la carte.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Attribution de valeur:

Le numéro d'homologation doit être fourni tel que publié par le site Internet de la Commission européenne correspondant, à savoir en incluant les traits d'union, par exemple. Le numéro d'homologation doit être aligné à gauche.

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 (CI) de cette carte (exigence 249 de l'annexe 1C). Le icSerialNumber associé au icManufacturingReferences identifie de manière unique le circuit de la carte. Le icSerialNumber seul n'identifie pas 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 du CI.

icManufacturingReferences indique l'identificateur du fabricant de CI.

2.14. CardConsecutiveIndex
Indice séquentiel de la carte considérée [définition h)].

CardConsecutiveIndex ::= IA5String(SIZE(1))

Attribution de valeur: (cf. annexe 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 1C).

```
CardControlActivityDataRecord ::= SEQUENCE {
    controlType                     ControlType,
    controlType                     ControlType,
    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 ainsi que l'État membre 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 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 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 et se rapportant aux activités du conducteur (exigences 267, 268, 292, 293, 321 et 344 de l'annexe 1C).

```
CardDriverActivity ::= SEQUENCE {
    activityPointerOldestDayRecord          INTEGER(0.. CardActivityLengthRange-1),
    activityPointerNewestRecord             INTEGER(0.. CardActivityLengthRange-1),
    activityDailyRecords                    OCTET STRING (SIZE(CardActivityLengthRange ) )
}
```

activityPointerOldestDayRecord indique avec précision le début de l'emplacement en mémoire (nombre d'octets comptés à partir du début de la chaîne) du relevé quotidien complet le plus ancien que comporte la chaîne activityDailyRecords. La valeur maximale correspond à la longueur de la chaîne.

activityPointerNewestRecord indique avec précision le début de l'emplacement en mémoire (nombre d'octets comptés à partir du début de la chaîne) du relevé quotidien le plus récent que comporte la chaîne activityDailyRecords. La valeur maximale correspond à la longueur de la chaîne.

activityDailyRecords indique l'espace disponible affecté à l'enregistrement 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 de relevés du type CardActivityDailyRecord. Lors de la première utilisation, le début de l'enregistrement du premier relevé coïncide avec le premier octet de la chaîne. Les relevés suivants sont enregistrés 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 d'aucune interruption susceptible d'affecter un élément d'information quelconque. Avant d'introduire de nouvelles données d'activité dans la chaîne (en étendant l'activityDailyRecord actuel ou en insérant un nouvel activityDailyRecord), lesquelles se substituent aux données d'activité les plus anciennes, il convient d'actualiser l'activityPointerOldestDayRecord pour rendre compte du nouvel emplacement en mémoire qu'occupe désormais le relevé quotidien complet le plus ancien et de mettre à zéro l'activityPreviousRecordLength de ce (nouveau) relevé quotidien complet le plus ancien.

2.18. CardDrivingLicenceInformation

Informations enregistrées sur une carte de conducteur et se rapportant aux données du permis de conduire du détenteur de la carte (exigence 259 et 284 de l'annexe 1C).

```
CardDrivingLicenceInformation ::= SEQUENCE {
    drivingLicenceIssuingAuthority          Name,
    drivingLicenceIssuingNation             NationNumeric,
    drivingLicenceNumber                    IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority indique l'autorité compétente pour la délivrance du permis de conduire.

drivingLicenceIssuingNation indique la nationalité de l'autorité compétente pour la délivrance du permis de conduire.

drivingLicenceNumber indique le numéro du permis de conduire.

2.19. CardEventData

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant aux événements associés au détenteur de la carte (exigences 260, 285, 318 et 341 de l'annexe 1C).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
    cardEventRecords                        SET SIZE(NoOfEventsPerType) OF CardEventRecord
}
```

CardEventData consiste en une séquence de cardEventRecords (à l'exception des relevés portant sur les tentatives éventuelles d'atteinte à la sécurité, lesquels sont regroupés dans le dernier ensemble de données de la séquence) dont l'agencement correspond à celui des EventFaultType rangés par ordre croissant.

cardEventRecords consiste en un jeu de relevés d'événement correspondant à un type d'événement donné (ou à cette catégorie d'événements dans laquelle se rangent les tentatives d'atteinte à la sécurité).

2.20. CardEventRecord

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant aux événements associés au détenteur de la carte (exigences 261, 286, 318 et 341 de l'annexe 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 ainsi que l'État membre 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 et se rapportant aux événements associés au détenteur de la carte (exigences 263, 288, 318 et 341 de l'annexe 1C).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
    cardFaultRecords                SET SIZE(NoOfFaultsPerType) OF CardFaultRecord
}
```

CardFaultData consiste en une séquence comportant un jeu de relevés des anomalies qui affectent l'appareil de contrôle suivi d'un jeu de relevés des anomalies qui affectent la ou les cartes utilisée(s).

cardFaultRecords consiste en un jeu de relevés des anomalies qui se rangent dans une catégorie donnée (appareil de contrôle ou carte).

2.22. CardFaultRecord

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant aux événements associés au détenteur de la carte (exigences 264, 289, 318 et 341 de l'annexe 1C).

```
CardFaultRecord ::= SEQUENCE {
    faultType                       EventFaultType,
    faultBeginTime                  TimeReal,
    faultEndTime                    TimeReal,
    faultVehicleRegistration        VehicleRegistrationIdentification
}
```

faultType indique le type d'anomalie.

faultBeginTime indique la date et l'heure de début de l'anomalie.

faultEndTime indique la date et l'heure de fin de l'anomalie.

faultVehicleRegistration indique le VRN ainsi que l'État membre 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 cette carte à circuit intégré (CI) (exigence 248 de l'annexe 1C).

```
CardIccIdentification ::= SEQUENCE {
        clockStop       OCTET STRING (SIZE(1)),
        cardExtendedSerialNumber ExtendedSerialNumber,
```

```
    cardApprovalNumber          CardApprovalNumber,
    cardPersonaliserID    ManufacturerCode,
    embedderIcAssemblerId       EmbedderIcAssemblerId,
    icIdentifier     OCTET STRING (SIZE(2))
}
```

clockStop indique le mode Clockstop défini dans l'appendice 2.

cardExtendedSerialNumber indique le numéro de série unique de la carte à circuit intégré spécifié par le type de données ExtendedSerialNumber.

cardApprovalNumber indique le numéro d'homologation de la carte.

cardPersonaliserID indique l'ID individuelle de la carte cryptée par le ManufacturerCode.

embedderIcAssemblerId fournit des informations à propos de l'intégrateur/assembleur de CI.

icIdentifier indique l'identificateur du CI monté sur la carte et de son fabricant défini dans la norme ISO/IEC 7816-6.

2.24. CardIdentification

Informations enregistrées sur une carte et se rapportant à l'identification de celle-ci (exigences 255, 280, 310, 333, 359, 365, 371 et 377 de l'annexe 1C).

```
CardIdentification ::= SEQUENCE {
    cardIssuingMemberState              NationNumeric,
    cardNumber                          CardNumber,
    cardIssuingAuthorityName            Name,
    cardIssueDate                       TimeReal,
    cardValidityBegin                   TimeReal,
    cardExpiryDate                      TimeReal
}
```

cardIssuingMemberState désigne le code de l'État membre émetteur de la carte.

cardNumber indique le numéro de carte de la carte considérée.

cardIssuingAuthorityName indique le nom de l'autorité compétente pour la délivrance de la carte considérée.

cardIssueDate indique la date de délivrance de la carte à son titulaire actuel.

cardValidityBegin indique la date de la première entrée en vigueur de la carte.

cardExpiryDate indique la date d'expiration de la carte.

2.25. CardMACertificate

Génération 2:

Certificat associé à la clé publique d'une carte destinée à son authentification avec une VU. La structure de ce certificat est spécifiée dans l'appendice 11.

CardMACertificate ::= Certificate

2.26. CardNumber

Un numéro de carte conforme à la 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 individuelle d'un conducteur recensé dans un État membre.

ownerIdentification indique l'identification individuelle d'une entreprise, d'un atelier ou d'un organisme de contrôle établis dans un État membre.

cardConsecutiveIndex indique l'indice séquentiel de la carte considérée.

cardReplacementIndex indique l'indice de remplacement de la carte.

cardRenewalIndex indique l'indice de renouvellement de la carte.

La première séquence de la sélection permet de coder un numéro de carte de conducteur, la seconde séquence de coder les numéros des cartes d'atelier, de contrôleur et d'entreprise.

2.27. CardPlaceDailyWorkPeriod
Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant aux lieux de début et/ou de fin des périodes de travail journalières (exigences 272, 297, 325 et 348 de l'annexe 1C).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
    placePointerNewestRecord        INTEGER(0 .. NoOfCardPlaceRecords-1),
    placeRecords                    SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord désigne l'indice du plus récent relevé de lieux mis à jour.
Attribution de valeur: nombre correspondant au numérateur du relevé de site, commençant par une série de ′0′ pour la première occurrence d'un relevé de site dans la structure considérée.

placeRecords indique le jeu de relevés contenant les données relatives aux lieux entrés.

2.28. CardPublicKey
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: (cf. Chapitre VII de la présente annexe).
′0′ Première édition.
Ordre croissant: ‘0 , … , 9 , A , … , Z’

2.31. CardReplacementIndex
Indice de remplacement d'une carte [définition j)].

CardReplacementIndex ::= IA5String(SIZE(1))

Attribution de valeur: (cf. Chapitre VII de la présente annexe).
′0′ Carte originale.
Ordre croissant: ‘0 , … , 9 , A , … , Z’

2.32. CardSignCertificate
Génération 2:

Certificat associé à la clé publique d'une carte en vue de la signature. La structure de ce certificat est spécifiée dans l'appendice 11.

CardSignCertificate ::= Certificate

2.33. CardSlotNumber
Code permettant de faire la distinction entre les deux lecteurs de carte d'une unité embarquée sur véhicule.

CardSlotNumber ::= INTEGER {
driverSlot (0),
co-driverSlot (1)
}

Affectation de valeur: pas spécifiée davantage.

2.34. CardSlotsStatus
Code indiquant le type des cartes insérées dans les deux lecteurs de l'unité embarquée.

CardSlotsStatus ::= OCTET STRING (SIZE(1))

Assignation de valeur — Octet aligné: ‘ccccdddd’B

‘cccc’B Identification du type de carte insérée dans le lecteur réservé au convoyeur
'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 dans un lecteur
‘0001’B une carte de conducteur est insérée dans un lecteur
′0010′B une carte d'atelier est insérée dans un lecteur
′0011′B une carte de contrôleur est insérée dans un lecteur
′0100′B une carte d'entreprise est insérée dans un lecteur.

2.35. CardSlotsStatusRecordArray
Génération 2:

Le CardSlotsStatus plus les métadonnées tels qu'utilisés dans le protocole de téléchargement.

CardSlotsStatusRecordArray ::= SEQUENCE {

recordType	RecordType,
recordSize	ENTIER(1..65535),
noOfRecords	ENTIER(0..65535),
records	SET SIZE(noOfRecords) OF CardSlotsStatus

}

recordType indique le type de relevé (CardSlotsStatus). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des CardSlotsStatus exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique le jeu de relevés de 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 Index des modifications apportées à la structure
‘00’H pour les applications de génération 1
‘01’H pour les applications de génération 2

‘bb’H Index des modifications concernant l'utilisation des éléments d'information définis pour la structure donnée par l'octet de poids fort.
‘00’H pour cette version d'applications de génération 1
‘00’H pour cette version d'applications de génération 2

2.37. CardVehicleRecord

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant à une période d'utilisation d'un véhicule donné pendant un jour civil déterminé (exigences 269, 294, 322 et 345 de l'annexe 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 d'un véhicule donné au début de la période d'utilisation considérée.

vehicleOdometerEnd indique la valeur affichée par le compteur kilométrique d'un véhicule donné à la fin de la période d'utilisation considérée.

vehicleFirstUse indique la date et l'heure du début de la période d'utilisation du véhicule.

vehicleLastUse indique la date et l'heure de la fin de la période d'utilisation du véhicule.

vehicleRegistration indique le VRN ainsi que l'État membre où le véhicule considéré est immatriculé.

vuDataBlockCounter indique la valeur affichée par le compteur de blocs de données de la VU lors de la dernière extraction de la période d'utilisation du véhicule.

Génération 2:

```
CardVehicleRecord ::= SEQUENCE {
    vehicleOdometerBegin                OdometerShort,
    vehicleOdometerEnd                  OdometerShort,
    vehicleFirstUse                     TimeReal,
    vehicleLastUse                      TimeReal,
    vehicleRegistration                 VehicleRegistrationIdentification,
    vuDataBlockCounter                  VuDataBlockCounter,
    vehicleIdentificationNumber         VehicleIdentificationNumber
}
```

Outre la génération 1, l'élément de données suivant est utilisé:

VehicleIdentificationNumber désigne le numéro d'identification du véhicule faisant référence au véhicule dans son entier.

2.38. CardVehiclesUsed

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant aux événements associés au détenteur de la carte (exigences 270, 295, 323 et 346 de l'annexe 1C).

```
CardVehiclesUsed := SEQUENCE {
    vehiclePointerNewestRecord ENTIER(0..NoOfCardVehicleRecords-1),
    cardVehicleRecords                  SET SIZE(NoOfCardVehicleRecords) OF CardVehicleRecord
}
```

vehiclePointerNewestRecord indique l'indice du dernier relevé de véhicule actualisé par le système.
Attribution de valeur: nombre correspondant au numérateur du relevé de véhicule, commençant par une série de ′0′ pour la première occurrence d'un relevé de véhicule dans la structure considérée.

cardVehicleRecords indique le jeu de relevés contenant des informations relatives aux véhicules utilisés.

2.39. CardVehicleUnitRecord

Génération 2:

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant aux événements associés au véhicule (exigences 303 et 351 de l'annexe 1C).

```
CardVehicleUnitRecord ::= SEQUENCE {
    timeStamp                           TimeReal,
    manufacturerCode                    ManufacturerCode,
    deviceID                            ENTIER(0..255),
    vuSoftwareVersion                   VuSoftwareVersion
}
```

timeStamp indique le début de la période d'utilisation du véhicule (c'est-à-dire de la première insertion de la carte dans l'unité embarquée sur véhicule pour cette période).

manufacturerCode identifie le fabricant de l'unité embarquée sur véhicule.

deviceID identifie le type d'unité embarquée sur le véhicule d'un fabricant. La valeur est propre au fabricant.

vuSoftwareVersion indique le numéro de la version du logiciel de l'unité embarquée sur véhicule.

2.40. CardVehicleUnitsUsed

Génération 2:

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant aux unités embarquées sur véhicules associées au détenteur de la carte (exigences 306 et 352 de l'annexe 1C).

```
CardVehicleUnitsUsed := SEQUENCE {
    vehicleUnitPointerNewestRecord      INTEGER(0..NoOfCardVehicleUnitRecords-1),
    cardVehicleUnitRecords              SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord indique l'indice du dernier relevé d'unité embarquée sur véhicule actualisé.
Attribution de valeur: nombre correspondant au numérateur du relevé de l'unité embarquée sur véhicule, commençant par une série de ′0′ pour la première occurrence d'un relevé d'unité embarquée sur véhicule dans la structure considérée.

cardVehicleUnitRecords indique le jeu de relevés contenant des informations relatives aux unités embarquées sur véhicules utilisés.

2.41. Certificat
Certificat d'une clé publique délivrée par un organisme de certification.

Génération 1:

Certificate ::= OCTET STRING (SIZE(194))

Attribution de valeur: signature numérique avec récupération partielle du contenu d'un certificat aux termes de l'appendice 11 «Mécanismes de sécurité communs»: signature (128 octets) | reste de clé publique (58 octets) | références de l'organisme de certification (8 octets).

Génération 2:

Certificate ::= OCTET STRING (SIZE(204..341))
Attribution de valeur:: cf. appendice 11

2.42. CertificateContent

Génération 1:

Le contenu (accessible) du certificat d'une clé publique aux termes de l'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'organisme de certification qui a délivré le certificat considéré. Ces données font également référence à la clé publique de cet organisme de certification.

certificateHolderAuthorisation identifie les droits du titulaire du certificat.

certificateEndOfValidity indique la date d'expiration administrative du certificat.

certificateHolderReference identifie le titulaire du certificat. Ces données font également référence à sa clé publique.

publicKey indique la clé publique certifiée par ce certificat.

2.43. CertificateRequestID Identification individuelle d'une demande de certificat.
Identification des droits d'un titulaire de certificat.

```
CertificateHolderAuthorisation ::= SEQUENCE {
    tachographApplicationID                 OCTET STRING(SIZE(6))
    equipmentType                           EquipmentType
}
```

Génération 1:

tachographApplicationID indique l'identificateur de l'application tachygraphique.
Attribution de valeur: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Cette ID d'application est un identificateur d'application exclusif non homologué, conforme à la norme ISO/IEC 7816-5.

equipmentType identifie 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 des États membres.

Génération 2:

tachographApplicationID indique les 6 octets les plus significatifs de l'identificateur d'application (AID) pour carte tachygraphique de deuxième génération. Le chapitre 6.2 spécifie l'AID pour l'application de carte tachygraphique.
Attribution de valeur: 'FF 53 4D 52 44 54'

equipmentType identifie le type d'équipement visé par le certificat et spécifié pour la génération 2.
Attribution de valeur: en conformité avec le type de données EquipmentType.

2.44. CertificateRequestID

Identification individuelle d'une demande de certificat. Elle peut également faire office d'identificateur de clé publique de l'unité embarquée sur véhicule en cas de méconnaissance du numéro de série de l'unité à laquelle la clé est destinée, lors de l'élaboration du certificat.

```
CertificateRequestID ::= SEQUENCE{
    requestSerialNumber                 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 identifie 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: Code du fabricant correspond au code numérique du fabricant qui a émis la demande de certificat.

2.45. CertificationAuthorityKID

Identificateur de la clé publique d'un organisme de certification (un État membre ou l'organisme de certification européen).

```
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'organisme de certification.

nationAlpha indique le code alphanumérique national de l'organisme de certification.

keySerialNumber est un numéro de série permettant de faire la distinction entre les différentes clés de l'organisme de certification si certaines clés font l'objet de modifications.

additionalInfo est un champ de deux octets autorisant l'introduction de codes supplémentaires (propres à l'organisme de certification).

caIdentifier est un identificateur permettant de faire la distinction entre l'identificateur d'une clé associée à un organisme 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 menées avec cette carte (exigence 373 et 379 de l'annexe 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 indique l'indice du dernier relevé d'activité de l'entreprise actualisé par le système.
Attribution de valeur: nombre correspondant au numérateur du relevé d'activité de l'entreprise, commençant par une série de ′0′ pour la première occurrence d'un relevé d'activité de l'entreprise dans la structure considérée.

companyActivityRecords indique le jeu regroupant l'ensemble des relevés d'activité de l'entreprise.

companyActivityRecord indique la séquence d'informations associée à une activité de l'entreprise.

companyActivityType indique le type de l'activité menée par l'entreprise.

companyActivityTime indique la date et l'heure de l'activité menée par l'entreprise.

cardNumberInformation indique le numéro de la carte et, le cas échéant, l'État membre où la carte téléchargée est délivrée.

vehicleRegistrationInformation indique le VRN ainsi que l'État membre d'immatriculation du véhicule téléchargés, verrouillés ou déverrouillés.

downloadPeriodBegin et **downloadPeriodEnd** indiquent, le cas échéant, la période téléchargée à partir de la VU.

2.47. CompanyActivityType
Code indiquant une activité menée par une entreprise recourant à l'utilisation 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 1C).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId          EquipmentType,
    cardStructureVersion            CardStructureVersion,
    noOfCompanyActivityRecords      NoOfCompanyActivityRecords
}
```

typeOfTachographCardId spécifie le type de la carte mise en application.

cardStructureVersion spécifie la version de la structure mise en œuvre au sein de la carte.

noOfCompanyActivityRecords indique le nombre des relevés d'activité d'entreprise que la carte est susceptible de sauvegarder.

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 1C).

```
CompanyCardHolderIdentification ::= SEQUENCE {
    companyName                     Name,
    companyAddress                  Address,
    cardHolderPreferredLanguage     Language
}
```

companyName indique le nom de l'entreprise du titulaire.

companyAddress indique l'adresse de l'entreprise du titulaire.

cardHolderPreferredLanguageindique la langue de travail préférentielle du titulaire.

2.50. ControlCardApplicationIdentification

Informations enregistrées sur une carte de contrôle et se rapportant à l'identification de l'application de la carte (exigences 357 et 363 de l'annexe 1C).

```
ControlCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId          EquipmentType,
    cardStructureVersion            CardStructureVersion,
    noOfControlActivityRecords      NoOfControlActivityRecords
}
```

typeOfTachographCardId spécifie le type de la carte mise en application.

cardStructureVersion spécifie la version de la structure mise en œuvre au sein de la carte.

noOfControlActivityRecords indique le nombre des relevés d'activité d'entreprise que la carte est susceptible de sauvegarder.

2.51. ControlCardControlActivityData

Informations enregistrées sur une carte de contrôle et se rapportant aux activités menées avec cette carte (exigences 361 et 367 de l'annexe 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 indique l'indice du dernier relevé d'activité de contrôle actualisé par le système.
Attribution de valeur: nombre correspondant au numérateur du relevé d'activité de contrôle, commençant par une série de ′0′ pour la première occurrence d'un relevé d'activité de contrôle dans la structure considérée.

controlActivityRecords indique le jeu regroupant l'ensemble des relevés d'activité de contrôle.

controlActivityRecord indique la séquence d'informations associée 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 ainsi que l'État membre qui délivre la carte contrôlée.

controlledVehicleRegistration indique le VRN ainsi que l'État membre d'immatriculation du véhicule dans lequel le contrôle a été exécuté.

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 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.

cardHolderPreferredLanguageindique la langue de travail préférentielle du titulaire.

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 1C.

ControlType ::= OCTET STRING (SIZE(1))

Génération 1:

Assignation de valeur — Octet aligné: ‘cvpdxxxx’B (8 bits)

‘c’B card downloading:
‘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 la VU:
‘0’B: pas de téléchargement de la VU pendant cette activité de contrôle,
‘1’B: téléchargement de la VU 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:

Assignation 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 la VU:
‘0’B: pas de téléchargement de la VU pendant cette activité de contrôle,
‘1’B: téléchargement de la VU pendant cette activité de contrôle.

‘p’B printing:
'0'B: pas d'impression pendant cette activité de contrôle,
‘1’B: exécution d'un tirage 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 contrôles routiers d'étalonnage:
‘0’B: paramètres d'étalonnage non vérifiés pendant cette activité de contrôle,
‘1’B: paramètres d'étalonnage vérifiés pendant cette activité de contrôle.

‘xxx’BRFU.

2.54. DailyPresenceCounter
Date et heure de l'appareil de contrôle.

CurrentDateTime ::= Temps réel

Affectation de valeur: pas spécifiée davantage.

2.55. CurrentDateTimeRecordArray
Génération 2:

L'heure et la date actuelles plus les métadonnées tels qu'utilisées dans le 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 de relevé (CurrentDateTime). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des CurrentDateTime exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records désigne un jeu de relevés de date et d'heure.

2.56. DailyPresenceCounter
Compteur enregistré sur une carte de conducteur ou d'atelier, incrémenté d'une unité par jour civil d'insertion de cette carte dans le lecteur d'une VU. Ce type de données est lié aux exigences 266, 299, 320 et 343 de l'annexe 1C.

DailyPresenceCounter ::= BCDString(SIZE(2))

Attribution de valeur: numérotation consécutive dont la valeur maximale est égale à 9 999, la numérotation recommençant par le numéro 0. Lors de la première entrée en vigueur d'une carte, le compteur correspondant 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	dénote explicitement l'absence de date.

2.58. DateOfDayDownloaded
Génération 2:

La date et l'heure du téléchargement.

DateOfDayDownloaded ::= TimeReal

Affectation de valeur: pas spécifiée davantage.

DateOfDayDownloadedRecordArray
Génération 2:

L'heure et la date du téléchargement plus les métadonnées tels qu'utilisées dans le 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 de relevé (DateOfDayDownloaded). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des CurrentDateTime exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records désigne le jeu de date et d'heure sur les relevés de téléchargements.

2.59. Distance
Distance parcourue (résultat du calcul de la différence entre deux valeurs affichées par le compteur kilométrique du véhicule considéré).

Distance ::= INTEGER(0..216-1)

Attribution de valeur: binaire sans signe. Valeur exprimée en km et se situant dans une plage d'exploitation comprise entre 0 et 9 999 km.

2.60. 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 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 mise en application.

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 susceptible de sauvegarder par type d'événement.

noOfFaultsPerType indique le nombre d'anomalies que la carte est susceptible de sauvegarder par type d'anomalie.

activityStructureLength indique le nombre d'octets susceptibles d'être affectés à l'enregistrement de relevés d'activité.

noOfCardVehicleRecords indique le nombre des relevés de véhicule que la carte est susceptible de mémoriser.

noOfCardPlaceRecords indique le nombre de sites que la carte est susceptible de mémoriser.

Génération 2:

```
DriverCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId              EquipmentType,
    cardStructureVersion                CardStructureVersion,
    noOfEventsPerType                   NoOfEventsPerType,
    noOfFaultsPerType                   NoOfFaultsPerType,
    activityStructureLength             CardActivityLengthRange,
    noOfCardVehicleRecords              NoOfCardVehicleRecords,
    noOfCardPlaceRecords                NoOfCardPlaceRecords,
    noOfGNSSCDRecords                   NoOfGNSSCDRecords,
    noOfSpecificConditionRecords        NoOfSpecificConditionRecords
}
```

Outre la génération 1, les éléments de données suivants sont utilisés:

noOfGNSSCDRecords indique le nombre de relevés de conduite continue GNSS que la carte est susceptible de sauvegarder.

noOfSpecificConditionRecords indique le nombre de relevés de conditions particulières que la carte est susceptible de mémoriser.

2.61. 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 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.

cardHolderPreferredLanguageindique la langue de travail préférentielle du titulaire.

2.62. DSRCSecurityData
Génération 2:

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 pour des détails complémentaires.

```
DSRCSecurityData ::= SEQUENCE {
    tagLenthPlainText               OCTET STRING(SIZE(2)),
    currentDateTime                 CurrentDateTime,
    ENTIER                          (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 véhicule**.**

counter énumère les messages RTM.

vuSerialNumber indique le numéro de série de l'unité embarquée sur 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).

2.63. EGFCertificate
Génération 2:

Certificat associé à la clé publique d'un dispositif GNSS destiné à l'authentification mutuel avec une VU. La structure de ce certificat est spécifiée dans l'appendice 11.

```
EGFCertificate ::= Certificate
```

2.64. EmbedderIcAssemblerId
Fournit les informations relatives à l'intégrateur de CI.

```
EmbedderIcAssemblerId ::= SEQUENCE{
    countryCode                 IA5String(SIZE(2)),
    moduleEmbedder              BCDString(SIZE(2)),
    manufacturerInformation     OCTET STRING(SIZE(1))
}
```

countryCode désigne le code à deux lettres du pays où se situe l'intégrateur du module conformément à la norme ISO 3166**.**

moduleEmbedder identifie l'intégrateur du module.

manufacturerInformation concerne l'usage interne du fabricant.

2.65. EntryTypeDailyWorkPeriod

Code permettant de faire la distinction entre le lieu 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, entrée manuelle du temps relatif (heure de début) (2),
    Fin, entrée manuelle du temps relatif (fin de la période de travail) (3),
    Début, temps relatif adopté par l'UE (4),
    Fin, temps relatif adopté par la VU (5)
}
```

Attribution de valeur: conforme à la norme ISO/IEC8824-1.

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, entrée manuelle du temps relatif (heure de début) (2),
    Fin, entrée manuelle du temps relatif (fin de la période de travail) (3),
    Début, temps relatif adopté par la VU (4),
    Fin, temps relatif adopté par la VU (5)
    début,                      related time based on GNSS data     (6)
    Fin                         related time based on GNSS data     (7)
}
```

Attribution de valeur: conforme à la norme ISO/IEC8824-1.

2.66. EquipmentType

Code permettant de faire la distinction entre différents types d'équipement pour l'application tachygraphique.

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 fabrication (5),
--Unité embarquée sur véhicule (6),
--Capteur de mouvement (7),
--RFU (8..255)
Attribution de valeur: conformément à la norme ISO/IEC8824-1.

La valeur 0 est réservée aux fins de la désignation d'un État membre ou de l'Europe dans le champ CHA des certificats.

Génération 2:

Les mêmes valeurs que pour la génération 1 servent pour les ajouts suivants:

--dispositif GNSS (8),
--Module de communication à distance (9),
--module d'interface ITS (10),
--Plaque (11), -- peut servir dans SealRecord
--M1/N1 Adapter (12), -- peut servir dans SealRecord
--Racine européenne CA (ERCA)
--État membre CA (MSCA)
--Connexion GNSS externe (15), -- peut servir dans SealRecord
--Inutilisé(16), -- utilisé dans SealDataVu
--RFU (17..255)

Remarque: les valeurs de génération 2 pour la plaque, l'adaptateur et la connexion externe GNSS ainsi que les valeurs de génération 1 pour l'unité embarquée sur véhicule et le capteur de mouvement peuvent servir en SealRecord, le cas échéant.

2.67. EventFaultType
Génération 1:

Clé publique européenne.

EuropeanPublicKey ::= PublicKey

2.68. EventFaultRecordPurpose

Code indiquant la raison de l'enregistrement d'un événement ou d'une anomalie.

```
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 survenu au cours de chacun des 10 derniers jours d'occurrence
‘02’H	l'un des 5 événements les plus longs enregistrés au cours des 365 derniers jours
‘03’H	le dernier événement survenu au cours de chacun des 10 derniers jours d'occurrence
‘04’H	l'événement le plus sérieux enregistré au cours de chacun des 10 derniers jours d'occurrence
‘05’H	l'un des 5 événements les plus sérieux enregistrés au cours des 365 derniers jours
‘06’H	le premier événement ou anomalie survenu après le dernier étalonnage
‘07’H	un événement ou une anomalie en cours
‘08’H à ‘7F’H	RFU
‘80’H à ‘FF’H	propre au fabricant

2.69. 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	dernière session incorrectement clôturée
‘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	RFU
‘1x’H	tentatives d'atteinte à la sécurité en rapport avec l'unité embarquée sur véhicule
‘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 l'entrée de données sur la carte
‘15’H	défaut d'intégrité affectant les données utilisateur mémorisées
‘16’H	erreur de transfert de données internes
‘17’H	ouverture illicite d'un boîtier,
‘18’H	sabotage du matériel
‘19’H à ‘1F’H	RFU
‘2x’H	tentatives d'atteinte à la sécurité en rapport avec le capteur de mouvement
‘20’H	absence d'informations complémentaires
‘21’H	échec d'une authentification
‘22’H	défaut d'intégrité affectant les données mémorisées
‘23’H	erreur de transfert de données internes
‘24’H	ouverture illicite d'un boîtier
‘25’H	sabotage du matériel
‘26’H à ‘2F’H	RFU
‘3x’H	anomalies affectant l'appareil de contrôle
‘30’H	absence d'informations complémentaires
‘31’H	anomalie interne affectant la VU,
‘32’H	anomalie affectant l'imprimante
‘33’H	anomalie affectant l'affichage
‘34’H	anomalie affectant le téléchargement
‘35’H	anomalie affectant le capteur de mouvement,
‘36’H à ‘3F’H	RFU
‘4x’H	anomalies affectant une carte
‘40’H	absence d'informations complémentaires
‘41’H à ‘4F’H	RFU
‘50’H à ‘7F’H	RFU

‘80’H à ‘FF’H	propre au fabricant

Génération 2:

Les mêmes valeurs que pour la génération 1 servent pour les ajouts suivants:

‘0B’H	conflit temporel (GNSS contre l'horloge interne de la VU)
‘0C’ à ‘0F’H	RFU
‘5x’H	événements liés au GNSS
‘50’H	absence d'informations complémentaires
‘51’H	anomalie du récepteur du dispositif GNSS interne
‘52’H	anomalie du récepteur du dispositif GNSS externe
‘53’H	anomalie de communication du dispositif GNSS externe
‘54’H	aucune donnée de position du dispositif GNSS,
‘55’H	détection de violation du dispositif GNSS
‘56’H	expiration du certificat du dispositif GNSS externe
‘57’H à ‘5F’H	RFU
‘6x’H	anomalies liées au module de communication à distance
‘60’H	absence d'informations complémentaires
‘61’H	anomalie sur le module de communication à distance
‘62’H	anomalie de communication sur le module de communication à distance
‘63’H à ‘6F’H	RFU
‘7x’H	anomalies sur l'interface STI
‘70’H	absence d'informations complémentaires
‘71’H à ‘7F’H	RFU.

2.70. ExtendedSealIdentifier

Génération 2:

L'identifiant de scellé étendu identifie uniquement un scellé (exigence 401, annexe 1C).

```
ExtendedSealIdentifier ::= SEQUENCE{
    manufacturerCode                CHAÎNE D’OCTETS (LONGUEUR(2))
    manufacturerCode                CHAÎNE D’OCTETS (LONGUEUR(2))
}
```

manufacturerCode correspond au code du fabricant du scellé.

sealIdentifier désigne l'identifiant du scellé, unique pour le fabricant.

2.71. ExtendedSerialNumber

Identification individuelle d'un équipement. Ce numéro peut également faire office d'identificateur de clé publique d'équipement.

Génération 1:

```
ExtendedSerialNumber ::= SEQUENCE{
    serialNumber                          ENTIER(0..2^32-1)
    monthYear BCDString[LONGUEUR(2)]
    type                                  CHAÎNE D'OCTETS [LONGUEUR(1)]
    manufacturerCode                      ManufacturerCode
}
```

serialNumber indique le numéro de série de l'équipement, propre au fabricant, ainsi que le type d'équipement, le mois et l'année ci-après.

monthYear identifie 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: désigne le code numérique identifiant un fabricant d'appareil homologué.

Génération 2:

```
ExtendedSerialNumber ::= SEQUENCE{
    serialNumber                          ENTIER(0..2^32-1)
    monthYear BCDString[LONGUEUR(2)]
    type                                  EquipmentType,
    manufacturerCode                      ManufacturerCode
}
```

serialNumber cf. génération 1

monthYear cf. génération 1

type indique le type d'équipement.

monthYear cf. génération 1

2.72. 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 qui a délivré la carte considérée.

cardNumber indique le numéro de la carte.

2.73. FullCardNumberAndGeneration

Génération 2:

Code permettant d'identifier avec certitude une carte tachygraphique et sa génération.

```
FullCardNumberAndGeneration ::= SEQUENCE {
    fullCardNumber                  FullCardNumber,
    generation                      Generation
}
```

fullCardNumber identifie la carte tachygraphique.

generation indique la génération de carte tachygraphique utilisée.

2.74. Generation
Génération 2:

Indique la génération de tachygraphe utilisé.

Generation ::= INTEGER(0..255)
Attribution de valeur:

‘00’H	RFU
‘01’H	Génération 1
‘02’H	Génération 2
‘03’H .. ‘FF’H	RFU

2.75. GeoCoordinates
Génération 2:

Les coordonnées longitudinales et latitudinales 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 respectivement les degrés et MM.M, les minutes.

```
GeoCoordinates ::= SEQUENCE {
    latitude                        ENTIER(-90000..90001),
    longitude                       ENTIER(-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.

2.76. GNSSAccuracy
Génération 2:

Exactitude des données de position du dispositif GNSS (définition eee). Cette exactitude est codée sous la forme d'une valeur entière et est un multiple (facteur 10) de la valeur X.Y fournie par la phrase GSA NMEA.

GNSSAccuracy ::= INTEGER(1..100)

2.77. GNSSContinuousDriving

Génération 2:

Informations enregistrées sur une carte de conducteur ou d'atelier, relatives à la position GNSS du véhicule lorsque le temps de conduite continue du conducteur atteint un multiple de trois heures (exigences 306 et 354, Annex 1C).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord          ENTIER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords       SLONGUEUR DÉFINIE(NoOfGNSSCDRecords) DE
                                      GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord désigne l'indice du dernier relevé de conduite continue GNSS actualisé par le système.

Attribution de valeur: nombre correspondant au numérateur du relevé de conduite continue GNSS, commençant par une série de ′0′ pour la première occurrence d'un relevé de conduite continue GNSS dans la structure considérée.

gnssContinuousDrivingRecords désigne le jeu de relevés contenant la date et l'heure lorsque la conduite continue atteint un multiple de trois heures, ainsi que les informations relatives à la position du véhicule.

2.78. GNSSContinuousDrivingRecord
Génération 2:

Informations enregistrées sur une carte de conducteur ou d'atelier, relatives à la position GNSS du véhicule lorsque le temps de conduite continue du conducteur atteint un multiple de trois heures (exigences 305 et 353, Annexe 1C).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                          TimeReal,
   gnssPlaceRecord                    GNSSPlaceRecord
}
```

timeStamp désigne la date et l'heure lorsque le temps de conduite continue du détenteur de la carte atteint un multiple de trois heures.

gnssPlaceRecord contient les informations relatives à la position du véhicule.

2.79. GNSSPlaceRecord
Génération 2:

informations relatives à la position GNSS du véhicule (exigences 108, 109, 110, 296, 305, 347 et 353, annexe 1C).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                          TimeReal,
   gnssAccuracy                       GNSSAccuracy,
   geoCoordinates                     GeoCoordinates
}
```

timeStamp indique la date et l'heure à laquelle la position GNSS du véhicule a été déterminée.

gnssAccuracy précise le degré d'exactitude des données de position GNSS.

geoCoordinates indique l'emplacement enregistré à l'aide du dispositif GNSS.

2.80. HighResOdometer
Valeur affichée par le compteur kilométrique du véhicule: distance totale parcourue par le véhicule en cours d'exploitation.

```
HighResOdometer ::= INTEGER(0..232-1)
```

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.

2.81. HighResTripDistance

Distance parcourue pendant tout ou partie d'un trajet.

HighResTripDistance ::= INTEGER(0..232-1)

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. HolderName
Nom et prénom(s) d'un détenteur de carte.

```
HolderName ::= SEQUENCE {
    holderSurname                   Name,
    holderFirstNames                Name
}
```

holderSurname indique le nom du titulaire. 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 titulaire.

2.83. 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 la VU. Faux signifie que le récepteur GNSS est externe.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.84. K-ConstantOfRecordingEquipment
Constante de l'appareil de contrôle (définition m).

K-ConstantOfRecordingEquipment ::= INTEGER(0..216-1)

Attribution de valeur: impulsions par kilomètre dans une plage d'exploitation comprise entre 0 et 64 255 imp/km.

2.85. KeyIdentifier
Identificateur unique d'une clé publique permettant de la désigner et de la sélectionner. Cet identificateur identifie également le titulaire de la clé.

```
KeyIdentifier ::= CHOICE {
    extendedSerialNumber            ExtendedSerialNumber,
    certificateRequestID            CertificateRequestID,
    certificationAuthorityKID       CertificationAuthorityKID
}
```

La première option permet de désigner la clé publique d'une unité embarquée sur véhicule ou d'une carte tachygraphique.

La seconde option permet de désigner la clé publique d'une unité embarquée sur véhicule (en cas de méconnaissance du numéro de série de l'unité embarquée, lors de l'élaboration du certificat).

La troisième option permet de désigner la clé publique d'un État membre.

2.86. KMWCKey
Génération 2:

Clé AES et version de clé associée utilisée pour la VU: couplage du capteur de mouvement. Pour tout détail complémentaire, cf. appendice 11.

```
KMWCKey ::= SEQUENCE {
    kMWCKey                         AESKey,
    keyVersion                      INTEGER (SIZE(1))
}
```

kMWCKey désigne la longueur de la clé AES concaténée avec la clé servant à la VU: couplage du capteur de mouvement.

keyVersion indique la version clé de la clé AES.

2.87. Language
Code identifiant une langue de travail.

Language ::= IA5String(SIZE(2))
Attribution de valeur: code composé de deux lettres minuscules, en conformité avec la norme ISO 639.

2.88. LastCardDownload
Date et heure, enregistrées sur une carte de conducteur, du dernier téléchargement d'une carte (à d'autres fins que le contrôle) (exigences 257 et 282, annexe 1C). Cette date peut être mise à jour par une VU ou tout lecteur de carte.

LastCardDownload ::= TimeReal
Affectation de valeur: pas spécifiée davantage.

2.89. LinkCertificate
Génération 2:

Certificat du lien entre les clés couplées conformément à l'autorité de certification racine européenne.
LinkCertificate ::= Certificate
2.90. L-TyreCircumference
Circonférence effective des pneumatiques (définition u).

L-TyreCircumference ::= INTEGER(0.. 216-1)
Attribution de valeur: valeur exprimée en 1/8 de mm et se situant dans une plage d'exploitation comprise entre 0 et 8 031 mm.

2.91. MAC
Génération 2:

Un total de contrôle cryptographique sur une longueur de 8, 12 ou 16 octets correspondant à des suites chiffrées spécifiées dans l'appendice 11.

```
MAC ::= CHOICE {
    mac8                    OCTET STRING (SIZE(8)),
    mac12                   OCTET STRING (SIZE(12)),
    mac16                   OCTET STRING (SIZE(12))
}
```

2.92. ManualInputFlag
Code permettant d'identifier si un détenteur de carte a procédé ou non à la saisie manuelle d'activités du conducteur lors de l'insertion de cette carte (exigence 081, annexe 1B. exigence 102, annexe 1C).

```
ManualInputFlag ::= INTEGER {
    noEntry                 (0)
    manualEntries           (1)
}
```
Affectation de valeur: pas spécifiée davantage.

2.93. ManufacturerCode

Code identifiant un fabricant d'appareil homologué.

ManufacturerCode ::= INTEGER(0..255)
Le laboratoire chargé des essais d'interopérabilité maintient à jour et publie la liste des codes de fabricants sur son site web (exigence 454, annexe 1C).

Les numéros ManufacturerCodes sont provisoirement attribués aux concepteurs de tachygraphes sur demande auprès du laboratoire chargé des essais d'interopérabilité.

2.94. ManufacturerSpecificEventFaultData
Génération 2:

Codes d'erreurs propres au fabricant simplifiant l'analyse des erreurs et la maintenance des unités embarquées sur les véhicules.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
    manufacturerCode                ManufacturerCode,
    manufacturerSpecificErrorCode   CHAÎNE D'OCTETS (LONGUEUR(3))
}
```

manufacturerCode identifie le fabricant de l'unité embarquée sur véhicule.

manufacturerSpecificErrorCode est un code d'erreur propre au fabricant.

2.95. MemberStatePublicKey
Certificat de la clé publique d'un État membre délivré par l'organisme de certification européen.

MemberStateCertificate ::= Certificate

2.96. MemberStateCertificateRecordArray
Génération 2:

Certificat de l'État membre plus les métadonnées tels qu'utilisés dans le protocole de téléchargement.

```
MemberStateCertificateRecordArray ::= SEQUENCE {
    recordType          RecordType,
    recordSize          ENTIER(1..65535),
    noOfRecords         ENTIER(0..65535),
    records             LONGUEUR DÉFINIE (noOfRecords) DE
                        MemberStateCertificate
}
```

recordType indique le type de relevé (MemberStateCertificate). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des MemberStateCertificate exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis. La valeur doit être définie sur 1, car les certificats peuvent présenter des longueurs variables.

records désigne le jeu de certificats des États membres.

2.97. MemberStatePublicKey
Génération 1:

Clé publique d'un État membre.

MemberStatePublicKey ::= PublicKey

2.98. Name

Un nom.

```
Name ::= SEQUENCE {
    codePage ENTIER (0..255),
    name CHAÎNE D'OCTETS (LONGUEUR(35))
}
```

codePage spécifie un jeu de caractères défini au chapitre 4,

name indique un nom encodé à l'aide du jeu de caractères spécifié.

2.99. NationAlpha
Renvoi alphabétique à un pays conformément 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 maintenue à jour sur le site web du laboratoire désigné pour effectuer les essais d'interopérabilité en vertu de l'exigence 440, annexe 1C.

2.100. Code numérique national
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 NationAlpha ou NationNumeric ne peut intervenir qu'après consultation, par le laboratoire désigné, des fabricants d'unités embarquées de tachygraphe numérique et intelligent homologuées.

2.101. NoOfCalibrationsSinceDownload
Nombre des relevés d'étalonnage qu'une carte d'atelier est susceptible de mémoriser.

Génération 1:

NoOfCalibrationRecords ::= INTEGER(0..255)
Attribution de valeur: cf. appendice 2.

Génération 2:

NoOfCalibrationRecords ::= INTEGER(0..216-1)
Attribution de valeur: cf. appendice 2.

2.102. NoOfCalibrationsSinceDownload
Compteur indiquant le nombre d'étalonnages exécutés avec une carte d'atelier depuis son dernier téléchargement (exigence 317 et 340, annexe 1C).

NoOfCalibrationsSinceDownload ::= INTEGER(0..216-1)

Attribution de valeur: absence d'informations complémentaires.

2.103. NoOfCardPlaceRecords
Nombre des relevés de site qu'une carte de conducteur ou d'atelier est susceptible de mémoriser.

Génération 1:

NoOfCardPlaceRecords ::= INTEGER(0..255)
Attribution de valeur: cf. appendice 2.

Génération 2:

NoOfCardPlaceRecords ::= INTEGER(0..216-1)

Attribution de valeur: cf. appendice 2.

2.104. NoOfCardVehicleRecords
Nombre des relevés de véhicule qu'une carte de conducteur ou d'atelier est susceptible de mémoriser.

NoOfCardVehicleRecords ::= INTEGER(0.. 2^{16}-1)

Attribution de valeur: cf. appendice 2.

2.105. NoOfCardVehicleUnitRecords
Génération 2:

Nombre de relevés utilisés par les unités embarquées sur le véhicule qu'une carte de conducteur ou d'atelier est susceptible de mémoriser.

NoOfCardVehicleUnitRecords ::= INTEGER(0.. 216-1)

Attribution de valeur: cf. appendice 2.

2.106. NoOfControlActivityRecords
Nombre des relevés d'activité d'entreprise qu'une carte d'entreprise est susceptible de mémoriser.

NoOfCompanyActivityRecords ::= INTEGER(0.. 216-1)

Attribution de valeur: cf. appendice 2.

2.107. NoOfEventsPerType
Nombre des relevés d'activité de contrôle qu'une carte de contrôleur est susceptible de mémoriser.

NoOfControlActivityRecords ::= INTEGER(0.. 216-1)
Attribution de valeur: cf. appendice 2.

2.108. NoOfEventsPerType
Nombre d'événements qu'une carte est susceptible de mémoriser par type d'événement.

NoOfEventsPerType ::= INTEGER(0..255)
Attribution de valeur: cf. appendice 2

2.109. NoOfFaultsPerType
Nombre d'anomalies qu'une carte est susceptible de mémoriser par type d'anomalie.

NoOfFaultsPerType ::= INTEGER(0..255)

Attribution de valeur: cf. appendice 2

2.110. NoOfGNSSCDRecords
Génération 2:

Nombre de relevés de conduite continue GNSS que la carte est susceptible de sauvegarder.

NoOfGNSSCDRecords ::= INTEGER(0..2^{16}-1)
Attribution de valeur: cf. appendice 2

2.111. NoOfSpecificConditionRecords
Génération 2:

Nombre de relevés de conditions particulières qu'une carte est susceptible de mémoriser.

NoOfSpecificConditionRecords ::= INTEGER(0..216-1)
Attribution de valeur: cf. appendice 2

2.112. 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 d'exploitation comprise entre 0 et 9 999 999 km.

2.113. OdometerValueMidnight

Valeur affichée par le compteur kilométrique du véhicule à minuit un jour donné (exigence 090, annexe 1B; exigence 113, annexe 1C).

OdometerValueMidnight ::= OdometerShort
Affectation de valeur: pas spécifiée davantage.

2.114. OdometerValueMidnightRecordArray
Génération 2:

OdometerValueMidnight plus les métadonnées tels qu'utilisés dans le 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 de relevé (OdometerValueMidnight). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des OdometerValueMidnight exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records désigne le jeu de relevés de OdometerValueMidnight.

2.115. OverspeedNumber
Nombre d'événements du 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 du type excès de vitesse n'est survenu depuis le dernier contrôle d'excès de vitesse, 1 signifie qu'un événement du type excès de vitesse est survenu depuis le dernier contrôle d'excès de vitesse … 255 signifie que le nombre des événements du type excès de vitesse enregistrés depuis le dernier contrôle d'excès de vitesse est égal ou supérieur à 255.

2.116. PlaceRecord
Informations relatives à un lieu de début ou de fin d'une période de travail journalière (exigences 108, 271, 296, 324 et 347, annexe 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 d'entrée.

dailyWorkPeriodCountry indique le pays entré.

dailyWorkPeriodRegion indique la région entrée.

vehicleOdometerValue indique la valeur affichée par le compteur kilométrique à l'heure de la saisie du lieu entré.

Génération 2:

```
PlaceRecord ::= SEQUENCE {
    entryTime                       TimeReal,
    entryTypeDailyWorkPeriod        EntryTypeDailyWorkPeriod,
    dailyWorkPeriodCountry          NationNumeric,
    dailyWorkPeriodRegion           RegionNumeric,
    vehicleOdometerValue            OdometerShort,
    entryGNSSPlaceRecord            GNSSPlaceRecord
}
```

Outre la génération 1, les composants suivants servent:

entryGNSSPlaceRecord désigne le lieu et l'heure enregistrés.

2.117. PreviousVehicleInfo

Informations relatives au véhicule précédemment utilisé par un conducteur lors de l'insertion de sa carte dans le lecteur d'une unité embarquée sur véhicule (exigence 081, annexe 1B; exigence 102, annexe 1C).

Génération 1:

```
PreviousVehicleInfo ::= SEQUENCE {
    vehicleRegistrationIdentification   VehicleRegistrationIdentification,
    cardWithdrawalTime                  TimeReal
}
```

vehicleRegistrationIdentification indique le VRN ainsi que l'État membre 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
}
```

Outre la génération 1, l'élément de données suivant est utilisé:

vuGeneration identifie la génération de l'unité embarquée sur véhicule.

2.118. 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.

2.119. RecordType

Génération 2:

Référence à un type de relevé. Ce type de données sert au 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,
‘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	RFU,
‘80’H à ‘FF’H	propre au fabricant

2.120. RegionAlpha

Référence alphabétique aux différentes régions d'un pays déterminé.

```
RegionAlpha ::= CHAÎNE IA5[LONGUEUR(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 maintenue à jour sur le site web du laboratoire désigné pour effectuer les essais d'interopérabilité.

2.121. Assignation de valeur:

Référence alphabétique aux 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 maintenue à jour sur le site web du laboratoire désigné pour effectuer les essais d’interopérabilité.

2.122. RemoteCommunicationModuleSerialNumber
Génération 2:

Numéro de série du module de communication à distance.

RemoteCommunicationModuleSerialNumber `::=` ExtendedSerialNumber

2.123. RSAKeyModulus
Génération 1:

Module d'une paire de clés RSA.

RSAKeyModulus ::= OCTET STRING (SIZE(128))
Attribution de valeur: Non-spécifié.

2.124. RSAKeyPublicExponent
Génération 1:

Exposant privé d'une paire de clés RSA.

RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))

Attribution de valeur: Non-spécifié.

2.125. RSAKeyPublicExponent
Génération 1:

Exposant public d'une paire de clés RSA.

RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))

Attribution de valeur: Non-spécifié.

2.126. RtmData
Génération 2:

Pour la définition de ce type de données, cf. appendice 14.

2.127. SealDataCard
Génération 2:

Ce type de données stocke les informations concernant les scellés liés aux différents composants d'un véhicule sur une carte. Ce type de données est lié à l'exigence 337, annexe 1C.

```
SealDataCard ::= SEQUENCE {
    noOfSealRecords                 INTEGER(1..5),
    sealRecords                     SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords désigne le nombre de relevés dans sealRecords**.**

sealRecords indique un jeu de relevés de scellés.

2.128. SealDataVu
Génération 2:

Ce type de données stocke les informations concernant les scellés liés aux différents composants d'un véhicule sur une unité embarquée sur le véhicule.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
    sealRecords                     SealRecord
}
```

sealRecords indique un jeu de relevés de scellés. S'il existe moins de 5 scellés disponibles, la valeur du type d'équipement dans tous les relevés de scellés inutilisés doit être définie sur 16, c'est-à-dire inutilisé.

2.129. SealRecord
Génération 2:

Ce type de données stocke des informations à propos d'un scellé lié au composant. Ce type de données est lié à l'exigence 337, annexe 1C.

```
SealRecord ::= SEQUENCE {
    equipmentType                   EquipmentType,
    extendedSealIdentifier          ExtendedSealIdentifier
}
```

equipmentType identifie le type d'équipement auquel le scellé est associé.

extendedSealIdentifier désigne l'identificateur du scellé associé à l'équipement concerné.

2.130. 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 fourni tel que publié par le site Internet de la Commission européenne correspondant, à savoir en incluant les traits d'union, par exemple. Le numéro d'homologation doit être aligné à gauche.

2.131. SensorExternalGNSSApprovalNumber
Génération 2:

Numéro d'homologation du dispositif GNSS externe.

SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))

Attribution de valeur:

Le numéro d'homologation doit être fourni tel que publié par le site Internet de la Commission européenne correspondant, à savoir en incluant les traits d'union, par exemple. Le numéro d'homologation doit être aligné à gauche.

2.132. SensorExternalGNSSCoupledRecord
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à l'identification du dispositif GNSS externe couplé avec cette unité embarquée (exigence 100, annexe 1C).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
    sensorSerialNumber                  SensorGNSSSerialNumber,
    sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
    sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber désigne le numéro de série du dispositif GNSS externe appairé à l'unité embarquée sur le véhicule.

sensorApprovalNumber désigne le numéro d'homologation de ce dispositif GNSS externe.

sensorCouplingDate indique la date de l'appariement entre ce dispositif GNSS externe avec l'unité embarquée sur véhicule.

2.133. SensorExternalGNSSIdentification
Génération 2:

Informations se rapportant à l'identification du dispositif GNSS externe (exigence 98, annexe 1C).

```
SensorExternalGNSSIdentification ::= SEQUENCE {
    sensorSerialNumber                  SensorGNSSSerialNumber,
    sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
    sensorSCIdentifier                  SensorExternalGNSSSCIdentifier,
    sensorOSIdentifier                  SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber désigne le numéro de série étendu du dispositif GNSS externe.

sensorApprovalNumber désigne le numéro d'homologation du dispositif GNSS externe.

sensorSCIdentifier indique l'identificateur du composant de sécurité du dispositif GNSS externe.

sensorOSIdentifier indique l'identificateur du système d'exploitation du dispositif GNSS externe.

2.134. SensorExternalGNSSInstallation

Génération 2:

Informations mémorisées dans le dispositif GNSS externe se rapportant à l'installation du capteur GNSS externe (exigence 123, annexe 1C).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
    sensorCouplingDateFirst             SensorGNSSCouplingDate,
    firstVuApprovalNumber               VuApprovalNumber,
    firstVuSerialNumber                 VuSerialNumber,
    sensorCouplingDateCurrent           SensorGNSSCouplingDate,
    currentVuApprovalNumber             VuApprovalNumber,
    currentVUSerialNumber               VuSerialNumber
}
```

sensorCouplingDateFirst indique la date du premier couplage entre une unité embarquée sur véhicule et le dispositif GNSS externe.

firstVuApprovalNumber indique le numéro d'homologation de la première unité embarquée sur véhicule couplée avec le dispositif GNSS externe.

firstVuSerialNumber indique le numéro de série de la première unité embarquée sur véhicule couplée avec le dispositif GNSS externe.

sensorCouplingDateCurrent indique la date du couplage actuel entre l'unité embarquée sur véhicule et le dispositif GNSS externe.

currentVuApprovalNumber désigne le numéro d'homologation de l'unité embarquée sur le véhicule actuellement couplée avec le dispositif GNSS externe.

currentVUSerialNumber désigne le numéro de série de l'unité embarquée sur le véhicule actuellement couplée avec le dispositif GNSS externe.

2.135. SensorExternalGNSSOSIdentifier
Génération 2:

Identificateur du système d'exploitation du dispositif GNSS externe.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Attribution de valeur: propre au fabricant.

2.136. SensorExternalGNSSSCIdentifier
Génération 2:

Ce type sert p. ex. 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.

2.137. SensorGNSSCouplingDate
Génération 2:

Date d'un couplage entre une unité embarquée sur véhicule et le dispositif GNSS externe.

SensorGNSSCouplingDate ::= TimeReal

Attribution de valeur: Non-spécifié.

2.138. SensorGNSSSerialNumber

Génération 2:

Ce type sert à stocker le numéro de série du récepteur GNSS situé à l'intérieur ou à l'extérieur de la VU.

Numéro de série du récepteur GNSS.

SensorGNSSSerialNumber ::= ExtendedSerialNumber

2.139. SensorIdentification
Informations enregistrées dans la mémoire d'un capteur de mouvement et se rapportant à l'identification de cet élément (exigence 077, annexe 1B et exigence 95, annexe 1C).

```
SensorIdentification ::= SEQUENCE {
    sensorSerialNumber              SensorSerialNumber,
    sensorApprovalNumber            SensorApprovalNumber,
    sensorSCIdentifier              SensorSCIdentifier,
    sensorOSIdentifier              SensorOSIdentifier
}
```

sensorSerialNumber indique le numéro de série étendu du capteur de mouvement (numéro de pièce et code du fabricant inclus).

sensorApprovalNumber indique le numéro d'homologation du capteur de mouvement.

sensorSCIdentifier indique l'identificateur du composant de sécurité du capteur de mouvement.

sensorOSIdentifier indique l'identificateur du système d'exploitation du capteur de mouvement.

2.140. SensorInstallation
Informations enregistrées dans la mémoire d'un capteur de mouvement et se rapportant à l'installation de cet élément (exigence 099, annexe 1B et exigence 122, annexe 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 sur véhicule.

firstVuApprovalNumber indique le numéro d'homologation de la première unité embarquée sur véhicule couplée avec le capteur de mouvement.

firstVuSerialNumber indique le numéro de série de la première unité embarquée sur véhicule couplée avec le capteur de mouvement.

sensorPairingDateCurrent indique la date du couplage actuel du capteur de mouvement avec l'unité embarquée sur véhicule.

currentVuApprovalNumber indique le numéro d'homologation de l'unité sur véhicule actuellement couplée avec le capteur de mouvement.

currentVUSerialNumber indique le numéro de série de l'unité sur véhicule actuellement couplée avec le capteur de mouvement.

2.141. SensorInstallationSecData

Informations enregistrées sur une carte d'atelier et se rapportant aux données de sécurité nécessaires au couplage de capteurs de mouvement avec des unités embarquées sur véhicule (exigences 308 et 331, annexe 1C).

Génération 1:

SensorInstallationSecData ::= TDesSessionKey

Attribution de valeur: conforme à la norme ISO 16844-3.

Génération 2:

Comme décrit dans l'appendice 11, une carte d'atelier doit mémoriser jusqu'à trois clés pour le couplage du capteur de mouvement situé sur la VU. Ces clés existent en différentes versions.

```
SensorInstallationSecData ::= SEQUENCE {
    kMWCKey1                        KMWCKey,
    kMWCKey2                        KMWCKey OPTIONAL,
    kMWCKey3                        KMWCKey OPTIONAL
}
```

2.142. SensorOSIdentifier
Identificateur du système d'exploitation du capteur de mouvement.

SensorOSIdentifier ::= IA5String(SIZE(2))

Attribution de valeur: propre au fabricant.

2.143. SensorPaired
Génération 1:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à l'identification du capteur de mouvement couplé avec cette unité embarquée (exigence 079, annexe 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 sur véhicule.

sensorApprovalNumber indique le numéro d'homologation du capteur de mouvement actuellement couplé avec l'unité embarquée sur véhicule.

sensorPairingDateFirst indique la date du premier couplage entre une unité sur véhicule et le capteur de mouvement actuellement couplé avec l'unité embarquée sur le véhicule considéré.

2.144. SensorPairedRecord

Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à l'identification du capteur de mouvement couplé avec cette unité embarquée (exigence 97, annexe 1C).

```
SensorPairedRecord ::= SEQUENCE {
    sensorSerialNumber              SensorSerialNumber,
    sensorApprovalNumber            SensorApprovalNumber,
    sensorPairingDate               SensorPairingDate
}
```

sensorSerialNumber indique le numéro de série du capteur de mouvement actuellement couplé avec l'unité embarquée sur véhicule.

sensorApprovalNumber indique le numéro d'homologation du capteur de mouvement.

sensorPairingDate indique une date d'appariement du capteur de mouvement avec l'unité embarquée sur véhicule.

2.145. SensorPairingDate
Date d'un couplage du capteur de mouvement avec une unité embarquée sur véhicule.

SensorPairingDate ::= TimeReal

Attribution de valeur: Non-spécifié.

2.146. SensorSCIdentifier
Identificateur du composant de sécurité du capteur de mouvement.

SensorSCIdentifier ::= IA5String(SIZE(8))

Attribution de valeur: propre au fabricant.

2.147. SensorSerialNumber
Numéro de série du capteur de mouvement.

SensorSerialNumber ::= ExtendedSerialNumber

2.148. Signature
Signature numérique.

Génération 1:

Signature ::= OCTET STRING (SIZE(128))

Attribution de valeur: en conformité avec l'appendice 11 (Mécanismes de sécurité communs).

Génération 2:

Signature ::= OCTET STRING (SIZE(64..132))

Attribution de valeur: en conformité avec l'appendice 11 (Mécanismes de sécurité communs).

2.149. SignatureRecordArray
Génération 2:

Jeu de signatures plus les métadonnées servant au protocole de téléchargement.

```
SignatureRecordArray ::= SEQUENCE {
    recordType                          RecordType,
    recordSize                          ENTIER(1..65535),
    noOfRecords                         ENTIER(0..65535),
    records                             SET SIZE(noOfRecords) OF Signature
}
```

recordType indique le type de relevé (Signature). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des signatures exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis. La valeur doit être définie sur 1, car les signatures peuvent présenter des longueurs variables.

records indique le jeu de relevés de signatures.

2.150. SimilarEventsNumber
Nombre d'événements similaires survenus un jour donné (exigence 094, annexe 1B; exigence 117, annexe 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 (et un seul d'entre eux a été enregistré), … 255 signifie que le jour considéré a vu la manifestation d'un nombre d'événements de ce type égal ou supérieur à 255.

2.151. SpecificConditionRecord
Informations enregistrées sur une carte de conducteur, une carte d'atelier ou une unité embarquée sur véhicule et se rapportant à une condition particulière (exigences 130, 276, 301, 328 et 355, annexe 1C).

```
SpecificConditionRecord ::= SEQUENCE {
    entryTime                           TimeReal,
    specificConditionType               SpecificConditionType
}
```

entryTime indique la date et l'heure d'entrée de ces données.

specificConditionType indique le code identifiant la condition particulière concernée.

2.152. SpecificConditions
Informations enregistrées sur une carte de conducteur, une carte d'atelier ou une unité embarquée sur véhicule et se rapportant à une condition particulière (exigences 131, 277, 302, 329 et 356, annexe 1C).

Génération 2:

```
SpecificConditions := SEQUENCE {
    conditionPointerNewestRecord        INTEGER(0..NoOfSpecificConditionRecords-1),
    specificConditionRecords            SET SIZE(NoOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

conditionPointerNewestRecord indique l'indice du dernier relevé de conditions particulières mis à jour.
Attribution de valeur: nombre correspondant au numérateur du relevé de conditions particulières, commençant par une série de ′0′ pour la première occurrence d'un relevé de conditions particulières dans la structure considérée.

specificConditionRecords indique le jeu de relevés contenant des informations relatives à des conditions particulières.

2.153. SpecificConditionType
Code identifiant une condition particulière (exigences 050b, 105a, 212a et 230a, annexe 1B; exigences 62, annexe 1C).

SpecificConditionType ::= INTEGER(0..255)

Génération 1:

Attribution de valeur:

‘00’H	RFU
′01′H	Hors champ — Début
′02′H	Hors champ — Fin
‘03’H	Trajet en ferry/train
‘04’H .. ‘FF’H	RFU

Génération 2:

Attribution de valeur:

‘00’H	RFU
′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	RFU

2.154. Speed
Vitesse du véhicule (km/h).

Speed ::= INTEGER(0..255)

Attribution de valeur: kilomètres à l'heure dans une plage d'exploitation comprise entre 0 et 220 km/h.

2.155. SpeedAuthorised
Vitesse maximale autorisée du véhicule (définition hh).

SpeedAuthorised ::= Speed

2.156. SpeedAverage
Vitesse moyenne mesurée par rapport à une durée préalablement définie (km/h).

SpeedAverage ::= Speed

2.157. SpeedMax
Vitesse maximale mesurée pendant une durée préalablement définie.

```
SpeedMax ::= Speed
```

2.158. TachographPayload
Génération 2:

Pour la définition de ce type de données, cf. appendice 14.

2.159. TachographPayloadEncrypted
Génération 2:

La charge du tachygraphe codée DER-TLV, c'est-à-dire les données codées envoyées dans le message RTM. Concernant le mécanisme de cryptage, 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 DER-TLV et doit être défini sur '87 (cf. appendice 11, partie B, chapitre 13).

length fait partie du codage 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.

2.160. TDesSessionKey
Génération 1:

Clé de session Triple DES.

```
TDesSessionKey ::= SEQUENCE {
    tDesKeyA                            OCTET STRING (SIZE(8)),
    tDesKeyB                            OCTET STRING  (SIZE(8))
}
```

Affectation de valeur: pas spécifiée davantage.

2.161. TimeReal
Code associé à un champ combinant date et heure exprimées en secondes à compter de 00h00m00s TUC le 1er janvier 1970.

```
TimeRealINTEGER:TimeRealRange ::= INTEGER(0..TimeRealRange)
```

Assignation de valeur — Octet aligné: nombre de secondes écoulées depuis minuit TUC, le 1er janvier 1970.

La date/heure future la plus avancée se situe en l'an 2106.

2.162. TyreSize
Désignation des dimensions des pneumatiques.

TyreSize ::= IA5String(SIZE(15))

Assignation de valeur: en conformité avec la directive 92/23/CEE du 31.3.1992 (JO L 129, p. 95).

2.163. VehicleIdentificationNumber
Numéro d'identification du véhicule (VIN) faisant référence au véhicule dans son entier; il s'agit habituellement du numéro de série du châssis ou du numéro de cadre.

VehicleIdentificationNumber ::= IA5String(SIZE(17))

Attribution de valeur: conformément à la norme ISO 3779.

2.164. VehicleIdentificationNumberRecordArray
Génération 2:

Numéro d'identification du véhicule plus les métadonnées tels qu'utilisés dans le 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 de relevé (VehicleIdentificationNumber). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VehicleIdentificationNumber exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records désigne le jeu des numéros d'identification des véhicules.

2.165. VehicleRegistrationIdentification
Identification d'un véhicule, unique à l'échelle de l'Europe (VIN et État membre).

```
VehicleRegistrationIdentification ::= SEQUENCE {
    vehicleRegistrationNation           NationNumeric,
    vehicleRegistrationNumber           VehicleRegistrationNumber
}
```

vehicleRegistrationNation indique le pays d'immatriculation du véhicule.

vehicleRegistrationNumber indique le numéro d'immatriculation du véhicule (VRN).

2.166. Numéro d'immatriculation du véhicule
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 encodé à l'aide du jeu de caractères spécifié.

Attribution de valeur: propre à chaque pays.

2.167. VehicleRegistrationNumberRecordArray
Génération 2:

Immatriculation du véhicule plus les métadonnées tels qu'utilisées dans le 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 de relevé (VehicleRegistrationNumber). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VehicleRegistrationNumber exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records désigne le jeu des immatriculations des véhicules.

2.168. VuAbility

Génération 2:

Informations stockées dans une VU concernant sa capacité à utiliser des cartes tachygraphiques de génération 1 (exigence 121, annexe 1C).

VuAbility ::= OCTET STRING (SIZE(1))

Assignation de valeur — Octet aligné: ‘xxxxxxxa’B (8 octets)

Pour la compatibilité avec 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 génération1,

‘xxxxxxx’B RFU

2.169. VuActivityDailyData
Génération 1:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux changements d'activité ainsi qu'aux changements d'état de conduite et/ou d'état de carte pour un jour civil donné (exigence 084, annexe 1B; exigences 105, 106 et 107, annexe 1C) et à l'état des lecteurs à 00h00 ce même jour.

```
VuActivityDailyData ::= SEQUENCE {
    noOfActivityChanges                 INTEGER SIZE(0..1440),
    activityChangeInfos                 SET SIZE(noOfActivityChanges) OF ActivityChangeInfo
}
```

noOfActivityChanges indique le nombre de mots que comporte le jeu ActivityChangeInfos.

activityChangeInfos indique le jeu de mots ActivityChangeInfo enregistrés dans la VU pour le jour considéré. Il comprend toujours deux mots ActivityChangeInfo donnant l'état des deux lecteurs à 00h00 ce même jour.

2.170. VuActivityDailyRecordArray
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux changements d'activité ainsi qu'aux changements d'état de conduite et/ou d'état de carte pour un jour civil donné (exigence 105, 106 et 107 annexe 1C) et à l'état des lecteurs à 00h00 ce même jour.

```
VuActivityDailyRecordArray ::= SEQUENCE {
    recordType                          RecordType,
    recordSize                          INTEGER(1..65535),
    noOfRecords                         INTEGER(0..65535),
    records                             SET SIZE(noOfRecords) OF ActivityChangeInfo
}
```

recordType indique le type de relevé (ActivityChangeInfo). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des ActivityChangeInfo exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records désigne le jeu de mots ActivityChangeInfo enregistrés dans la VU pour le jour considéré. Il comprend toujours deux mots ActivityChangeInfo donnant l'état des deux lecteurs à 00h00 ce même jour.

2.171. VuApprovalNumber
Numéro d'homologation de l'unité embarquée sur 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 fourni tel que publié par le site Internet de la Commission européenne correspondant, à savoir en incluant les traits d'union, par exemple. Le numéro d'homologation doit être aligné à gauche.

2.172. VuCalibrationData
Génération 1:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux étalonnages successifs de l'appareil d'enregistrement (exigence 098, annexe 1B).

```
VuCalibrationData ::= SEQUENCE {
    noOfVuCalibrationRecords                INTEGER(0..255),
    vuCalibrationRecords                    SET SIZE(noOfVuCalibrationRecords) OF VuCalibrationRecord
}
```

noOfVuCalibrationRecords indique le nombre des relevés que contient le jeu vuCalibrationRecords.

vuCalibrationRecords indique le jeu de relevés d'étalonnage.

2.173. VuCalibrationRecord
Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux étalonnages successifs de l'appareil d'enregistrement (exigence 098, annexe 1B; exigences 119 et 120, annexe 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 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 indique la désignation de 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 valeurs accordées à la date et à l'heure.

nextCalibrationDate indique la date du prochain étalonnage correspondant au type spécifié dans le champ CalibrationPurpose et auquel l'organisme d'inspection agréé doit procéder.

Génération 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,
    sealDataVu                          SealDataVu
}
```

Outre la génération 1, l'élément de données suivant est utilisé:

sealDataVu fournit des informations relatives aux scellés liés aux différents composants du véhicule.

2.174. VuCalibrationRecordArray
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux étalonnages successifs de l'appareil d'enregistrement (exigence 119 et 120, annexe 1C).

```
VuCalibrationRecordArray ::= SEQUENCE {
    recordType                          RecordType,
    recordSize                          INTEGER(1..65535),
    noOfRecords                         INTEGER(0..65535),
    records                             SET SIZE(noOfRecords) OF VuCalibrationRecord
}
```

recordType indique le type de relevé (VuCalibrationRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuCalibrationRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique le jeu de relevés d'étalonnage.

2.175. VuCardIWData
Génération 1:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux cycles d'insertion et de retrait des cartes de conducteur ou d'atelier dans le lecteur approprié de cette unité embarquée (exigence 081, annexe 1B et exigence 103, annexe 1C).

```
VuCardIWData ::= SEQUENCE {
    noOfIWRecords                   INTEGER(0..2^16-1),
    vuCardIWRecords                 SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords désigne le nombre de relevés dans le jeu vuCardIWRecords

vuCardIWRecords désigne un jeu de relevés portant sur les cycles d'insertion et de retrait des cartes.

2.176. VuCardIWRecord
Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux cycles d'insertion et de retrait des cartes de conducteur ou d'atelier dans le lecteur approprié de cette unité embarquée (exigence 081, annexe 1B et exigence 102, annexe 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 conducteur ou du détenteur de la carte d'atelier, tels qu'ils sont enregistrés sur celle-ci.

fullCardNumber indique le type de carte, l'État membre où est délivrée la carte et le numéro de celle-ci, tels qu'ils sont enregistrés sur la carte.

cardExpiryDate indique la date d'expiration de la carte telle qu'elle est 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 la fente duquel 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 relatives au précédent véhicule utilisé par le conducteur, telles qu'elles sont enregistrées sur la carte.

manualInputFlag correspond à un drapeau permettant d'identifier si le détenteur de la carte a procédé ou non à la saisie manuelle d'activités du conducteur lors de l'insertion de cette 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
}
```

La structure de données de génération 2 n'utilise pas fullCardNumber, mais plutôt les éléments suivants.

fullCardNumberAndGeneration indique le type de carte, l'État membre où elle a été délivrée, son numéro et sa génération, tels qu'ils sont enregistrés sur la carte.

2.177. VuCardIWRecordArray
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux cycles d'insertion et de retrait des cartes de conducteur ou d'atelier dans le lecteur approprié de cette unité embarquée (exigence 103, annexe 1C).

```
VuCardIWRecordArray ::= SEQUENCE {
    recordType                              RecordType,
    recordSize                              INTEGER(1..65535),
    noOfRecords                             INTEGER(0..65535),
    records                                 SET SIZE(noOfRecords) OF VuCardIWRecord
}
```

recordType indique le type de relevé (VuCardIWRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuCardIWRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records désigne un jeu de relevés portant sur les cycles d'insertion et de retrait des cartes.

2.178. VuCardRecord
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à la carte tachygraphique utilisée (exigences 132, annexe 1C).

```
VuCardRecord ::= SEQUENCE {
    cardExtendedSerialNumber            ExtendedSerialNumber,
    cardPersonaliserID                  OCTET STRING(SIZE(1)),
    typeofTachographCardID              EquipmentType,
    cardStructureVersion                CardStructureVersion,
    cardNumber                          CardNumber
}
```

cardExtendedSerialNumber tel qu'extrait du fichier EF_ICC sous le FM de la carte.

cardPersonaliserID tel qu'extrait du fichier EF_ICC sous le FM de la carte.

typeOfTachographCardId tel qu'extrait du fichier élémentaire EF_Application_Identification sous le fichier spécialisé DF_Tachograph_G2

cardStructureVersion telle qu'extraite du fichier élémentaire EF_Application_Identification sous le fichier spécialisé DF_Tachograph_G2

cardNumber tel qu'extrait du fichier élémentaire FE_Identification sous le fichier spécialisé DF_Tachograph_G2.

2.179. VuCardRecordArray
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux cartes tachygraphiques utilisées par cette VU. Ces informations servent à l'analyse de la VU: problèmes de cartes (exigence 132, annexe 1C).

```
VuCardRecordArray ::= SEQUENCE {
    recordType                          RecordType,
    recordSize                          INTEGER(1..65535),
    noOfRecords                         INTEGER(0..65535),
    records                             SET SIZE(noOfRecords) OF VuCardRecord
}
```

recordType indique le type de relevé (VuCardRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuCardRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records désigne un jeu de relevés portant sur les cartes tachygraphiques utilisées par la VU.

2.180. VuCertificate
Certificat associé à la clé publique d'une unité embarquée sur véhicule.

```
VuCertificate ::= Certificate
```

2.181. VuCertificateRecordArray
Génération 2:

Certificat de la VU plus les métadonnées tels qu'utilisés dans le 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 de relevé (VuCertificate). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuCertificate exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis. La valeur doit être définie sur 1, car les certificats peuvent présenter des longueurs variables.

records désigne un jeu de certificats de VU.

2.182. VuCompanyLocksData
Génération 1:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux verrouillages d'entreprise (exigence 104, annexe 1B).

```
VuCompanyLocksData ::= SEQUENCE {
    noOfLocks                           INTEGER(0..255),
    vuCompanyLocksRecords               SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks indique le nombre de verrouillages répertoriés dans les vuCompanyLocksRecords.

vuCompanyLocksRecords correspond au jeu de relevés des verrouillages d'entreprise.

2.183. VuCompanyLocksRecord
Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à un verrouillage d'entreprise déterminé (exigence 104, annexe 1B; exigence 128, annexe 1C).

Génération 1:

```
VuCompanyLocksRecord ::= SEQUENCE {
    lockInTime                          TimeReal,
    lockOutTime                         TimeReal,
    companyName                         Name,
    companyAddress                      Address,
    companyCardNumber                   FullCardNumber
}
```

lockInTime, lockOutTime indiquent les dates et heures de verrouillage et de déverrouillage.

companyName, companyAddress indiquent les nom et adresse de l'entreprise en rapport avec le verrouillage.

companyCardNumber identifie la carte utilisée lors du verrouillage.

Génération 2:

```
VuCompanyLocksRecord ::= SEQUENCE {
    lockInTime                          TimeReal,
    lockOutTime                         TimeReal,
    companyName                         Name,
    companyAddress                      Address,
    fullCardNumberAndGeneration         FullCardNumberAndGeneration,
}
```

La structure de données de génération 2 n'utilise pas companyCardNumber, mais plutôt l'élément suivant.

companyCardNumberAndGeneration identifie la carte utilisée lors du verrouillage et sa génération.

2.184. VuCompanyLocksRecordArray
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux verrouillages d'entreprise (exigence 128, annexe 1C).

```
VuCompanyLocksRecordArray ::= SEQUENCE {
    recordType                          RecordType,
    recordSize                          INTEGER(1..65535),
    noOfRecords                         INTEGER(0..65535),
    records                             SET SIZE(noOfRecords) OF VuCompanyLocksRecord
}
```

recordType indique le type de relevé (VuCompanyLocksRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuCompanyLocksRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis. Valeur 0..255.

records correspond au jeu de relevés des verrouillages d'entreprise.

2.185. VuControlActivityData
Génération 1:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux contrôles exécutés à l'aide de cette VU (exigence 102, annexe 1B).

```
VuControlActivityData ::= SEQUENCE {
    noOfControls                        INTEGER(0..20),
    vuControlActivityRecords            SET SIZE(noOfControls) OF VuControlActivityRecord
}
```

noOfControls indique le nombre de contrôles répertoriés dans les vuControlActivityRecords.

vuControlActivityRecords indique le jeu des relevés d'activité de contrôle.

2.186. VuControlActivityRecord

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux contrôles exécutés à l'aide de cette VU (exigence 102, annexe 1B; exigence 126, annexe 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,
    fullCardNumberAndGeneration     FullCardNumberAndGeneration,
    downloadPeriodBeginTime         TimeReal,
    downloadPeriodEndTime           TimeReal
}
```

La structure de données de génération 2 n'utilise pas controlCardNumber, mais plutôt les éléments suivants.

controlCardNumberAndGeneration identifie la carte de contrôleur utilisée lors du contrôle ainsi que sa génération.

2.187. VuControlActivityRecordArray
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux contrôles exécutés à l'aide de cette VU (exigence 126, annexe 1C).

```
VuControlActivityRecordArray ::= SEQUENCE {
    recordType                      RecordType,
    recordSize                      INTEGER(1..65535),
    noOfRecords                     INTEGER(0..65535),
    records                         SET SIZE(noOfRecords) OF VuControlActivityRecord
}
```

recordType indique le type de relevé (VuControlActivityRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuControlActivityRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique le jeu regroupant l'ensemble des relevés d'activité de contrôle de la VU.

2.188. VuDataBlockCounter

Compteur enregistré sur une carte et identifiant séquentiellement les cycles d'insertion et de retrait de la carte sur le lecteur approprié d'unités embarquées sur véhicules.

VuDataBlockCounter ::= BCDString(SIZE(2))

Attribution de valeur: numérotation consécutive dont la valeur maximale est égale à 9 999, la numérotation recommençant par le numéro 0.

2.189. VuDetailedSpeedBlock
Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à l'évolution de la vitesse du véhicule pendant une minute au cours de laquelle le véhicule était en mouvement (exigence 093, annexe 1B; exigence 116, annexe 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).

2.190. VuDetailedSpeedBlockRecordArray
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à 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 de relevé (VuDetailedSpeedBlock). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuDetailedSpeedBlock exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique le jeu de blocs de mesure de la vitesse instantanée.

2.191. VuDetailedSpeedData
Génération 1:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à 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 des blocs de vitesse que comporte le jeu de vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks indique le jeu de blocs de mesure de la vitesse instantanée.

2.192. VuDownloadablePeriod

Dates les plus ancienne et récente pour lesquelles une unité embarquée sur véhicule détient des données relatives aux activités des conducteurs (exigences 081, 084 ou 087, annexe 1B; exigences 102, 105 et 108, annexe 1C).

```
VuDownloadablePeriod ::= SEQUENCE {
    minDownloadableTime                 TimeReal
    maxDownloadableTime                 TimeReal
}
```

minDownloadableTime indique les date et heure de l'insertion de carte, de l'entrée de site ou du changement d'activité le plus ancien enregistrées dans la mémoire de l'unité embarquée sur véhicule.

maxDownloadableTime indique les date et heure du retrait de carte, de l'entrée de site ou du changement d'activité le plus récent enregistrées dans la mémoire de l'unité embarquée sur véhicule.

2.193. VuDownloadablePeriodRecordArray
Génération 2:

VUDownloadablePeriod plus les métadonnées tels qu'utilisés dans le 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 de relevé (VuDownloadablePeriod). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuDownloadablePeriod exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique le jeu de relevés VuDownloadablePeriod.

2.194. VuDownloadActivityData
Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant au plus récent téléchargement (exigence 105, annexe 1B; exigence 129, annexe 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
}
```

La structure de données de génération 2 n'utilise pas fullCardNumber, mais plutôt les éléments suivants.

fullCardNumberAndGeneration identifie la carte utilisée pour autoriser le téléchargement ainsi que sa génération.

2.195. VuDownloadActivityDataRecordArray
Génération 2:

Informations se rapportant au dernier téléchargement de la VU (exigence 129, annexe 1C).

```
VuDownloadActivityDataRecordArray ::= SEQUENCE {
    recordType                          RecordType,
    recordSize                          INTEGER(1..65535),
    noOfRecords                         INTEGER(0..65535),
    records                             SET SIZE(noOfRecords) OF VuDownloadActivityData
}
```

recordType indique le type de relevé (VuDownloadActivityData). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuDownloadActivityData exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records désigne le jeu regroupant l'ensemble des relevés de données d'activité relatives au téléchargement.

2.196. VuEventData
Génération 1:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à divers événements (exigence 094, annexe 1B, à l'exception des événements du type excès de vitesse).

```
VuEventData ::= SEQUENCE {
    noOfVuEvents                        INTEGER(0..255),
    vuEventRecords                      SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents indique le nombre des événements répertoriés dans le jeu des vuEventRecords.

vuEventRecords indique un jeu de relevés d'événements.

2.197. VuEventRecord
Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à divers événements (exigence 094, annexe 1B; exigence 117, annexe 1C, à l'exception des événements du 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 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.

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 convoyeur, 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 convoyeur, à la fin de l'événement.

similarEventsNumber indique le nombre d'événements similaires survenus le même jour.

Cette séquence s'utilise pour tous les événements, sauf ceux du type excès de vitesse.

Génération 2:

Outre la génération 1, les éléments de données suivants sont utilisés:

manufacturerSpecificEventFaultData contient des informations complémentaires propres au fabricant et se rapportant à l'événement.

La structure de données de génération 2 n'utilise pas cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd et cardNumberCodriverSlotEnd, mais plutôt les éléments 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 convoyeur 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 convoyeur 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 désigne la date et l'heure de l'appareil de contrôle.

eventEndTime indique la date et l'heure du dispositif GNSS.

2.198. VuEventRecordArray
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à divers événements (exigence 117, annexe 1C, à l'exception des événements du 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 de relevé (VuEventRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuEventRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique un jeu de relevés d'événements.

2.199. VuFaultData

Génération 1:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à diverses anomalies (exigence 096, annexe 1B).

```
VuFaultData ::= SEQUENCE {
    noOfVuFaults                    INTEGER(0..255),
    vuFaultRecords                  SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults indique le nombre des anomalies répertoriées dans le jeu des vuFaultRecords.

vuFaultRecords indique un jeu de relevés d'anomalies.

2.200. VuFaultRecord
Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à une anomalie (exigence 096, annexe 1B; exigence 118, annexe 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 de l'enregistrement de l'anomalie considérée.

faultBeginTime indique la date et l'heure de début de l'anomalie.

faultEndTime indique la date et l'heure de 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 convoyeur, 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 convoyeur, à la fin de l'anomalie.

Génération 2:

```
VuFaultRecord ::= SEQUENCE {
    faultType                       EventFaultType,
    faultRecordPurpose              EventFaultRecordPurpose,
    faultBeginTime                  TimeReal,
    faultEndTime                    TimeReal,
    cardNumberAndGenDriverSlotBegin     FullCardNumberAndGeneration,
    cardNumberAndGenDriverSlotBegin     FullCardNumberAndGeneration,
    cardNumberAndGenDriverSlotEnd       FullCardNumberAndGeneration,
    cardNumberAndGenCodriverSlotEnd     FullCardNumberAndGeneration,
    manufacturerSpecificEventFaultData  ManufacturerSpecificEventFaultData
}
```

Outre la génération 1, l'élément de données suivant est utilisé:

manufacturerSpecificEventFaultData contient des informations complémentaires propres au fabricant et se rapportant à l'événement.

La structure de données de génération 2 n'utilise pas cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd et cardNumberCodriverSlotEnd, mais plutôt les éléments 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 convoyeur 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 convoyeur ainsi que sa génération, à la fin de l'anomalie.

2.201. VuFaultRecordArray
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à diverses anomalies (exigence 118, annexe 1C).

```
VuFaultRecordArray ::= SEQUENCE {
    recordType                  RecordType,
    recordSize                  INTEGER(1..65535),
    noOfRecords                 INTEGER(0..65535),
    records                     SET SIZE(noOfRecords) OF VuFaultRecord
}
```

recordType indique le type de relevé (VuFaultRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuFaultRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique un jeu de relevés d'anomalies.

2.202. VuGNSSCDRecord
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule relatives à la position GNSS du véhicule lorsque le temps de conduite continue du conducteur atteint un multiple de trois heures (exigences 108 et 110, Annexe 1C).

```
VuGNSSCDRecord ::= SEQUENCE {
    timeStamp                       TimeReal,
    cardNumberAndGenDriverSlotEnd       FullCardNumberAndGeneration,
    cardNumberAndGenDriverSlotEnd       FullCardNumberAndGeneration,
    gnssPlaceRecord                 GNSSPlaceRecord
}
```

timeStamp désigne la date et l'heure lorsque le temps de conduite continue 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 convoyeur ainsi que sa génération.

gnssPlaceRecord contient les informations relatives à la position du véhicule.

2.203. VuGNSSCDRecordArray
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule relatives à la position GNSS du véhicule lorsque le temps de conduite continue du conducteur atteint un multiple de trois heures (exigences 108 et 110, Annex 1C).

```
VuGNSSCDRecordArray ::= SEQUENCE {
    recordType                  RecordType,
    recordSize                  INTEGER(1..65535),
    noOfRecords                 INTEGER(0..65535),
    records                     SET SIZE(noOfRecords) OF VuGNSSCDRecord
}
```

recordType indique le type de relevé (VuGNSSCDRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuGNSSCDRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records désigne un jeu de relevés de conduite continue GNSS.

2.204. VuIdentification

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à l'identification de l'unité embarquée (exigence 075, annexe 1B; exigences 93 et 121, annexe 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 sur véhicule.

vuManufacturerAddress indique l'adresse du fabricant de l'unité embarquée sur véhicule.

vuPartNumber indique le numéro de pièce de l'unité embarquée sur véhicule.

vuSerialNumber indique le numéro de série de l'unité embarquée sur véhicule.

vuSoftwareIdentification identifie le logiciel mis en œuvre au sein de l'unité embarquée sur véhicule.

vuManufacturingDate indique la date de fabrication de l'unité embarquée sur véhicule.

vuApprovalNumber indique le numéro d'homologation de l'unité embarquée sur véhicule.

Génération 2:

```
VuIdentification ::= SEQUENCE {
    vuManufacturerName              VuManufacturerName,
    vuManufacturerAddress           VuManufacturerAddress,
    vuPartNumber                    VuPartNumber,
    vuSerialNumber                  VuSerialNumber,
    vuSoftwareIdentification        VuSoftwareIdentification,
    vuManufacturingDate             VuManufacturingDate,
    vuApprovalNumber                VuApprovalNumber,
    vuGeneration                    Generation
    vuAbility                       VuAbility
}
```

Outre la génération 1, l'élément de données suivant est utilisé:

vuGeneration identifie la génération de l'unité embarquée sur véhicule.

vuAbility fournit des informations sur l'éventuelle compatibilité de la VU avec les cartes tachygraphiques de génération 1.

2.205. VuIdentificationRecordArray
Génération 2:

VuIdentification plus les métadonnées tels qu'utilisés dans le 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 de relevé (VuIdentification). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuIdentification exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique un jeu de relevés VuIdentification.

2.206. VuITSConsentRecord
Génération 2:

Informations stockées dans une unité embarquée sur véhicule relatives à l'accord d'un conducteur sur l'utilisation des Intelligent Transport Systems.

```
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 désigne un drapeau qui signale si le conducteur a donné son accord sur l'utilisation des Intelligent Transport Systems avec ce véhicule ou cette unité embarquée sur véhicule.

Attribution de valeur:

VRAI indique l'accord du conducteur sur l'utilisation des Intelligent Transport Systems.

FAUX indique le refus du conducteur sur l'utilisation des Intelligent Transport Systems.

2.207. VuITSConsentRecordArray
Génération 2:

Informations stockées dans une unité embarquée sur véhicule relatives à l'accord d'un conducteur sur l'utilisation des Intelligent Transport Systems (exigence 200, annexe 1C).

```
VuITSConsentRecordArray ::= SEQUENCE {
    recordType                          RecordType,
    recordSize                          INTEGER(1..65535),
    noOfRecords                         INTEGER(0..65535),
    records                             SET SIZE(noOfRecords) OF VuITSConsentRecord
}
```

recordType indique le type de relevé (VuITSConsentRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuITSConsentRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique un jeu de relevés d'accords STI.

2.208. VuManufacturerAddress
Adresse du fabricant de l'unité embarquée sur véhicule.

VuManufacturerAddress ::= Address
Attribution de valeur: Non-spécifié.

2.209. VuManufacturerName
Nom du fabricant de l'unité embarquée sur véhicule.

VuManufacturerName ::= Name
Attribution de valeur: Non-spécifié.

2.210. VuManufacturingDate
Date de fabrication de l'unité embarquée sur véhicule.

VuManufacturingDate ::= TimeReal
Attribution de valeur: Non-spécifié.

2.211. VuOverSpeedingControlData
Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux événements du type excès de vitesse survenus depuis le dernier contrôle d'excès de vitesse (exigence 095, annexe 1B; exigence 117, annexe 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 constaté depuis ce contrôle d'excès de vitesse.

numberOfOverspeedSince indique le nombre d'événements du type excès de vitesse survenus depuis le dernier contrôle d'excès de vitesse.

2.212. VuOverSpeedingControlDataRecordArray
Génération 2:

VuOverSpeedingControlData plus les métadonnées tels qu'utilisés dans le 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 de relevé (VuOverSpeedingControlData). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuOverSpeedingControlData exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique un jeu de relevés de données relatives au contrôle d'excès de vitesse.

2.213. VuOverSpeedingEventData
Génération 1:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux événements du type excès de vitesse (exigence 094, annexe 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 indique un jeu de relevés d'événements du type excès de vitesse.

2.214. VuOverSpeedingEventRecord
Génération 1:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux événements du type excès de vitesse (exigence 094, annexe 1B; exigence 117, annexe 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 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.

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 similaires survenus le même jour.

Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux événements du type excès de vitesse (exigence 094, annexe 1B; exigence 117, annexe 1C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
    eventType                          EventFaultType,
    eventRecordPurpose                 EventFaultRecordPurpose,
    eventBeginTime                     TimeReal,
    eventEndTime                       TimeReal,
    maxSpeedValue                      SpeedMax,
    averageSpeedValue                  SpeedAverage,
    cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
    similarEventsNumber                SimilarEventsNumber
}
```

La structure de données de génération 2 n'utilise pas cardNumberDriverSlotBegin, mais plutôt l'élément suivant:

cardNumberAndGenDriverSlotBegin identifie la carte insérée dans le lecteur réservé au conducteur ainsi que sa génération, au début de l'événement.

2.215. VuOverSpeedingEventRecordArray
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux événements du type excès de vitesse (exigence 117, annexe 1C).

```
VuOverSpeedingEventRecordArray ::= SEQUENCE {
    recordType                         RecordType,
    recordSize                         INTEGER(1..65535),
    noOfRecords                        INTEGER(0..65535),
    records                            SET SIZE(noOfRecords) OF VuOverSpeedingEventRecord
}
```

recordType indique le type de relevé (VuOverSpeedingEventRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuOverSpeedingEventRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique un jeu de relevés d'événements du type excès de vitesse.

2.216. VuPartNumber
Numéro de pièce de l'unité embarquée sur véhicule.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Attribution de valeur: propre au fabricant de la VU.

2.217. VuPlaceDailyWorkPeriodData
Génération 1:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux lieux de début ou de fin des périodes de travail journalières des conducteurs (exigence 087, annexe 1B; exigences 108 et 110, annexe 1C).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
    noOfPlaceRecords                   INTEGER(0..255),
    vuPlaceDailyWorkPeriodRecords      SET SIZE(noOfPlaceRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords indique le nombre des relevés répertoriés dans le jeu vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords indique un jeu de relevés de lieux.

2.218. VuPlaceDailyWorkPeriodRecord
Génération 1:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux lieux de début ou de fin des périodes de travail journalières des conducteurs (exigence 087, annexe 1B; exigences 108 et 110, annexe 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
    fullCardNumber                  FullCardNumber,
    placeRecord                     PlaceRecord
}
```

fullCardNumber indique le type de carte, l'État membre où elle a été délivrée et son numéro.

placeRecord contient les informations relatives au lieu entré.

Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux lieux de début ou de fin des périodes de travail journalières des conducteurs (exigence 087, annexe 1B; exigences 108 et 110, annexe 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
    fullCardNumberAndGeneration     FullCardNumberAndGeneration,
    placeRecord                     PlaceRecord
}
```

La structure de données de génération 2 n'utilise pas fullCardNumber, mais plutôt l'élément suivant:

fullCardNumberAndGeneration indique le type de carte, l'État membre où elle a été délivrée, son numéro et sa génération, tels qu'ils sont enregistrés sur la carte.

2.219. VuPlaceDailyWorkPeriodRecordArray
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux lieux de début ou de fin des périodes de travail journalières des conducteurs (exigence 108 et 110, annexe 1C).

```
VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {
    recordType                      RecordType,
    recordSize                      INTEGER(1..65535),
    noOfRecords                     INTEGER(0..65535),
    records                         SET SIZE(noOfRecords) OF VuPlaceDailyWorkPeriodRecord
}
```

recordType indique le type de relevé (VuPlaceDailyWorkPeriodRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuPlaceDailyWorkPeriodRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique un jeu de relevés de lieux.

2.220. VuPublicKey
Génération 1:

Clé privée d'une unité embarquée sur véhicule.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.221. VuPublicKey

Génération 1:

Clé publique d'une unité embarquée sur véhicule.

VuPublicKey ::= PublicKey

2.222. VuSerialNumber

Numéro de série de l'unité embarquée sur véhicule (exigence 075, annexe 1B; exigence 93, annexe 1C).

VuSerialNumber ::= ExtendedSerialNumber

2.223. VuSoftInstallationDate

Date d'installation de la version du logiciel d'exploitation de l'unité embarquée sur véhicule.

VuSoftInstallationDate ::= TimeReal

Attribution de valeur: Non-spécifié.

2.224. VuSoftwareIdentification

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant au logiciel installé.

```
VuSoftwareIdentification ::= SEQUENCE {
    vuSoftwareVersion                   VuSoftwareVersion,
    vuSoftInstallationDate              VuSoftInstallationDate
}
```

vuSoftwareVersion indique le numéro de la version du logiciel de l'unité embarquée sur véhicule.

vuSoftInstallationDate indique la date d'installation de cette version du logiciel.

2.225. VuSoftwareVersion

Numéro de la version du logiciel de l'unité embarquée sur véhicule.

VuSoftwareVersion ::= IA5String(SIZE(4))

Attribution de valeur: Non-spécifié.

2.226. VuSpecificConditionData

Génération 1:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux conditions particulières.

```
VuSpecificConditionData ::= SEQUENCE {
    NoOfSpecificConditionRecords = INTEGER(0..216-1)
    specificConditionRecords            SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords indique le nombre des relevés répertoriés dans le jeu specificConditionRecords.

specificConditionRecords indique un jeu de relevés relatifs à des conditions particulières.

2.227. VuSpecificConditionRecordArray

Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux conditions particulières (exigence 130, annexe 1C).

```
VuSpecificConditionRecordArray ::= SEQUENCE {
    recordType                          RecordType,
    recordSize                          INTEGER(1..65535),
    noOfRecords                         INTEGER(0..65535),
    records                             SET SIZE(noOfRecords) OF SpecificConditionRecord
}
```

recordType indique le type de relevé (SpecificConditionRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des SpecificConditionRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique un jeu de relevés relatifs à des conditions particulières.

2.228. VuTimeAdjustmentData
Génération 1:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux remises à l'heure exécutées hors du cadre d'un étalonnage complet (exigence 101, annexe 1B).

```
VuTimeAdjustmentData ::= SEQUENCE {
    noOfVuTimeAdjRecords                INTEGER(0..6),
    vuTimeAdjustmentRecords             SET SIZE(noOfVuTimeAdjRecords) OF
                                        VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords indique le nombre des relevés répertoriés dans le jeu vuTimeAdjustmentRecords**.**

vuTimeAdjustmentRecords indique un jeu de relevés de remises à l'heure.

2.229. VuTimeAdjustmentGNSSRecord
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à une remise à l'heure exécutée sur la base des données horaires du GNSS (exigences 124 et 125, annexe 1C).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
    oldTimeValue                        TimeReal,
    newTimeValue                        TimeReal
}
```

oldTimeValue, newTimeValue indiquent les anciennes et nouvelles valeurs accordées à la date et à l'heure.

2.230. VuTimeAdjustmentGNSSRecordArray
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à une remise à l'heure exécutée sur la base des données horaires du GNSS (exigences 124 et 125, annexe 1C).

```
VuTimeAdjustmentGNSSRecordArray ::= SEQUENCE {
    recordType                          RecordType,
    recordSize                          INTEGER(1..65535),
    noOfRecords                         INTEGER(0..65535),
    records                             SET SIZE(noOfRecords) OF VuTimeAdjustmentGNSSRecord
}
```

recordType indique le type de relevé (VuTimeAdjustmentGNSSRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuTimeAdjustmentGNSSRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique un jeu de relevés de remises à l'heure GNSS.

2.231. VuTimeAdjustmentRecord

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux remises à l'heure exécutées hors du cadre d'un étalonnage complet (exigence 101, annexe 1B; exigences 124 et 125, annexe 1C).

Génération 1:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
    oldTimeValue                        TimeReal,
    newTimeValue                        TimeReal,
    workshopName                        Name,
    workshopAddress                     Address,
    workshopCardNumber                  FullCardNumber
}
```

oldTimeValue, newTimeValue indiquent les anciennes et nouvelles valeurs accordées à la date et à l'heure.

workshopName, workshopAddress indiquent les nom et adresse de l'atelier.

workshopCardNumber identifie la carte d'atelier utilisée pour exécuter la remise à l'heure.

Génération 2:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
    oldTimeValue                        TimeReal,
    newTimeValue                        TimeReal,
    workshopName                        Name,
    workshopAddress                     Address,
    fullCardNumberAndGeneration         FullCardNumberAndGeneration,
}
```

La structure de données de génération 2 n'utilise pas workshopCardNumber, mais plutôt l'élément suivant:

workshopCardNumberAndGeneration identifie la carte d'atelier utilisée pour exécuter la remise à l'heure ainsi que sa génération.

2.232. VuTimeAdjustmentRecordArray

Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux remises à l'heure exécutées hors du cadre d'un étalonnage complet (exigences 124 et 125, annexe 1C).

```
VuTimeAdjustmentRecordArray ::= SEQUENCE {
    recordType                          RecordType,
    recordSize                          INTEGER(1..65535),
    noOfRecords                         INTEGER(0..65535),
    records                             SET SIZE(noOfRecords) OF VuTimeAdjustmentRecord
}
```

recordType indique le type de relevé (VuTimeAdjustmentRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuTimeAdjustmentRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique un jeu de relevés de remises à l'heure.

2.233. 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 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 mise en application.

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 susceptible de sauvegarder par type d'événement.

noOfFaultsPerType indique le nombre d'anomalies que la carte est susceptible de sauvegarder par type d'anomalie.

activityStructureLength indique le nombre d'octets susceptibles d'être affectés à l'enregistrement de relevés d'activité.

noOfCardVehicleRecords indique le nombre des relevés de véhicule que la carte est susceptible de mémoriser.

noOfCardPlaceRecords indique le nombre de sites que la carte est susceptible de mémoriser.

noOfCalibrationRecords indique le nombre des relevés d'étalonnage que la carte est susceptible de mémoriser.

Génération 2:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId              EquipmentType,
    cardStructureVersion                CardStructureVersion,
    noOfEventsPerType                   NoOfEventsPerType,
    noOfFaultsPerType                   NoOfFaultsPerType,
    activityStructureLength             CardActivityLengthRange,
    noOfCardVehicleRecords              NoOfCardVehicleRecords,
    noOfCardPlaceRecords                NoOfCardPlaceRecords,
    noOfCalibrationRecords              NoOfCalibrationRecords,
    noOfGNSSCDRecords                   NoOfGNSSCDRecords,
    noOfSpecificConditionRecords        NoOfSpecificConditionRecords
}
```

Outre la génération 1, les éléments de données suivants sont utilisés:

noOfGNSSCDRecords indique le nombre de relevés de conduite continue GNSS que la carte est susceptible de sauvegarder.

noOfSpecificConditionRecords indique le nombre de relevés de conditions particulières que la carte est susceptible de mémoriser.

2.234. WorkshopCardCalibrationData

Informations enregistrées sur une carte d'atelier et se rapportant aux activités d'atelier menées avec cette carte (exigences 314, 316, 337 et 339, annexe 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 exécutés avec la carte.

calibrationPointerNewestRecord indique l'indice du dernier relevé d'étalonnages mis à jour.
Attribution de valeur: nombre correspondant au numérateur du relevé d'étalonnage, commençant par une série de ′0′ pour la première occurrence d'un relevé d'étalonnage dans la structure considérée.

calibrationRecords indique le jeu de relevés contenant des données d'étalonnage et/ou de réglage temporel.

2.235. WorkshopCardCalibrationRecord

Informations enregistrées sur une carte d'atelier et se rapportant à un étalonnage exécuté avec la carte (exigences 314 et 337, annexe 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 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 indique la désignation de la dimension 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 valeurs accordées à la date et à l'heure.

nextCalibrationDate indique la date du prochain étalonnage correspondant au type spécifié dans le champ CalibrationPurpose et auquel l'organisme d'inspection agréé doit procéder.

vuPartNumber, **vuSerialNumber** et **sensorSerialNumber** constituent les éléments d'information nécessaires à l'identification de l'appareil d'enregistrement.

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
}
```

Outre la génération 1, les éléments de données suivants sont utilisés:

sensorGNSSSerialNumber qui identifie un dispositif GNSS externe.

rcmSerialNumber qui identifie un module de communication à distance.

sealDataCard fournit des informations relatives aux scellés liés aux différents composants du véhicule.

2.236. WorkshopCardHolderIdentification

Informations enregistrées sur une carte d'atelier et se rapportant à l'identification du détenteur de la carte (exigence 311 et 334, annexe 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 (p.ex. le nom du mécanicien).

cardHolderPreferredLanguage indique la langue de travail préférentielle du titulaire.

2.237. WorkshopCardPIN

Numéro d'identification individuel de la carte d'atelier (exigences 309 et 332, annexe 1C).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Attribution de valeur: le numéro d'identification individuel connu du détenteur de la carte, complété à droite d'une série d'octets ′FF′ susceptible de compter 8 octets.

2.238. W-VehicleCharacteristicConstant

Coefficient caractéristique du véhicule (définition k).

W-VehicleCharacteristicConstant ::= INTEGER(0..216-1))

Attribution de valeur: Impulsions par kilomètre dans la plage d'exploitation 0 à 64 255 imp/km.

2.239. VuPowerSupplyInterruptionRecord
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux événements du type interruption de l'alimentation électrique (exigence 117, annexe 1C).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
    eventType                           EventFaultType,
    eventRecordPurpose                  EventFaultRecordPurpose,
    eventBeginTime                      TimeReal,
    eventEndTime                        TimeReal,
    cardNumberAndGenDriverSlotBegin     FullCardNumberAndGeneration,
    cardNumberAndGenDriverSlotEnd       FullCardNumberAndGeneration,
    cardNumberAndGenDriverSlotBegin     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 convoyeur ainsi que sa génération, au début de l'événement.

cardNumberAndGenCodriverSlotEnd identifie la carte insérée dans le lecteur réservé au convoyeur ainsi que sa génération, à la fin de l'événement.

similarEventsNumber indique le nombre d'événements similaires survenus le même jour.

2.240. VuPowerSupplyInterruptionRecordArray
Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux événements du type excès de vitesse (exigence 117, annexe 1C).

```
VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {
    recordType                                  RecordType,
    recordSize                                  INTEGER(1..65535),
    noOfRecords                                 INTEGER(0..65535),
    records                                     SET SIZE(noOfRecords) OF VuPowerSupplyInterruptionRecord
}
```

recordType indique le type de relevé (VuPowerSupplyInterruptionRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des VuPowerSupplyInterruptionRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique un jeu de relevés d'événements du type interruptions de l'alimentation électrique.

2.241. VuSensorExternalGNSSCoupledRecordArray
Génération 2:

Jeu de 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 de relevé (SensorExternalGNSSCoupledRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des SensorExternalGNSSCoupledRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records désigne un jeu de relevés couplés au dispositif GNSS externe du capteur.

2.242. VuSensorPairedRecordArray
Génération 2:

Jeu de 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 de relevé (SensorPairedRecord). **Attribution de valeur:** Cf. RecordType

recordSize indique la taille des SensorPairedRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records indique un jeu de relevés d'appariement du capteur.

3. Définitions des plages de valeurs et de dimensions

Définition des variables employées dans les définitions du paragraphe 2.

Plage de temps réelle ::= 2^{32}-1

4. Jeux de caractères

Les chaînes IA5 se composent par définition de caractères ASCII aux termes de la norme ISO/IEC 8824-1. Pour plus de lisibilité et pour faciliter la désignation des caractères, leur assignation de valeur est indiquée ci-après. En cas de divergence, la norme ISO/IEC 8824-1 l'emporte sur cette 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 de caractères décimaux 161 à 255 des jeux de caractères standard à 8 bits suivants, spécifiés par leur numéro de page de code:

Jeu de caractères standard	Code Page (Décimal)
ISO/IEC 8859-1 Latin-1 Européen occidental	1
ISO/IEC 8859-2 Latin-2 Européen central	2
ISO/IEC 8859-3 Latin-3 Européen du sud	3
ISO/IEC 8859-5 Latin/Cyrillique	5
ISO/IEC 8859-7 Latin/Grec	7
ISO/IEC 8859-9 Latin-5 Turc	9
ISO/IEC 8859-13 Latin-7 Balte	13
ISO/IEC 8859-15 Latin-9	15
ISO/IEC 8859-16 Latin-10 Européen du sud-est	16
KOI8-R Latin/Cyrillique	80
KOI8-U Latin/Cyrillique	85

5. Encodage

Si les règles de codage ASN.1 s'appliquent aux différents types de données définis, leur codage doit être conforme à la norme ISO/IEC 8825-2, variante alignée.

6. Identificateurs d'objets et identificateurs d'applications

6.1. Identificateurs d'objets

Les identificateurs d'objets (IDO) répertoriés dans le présent chapitre concernent exclusivement la génération 2. Ces IDO sont spécifiés dans le rapport technique TR-03110-3 et rappelés aux présentes à titre d'exhaustivité. Ces IDO sont contenus dans la sous-arborescence bsi-de:

```
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 VU

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 la VU est exécutée 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 point est 0.4.0.127.0.7.2.2.2.2.4.

	Notation par point	Notation d'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'authentifiation destinés aux circuits
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 devant être exécutée 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 en mode d'exploitation 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 point est 0.4.0.127.0.7.2.2.3.2.2.

	Notation par point	Notation d'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. Identificateur d'application
Génération 2:

L'identificateur d'applications (AID) destiné au dispositif GNSS externe (génération 2) est communiqué par 'FF 44 54 45 47 4D'. Il s'agit d'un AID exclusif conforme à la norme ISO/IEC 7816-4.

Remarque: les 5 derniers octets codent le DTEGM pour le dispositif GNSS externe de tachygraphe intelligent.

L'identificateur d'applications destiné aux applications de cartes tachygraphiques (génération 2) est communiqué par 'FF 53 4D 52 44 54'. Il s'agit d'un AID exclusif conforme à la norme ISO/IEC 7816-4.

FR

APPENDICE 2. SPÉCIFICATION DES CARTES TACHYGRAPHIQUES

Date: 02-02-2016

TABLE DES MATIERES

1. Introduction

1.1. Abréviations

Aux fins du présent appendice, les abréviations utilisées sont les suivantes.

AC	Conditions d'accès
AES	Norme de chiffrement avancé (Advanced Encryption Standard)
AID	Identifiant d'application
ALW	Toujours
APDU	Unité de données de protocole d'application (structure de contrôle)
ATR	Réponse pour remise à zéro
AUT	Authentifié
C6, C7	Contacts numéros 6 et 7 de la carte conformément aux dispositions de la norme ISO/IEC 7816-2
cc	cycles d'horloge (clock cycles)
CHV	Informations de vérification de l'identité des titulaires
CLA	Octet de classe de commande APDU
DSRC	Communication spécialisée à courte portée
DF	Fichier spécialisé. Un DF contient d'autres fichiers (EF ou DF)
ECC	Cryptographie à courbe elliptique
EF	Fichier élémentaire
etu	unité de temps élémentaire
G1	Génération 1
G2	Génération 2
IC	Circuit intégré
ICC	Carte à circuit intégré
ID	Identificateur
IFD	Périphérique d'interface
IFS	Longueur de la zone d'information
IFSC	Longueur de la zone d'information pour la carte
IFSD	Périphérique de longueur de la zone d'information (pour le terminal)
INS	Octet d'instruction d'une commande APDU
Lc	Longueur des données entrantes pour une commande APDU
Le	Longueur des données attendues (données sortantes pour une commande)
MF	Fichier maître (DF racine)
NAD	Adresse du nœud servant au protocole T = 1
NEV	Jamais
P1-P2	Octets de paramètre
PIN	Numéro d'identification personnel
PRO SM	Protégé avec messagerie sécurisée
PTS	Sélection de transmission de protocole
RFU	Réservé à une utilisation ultérieure
RST	Réinitialisation (de la carte)
SFID	Identificateur court de l'EF
SM	Messagerie sécurisée
SW1-SW2	Octets d'état
TS	Caractère ATR initial
VPP	Tension de programmation
VU	Unité embarquée sur le véhicule
XXh	Valeur XX en notation hexadécimale
'**XXh**'	Valeur XX en notation hexadécimale
||	Symbole de concaténation 03||04=0304

1.2. Références

Les références suivantes sont utilisées dans le présent appendice:

ISO/IEC 7816-2	Identification cards - Integrated circuit cards - Part 2: Dimensions and location of the contacts. ISO/IEC 7816-2:2007.
ISO/IEC 7816-3	Identification cards - Integrated circuit cards - Part 3: Electrical interface and transmission protocols. ISO/IEC 7816-3:2006.
ISO/IEC 7816-4	Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange. ISO/IEC 7816-4:2013 + Cor 1: 2014.
ISO/IEC 7816-6	Identification cards - Integrated circuit cards - Part 6: Interindustry data elements for interchange. ISO/IEC 7816-6:2004 + Cor 1: 2006.
ISO/IEC 7816-8	Identification cards - Integrated circuit cards - Part 8: Commands for security operations. ISO/IEC 7816-8:2004.
ISO/IEC 9797-2	Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function. ISO/IEC 9797-2:2011.

2. Caractéristiques électriques et physiques

TCS_01 Tous les signaux électriques doivent respecter la norme ISO/IEC 7816-3 sauf disposition contraire.

TCS_02 L'emplacement et les dimensions des contacts de la carte doivent respecter la norme ISO/IEC 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/IEC 7816-3.

TCS_04 La carte doit fonctionner à Vcc = 3 V (± 0,3 V) ou à Vcc = 5 V (± 0,5 V).

Le choix de la tension doit respecter la norme ISO/IEC 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 IFD quelconque ne sera pas connectée. Si le contact C6 est susceptible d'être connecté à la tension d'alimentation V_{cc} de la carte, il ne peut 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 ainsi qu'à des fréquences supérieures. Au cours d'une même session de carte, la fréquence d'horloge est susceptible de subir des fluctuations de l'ordre de ± 2 %. La fréquence d'horloge est générée par l'unité embarquée sur véhicule et non par la carte considérée. Le coefficient d'utilisation peut varier entre 40 et 60 %.

TCS_07 Il est possible d'interrompre l'horloge externe dans les conditions enregistrées dans le fichier sur carte EF ICC. 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

Inférieur	*Supérieur*		
Bit 3	**Bit 2**	**Bit 1**	
1	0	0	Clockstop autorisé uniquement au niveau inférieur

Les bits 4 à 8 ne sont pas utilisés.

2.4. Contacts d'E/S

TCS_08 Le contact d'E/S C7 autorise la réception et l'émission de données en provenance comme à destination du IFD concerné. En cours d'exploitation, la carte et l'IFD 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. Sauf en émission, la carte passe systématiquement en mode réception.

2.5. États de la carte

TCS_09 La carte fonctionne selon deux états lorsque la tension d'alimentation est appliquée:

État d'exploitation lors de l'exécution de commandes ou en interfaçage avec une unité numérique;
État de repos dans tous les autres cas de figure; dans cet état, la carte doit mémoriser toutes les données utiles.

3. Matériel et communication

3.1. Introduction

Les fonctions minimales requises par les cartes tachygraphiques et les VU pour garantir des conditions d'exploitation et d'interopérabilité satisfaisantes font l'objet d'une description détaillée dans le présent paragraphe.

Les cartes tachygraphiques doivent être aussi conformes que possible aux normes ISO/IEC en vigueur (et à la norme ISO/IEC 7816 en particulier). Toutefois, les commandes et protocoles font l'objet d'une description détaillée afin de fournir, s'il y a lieu, quelques précisions sur certains usages restreints ou certaines différences éventuelles. Sauf indication contraire, les commandes spécifiées sont toutes conformes aux normes dont il est question.

3.2. Protocole de transmission

TCS_10 Le protocole de transmission doit être conforme à la norme ISO/IEC 7816-3 pour T = 0 et T = 1. En particulier, la VU doit être à même de reconnaître les extensions de délai d'attente que lui envoie la carte.

3.2.1 Protocoles

TCS_11 La carte doit être à même de fournir les protocoles **T=0** et **T=1**. De plus, la carte doit 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 indispensable pour adopter le protocole **T=1**.

TCS_13 Les périphériques doivent prendre en charge la **convention directe** que comportent ces deux protocoles. En conséquence, la convention directe est obligatoire pour la carte.

TCS_14 L'ATR doit présenter l'octet **Longueur de la zone d'information pour la carte** au niveau du caractère TA3. Valeur minimale: 'F0h' (= 240 octets).

Les restrictions qui suivent s'appliquent aux protocoles:

TCS_15 **T=0**

- Le périphérique d'interface doit prendre en charge une réponse au niveau de l'E/S après le front montant du signal sur RST à partir de 400 cc.
- Le périphérique d'interface doit être à même de lire des caractères séparés par 12 etu.
- Le périphérique d'interface doit être capable de reconnaître un caractère erroné et sa répétition, même s'ils sont séparés par 13 etu. En cas de détection d'un caractère erroné, le signal d'erreur peut se manifester à l'E/S dans un délai compris entre 1 et 2 etu. Le périphérique doit être en mesure de supporter un retard d'une etu.
- 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 etu. Cette disposition s'applique également au caractère d'accusé de réception 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 (obtenir une réponse) ne peut s'utiliser 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').
- S-block ABORT: inutilisé.
- S-block VPP state error: inutilisé.
- La longueur totale de chaînage associée à une zone de données ne doit pas dépasser 255 octets (pour être garantie par l'IFD).
- L'IFD doit indiquer l'IFSD immédiatement après l'ATR. L'IFD doit émettre la demande de S-Block IFS après l'ATR et la carte doit lui renvoyer le S-Block IFS. Il est recommandé d'accorder la valeur suivante à l'IFSD: 254 octets.
- La carte ne doit pas demander de réajustement de l'IFS.

3.2.2 ATR

TCS_17 Le périphérique procède à un contrôle des octets ATR conformément à la norme ISO/IEC 7816-3. Les caractères historiques de l'ATR ne doivent être soumis à aucune vérification.

Exemple de ATR biprotocole de base conforme à la norme ISO/IEC 7816-3

Character	*Value*	*Remarks*
TS	‘3Bh’	Indicates direct convention.
T0	‘85h’	TD1 present; 5 historical bytes are presents.
TD1	‘80h’	TD2 present; T=0 to be used
TD2	‘11h’	TA3 present; T=1 to be used
TA3	‘XXh’ (at least ‘F0h’)	Information Field Size Card (IFSC)
TH1 to TH5	‘XXh’	Historical characters
TCK	‘XXh’	Check Character (exclusive XOR)

TCS_18 Après la réponse pour remise à zéro (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 le suivant: T=0. Pour sélectionner le protocole T=1, le périphérique doit envoyer à la carte un message de PTS (également désigné par l'abréviation PPS).

TCS_20 Tout comme les protocoles T=0 et T=1, la PTS de base autorisant la permutation des protocoles est également obligatoire pour la carte.

La PTS s'utilise, conformément aux dispositions de la norme ISO/IEC 7816-3, pour passer à des débits binaires supérieurs à celui proposé par défaut, le cas échéant, par la carte au niveau de l'ATR [octet TA(1)].

L'emploi de débits binaires supérieurs est facultatif pour la carte.

TCS_21 Si la carte ne prend en charge que le débit binaire par défaut (ou si le débit binaire sélectionné n'est pas pris en charge), la carte doit répondre correctement à la PTS en omettant l'octet PPS1, conformément à la norme ISO/IEC 7816-3.

Ci-après figure une série d'exemples de PTS de base destinés à la sélection de protocoles:

Character	*Value*	*Remarks*
PPSS	'FFh'	The Initiate Character.
PPS0	'00h' or '01h'	PPS1 to PPS3 are not present; '00h' to select T0, '01h' to select T1.
PK	'XXh'	Check Character: 'XXh' = 'FFh' if PPS0 = '00h', 'XXh' = 'FEh' if PPS0 = '01h'.

3.3. Conditions d'accès

TCS_22 Les conditions d'accès définissent les conditions de sécurité correspondant à un mode d'accès (une commande). Les conditions d'accès doivent être satisfaites pour que la commande soit traitée.

TCS_23 Les conditions d'accès applicables à la carte tachygraphique se définissent comme suit:

Abréviation	*Signification*
ALW	L'action toujours envisageable peut être exécutée sans restriction. La commande et sa réponse APDU sont envoyées en texte clair, sans messagerie sécurisée.
NEV	L'action n'est jamais envisageable.
PLAIN-C	La commande APDU est envoyée en texte clair, 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 de l'authentification de génération 1 (cf. appendice 11 partie A) a réussi.
SM-MAC-G1	L'APDU (commande et réponse) doit être effectuée avec la messagerie sécurisée de génération 1 en mode authentification uniquement (cf. appendice 11 partie A).
SM-C-MAC-G1	L'APDU doit être effectuée avec la messagerie sécurisée de génération 1 en mode authentification uniquement (cf. appendice 11 partie A).
SM-R-ENC-G1	La réponse APDU doit être effectuée avec la messagerie sécurisée de génération 1 en mode chiffrement (cf. appendice 11 partie A), c'est-à-dire sans renvoi de code d'authentification de message.
SM-R-ENC-MAC-	La réponse APDU doit être effectuée avec la messagerie sécurisée de génération 1 en mode chiffrement puis authentification (cf.

Abréviation	*Signification*
G1	appendice 11 partie A).
SM-MAC-G2	L'APDU (commande et réponse) doit être effectuée avec la messagerie sécurisée de génération 2 en mode authentification uniquement (cf. appendice 11 partie B).
SM-C-MAC-G2	La commande APDU doit être effectuée avec la messagerie sécurisée de génération 2 en mode authentification uniquement (cf. appendice 11 partie B).
SM-R-ENC-MAC-G2	La réponse APDU doit être effectuée avec la messagerie sécurisée de génération 2 en mode chiffrement puis authentification (cf. appendice 11 partie B).

TCS_24 Ces conditions de sécurité peuvent être liées selon les manières suivantes:

- **ET**: Toutes les conditions de sécurité doivent être remplies
- **OU**: Au moins l'une des conditions de sécurité doit être remplie

Les conditions d'accès au système de fichiers, à savoir les commandes SELECT, READ BINARY and UPDATE BINARY sont spécifiées au chapitre 4. Les conditions d'accès des autres commandes sont spécifiées dans les tableaux suivants.

TCS_25 Dans l'application DF Tachograph G1, les conditions d'accès suivantes sont appliquées:

Commande	*Carte du conducteur*	*Carte atelier*	*Carte de contrôle*	*Carte d'entreprise*
External Authenticate				
• Pour l'authentification de génération 1	ALW	ALW	ALW	ALW
• Pour l'authentification de génération 2	ALW	**PWD**	ALW	ALW
Internal Authenticate	ALW	**PWD**	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Sans objet	Sans objet	Sans objet	Sans objet
PSO: Compute Digital Signature	ALW OU SM-MAC-G2	ALW OU SM-MAC-G2	Sans objet	Sans objet
PSO: Hash	Sans objet	Sans objet	ALW	Sans objet
PSO: Hash of File	ALW OU SM-MAC-G2	ALW OU SM-MAC-G2	Sans objet	Sans objet

Commande	*Carte du conducteur*	*Carte atelier*	*Carte de contrôle*	*Carte d'entreprise*
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Sans objet	Sans objet	ALW	Sans objet
Verify	Sans objet	ALW	Sans objet	Sans objet

TCS_26 Dans l'application DF Tachograph_G2, les conditions d'accès suivantes sont appliquées:

Commande	*Carte du conducteur*	*Carte atelier*	*Carte de contrôle*	*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	ALW	**PWD**	ALW	ALW
Internal Authenticate	Sans objet	Sans objet	Sans objet	Sans objet
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Sans objet	ALW	ALW	Sans objet
PSO: Compute Digital Signature	ALW OU SM-MAC-G2	ALW OU SM-MAC-G2	Sans objet	Sans objet
PSO: Hash	Sans objet	Sans objet	ALW	Sans objet
PSO: Hash of File	ALW OU SM-MAC-G2	ALW OU SM-MAC-G2	Sans objet	Sans objet
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Sans objet	Sans objet	ALW	Sans objet
Verify	Sans objet	ALW	Sans objet	Sans objet

TCS_27 Dans le MF, les conditions d'accès suivantes sont appliquées:

Commande	*Carte du conducteur*	*Carte atelier*	*Carte de contrôle*	*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	ALW	**PWD**	ALW	ALW
Internal Authenticate	Sans objet	Sans objet	Sans objet	Sans objet
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
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
PSO: Hash of File	Sans objet	Sans objet	Sans objet	Sans objet
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Sans objet	ALW	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 ALW (ou PLAIN-C), la carte peut accepter une commande avec messagerie sécurisée (mode chiffrement et/ou authentification). Si la condition de sécurité exige la messagerie sécurisée avec le mode d'authentification, la carte tachygraphique peut accepter une commande avec messagerie sécurisée de même génération en mode chiffrement et authentification.

Remarque: les descriptions de commande fournissent des informations complémentaires sur leur prise en charge pour les différents types de cartes tachygraphiques et les divers DF.

3.4. Vue d'ensemble des commandes et des codes d'erreur

Les commandes et la structure des fichiers découlent de la norme ISO/IEC 7816-4 et sont conformes à ses dispositions.

Cette section décrit les paires commande-réponse APDU suivantes. Les variantes de commande prises en charge par les applications de génération 1 et 2 sont spécifiées dans les descriptions de commande correspondantes.

Commande	*INS*
SELECT	‘A4h’
READ BINARY	‘B0h’, ‘B1h’
UPDATE BINARY	‘D6h’, ‘D7h’
GET CHALLENGE	‘84h’

Commande	*INS*
VERIFY	‘20h’
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 SW1 et SW2 accompagnent tout message de réponse. Ils indiquent l'état de traitement de la commande correspondante.

SW1	*SW2*	*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 de l'authentification (Avertissement)
63	CX	CHV erronées (PIN). Compteur de tentatives restantes assuré 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

SW1	*SW2*	*Signification*
66	88	Erreur de sécurité: Total de contrôle cryptographique erroné (en cours de 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 prévisible
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 des objets informatifs SM prévus
69	88	Objets informatifs SM incorrects
6A	80	Paramètres incorrects dans les zones de données
6A	82	Fichier introuvable
6A	86	Paramètres P1-P2 erronés
6A	88	Données désignées introuvables
6B	00	Paramètres erronés (déplacement hors de l'EF)
6C	XX	Longueur erronée, le SW2 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

TCS_30 Si plusieurs conditions d'erreurs sont satisfaites dans une commande APDU, 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 11 (Mécanismes de sécurité communs pour les tachygraphes de génération 1 et 2) constitue une source d'informations pertinentes concernant les opérations cryptographiques en jeu.

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 celui-ci demeurent vides.

TCS_31 Si la présence des deux octets de longueur (Lc et Le) est requise, la commande décrite doit être scindée en deux parties si l'IFD emploie le protocole T=0: l'IFD envoie la commande décrite avec P3=Lc + données, puis il envoie une commande GET_RESPONSE (cf. paragraphe **Error! Reference source not found.**) avec P3=Le.

TCS_32 Si la présence des deux octets de longueur est requise et si 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, l'IFD doit envoyer la première commande avec P3=Lc + données, 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, l'IFD doit générer une commande GET RESPONSE avec P3=La pour procéder à la lecture des données.

TCS_33 Une carte tachygraphique peut prendre en charge des zones de longueur étendue conformément à la norme ISO/IEC 7816-4, de manière facultative. Une carte tachygraphique prenant en charge des zones de longueur étendue doit:

- indiquer la prise en charge de la zone de longueur étendue dans l'ATR;
- prévoir les tailles de tampon pris en charge au moyen d'informations de longueur étendue dans l'EF ATR/INFO cf. 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, cf. TCS_147.
- prendre en charge les zones de longueur étendue pour les générations 1 et 2 d'application tachygraphique.

Remarques:
Toutes les commandes sont spécifiées pour les zones de longueur courte. L'utilisation d'APDU de longueur étendue découle clairement de la norme ISO/IEC 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 en appendice 11. Les conditions d'accès à une commande indiquent clairement si la commande prend ou non en charge la messagerie sécurisée et si la commande prend ou non en charge la messagerie sécurisée de génération 1 et/ou 2. Certaines variantes de commandes sont décrites avec la messagerie sécurisée afin d'illustrer l'utilisation de cette dernière.

TCS_34 La VU doit prendre en charge la totalité de la génération 2 de VU: protocole d'authentification mutuelle de la carte pour une session comprenant la vérification du certificat (le cas échéant) soit dans le DF Tachograph, soit dans le DF Tachograph_G2, soit dans le MF.

3.5.1 SELECT

Cette commande est conforme à la norme ISO/IEC 7816-4, mais elle se caractérise par un usage restreint en 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 de fichier présentée

3.5.1.1 Sélection par nom (AID)

Cette commande permet de sélectionner un DF d'application enregistré sur la carte.

TCS_35 Cette commande s'exécute à partir d'un point quelconque de la structure des fichiers (après l'ATR ou à tout moment).

TCS_36 La sélection d'une application réinitialise l'environnement de sécurité actif. Après avoir procédé à la sélection de l'application, aucune clé publique active n'est plus 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 sont perdues.

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**
SW	2	'XXXXh'	Mots d'état (SW1, SW2)

- 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, l'exigence d'une réponse après réception de la commande SELECT entraîne le renvoi de 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**'.

3.5.1.2 Sélection d'un fichier élémentaire au moyen de son identificateur de fichier

TCS_39 **Message de commande**

TCS_40 Une carte tachygraphique doit prendre en charge la génération 2 de messagerie sécurisée comme le précise l'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
P2	1	'0Ch'	Aucune réponse attendue
Lc	1	'02h'	Nombre d'octets envoyé 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*
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

- 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, l'exigence d'une réponse après réception de la commande SELECT entraîne le renvoi de 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**'.

3.5.2 READ BINARY

Cette commande est conforme à la norme ISO/IEC 7816-4, mais elle se caractérise par un usage restreint en comparaison avec 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 intégrant, le cas échéant, dans une structure de messagerie sécurisée.

3.5.2.1 Commande avec déplacement P1-P2.

Cette commande permet à l'IFD de lire les données de l'EF sélectionné sans messagerie sécurisée.

Remarque: cette commande sans messagerie sécurisée ne peut servir qu'à lire un fichier prenant en charge la condition de sécurité ALW en mode Read Access.

TCS_42 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	‘00h’	
INS	1	‘B0h’	Read Binary
P1	1	‘XXh’	Déplacement en octets à compter du début du fichier: octet le plus significatif
P2	1	‘XXh’	Déplacement 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
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

♦ 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 déplacement n'est pas compatible avec la taille de l'EF (déplacement > taille de l'EF), le logiciel renvoie l'état de traitement '**6B00**'.
- Si la taille des données à lire n'est pas compatible avec la taille de l'EF (déplacement + 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**'.
- 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 à l'IFD 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 SM-R-ENC-MAC-G1 (génération 1) ou SM-R-ENC-MAC-G2 (génération 2) est exigée.

TCS_44 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'0Ch'	Messagerie sécurisée demandée
INS	1	'B0h'	Read Binary
P1	1	'XXh'	P1 (déplacement en octets à compter du début du fichier): octet le plus significatif
P2	1	'XXh'	P2 (déplacement en octets à compter du début du fichier): octet le moins significatif
Lc	1	'XXh'	Longueur des données d'entrée pour la messagerie sécurisée
#6	1	'97h'	$T_{LE:}$ balise de spécification de longueur attendue
#7	1	'01h'	L_{LE}: longueur de longueur attendue
#8	1	'NNh'	Spécification de longueur attendue (Le original): nombre d'octets à lire
#9	1	'8Eh'	T_{CC}: balise indiquant le total de contrôle cryptographique
#10	1	'XXh'	L_{CC}: longueur du total de contrôle cryptographique suivant '04h' pour la messagerie sécurisée de génération 1 (cf. appendice 11 partie A) '08h', '0Ch' ou '10h' selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (cf. appendice 11 partie B)
#11-#(10+L)	L	'XX..XXh'	Total de contrôle cryptographique
Le	1	'00h'	Conformément à la norme ISO/IEC 7816-4

TCS_45 **Message de réponse si SM-R-ENC-MAC-G1 (génération 1) / SM-R-ENC-MAC-G2 (génération 2) n'est pas requis et si le format d'entrée de la messagerie sécurisée est correct:**

Octet	*Longueur*	*Valeur*	*Description*
#1	1	'99h'	Balise d'état de traitement (SW1-SW2): facultatif pour la messagerie sécurisée de génération 1
#2	1	'02h'	Longueur de l'état de traitement

Octet	*Longueur*	*Valeur*	*Description*
#3 - #4	2	‘XX XXh’	État de traitement de l'APDU de réponse non protégée
#5	1	‘81h’	TPV: balise indiquant la valeur des données ordinaires
#6	L	‘NNh’ ou ‘81 NNh’	LPV: longueur des données renvoyées (=Le original). L équivaut à 2 octets si LPV > 127 octets
#(6+L)-#(5+L+NN)	NN	‘XX..XXh’	Valeur des données ordinaires
#(6+L+NN)	1	‘8Eh’	TCC: balise indiquant le total de contrôle cryptographique
#(7+L+NN)	1	‘XXh’	LCC: longueur du total de contrôle cryptographique suivant ‘04h’ pour la messagerie sécurisée de génération 1 (cf. appendice 11 partie A) ‘08h’, ‘0Ch’ ou ‘10h’ selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (cf. appendice 11 partie B)
#(8+L+NN)-#(7+M+L+NN)	M	‘XX..XXh’	Total de contrôle cryptographique
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

TCS_46 **Message de réponse si SM-R-ENC-MAC-G1 (génération 1) / SM-R-ENC-MAC-G2 (génération 2) est requis et si le format d'entrée de la messagerie sécurisée est correct:**

Octet	*Longueur*	*Valeur*	*Description*
#1	1	‘87h’	$T_{PI\ CG}$: balise indiquant des données codées (cryptogramme)
#2	L	‘MMh’ ou ‘81 MMh’	$L_{PI\ CG}$: longueur des données chiffrées renvoyées (différentes du Le original de la commande en raison du remplissage). L équivaut à 2 octets si $L_{PI\ CG}$ > 127 octets
#(2+L)-#(1+L+MM)	MM	‘01XX..XXh’	Données codées: cryptogramme et indicateur de remplissage
#(2+L+MM)	1	‘99h’	Balise d'état de traitement (SW1-SW2): facultatif pour la messagerie sécurisée de génération 1
#(3+L+MM)	1	‘02h’	Longueur de l'état de traitement
#(4+L+MM) - #(5+L+MM)	2	‘XX XXh’	État de traitement de l'APDU de réponse non protégée
#(6+L+MM)	1	‘8Eh’	T_{CC}: balise indiquant le total de contrôle cryptographique
#(7+L+MM)	1	‘XXh’	L_{CC}: longueur du total de contrôle cryptographique suivant ‘04h’ pour la messagerie sécurisée de génération 1 (cf. appendice 11 partie A) ‘08h’, ‘0Ch’ ou ‘10h’ selon la longueur de clé AES pour la messagerie sécurisée de génération 2

Octet	*Longueur*	*Valeur*	*Description*
			(cf. appendice 11 partie B)
#(8+L+MM)-#(7+N+L+MM)	N	'XX..XXh'	Total de contrôle cryptographique
SW	2	'XXXXh'	Mots d'état (SW1, SW2)

Il se peut que la commande READ BINARY renvoie des états de traitement normaux listés en TCS_43 sous la balise '99h' comme décrit en TCS_59 en adoptant la structure de réponse de la messagerie sécurisée.

Par ailleurs, certaines erreurs propres à la messagerie sécurisée sont susceptibles de se manifester. Dans ce cas, le logiciel se contente de renvoyer l'état de traitement concerné sans impliquer aucune structure de messagerie sécurisée:

TCS_47 **Message de réponse si le format d'entrée de la messagerie sécurisée est incorrect**

Octet	*Longueur*	*Valeur*	*Description*
SW	2	'XXXXh'	Mots d'état (SW1, SW2)

- 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, l'IFD doit réexécuter le processus d'authentification mutuel approprié pour définir une nouvelle clé de session).
- Si certains objets informatifs attendus (comme précisé 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 informatifs sont incorrects, le logiciel renvoie l'état de traitement '**6988**': cette erreur se produit si toutes les balises requises sont présentes, mais si 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 EF court

Cette variante de commande permet à l'IFD de sélectionner un EF à l'aide d'un identificateur EF court et de lire des données à partir 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 donné. Ces identificateurs EF courts figurent au chapitre 4.

TCS_49 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1			le bit 8 est mis à 1 les bits 7 et 6 sont mis à 00 les bits 5 - 1 codent l'identificateur EF court de l'EF
	1	'XXh'	correspondant
P2			Code un déplacement de 0 à 255 octets dans l'EF référencé par
	1	'XXh'	P1
Le	1	'XXh'	Longueur des données attendue. Nombre d'octets à extraire.

Remarque: les identificateurs EF courts servant à l'application tachygraphique de génération 2 figurent au chapitre 4.

Si P1 code un identificateur EF court et que la commande réussit, 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
SW	2	'XXXXh'	Mots d'état (SW1, SW2)

- Si la commande aboutit, la carte renvoie l'état '**9000**'.
- Si le logiciel ne parvient pas à trouver le fichier correspondant à l'identificateur 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 déplacement n'est pas compatible avec la taille de l'EF (déplacement > taille de l'EF), le logiciel renvoie l'état de traitement '**6B00**'.
- Si la taille des données à lire n'est pas compatible avec la taille de l'EF (déplacement + 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**'.
- 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 à l'IFD d'extraire des données d'un EF contenant 32 768 octets ou davantage.

TCS_51 Une carte tachygraphique prenant en charge les EF dotés de 32 768 octets ou davantage doit prendre en charge cette variante de commande concernant les EF. Une carte tachygraphique peut prendre en charge ou non cette variante de commande pour les autres EF à l'exception de l'EF Sensor_Installation_Data cf. TCS_156 et TCS_160.

TCS_52 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	
INS	1	'B1h'	Read Binary
P1	1	'00h'	
P2	1	'00h'	EF actif
Lc	1	'NNh'	Longueur Lc de l'objet informatif déplacé.
#6-#(5+NN)			Déplacement de l'objet informatif:
			Balise '54h'
		'XX..XXh'	Longueur '01h' ou '02h'
	NN	'	Valeur déplacement
Le	1	'XXh'	Nombre d'octets à extraire.

L'IFD doit coder la longueur de l'objet informatif déplacé sur un minimum d'octets. C'est-à-dire que, à l'aide de l'octet de longueur '01h', l'IFD doit coder un déplacement de 0 à 255 et, à l'aide de l'octet de longueur '02h', un déplacement de '256' jusqu'à '65 535' octets.

TCS_53 **Message de réponse**

Octet	*Longueur*	*Valeur*	*Description*
#1-#L	L	'XX..XXh	Les données extraites sont intégrées dans un objet informatif

Octet	*Longueur*	*Valeur*	*Description*
		’	discrétionnaire avec une balise '53h'.
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

- 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 déplacement n'est pas compatible avec la taille de l'EF (déplacement > 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 (déplacement + 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 ‘**6581**’.
- 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 SM-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’	
P2	1	‘00h’	EF actif
Lc	1	‘XXh’	Longueur de la zone de données sécurisée
#6	1	‘B3h’	Balise indiquant la valeur des données ordinaires codées dans BER-TLV
#7	1	‘NNh’	LPV: longueur des données transmises
#(8)-#(7+NN)	NN	‘XX..XXh’	Données ordinaires codées dans BER-TLV, c'est-à-dire l'objet informatif déplacé doté de la balise '54'
#(8+NN)	1	‘97h’	TLE: balise de spécification de longueur attendue
#(9+NN)	1	‘01h’	LLE: longueur de longueur attendue
#(10+NN)	1	‘XXh’	Spécification de longueur prévisible (Le original): nombre d'octets à extraire
#(11+NN)	1	‘8Eh’	TCC: balise indiquant le total de contrôle cryptographique
#(12+NN)	1	‘XXh’	LCC: longueur du total de contrôle cryptographique suivant ‘08h’, ‘0Ch’ ou ‘10h’ selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (cf. appendice 11 partie B)
#(13+NN)-#(12+M+NN)	M	‘XX..XXh’	Total de contrôle cryptographique
Le	1	‘00h’	Conformément à la norme ISO/IEC 7816-4

TCS_55 Message de réponse si la commande réussit

Octet	*Longueur*	*Valeur*	*Description*
#1	1	‘B3h’	Données ordinaires codées dans BER-TLV
#2			L_{PV}: longueur des données renvoyées (=Le original).
		‘NNh’ ou	
	L	‘81 NNh’	L équivaut à 2 octets si L_{PV} > 127 octets
#(2+L)-#(1+L+NN)			Valeur de données ordinaires codées dans BER-TLV, c'est-à-dire les données extraites intégrées dans un objet informatif discrétionnaire doté de la balise '53h'
	NN	‘XX..XXh’	
#(2+L+NN)			État de traitement de l'APDU de réponse non protégée
	1	‘99h’	
#(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
#(6+L+NN)			T_{CC}: balise indiquant le total de contrôle cryptographique
	1	‘8Eh’	
#(7+L+NN)			L_{CC}: longueur du total de contrôle cryptographique suivant
	1	‘XXh’	‘08h’, ‘0Ch’ ou ‘10h’ selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (cf. appendice 11 partie B)
#(8+L+NN)- #(7+M+L+NN)	M	‘XX..XXh’	Total de contrôle cryptographique
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

3.5.3 UPDATE BINARY

Cette commande est conforme à la norme ISO/IEC 7816-4, mais elle se caractérise par un usage restreint en comparaison avec la commande analogue définie dans cette norme.

Le message de commande UPDATE BINARY lance l'actualisation (effacement + enregistrement) des bits déjà présents dans un EF avec les bits que recèle la commande APDU.

3.5.3.1 Commande avec déplacement P1-P2.

Cette commande permet à l'IFD d'enregistrer des données dans l'EF sélectionné, sans que la carte s'assure de 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 ALW en mode Update Access.

TCS_56 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	‘00h’	
INS	1	‘D6h’	Update Binary
P1	1	‘XXh’	Déplacement en octets à compter du début du fichier: octet le plus significatif
P2	1	‘XXh’	Déplacement en octets à compter du début du fichier: octet le moins significatif

Octet	*Longueur*	*Valeur*	*Description*
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*
SW	2	'XXXXh'	Mots d'état (SW1, SW2)

- 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 déplacement n'est pas compatible avec la taille de l'EF (déplacement > taille de l'EF), le logiciel renvoie l'état de traitement '**6B00**'.
- Si le volume des données à enregistrer est n'est pas compatible avec la taille de l'EF (déplacement + 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 est impossible, le logiciel renvoie l'état de traitement **'6581'**.

3.5.3.1.1 Commande avec messagerie sécurisée (exemples)

Cette commande permet à l'IFD d'enregistrer des données dans l'EF sélectionné, la carte s'assurant de l'intégrité des données reçues. Aucune confidentialité n'étant requise, les données ne sont pas codées.

TCS_58 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'0Ch'	Messagerie sécurisée demandée
INS	1	'D6h'	Update Binary
P1			Déplacement en octets à compter du début du fichier:
	1	'XXh'	octet le plus significatif
P2			Déplacement en octets à compter du début du fichier:
	1	'XXh'	octet le moins significatif
Lc	1	'XXh'	Longueur de la zone de données sécurisée
#6	1	'81h'	T_{PV}: balise indiquant la valeur des données ordinaires
#7	L	'NNh' ou '81 NNh'	L_{PV}: longueur des données transmises L équivaut à 2 octets si L_{PV} > 127 octets
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Valeur des données ordinaires (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

Octet	*Longueur*	*Valeur*	*Description*
			sécurisée de génération 1 (cf. appendice 11 partie A)
			'08h', '0Ch' ou '10h' selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (cf. 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/IEC 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_{SW}: balise indiquant des mots d'état (à protéger par CC)
#2	1	'02h'	L_{SW}: 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			L_{CC}: longueur du total de contrôle cryptographique suivant
			'04h' pour la messagerie sécurisée de génération 1 (cf. appendice 11 partie A)
	1	'XXh'	'08h', '0Ch' ou '10h' selon la longueur de clé AES pour la messagerie sécurisée de génération 2 (cf. appendice 11 partie B)
#7-#(6+L)	L	'XX..XXh'	Total de contrôle cryptographique
SW	2	'XXXXh'	Mots d'état (SW1, SW2)

La structure des messages de réponse décrite plus haut permet de renvoyer les états de traitement «normaux» précisés pour la commande UPDATE BINARY sans messagerie sécurisée (cf. par. 3.5.3.1).

Par ailleurs, certaines erreurs propres à la messagerie sécurisée sont susceptibles de se produire. Dans ce cas, le logiciel se contente de renvoyer l'état de traitement concerné sans impliquer aucune structure de messagerie sécurisée:

TCS_60 **Message de réponse en cas d'erreur affectant la messagerie sécurisée**

Octet	*Longueur*	*Valeur*	*Description*
SW	2	'XXXXh'	Mots d'état (SW1, SW2)

- Si aucune clé de session active n'est disponible, le logiciel renvoie l'état de traitement **'6A88'**.
- Si certains objets informatifs attendus (comme précisé 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 informatifs sont incorrects, le logiciel renvoie l'état de traitement '**6988**': cette erreur se produit si toutes les balises requises sont présentes, mais si 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 EF court

Cette variante de commande permet à l'IFD 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 donné. Ces identificateurs EF courts figurent 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 EF court de l'EF correspondant
P2	1	'XXh'	Code un déplacement de 0 à 255 octets dans l'EF référencé par P1
Lc	1	'NNh'	Longueur Lc des données à actualiser. Nombre d'octets à enregistrer.
#6-#(5+NN)	NN	'XX..XXh'	Données à enregistrer

TCS_63 **Message de réponse**

Octet	*Longueur*	*Valeur*	*Description*
SW	2	'XXXXh'	Mots d'état (SW1, SW2)

Remarque: les identificateurs EF courts servant à l'application tachygraphique de génération 2 figurent au chapitre 4.

Si P1 code un identificateur EF court et que la commande réussit, 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 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 déplacement n'est pas compatible avec la taille de l'EF (déplacement > taille de l'EF), le logiciel renvoie l'état de traitement '**6B00**'.
- Si le volume des données à enregistrer est n'est pas compatible avec la taille de l'EF (déplacement + 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**'.
- Si l'enregistrement est impossible, le logiciel renvoie l'état de traitement **'6581'**.

3.5.3.3 Commande avec octet d'instruction impair

Cette variante de commande permet à l'IFD d'enregistrer des données dans un EF contenant 32 768 octets ou davantage.

TCS_64 Une carte tachygraphique prenant en charge les EF dotés de 32 768 octets ou davantage doit prendre en charge cette variante de commande concernant les EF. Une carte tachygraphique peut prendre en charge ou non cette variante de commande pour d'autres EF.

TCS_65 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	‘00h’	
INS	1	‘D7h’	Update Binary
P1	1	‘00h’	
P2	1	‘00h’	EF actif
Lc	1	‘NNh’	Longueur Lc des données dans la zone de données de la commande
#6-#(5+NN)	NN	‘XX..XXh’	Déplacement de l'objet informatif doté de la balise '54h' || Objet informatif discrétionnaire doté de la balise '53h' qui intègre les données à enregistrer

L'IFD doit coder la longueur de l'objet informatif déplacé et de l'objet informatif discrétionnaire sur un minimum d'octets. C'est-à-dire que, à l'aide de l'octet de longueur '01h', l'IFD doit coder un déplacement/une longueur de 0 à 255 et, à l'aide de l'octet de longueur '02h', un déplacement/une longueur de '256' jusqu'à '65 535' octets.

TCS_66 **Message de réponse**

Octet	*Longueur*	*Valeur*	*Description*
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

- 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 déplacement n'est pas compatible avec la taille de l'EF (déplacement > taille de l'EF), le logiciel renvoie l'état de traitement ‘**6B00**’.
- Si le volume des données à enregistrer est n'est pas compatible avec la taille de l'EF (déplacement + 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 est impossible, 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 SM-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’	
P2	1	‘00h’	EF actif
Lc	1	‘XXh’	Longueur de la zone de données sécurisée
#6	1	‘B3h’	Balise indiquant la valeur des données ordinaires codées dans BER-TLV
#7	L	‘NNh’ ou ‘81 NNh’	L_{PV}: longueur des données transmises L équivaut à 2 octets si L_{PV} > 127 octets
#(7+L)-#(6+L+NN)	NN	‘XX..XXh’	Données ordinaires codées dans BER-TLV, c.-à-d. le déplacement de l'objet informatif doté de la balise '54h' || Objet informatif discrétionnaire doté de la balise '53h' qui intègre les données à enregistrer

Octet	*Longueur*	*Valeur*	*Description*
#(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 (cf. 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/IEC 7816-4

TCS_68 Message de réponse si la commande réussit

Octet	*Longueur*	*Valeur*	*Description*
#1	1	‘99h’	T_{SW}: balise indiquant des mots d'état (à protéger par CC)
#2	1	‘02h’	L_{SW}: 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 (cf. appendice 11 partie B)
#7-#(6+L)	L	‘XX..XXh’	Total de contrôle cryptographique
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

3.5.4 GET CHALLENGE

Cette commande est conforme à la norme ISO/IEC 7816-4, mais elle se caractérise par un usage restreint en comparaison avec la commande analogue définie dans cette norme.

La commande GET CHALLENGE (obtenir un challenge) demande à la carte d'émettre un challenge afin de l'utiliser dans le cadre d'une procédure liée à la sécurité et comportant l'envoi d'un cryptogramme ou de données chiffrées à la carte.

TCS_69 Le challenge émis par la carte n'est valable que pour la commande suivante (laquelle a recours à un challenge) 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 du challenge attendu)

TCS_71 **Message de réponse**

Octet	*Longueur*	*Valeur*	*Description*
#1-#8	8	‘XX..XXh’	Challenge
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

- 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

Cette commande est conforme à la norme ISO/IEC 7816-4, mais elle se caractérise par un usage restreint en comparaison avec la commande analogue définie dans cette norme.

Seule la carte d'atelier doit prendre en charge cette commande.

D'autres types de cartes tachygraphiques peuvent déclencher ou non cette commande, mais pour ces cartes aucune référence CHV n'est personnalisée. Par conséquent, ces cartes ne peuvent pas exécuter cette commande. Pour d'autres types de cartes tachygraphiques que les cartes d'atelier, le comportement, c'est-à-dire le code d'erreur renvoyé, sort du champ de la présente spécification, si cette commande est envoyée.

La commande VERIFY lance, au niveau de la carte, la comparaison entre les données CHV (PIN) envoyées et les données CHV de référence enregistrées dans la mémoire de la carte.

TCS_72 Le PIN renseigné par l'utilisateur doit être codé en code ASCII et complété à droite d'une série d'octets 'FFh' jusqu'à atteindre une longueur de 8 octets, par l'IFD; cf. le type de données WorkshopCardPIN en appendice 1.

TCS_73 Les applications tachygraphiques de génération 1 et 2 doivent utiliser la même référence CHV.

TCS_74 La carte tachygraphique doit contrôler si la commande est correctement codée. Si la commande n'est pas correctement codée, la carte ne doit pas comparer les valeurs CHV, ni décrémenter le compteur CHV de tentatives restantes, ni réinitialiser l'état de sécurité «PIN_Verified». Elle doit abandonner la commande. Une commande est correctement codée si les octets CLA, INS, P1, P2, Lc ont les valeurs spécifiées, Le est absent et la zone de données de la commande a la longueur adéquate.

TCS_75 Si la commande aboutit, le compteur de tentatives CHV restantes est réinitialisé. La valeur initiale du compteur de tentatives CHV restantes est de 5. Si la commande aboutit, la carte définit l'état de sécurité interne «PIN_Verified». La carte réinitialise cet état de sécurité si la carte est réinitialisée ou si le code CHV transmis par la commande ne correspond pas à la CHV de référence stockée.

Remarque: utiliser la même CHV de référence et un état de sécurité global évite à un employé d'atelier de devoir renseigner à nouveau le PIN après avoir sélectionné un autre DF d'application tachygraphique.

TCS_76 La carte enregistre l'échec d'une comparaison, c'est-à-dire que le compteur de tentatives CHV restantes doit être décrémenté d'une unité afin de restreindre le nombre de nouvelles tentatives d'utilisation de la CHV 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 (la CHV vérifiée est implicitement connue)
Lc	1	‘08h’	Longueur du code CHV transmis
#6-#13	8	‘XX..XXh’	CHV

TCS_78 **Message de réponse**

Octet	*Longueur*	*Valeur*	*Description*
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

-
- Si la commande aboutit, la carte renvoie l'état '**9000**'.
- Si les CHV de référence sont introuvables, le logiciel renvoie l'état de traitement **‘6A88’**.
- Si les CHV sont bloquées (le compteur de tentatives CHV restantes est nul), le logiciel renvoie l'état de traitement **‘6983’**. Une fois dans cet état, les CHV 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 CHV restantes).
- Si les CHV 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

Cette commande est conforme à la norme ISO/IEC 7816-4.

Cette commande (indispensable et exclusivement disponible pour le protocole T=0) permet d'assurer la transmission de données préparées entre la carte et le périphérique d'interface (cas où une commande aurait inclus les deux octets Lc et Le).

La commande GET RESPONSE doit être émise immédiatement après la commande de préparation des données, sinon la perte de ces dernières est inévitable. Après exécution de la commande GET RESPONSE (sauf si l'erreur ‘**61xx**’ ou ‘**6Cxx**’ s'est produite, cf. ci-après), les données préalablement préparées 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
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

- 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 pour 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 elle 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

Cette commande est conforme à la norme ISO/IEC 7816-8, mais elle se caractérise par un usage restreint en comparaison avec la commande analogue définie dans cette norme.

La carte utilise la commande VERIFY CERTIFICATE pour obtenir une clé publique venant 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 mémorisée dans l'environnement de sécurité aux fins d'utilisation ultérieure. 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 (cf. paragraphe 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.

TCS_84 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'00h'	
INS	1	'2Ah'	Exécution d'une opération de sécurité
P1	1	'00h'	P1
P2	1	'AEh'	P2: données codées non BER-TLV (concaténation d'éléments de données)
Lc	1	'C2h'	Lc: longueur du certificat, 194 octets
#6-#199	194	'XX..XXh'	Certificat: concaténation des éléments de données (décrits en appendice 11)

TCS_85 **Message de réponse**

Octet	*Longueur*	*Valeur*	*Description*
SW	2	'XXXXh'	Mots d'état (SW1, SW2)

- 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 fait l'objet d'une description détaillée à l'appendice 11 pour G1 et G2.
- 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'**.
- Uniquement pour la génération 1: si la clé publique sélectionnée (utilisée pour dévoiler le certificat) a un CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) différent de ′00′ (donc n'est pas celle d'un État membre ni de l'Europe), 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 pas être transmis dans une seule APDU. Dans ce cas, le chaînage de commande conformément à la norme ISO/IEC 7816-4 doit s'appliquer. Le certificat doit être transmis en deux PSO successifs. Vérifier l'APDU du certificat.

La structure du certificat et les paramètres de domaine sont définis à l'appendice 11.

TCS_86 La commande est exécutable dans le MF, DF Tachograph et DF Tachograph_G2, cf. TCS_33.

TCS_87 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*
CLA			L'octet CLA indique un chaînage de commandes:
			'00h" unique ou dernière commande de la chaîne
	1	'X0h'	'10h' pas la dernière commande d'une chaîne
INS	1	'2Ah'	Exécution d'une opération de sécurité
P1	1	'00h'	
P2	1	'BEh'	Vérifier le certificat autodescriptif
Lc			Longueur de la zone de données de commande, cf. TCS_88 et
	1	'XXh'	TCS_89.
#6-#5+L			Données codées DER-TLV: l'objet informatif Corps du certificat ECC désigne le premier objet informatif concaténé et l'objet informatif Signature du certificat ECC désigne le deuxième objet informatif ou une partie de cette concaténation. La balise '7F21' et
		'XX..XXh	la longueur correspondante ne doivent pas être transmises.
	L	'	L'ordre de ces objets informatifs est fixe.

TCS_88 Pour les APDU courtes, les dispositions suivantes s'appliquent: l'IFD doit utiliser le moins d'APDU possible pour transmettre la charge 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 d'informations, cf. TCS_14. Si l'IFD a un autre comportement, celui de la carte sort du périmètre.

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. L'IFD doit utiliser le moins d'APDU possible pour transmettre la charge de la commande et transmettre le maximum d'octets dans la première APDU de commande. Si l'IFD adopte un autre comportement, celui de la carte sort du périmètre.

Remarque: l'appendice 11 prévoit que la carte stocke le certificat ou les contenus pertinents du certificat et actualise son currentAuthenticatedTime.

La structure de message de réponse et les mots d'état figurent en TCS_85.

TCS_90 Outre les codes d'erreurs listés en TCS_85, la carte peut également renvoyer les codes d'erreur suivants:

- Si la clé publique sélectionnée (utilisée pour dévoiler le certificat) possède un CHA.LSB (CertificateHolderAuthorisation.equipmentType) inadapté à la vérification du certificat telle que prévue par l'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**' (également utilisé dans le cas où les objets informatifs ne sont pas envoyés dans l'ordre spécifié).

3.5.8 INTERNAL AUTHENTICATE

Cette commande est conforme à la norme ISO/IEC 7816-4.

TCS_91 Toutes les cartes tachygraphiques doivent prendre en charge cette commande dans le DF Tachograph de génération 1. La commande peut ou non être accessible dans le MF et/ou le DF Tachograph_G2. 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 à l'IFD d'authentifier la carte. Le processus d'authentification fait l'objet d'une description détaillée à l'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 plus de détails, reportez-vous à l'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’	Challenge utilisé pour authentifier la carte
#14 -#21	8	‘XX..XXh’	VU.CHR (cf. appendice 11)
Le	1	‘80h’	Longueur des données attendue en provenance de la carte

TCS_94 **Message de réponse**

Octet	*Longueur*	*Valeur*	*Description*
#1-#128	128	‘XX..XXh’	Jeton d'authentification de carte (cf. appendice 11)
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

- 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 la VU.CHR 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 active, pour autant qu'elle existe, est effacée et cesse d'être disponible. Pour disposer d'une nouvelle clé de session, il convient d'exécuter avec succès la commande EXTERNAL AUTHENTICATE pour le mécanisme d'authentification de génération 1.

3.5.9 EXTERNAL AUTHENTICATE

Cette commande est conforme à la norme ISO/IEC 7816-4.

La commande EXTERNAL AUTHENTICATE (authentification externe) permet à la carte d'authentifier l'IFD. Le processus d'authentification fait l'objet d'une description détaillée à l'appendice 11 pour le tachygraphe G1 et G2 (authentification VU).

TCS_96 La variante de la commande pour le 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 pour l'authentification mutuelle de la carte VU de deuxième génération est exécutable dans le MF, DF Tachograph et DF Tachograph_G2, cf. TCS_34.

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)			Authentification de génération 1: cryptogramme (cf. appendice 11 partie A)
	L	‘XX..XXh’	Authentification de génération 2: signature générée par l'IFD (cf. appendice 11 partie B)

TCS_99 **Message de réponse**

Octet	*Longueur*	*Valeur*	*Description*
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

- Si la commande aboutit, la carte renvoie l'état '**9000**'.
- Si le CHA de la clé publique active n'est pas la concaténation de l'AID de l'application tachygraphique et d'un type d'équipement VU, 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 pour l'authentification de génération 2 peut également renvoyer les codes d'erreurs suivants:
- Si la vérification de signature échoue, la carte renvoie ‘**6300**’.

3.5.10 GENERAL AUTHENTICATE

Cette commande sert au protocole d'authentification du circuit intégré de génération 2 défini dans l'appendice 11 partie B conformément à la norme ISO/IEC 7816-4.

TCS_100 La commande est exécutable dans le MF, DF Tachograph et DF Tachograph_G2, cf. 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 ultérieure
#6-#(5+L)	L	‘7Ch’ + L_{7C} + ‘80h’ + L_{80} +	Valeur de la clé publique éphémère et codée DER-TLV (cf. appendice 11)

Octet	*Longueur*	*Valeur*	*Description*
		'XX..XXh'	La VU doit envoyer les objets informatifs dans cet ordre.

TCS_102 **Message de réponse**

Octet	*Longueur*	*Valeur*	*Description*
#1-#L		'7Ch' + L_{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L_{82} +	Données d'authentification dynamique codées DER-TLV: jeton 'nonce' et d'authentification (cf. appendice 11)
	L	'XX..XXh'	
SW	2	'XXXXh'	Mots d'état (SW1, SW2)

- 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 informatif 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**'; et
- 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

Cette commande permet de définir une clé publique aux fins d'authentification.

3.5.11.1 Commande de génération 1: paire de réponses

Cette commande est conforme à la norme ISO/IEC 7816-4. Son usage est restreint relativement à 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 suivante MSE correcte ou 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 mentionnée valable pour l'ensemble des opérations cryptographiques
P2	1	'B6h'	P2 (données mentionnées concernant la signature numérique)
Lc	1	'0Ah'	Lc: longueur de la zone de données ultérieure
#6	1	'83h'	Balise indiquant une clé publique en cas d'asymétrie
#7	1	'08h'	Longueur de la référence (identificateur de clé)
#8-#15	8	'XX..XXh'	Identificateur de clé conforme aux dispositions énoncées à l'appendice 11

TCS_107 **Message de réponse**

Octet	Longueur	Valeur	Description
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

- Si la commande aboutit, la carte renvoie l'état '**9000**'.
- Si la clé mentionnée n'est pas présente dans la mémoire de la carte, le logiciel renvoie l'état de traitement **‘6A88’**.
- S'il manque certains objets informatifs 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 informatifs 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 la MSE suivante: versions de commande définies et conformes à la norme ISO/IEC 7816-4. Ces versions de commande ne sont pas prises en charge pour l'authentification de génération 1.

3.5.11.2.1 Authentification de circuit MSE:SET AT

La commande MSE:SET AT suivante sert à sélectionner les paramètres d'authentification du circuit effectuée par une commande ultérieure d'authentification générale.

TCS_108 La commande est exécutable dans le MF, DF Tachograph et DF Tachograph_G2, cf. TCS_34.

TCS_109 **Message de commande MSE SET:AT pour authentifier un circuit**

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 ultérieure
#6-#(5+L)			Référence de mécanisme cryptographique codé DER-TLV: identificateur d'objet pour l'authentification de circuit (valeur uniquement, balise '06h' absente).
			Cf. appendice 1 pour les valeurs des identificateurs d'objets; utiliser la notation en octets. Cf. appendice 11 pour les instructions relatives à la sélection de l'un des identificateurs d'objet.
	L	’80h’ + ‘0Ah’ + ‘XX..XXh’	

3.5.11.2.2 Authentification de VU MSE:SET AT

La commande MSE:SET AT suivante sert à sélectionner les paramètres et les clés de l'authentification de la VU effectuée par une commande ultérieure External Authenticate.

TCS_110 La commande est exécutable dans le MF, DF Tachograph et DF Tachograph_G2, cf. TCS_34.

TCS_111 **Message de commande MSE:SET AT pour authentifier une VU**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Définit l'authentification externe
P2	1	‘A4h’	Authentification
Lc	1	‘NNh’	Lc: longueur de la zone de données ultérieure
#6-#(5+L)			Référence de mécanisme cryptographique codé DER-TLV: identificateur d'objet pour l'authentification de VU (valeur uniquement, balise '06h' absente).
		’80h’ + ‘0Ah’ + ‘XX..XXh’	Cf. appendice 1 pour les valeurs des identificateurs d'objets; utiliser la notation en octets. Cf. appendice 11 pour les instructions relatives à la sélection de l'un des identificateurs d'objet.
		‘83h’ + ‘08h’ + ‘XX..XXh’	Référence codée DER-TLV de la clé publique de la VU par la Référence du titulaire de certificat mentionnée dans son certificat.
	L	‘91h’ + L_{91} + ‘XX..XXh’	Représentation comprimée et codée DER-TLV de la clé publique éphémère de la VU qui servira lors de l'authentification du circuit (cf. appendice 11)

3.5.11.2.3 MSE:SET DST

La commande MSE:SET DST suivante sert à définir une clé publique, soit

- en vue de vérifier une signature fournie dans un PSO ultérieur: commande Verify Digital Signature, soit
- en vue de vérifier une signature ou un certificat fourni dans un PSO ultérieur: commande Verify Certificate.

TCS_112 La commande est exécutable dans le MF, DF Tachograph et DF Tachograph_G2, cf. 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 vérification
P2	1	‘B6h’	Signature numérique
Lc	1	‘NNh’	Lc: longueur de la zone de données ultérieure
#6-#(5+L)			Référence codée DER-TLV d'une clé publique, c'est-à-dire la référence du titulaire de certificat dans le certificat de la clé publique (cf. appendice 11)
		’83h’ + ‘08h’	
	L	+ ‘XX...XXh’	

Pour toutes les versions de commande, la structure du message de réponse et les mots d'état proviennent:

TCS_114 **Message de réponse**

Octet	Longueur	Valeur	Description
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

- Si la commande aboutit, la carte renvoie l'état '**9000**'. Le protocole a été sélectionné et initialisé.
- **‘6A80’** indique des paramètres incorrects dans les zones de données de la commande.
- **‘6A88’** indique que les données de référence (p. ex. une clé mentionnée) ne sont pas disponibles.

3.5.12 PSO: HASH

Cette commande permet de transférer vers la carte le résultat du calcul de hachage auquel certaines données pourraient être soumises. Cette commande s'emploie lors de la vérification de signatures numériques. La valeur de hachage est enregistrée temporairement en vue d'une commande PSO ultérieure: Verify Digital Signature.

Cette commande est conforme à la norme ISO/IEC 7816-8. Son usage est restreint relativement à la norme en question. Seule la carte de contrôle doit prendre en charge cette commande dans le DF Tachograph et 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.

L'application de la carte de contrôle 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
P1	1	‘90h’	Renvoie d'un code de hachage
P2	1	‘A0h’	Balise: zone de données contenant les DO appropriés 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 (cf. appendice 11 partie A) ‘20h’, ‘30h’ ou ‘40h’ pour l'application de génération 2 (cf. appendice 11 partie B)
#8-#(7+L)	L	‘XX..XXh’	Code de hachage

TCS_117 **Message de réponse**

Octet	*Longueur*	*Valeur*	*Description*
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

- Si la commande aboutit, la carte renvoie l'état '**9000**'.
- S'il manque certains objets informatifs attendus (comme précisé 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 informatifs sont incorrects, le logiciel renvoie l'état de traitement **‘6988’**. Cette erreur survient si la balise requise est présente mais d'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

Cette commande n'est pas conforme à la norme ISO/IEC 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 exécuter cette commande. Si une carte d'entreprise ou de contrôle exécute cette commande, la commande doit être exécutée conformément aux dispositions du présent chapitre.

La commande peut ou non être accessible dans le MF. Dans ce cas, la commande doit être exécutée comme le prévoit le présent chapitre, à savoir sans autoriser le calcul d'une valeur de hachage, mais avec abandon et communication d'un code d'erreur approprié.

TCS_118 La commande PERFORM HASH of FILE s'utilise 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 listés au chapitre 4 sous les DF_Tachograph et DF_Tachograph_G2 et en tenant compte des exceptions suivantes. Une carte tachygraphique ne doit pas prendre en charge la 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. Par la suite, son utilisation permettra d'obtenir une signature numérique du fichier en recourant à 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: 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 SHA-1 et SHA-2 (256, 384 et 512 bits).

TCS_124 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	‘80h’	CLA
INS	1	‘2Ah’	Exécution d'une opération de sécurité
P1	1	‘90h’	Balise: Hash
P2			P2: indique l'algorithme à utiliser pour le hachage des données du fichier transparent sélectionné:
			‘00h’ pour SHA-1
			‘01h’ pour SHA-256
			‘02h’ pour SHA-384
	1	‘XXh’	‘03h’ pour SHA-512

TCS_125 **Message de réponse**

Octet	Longueur	Valeur	Description
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

- Si la commande aboutit, la carte renvoie l'état '**9000**'.
- Si l'EF actif n'autorise 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

Cette commande permet de calculer la signature numérique du code de hachage préalablement calculé (cf. commande PERFORM HASH of FILE, paragraphe 3.5.13).

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 d'aucune clé de signature. Par conséquent, ces cartes ne peuvent pas exécuter cette commande mais l'abandonnent avec un code d'erreur approprié.

La commande peut ou non être accessible dans le MF. Dans ce cas, la commande est abandonnée avec un code d'erreur approprié.

Cette commande est conforme à la norme ISO/IEC 7816-8. Son usage est restreint relativement à 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 sert à calculer la signature numérique et est implicitement connue de la carte.

TCS_128 L'application tachygraphique de génération 1 exécute une signature numérique à l'aide d'une méthode de remplissage conforme avec la norme PKCS1 (cf. appendice 11 pour toute information complémentaire).

TCS_129 L'application tachygraphique de génération 2 calcule une signature numérique basée sur une courbe elliptique (cf. appendice 11 pour toute information complémentaire).

TCS_130 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Exécution d'une opération de sécurité
P1	1	‘9Eh’	Signature numérique à renvoyer
P2			Balise: zone de données contenant les données à signer. Comme aucune zone de données n'est incluse, les données sont supposées
	1	‘9Ah’	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 du hachage préalablement calculé
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

- 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

Cette commande sert à vérifier la signature numérique fournie en entrée, dont la carte connaît le hachage. La carte connaît implicitement l'algorithme de signature.

Cette commande est conforme à la norme ISO/IEC 7816-8. Son usage est restreint relativement à la norme en question.

Seule la carte de contrôle doit prendre en charge cette commande dans le DF Tachograph et 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 à l'aide de la précédente commande MANAGE SECURITY ENVIRONMENT MSE: Set DST et du code de hachage antérieur introduit à l'aide 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
P1	1	‘00h’	
P2	1	‘A8h’	Balise: zone de données contenant les DO pertinents pour la vérification
Lc	1	‘83h’	Longueur Lc de la zone de données suivante
6	1	‘9Eh’	Balise indiquant une signature numérique
#7-#8			Longueur de la signature numérique:
			128 octets codés conformément à l'appendice 11 partie A pour l'application tachygraphique de génération 1;
	2	‘81 XXh’	selon la courbe retenue pour l'application tachygraphique de génération 2 (cf. appendice 11 partie B).
#9-#(8+L)	L	‘XX..XXh’	Contenu de la signature numérique

TCS_134 **Message de réponse**

Octet	*Longueur*	*Valeur*	*Description*
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

- 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 figure en appendice 11.
- Si aucune clé publique n'est sélectionnée, le logiciel renvoie l'état de traitement **‘6A88’**.
- S'il manque certains objets informatifs attendus (comme précisé 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 informatifs 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 informatifs requis est incorrecte.
- Si la clé publique sélectionnée est considérée comme altérée, le logiciel renvoie l'état de traitement **‘6400’** ou **‘6581’**.

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 VU et adressées à une autorité de contrôle ou un atelier au moyen d'un lien DSRC. Cette carte extrait la clé de cryptage et la clé MAC servant à sécuriser le message DSRC comme le décrit l'appendice 11 partie B chapitre 13.

Seules les cartes de contrôle et d'atelier doivent prendre en charge cette commande dans le DF Tachograph_G2.

D'autres types de cartes tachygraphiques peuvent ou non mettre en œuvre cette commande, mais ne disposent d'aucune clé maîtresse DSRC. Par conséquent, ces cartes ne peuvent pas exécuter cette commande, mais l'abandonnent avec un code d'erreur approprié.

La commande peut ou non être accessible dans le MF et/ou le DF Tachograph. Dans ce cas, la commande est abandonnée avec un code d'erreur approprié.

TCS_135 La clé maîtresse DSRC est accessible uniquement dans le DF Tachograph_G2, c'est-à-dire que la carte de contrôle et d'atelier doivent prendre en charge l'exécution de la commande uniquement dans le DF Tachograph_G2.

TCS_136 La commande doit uniquement décrypter les données DSRC et vérifier le total de contrôle cryptographique, mais sans interpréter les données d'entrée.

TCS_137 L'ordre des objets informatifs dans la zone de données de la commande est défini par cette spécification.

TCS_138 **Message de commande**

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	‘80h’	CLA propriétaire
INS	1	‘2Ah’	Exécution d'une opération de sécurité
P1	1	‘80h’	Données de réponse: valeur ordinaire
P2	1	‘B0h’	Données de la commande: valeur ordinaire codée BER-TLV et incluant des SM-DO
Lc	1	‘NNh’	Longueur Lc de la zone de données suivante
#6-#(5+L)	L	‘87h’ + L87 + ‘XX..XXh’	Indicateur de contenu de remplissage codé DER-TLV suivi d'une charge tachygraphique codée. Pour l'octet de l'indicateur de contenu de remplissage, il est impératif d'utiliser la valeur '00h' ('aucune autre information' conformément à la norme ISO/IEC 7816-4:2013 Tableau 52). Concernant le mécanisme de cryptage, cf. appendice 11 partie B chapitre 13. Les valeurs autorisées pour la longueur L87 sont les multiples de la longueur du bloc AES plus 1 pour l'octet indicateur du contenu de remplissage, soit entre 17 octets et 193 octets inclus. Remarque: cf. ISO/IEC 7816-4:2013 Tableau 49 pour l'objet informatif de la SM doté de la balise ‘87h’.
		‘81h’ + ‘10h’	Gabarit de référence et de contrôle de la confidentialité codé DER-TLV destiné à héberger la concaténation des éléments de données suivants (cf. appendice 1 DSRCSecurityData et appendice 11 partie B chapitre 13). timbre horodateur sur 4 octets; compteur sur 3 octets; numéro de série de la VU sur 8 octets; version de la clé maîtresse DSRC sur 1 octet. Remarque: cf. ISO/IEC 7816-4:2013 Tableau 49 pour l'objet informatif de la SM doté de la balise ‘81h’.
		‘8Eh’ + L8E + ‘XX..XXh’	MAC codé DER-TLV sur le message DSRC. Pour l'algorithme et le calcul des MAC, cf. appendice 11 partie B chapitre 13.

Octet	*Longueur*	*Valeur*	*Description*
			Remarque: cf. ISO/IEC 7816-4:2013 Tableau 49 pour l'objet informatif de la SM doté de la balise ‘8Eh’.

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)
SW	2	‘XXXXh’	Mots d'état (SW1, SW2)

- Si la commande aboutit, la carte renvoie l'état '**9000**'.
- **‘6A80’** indique si des paramètres incorrects sont envoyés dans la zone de données de la commande (également utilisé dans le cas où les objets informatifs ne sont pas envoyés dans l'ordre spécifié).
- **‘6A88’** indique que les données de référence (p.ex. la clé maîtresse DSRC mentionnée) ne sont pas disponibles.
- **‘6900’** indique l'échec de la vérification du total de contrôle cryptographique ou du décryptage des données.

4. Structure des cartes tachygraphiques

Le présent paragraphe définit les structures de fichiers des cartes tachygraphiques en vue du stockage des données accessibles.

Il n'apporte aucune précision quant à leur structure interne, laquelle dépend du fabricant (en-têtes de fichier par exemple). Il n'aborde pas non plus l'archivage et le traitement d'éléments de données à usage interne tels que les `EuropeanPublicKey`, `CardPrivateKey, TDesSessionKey` ou `WorkshopCardPin`.

TCS_140 Une carte tachygraphique de génération 2 doit héberger le fichier maître (MF) et deux applications tachygraphiques de génération 1 et de génération 2 de type identique (p. ex. des applications de cartes de conducteur).

TCS_141 Une carte tachygraphique doit prendre en charge au moins 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 les applications correspondantes.

Les nombres minimum et maximum d'enregistrements sont définis au présent chapitre pour les différentes applications. Pour les conditions de sécurité servant aux conditions d'accès dans le présent chapitre, consulter le chapitre 3.3. En règle générale, le mode d'accès «read» indique la commande READ BINARY avec les octets pairs et le cas échéant les octets impairs INS à l'exception de l'EF Sensor_Installation_Data de la carte d'atelier, cf. TCS_156 et TCS_160. Le mode d'accès «update» indique la commande Update Binary avec les octets pairs et le cas échéant les octets impairs INS ainsi que le mode d'accès «select» et la commande SELECT.

4.1. Fichier Maître (MF)

TCS_142 Après personnalisation, le fichier maître MF doit avoir la structure de fichier et les conditions d'accès au fichier permanentes suivantes:

Remarque: l'identificateur d'EF court SFID est communiqué sous la forme d'un nombre décimal, p. ex. la valeur 30 correspond au nombre binaire 11110.

				Conditions d'accès	
Fichier		**ID de fichier**	**SFID**	**Lire/Sélectionner**	**Actualiser**
MF		‘3F00h’			
E	ICC	‘0002h’		ALW	NEV
E	IC	‘0005h’		ALW	NEV
E	DIR	‘2F00h’	30	ALW	NEV
E	ATR/INFO (conditionnel)	‘2F01h’	29	ALW	NEV

				Conditions d'accès	
E					
E	Extended_Length (conditional)	‘0006h’	28	ALW	NEV
D	Tachograph	‘0500h’		SC1	
D	Tachograph_G2			SC1	

Dans ce tableau, est utilisée l'abréviation suivante pour la condition de sécurité:
SC1 ALW OU SM-MAC-G2

TCS_143 La structure de tous les EF doit être transparente.

TCS_144 Le fichier maître MF doit avoir la structure de données suivante:

File / Data element	**No of Records**	**Size (bytes) Min.**	**Max.**	**Default Values**
MF	*6*		*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*	
See TCS_145		*20*	*20*	{00..00}
EF ATR/INFO		*7*	*128*	
See TCS_146		*7*	*128*	{00..00}
EF EXTENDED_LENGTH		*3*	*3*	
See TCS_147		*3*	*3*	{00..00}
DF Tachograph				
DF Tachograph_G2				

TCS_145 Le fichier élémentaire EF DIR doit contenir les objets informatifs liés 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 informatifs de longueur étendue (DO’7F66’) conformément à la norme ISO/IEC 7816-4:2013 clause 12.7.1.

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 informatif suivant: ’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 la 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 fichier et les conditions d'accès au fichier permanentes suivantes:

		Conditions d'accès		
Fichier	**ID de fichier**	**Lire**	**Sélect.**	**Actualiser**
DF Tachograph	'0500h'		SC1	
EF Application_Identification	'0501h'	SC2	SC1	NEV
EF Card_Certificate	'C100h'	SC2	SC1	NEV
EF CA_Certificate	'C108h'	SC2	SC1	NEV
EF Identification	'0520h'	SC2	SC1	NEV
EF Card_Download	'050Eh'	SC2	SC1	SC1
EF Driving_Licence_Info	'0521h'	SC2	SC1	NEV
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, sont utilisées les abréviations suivantes concernant les conditions de sécurité:
SC1 ALW OU SM-MAC-G2
SC2 ALW OU SM-MAC-G1 OU SM-MAC-G2
SC3 SM-MAC-G1 OU SM-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 avoir la structure de données suivante:

File / Data element	**No of Records**	**Size (bytes) Min.**	**Max.**	**Default Values**
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	{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	
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 Les valeurs suivantes, qui servent à fournir les tailles dans le tableau ci-dessus, correspondent aux valeurs de nombre de relevés minimum et maximum que doit utiliser la structure des données de la carte du 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 modifications d'activité)	13 776 octets (28 jours * 240 modifications 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 fichier et les conditions d'accès au fichier permanentes suivantes.

Remarque: l'identificateur d'EF court SFID est communiqué sous la forme d'un nombre décimal, p. ex. la valeur 30 correspond au nombre binaire 11110.

			Conditions d'accès	
Fichier	**ID fichier**	**SFID**	**Lire/Sélect.**	**Actualiser**
DF Tachograph_G2			SC1	
EF Application_Identification	‘0501h’	1	SC1	NEV
EF CardMA_Certificate	‘C100h’	2	SC1	NEV
EF CardSignCertificate	‘C101h’	*3*	SC1	NEV
EF CA_Certificate	‘C108h’	4	SC1	NEV
EF Link_Certificate	‘C109h’	5	SC1	NEV
EF Identification	‘0520h’	6	SC1	NEV
EF Card_Download	‘050Eh’	*7*	SC1	SC1
EF Driving_Licence_Info	‘0521h’	*10*	SC1	NEV
EF Events_Data	‘0502h’	12	SC1	SM-MAC-G2
EF Faults_Data	‘0503h’	13	SC1	SM-MAC-G2
EF Driver_Activity_Data	‘0504h’	14	SC1	SM-MAC-G2
EF Vehicles_Used	‘0505h’	15	SC1	SM-MAC-G2
EF Places	‘0506h’	16	SC1	SM-MAC-G2
EF Current_Usage	‘0507h’	17	SC1	SM-MAC-G2
EF Control_Activity_Data	‘0508h’	18	SC1	SM-MAC-G2
EF Specific_Conditions	‘0522h’	*19*	SC1	SM-MAC-G2
EF VehicleUnits_Used	‘0523h’	*20*	SC1	SM-MAC-G2
EF GNSS_Places	‘0524h’	21	SC1	SM-MAC-G2

Dans le tableau ci-dessus, est utilisée l'abréviation suivante concernant la condition de sécurité:
SC1 ALW OU SM-MAC-G2

TCS_153 La structure de tous les EF doit être transparente.

TCS_154 L'application de la carte de conducteur de génération 2 doit avoir la structure de données suivante:

File / Data element	**No of Records**	**Size (bytes) Min.**	**Max.**	**Default Values**
DF Tachograph_G2		*19510*	*39306*	
EF Application_Identification		*15*	*15*	
DriverCardApplicationIdentification		*15*	*15*	
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}
noOfGNSSCDRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00}
EF CardMA_Certificate		*204*	*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		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{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	
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		*1584*	*3168*	
CardEventData		*1584*	*3168*	
cardEventRecords	11	*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		*4034*	*9602*	

└CardVehiclesUsed		*4034*	*9602*	
├vehiclePointerNewestRecord		2	2	{00 00}
└cardVehicleRecords		*4032*	*9600*	
└CardVehicleRecord	n_3	*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		*1766*	*2354*	
└CardPlaceDailyWorkPeriod		*1766*	*2354*	
├placePointerNewestRecord		2	2	{00 00}
└placeRecords		*1764*	*2352*	
└PlaceRecord	n_4	*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				
├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		*282*	*562*	
SpecificConditions		*282*	*562*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		*280*	*560*	
SpecificConditionRecord	n_9	*5*	*5*	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF VehicleUnits_Used		*842*	*2002*	
CardVehicleUnitsUsed		*842*	*2002*	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		*840*	*2000*	
CardVehicleUnitRecord	n_7	*10*	*10*	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*3782*	*5042*	
GNSSContinuousDriving		*3782*	*5042*	
gnssCDPointerNewestRecord		2	2	{00 00}
gnssContinuousDrivingRecords		3780	5040	{00}
GNSSContinuousDrivingRecord	n_8	*15*	*15*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}

TCS_155 Les valeurs suivantes, qui servent à fournir les tailles dans le tableau ci-dessus, correspondent aux valeurs de nombre de relevés minimum et maximum que doit utiliser la structure des données de la carte du conducteur pour une application de génération 2:

		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 modifications d'activité)	13 776 octets (28 jours * 240 modifications d'activité)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. Applications de la carte 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 fichier et les conditions d'accès au fichier permanentes suivantes:

		Conditions d'accès		
Fichier	**ID fichier**	**Lire**	**Sélect.**	**Actualiser**
DF Tachograph	‘0500h’		SC1	
EF Application_Identification	‘0501h’	SC2	SC1	NEV
EF Card_Certificate	‘C100h’	SC2	SC1	NEV
EF CA_Certificate	‘C108h’	SC2	SC1	NEV
EF Identification	‘0520h’	SC2	SC1	NEV
EF Card_Download	‘0509h’	SC2	SC1	**SC1**
EF Calibration	‘050Ah’	SC2	SC1	SC3
EF Sensor_Installation_Data	‘050Bh’	**SC4**	SC1	NEV
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, sont utilisées les abréviations suivantes concernant les conditions de sécurité:

SC1 ALW OU SM-MAC-G2

SC2 ALW OU SM-MAC-G1 OU SM-MAC-G2

SC3 SM-MAC-G1 OU SM-MAC-G2

SC4 Concernant la commande READ BINARY avec des octets pairs INS:
(PLAIN-C AND SM-R-ENC-G1) OU (SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) OU (SM-C-MAC-G2 AND SM-R-ENC-MAC-G2)
Pour la commande READ BINARY avec octet impair INS (si pris en charge): NEV

TCS_157 La structure de tous les EF doit être transparente.

TCS_158 L'application de la carte d'atelier de génération 1 doit avoir la structure de données suivante:

File / Data element	**No of Records**	**Taille (octets) Min.**	**Max.**	**Default Values**
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}
calibrationRecords		*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}
nextCalibrationDate		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*	
CardEventData		*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*	
CardFaultData		*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}
placeRecords		*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 Les valeurs suivantes, qui servent à fournir les tailles dans le tableau ci-dessus, correspondent aux valeurs de nombre de relevés minimum et maximum que doit utiliser la structure des 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 modifications d'activité)	492 octets (1 jour * 240 modifications 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 fichier et les conditions d'accès au fichier permanentes suivantes.

Remarque: l'identificateur d'EF court SFID est communiqué sous la forme d'un nombre décimal, p. ex. la valeur 30 correspond au nombre binaire 11110.

			Conditions d'accès		
Fichier	**ID fichier**	**SFID**	**Lire**	**Sélect.**	**Actualiser**
DF Tachograph_G2			SC1	SC1	
EF Application_Identification	‘0501h’	1	SC1	SC1	NEV
EF CardMA_Certificate	‘C100h’	2	SC1	SC1	NEV
EF CardSignCertificate	‘C101h’	*3*	SC1	SC1	NEV
EF CA_Certificate	‘C108h’	4	SC1	SC1	NEV
EF Link_Certificate	‘C109h’	5	SC1	SC1	NEV
EF Identification	‘0520h’	6	SC1	SC1	NEV
EF Card_Download	‘0509h’	*7*	SC1	SC1	SC1
EF Calibration	‘050Ah’	10	SC1	SC1	SM-MAC-
EF Sensor_Installation_Data	‘050Bh’	11	**SC5**	SM-MAC-	NEV
EF Events_Data	‘0502h’	12	SC1	SC1	SM-MAC-
EF Faults_Data	‘0503h’	13	SC1	SC1	SM-MAC-
EF Driver_Activity_Data	‘0504h’	14	SC1	SC1	SM-MAC-
EF Vehicles_Used	‘0505h’	15	SC1	SC1	SM-MAC-
EF Places	‘0506h’	16	SC1	SC1	SM-MAC-
EF Current_Usage	‘0507h’	17	SC1	SC1	SM-MAC-

					Conditions d'accès
EF Control_Activity_Data	‘0508h’	18	SC1	SC1	SM-MAC-
EF Specific_Conditions	‘0522h’	*19*	SC1	SC1	SM-MAC-
EF VehicleUnits_Used	‘0523h’	*20*	SC1	SC1	SM-MAC-
EF GNSS_Places	‘0524h’	21	SC1	SC1	SM-MAC-

Dans le tableau ci-dessus, sont utilisées les abréviations suivantes concernant les conditions de sécurité:
SC1 ALW OU SM-MAC-G2
SC5 Concernant la commande Read Binary avec des octets pairs INS: SM-C-MAC-G2 ET SM-R-ENC-MAC-G2
Concernant la commande Read Binary avec des octets impairs INS (si pris en charge): NEV

TCS_161 La structure de tous les EF doit être transparente.

TCS_162 L'application de la carte d'atelier de génération 2 doit avoir la structure de données suivante:

File / Data element	**No of Records**	**Taille (octets) Min.**	**Max.**	**Default Values**
DF Tachograph_G2		*17837*	*47163*	
EF Application_Identification		*17*	*17*	
WorkshopCardApplicationIdentification		*17*	*17*	
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}
noOfCalibrationRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
EF CardMA_Certificate		*204*	*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		*14788*	*42844*	
└WorkshopCardCalibrationData		*14788*	*42844*	
├calibrationTotalNumber		2	2	{00 00}
├calibrationPointerNewestRecord		2	2	{00}
└calibrationRecords		*14784*	*42840*	
└WorkshopCardCalibrationRecord	n_5	*168*	*168*	
├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		*46*	*46*	
├noOfSealRecords		1	1	{00}
└SealRecords		45	45	
└SealRecord	5	9	9	
├equipmentType		1	1	{00}
└extendedSealIdentifier		8	8	{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	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*	
└CardFaultData		*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		*194*	*386*	
CardVehiclesUsed		*194*	*386*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*192*	*384*	
CardVehicleRecord	n_3	*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	n_4	*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	n_7	*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		*262*	*362*	
GNSSContinuousDriving		*262*	*362*	
gnssCDPointerNewestRecord		2	2	{00 00}
gnssContinuousDrivingRecords		*260*	*360*	
GNSSContinuousDrivingRecord	n_8	*15*	*15*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
EF Specific_Conditions		*12*	*22*	
SpecificConditions		*12*	*22*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		*10*	*20*	
SpecificConditionRecord	n_9	*5*	*5*	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}

TCS_163 Les valeurs suivantes, qui servent à fournir les tailles dans le tableau ci-dessus, correspondent aux valeurs de nombre de relevés minimum et maximum que doit utiliser la structure des données de la carte d'atelier pour une application de génération 2:

		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 modifications d'activité)	492 octets (1 jour * 240 modifications d'activité)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	*24*
n_9	NoOfSpecificConditionRecords	2	4

4.4. Applications de la carte de contrôle

4.4.1 Application de la carte de contrôle de génération 1

TCS_164 Après personnalisation, l'application de la carte de contrôle de génération 1 doit avoir la structure de fichier et les conditions d'accès au fichier permanentes suivantes:

		Conditions d'accès		
Fichier	**ID fichier**	**Lire**	**Sélect.**	**Actualiser**
DF Tachograph	‘0500h’			
EF Application_Identification	‘0501h’	SC2	SC1	NEV
EF Card_Certificate	‘C100h’	SC2	SC1	NEV
EF CA_Certificate	‘C108h’	SC2	SC1	NEV
EF Identification	‘0520h’	**SC6**	SC1	NEV
EF Controller_Activity_Data	‘050Ch’	SC2	SC1	SC3

Dans le tableau ci-dessus, sont utilisées les abréviations suivantes concernant les conditions de sécurité:
SC1 ALW OU SM-MAC-G2
SC2 ALW OU SM-MAC-G1 OU SM-MAC-G2
SC3 SM-MAC-G1 OU SM-MAC-G2
SC6 EXT-AUT-G1 OU SM-MAC-G1 OU SM-MAC-G2

TCS_165 La structure de tous les EF doit être transparente.

TCS_166 L'application de la carte de contrôle de génération 1 doit avoir la structure de données suivante:

File / Data element	**No of Records**	**Taille (octets) Min.**	**Max.**	
DF Tachograph		*11186*	*2pageapp*	
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 Les valeurs suivantes, qui servent à fournir les tailles dans le tableau ci-dessus, correspondent aux valeurs de nombre de relevés minimum et maximum que doit utiliser la structure des données de la carte de contrôle pour une application de génération 1:

		Min.	*Max.*
n_7	NoOfControlActivityRecords	230	520

4.4.2 Application de la carte de contrôle de génération 2

TCS_168 Après personnalisation, l'application de la carte de contrôle de génération 2 doit avoir la structure de fichier et les conditions d'accès au fichier permanentes suivantes:

Remarque: l'identificateur d'EF court SFID est communiqué sous la forme d'un nombre décimal, p. ex. la valeur 30 correspond au nombre binaire 11110.

			Conditions d'accès	
Fichier	ID fichier	SFID	Lire/Sélect.	Actualiser
DF Tachograph_G2			SC1	
EF Application_Identification	'0501h'	1	SC1	NEV

				Conditions d'accès
EF CardMA_Certificate	‘C100h’	2	SC1	NEV
EF CA_Certificate	‘C108h’	4	SC1	NEV
EF Link_Certificate	‘C109h’	5	SC1	NEV
EF Identification	‘0520h’	6	SC1	NEV
EF Controller_Activity_Data	‘050Ch’	14	SC1	SM-MAC-G2

Dans le tableau ci-dessus, est utilisée l'abréviation suivante concernant la condition de sécurité:
SC1 ALW OU SM-MAC-G2

TCS_169 La structure de tous les EF doit être transparente.

TCS_170 L'application de la carte de contrôle de génération 2 doit avoir la structure de données suivante:

File / Data element	**No of Records**	**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, 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_171 Les valeurs suivantes, qui servent à fournir les tailles dans le tableau ci-dessus, correspondent aux valeurs de nombre de relevés minimum et maximum que doit utiliser la structure des données de la carte de contrôle pour une application de génération 2:

		Min.	*Max.*
n_7	NoOfControlActivityRecords	230	520

4.5. Applications de la carte 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 fichier et les conditions d'accès au fichier permanentes suivantes:

		Conditions d'accès		
Fichier	**ID fichier**	**Lire**	**Sélect.**	**Actualiser**
DF Tachograph	'0500h'		SC1	
EF Application_Identification	'0501h'	SC2	SC1	NEV
EF Card_Certificate	'C100h'	SC2	SC1	NEV
EF CA_Certificate	'C108h'	SC2	SC1	NEV
EF Identification	'0520h'	**SC6**	SC1	NEV
EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

Dans le tableau ci-dessus, sont utilisées les abréviations suivantes concernant les conditions de sécurité:
SC1 ALW OU SM-MAC-G2
SC2 ALW OU SM-MAC-G1 OU SM-MAC-G2
SC3 SM-MAC-G1 OU SM-MAC-G2
SC6 EXT-AUT-G1 OU SM-MAC-G1 OU SM-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 avoir la structure de données suivante:

File / Data element	**No of Records**	**Size (bytes) Min.**	**Max.**	**Default Values**
		11114	*24454*	
E F 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, 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	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, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_175 Les valeurs suivantes, qui servent à fournir les tailles dans le tableau ci-dessus, correspondent aux valeurs de nombre de relevés minimum et maximum que doit utiliser la structure des 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 fichier et les conditions d'accès au fichier permanentes suivantes:

Remarque: l'identificateur d'EF court SFID est communiqué sous la forme d'un nombre décimal, p. ex. la valeur 30 correspond au nombre binaire 11110.

			Conditions d'accès	
Fichier	ID fichier	SFID	Lire/Sélect.	Actualiser
DF Tachograph_G2			SC1	
EF Application_Identification				
	‘0501h’	1	SC1	NEV
EF CardMA_Certificate	‘C100h’	2	SC1	NEV
EF CA_Certificate	‘C108h’	4	SC1	NEV
EF Link_Certificate	‘C109h’	5	SC1	NEV
EF Identification	‘0520h’	6	SC1	NEV
EF Company_Activity_Data	‘050Eh’	14	SC1	SM-MAC-C2

	Conditions d'accès

Dans le tableau ci-dessus, est utilisée l'abréviation suivante concernant les conditions de sécurité:
SC1 ALW OU SM-MAC-G2

TCS_177 La structure de tous les EF doit être transparente.

TCS_178 L'application de la carte d'entreprise de génération 2 doit avoir la structure de données suivante:

File / Data element	No of Records	Size (bytes) Min.	Max.	Default Values
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, 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	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, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_179 Les valeurs suivantes, qui servent à fournir les tailles dans le tableau ci-dessus, correspondent aux valeurs de nombre de relevés minimum et maximum que doit utiliser la structure des données de la carte d'entreprise pour une application de génération 2:

		Min.	Max.
n_8	NoOfCompanyActivityRecords	230	520

FR

APPENDICE 3. PICTOGRAMMES

PIC_001 Le tachygraphe est susceptible d'employer les pictogrammes et combinaisons de pictogrammes qui suivent (ou des pictogrammes et combinaisons de pictogrammes suffisamment semblables pour être identifiables à ceux-ci sans ambiguïté):

5. PICTOGRAMMES DE BASE

	Ressources humaines	**Actions**	**Modes d'exploitation**
	Entreprise		Mode entreprise
	Contrôleur	Contrôle	Mode de contrôle
	Conducteur	Route	Mode opérationnel
	Atelier/Poste d'essai	Inspection/Étalonnage	Mode étalonnage
	Fabricant		

	Activités	**Durée**
	Disponible	Période de disponibilité en cours
	Conduite	Temps de conduite continue
	Repos	Période de repos en cours
	Autres tâches	Période de travail en cours
	Pause	Temps de pause cumulé
?	Inconnue	

	Équipements	**Fonctions**
1	Lecteur «conducteur»	
2	Lecteur «convoyeur»	
	Cartc	
	Horloge	
	Écran	Affichage
	Mémoire externe	Téléchargement
	Alimentation	
	Imprimante/Tirage	Impression
	Capteur	
	Type de pneumatique	
	Véhicule/Unité embarquée sur le véhicule (UEV)	
	Dispositif GNSS	
	Dispositif de détection à distance	
	Interface STI	

	Conditions spécifiques
OUT	Hors limites
	Traversée en ferry/train

Divers

!	Évènements	✕	Anomalies
⏵	⏵ Début de la période journalière de travail	⏯	⏯ Fin de la période journalière de travail
●	● Adresse		
M	M Saisie manuelle des activités du conducteur		
🔒	🔒 Sécurité		
>	Vitesse		
◷	◷ Temps		
Σ	Total/Synthèse		

Qualificatifs

24h	Journalier
I	Hebdomadaire
II	Bihebdomadaire
✚	✚ De ou vers

6. COMBINAISONS DE PICTOGRAMMES

Divers

🏛 ●	Lieu du contrôle		
● ⏵	● ⏵ Site de début de la période de travail journalière	⏯ ●	⏯ ● Site de fin de la période de travail journalière
◷ ✚	◷ ✚ De (heure)	✚ ◷	✚ ◷ À (heure)
🚙 ✚	🚙 ✚ Du véhicule		
OUT ✚	OUT ✚ Hors limites, début	✚ OUT	✚ OUT Hors limites, fin

Cartes

⊙ 🖬	⊙ 🖬 Carte du conducteur
🏠 🖬	🏠 🖬 Carte d'entreprise
🏛 🖬	🏛 🖬 Carte de contrôleur
T 🖬	T 🖬 Carte d'atelier
🖬 – – –	Pas de carte

Route

⊙ ⊙	⊙ ⊙ Conduite en équipage
⊙ I	⊙ I Temps de conduite hebdomadaire
⊙ II	⊙ II Temps de conduite bihebdomadaire

Tirages

24h 🖬 ⏬	🖬 ⏬ Tirage quotidien des activités du conducteur extraites de la carte
24h 🚙 ⏬	🚙 ⏬ Tirage quotidien des activités du conducteur extraites de l'UEV
! ✕ 🖬 ⏬	! ✕ 🖬 ⏬ Tirage des anomalies et événements extraits d'une carte
! ✕ 🚙 ⏬	! ✕ 🚙 ⏬ Tirage des anomalies et événements extraits de l'UEV
T ◷ ⏬	T ◷ ⏬ Tirage des données techniques
> > ⏬	> > ⏬ Tirage des dépassements de la vitesse autorisée

Événements

! 🖬	! 🖬 Insertion d'une carte erronée


Conflit de carte


Dépassement du temps imparti


Conduite sans carte appropriée


Insertion d'une carte en cours de route


Clôture incorrecte de la dernière session


Dépassement de la vitesse autorisée


Coupure d'alimentation électrique


Erreur au niveau des données de mouvement


Conflit concernant le mouvement du véhicule


Atteinte à la sécurité


Réglage de l'heure (en atelier)


Contrôle de dépassement de la vitesse autorisée

Défauts

Carte défectueuse (logement de carte du conducteur)


Carte défectueuse (logement de carte du convoyeur)


Anomalie de l'affichage


Anomalie de téléchargement


Anomalie de l'imprimante


Anomalie du capteur


Défaillance interne de la VU


Anomalie du dispositif GNSS


Anomalie de détection à distance

Procédure de saisie manuelle


Même période journalière de travail?

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 associées à autant d'identificateurs d'enregistrement ou de blocs d'impression sont définies à l'appendice 4.

FR

APPENDICE 4. TIRAGES PAPIER

TABLE DES MATIERES

1. Généralités

Toute sortie imprimée se compose d'une succession de blocs de données séquencés susceptibles d'être désignés par un identificateur de bloc.

Un bloc de données contient un ou plusieurs enregistrements désignés, le cas échéant, par 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 d'information est inconnu ou ne doit pas être imprimé en raison de l'existence 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 nécessite aucune impression, 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 le passage des centaines aux milliers et des milliers aux 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 (noms et adresses).

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** identifient le texte en clair à imprimer (au tirage, les caractères sont normaux),
- les caractères normaux indiquent à l'affichage des variables (pictogrammes ou données) remplacées au tirage par leurs valeurs respectives,
- les noms de variable s'accompagnent de traits de soulignement indiquant la longueur élémentaire disponible pour la variable considérée,
- les dates respectent par défaut le format «jj/mm/aaaa» (jour, mois, année). L'application du format «jj.mm.aaaa» est également envisageable,
- la rubrique «identification de carte» se compose des éléments suivants: type de carte indiqué par une combinaison de pictogrammes, code de l'État membre d'émission de la carte, 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:

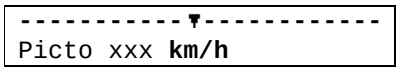
P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Combinaison de pictogrammes		Code de l'État membre d'émission				14 premiers caractères du numéro de la carte (comprenant, le cas échéant, un indice séquentiel)														Indice de remplacement		Indice de renouvellement

PRT_007 Les tirages se composent des blocs et/ou enregistrements de données qui suivent. 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 sortie imprimée***

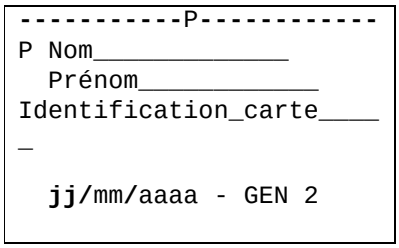
Identificateur de bloc
Combinaison de pictogrammes d'impression (cf. appendice 3); réglage du dispositif limiteur de vitesse (impression uniquement en cas de dépassement de la vitesse autorisée)



3 ***Identification du titulaire de la carte***

Identificateur de bloc. P = pictogramme individuel
Nom du titulaire de la carte
Prénom(s) du titulaire de la carte (le cas échéant)
Identification de carte

Date d'expiration de la carte (le cas échéant) et génération de la carte (GEN 1 ou GEN 2)*

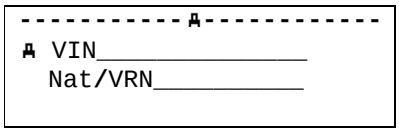


Si la carte considérée n'est pas individuelle et ne contient aucun nom de titulaire, le nom de l'entreprise, de l'atelier ou de l'organisme de contrôle concerné est imprimé en lieu et place de celui-ci.

* Seul un tachygraphe intelligent peut imprimer la génération de la carte.

4 ***Identification du véhicule***

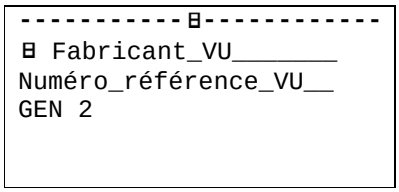
Identificateur de bloc
VIN
État membre dans lequel le véhicule est immatriculé et numéro d'immatriculation du véhicule (VRN)



5 ***Identification de la VU***

Identificateur de bloc
Nom du fabricant de la VU
Numéro de référence de la VU

Génération de la VU*

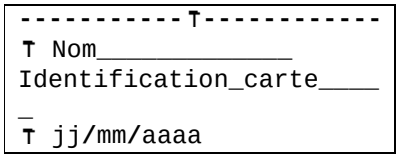


* Seul un tachygraphe intelligent peut imprimer la génération de la carte.

6 ***Dernier étalonnage du tachygraphe***

Identificateur de bloc
Nom de l'atelier
Identification de la carte d'atelier

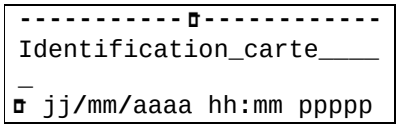
Date de l'étalonnage



7 ***Dernier contrôle (par un contrôleur)***

Identificateur de bloc
Identification de la carte du contrôleur

Date, heure et type de contrôle



Type de contrôle: combinaison composée de cinq pictogrammes au maximum. Le type de contrôle est susceptible de correspondre à l'un des pictogrammes suivants (ou à leur combinaison):
: téléchargement à partir d'une carte, : téléchargement à partir de la VU, : impression, : affichage, : contrôle

routier de l'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) + compteur de présence quotidienne de la carte

```
-----------⊙------------
    jj/mm/aaaa xxx
```

8a *Condition hors champ au début de cette journée* (laisser vide si pas de condition hors champ ouverte)

```
----------OUT-----------
```

8.1 *Période pendant laquelle la carte n'était pas présente dans son 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 de lecteur
État membre dans lequel le véhicule est immatriculé et numéro d'immatriculation du véhicule (VRN)
Kilométrage indiqué au compteur du véhicule lors de l'insertion de la carte

```
  ---------S---------

 Nat/VRN__________

  x xxx xxx km
```

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 *Conditions particulières.* Heure de saisie, pictogramme (ou combinaison de pictogrammes) associé aux conditions particulières.

```
        hh:mm ---pppp---
```

8.4 *Retrait de carte*

Kilométrage indiqué au compteur du véhicule et distance parcourue depuis la dernière insertion de la carte pour laquelle le kilométrage affiché est connu

```
  x xxx xxx km; x xxx km
```

9 ***Activités du conducteur enregistrées sur une VU par lecteur de carte, par ordre chronologique***

Identificateur de bloc
Date de consultation (jour civil dont les données font l'objet du tirage)
Kilométrage affiché au compteur du véhicule à 00:00 et 24:00

```
-----------⊙------------
       jj/mm/aaaa

x xxx xxx - x xxx xxx km
```

10 ***Activités menées dans le 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'était présente dans le lecteur S*

Identificateur d'enregistrement
Lecteur vide de carte
Kilométrage indiqué au compteur au début de la période considérée

```
  --------------------
⊙▪---
  x xxx xxx km
```

10.2 *Insertion de la carte*

F 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) et génération de la carte (GEN 1 ou GEN 2)*
État membre dans lequel le véhicule précédent utilisé est immatriculé et numéro d'immatriculation de ce véhicule
Date et heure de retrait de la carte du véhicule précédent
Ligne vierge
Kilométrage indiqué au compteur lors de l'insertion de la carte, drapeau de saisie manuelle d'activités 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 donné pour le bloc 10.2 est celui correspondant à la dernière insertion de carte disponible avant le jour concerné.

```
  --------------------
⊙ Nom_______________
  Prénom_____________
Identification_carte_____
  jj/mm/aaaa - GEN 2

 →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, espaces vides si SEUL)

```
A        hh:mm hhhmm ⊙⊙
```

10.3 a *Conditions particulières.* Heure de saisie, pictogramme (ou combinaison de pictogrammes) associé aux conditions particulières.

```
         hh:mm ---pppp---
```

10.4 *Retrait de carte ou fin de période «sans carte»*
Kilométrage indiqué au compteur du véhicule lors du 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 VU des périodes sans carte dans le lecteur du conducteur***
Identificateur de bloc

```
1⊙▪---
```

11.2 ***Synthèse VU des périodes sans carte dans le lecteur du convoyeur***
Identificateur de bloc

```
2⊙▪---
```

11.3 ***Synthèse VU quotidienne 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,
Kilométrage indiqué au compteur

```
pihh:mm Pay Rég

  x xxx xxx km
```

11.5 *Saisie du lieu de début et/ou de fin d'une période de travail journalière*
et après 3 heures, le temps de conduite continue

```
⁘ hh:mm
```

Kilométrage indiqué au compteur

```
x xxx xxx km
```

11.6 *Totaux par activité (extraits d'une carte)*

Durée totale du temps de conduite, distance parcourue
Durée totale de la période de travail et de disponibilité effective
Durée totale de la période de repos et d'activité non répertoriée
Durée totale des activités de l'équipage

```
hhhmm  x xxx km
hhhmm  hhhmm
hhhmm  ? hhhmm
hhhmm
```

11.7 *Totaux par activité (périodes sans carte insérée dans le lecteur conducteur)*

Durée totale du temps de conduite, distance parcourue
Durée totale de la période de travail et de disponibilité effective
Durée totale de la période de repos

```
hhhmm  x xxx km
hhhmm  hhhmm
hhhmm
```

11.8 *Totaux par activité (périodes sans carte insérée dans le lecteur convoyeur)*

Durée totale de la période de travail et de disponibilité effective
Durée totale de la période de repos

```
hhhmm  hhhmm
hhhmm
```

11.9 *Totaux par activité (et par conducteur, les deux lecteurs étant inclus dans leur calcul)*

Durée totale du temps de conduite, distance parcourue
Durée totale de la période de travail et de disponibilité
Durée totale de la période de repos
Durée totale des activités de l'équipage

```
hhhmm  x xxx km
hhhmm  hhhmm
hhhmm
hhhmm
```

Si un tirage papier journalier est demandé pour la journée en cours, l'établissement des informations de synthèse 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 d'enregistrement, date et heure de début
Code d'événement/anomalie supplémentaire (le cas échéant), durée
État membre où est immatriculé le véhicule sur lequel l'événement ou l'anomalie s'est manifesté(e) et numéro d'immatriculation (VRN) de ce véhicule

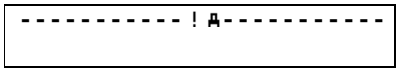
```
--------------------
Pic (p) jj/mm/aaaa hh:mm

!xx
hhhmm
Nat/VRN__________
```

13 ***Événements et/ou anomalies enregistrés ou en cours dans une VU***

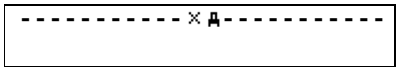
13.1 Identificateur de bloc pour les 5 derniers «événements et anomalies» extraits d'une VU

```
----------!×----------
```

13.2 Identificateur de bloc pour l'ensemble des «événements» enregistrés ou en cours dans une VU

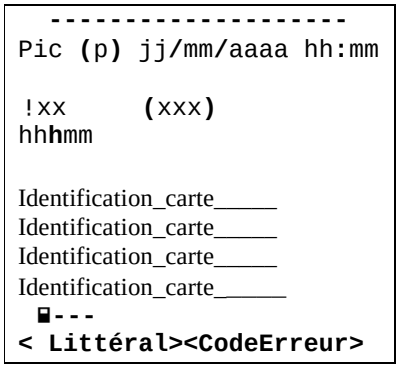


13.3 Identificateur de bloc pour l'ensemble des «anomalies» enregistrées ou en cours dans une VU



13.4 *Enregistrement d'événement et/ou d'anomalie*
Identificateur d'enregistrement
Pictogramme d'événement/anomalie, motif d'enregistrement, date et heure de début
Code d'événement/anomalie supplémentaire (le cas échéant), nombre d'événements analogues 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)

Cas où aucune carte n'a été insérée
Données spécifiques du fabricant

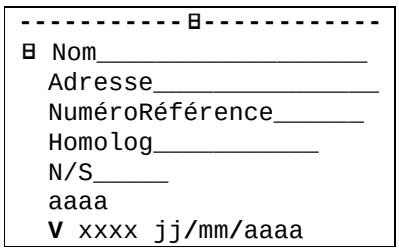


Le motif d'enregistrement (p) prend la forme d'un code numérique indiquant la raison pour laquelle l'événement ou l'anomalie constaté a été enregistré et codé en conformité avec l'élément d'information EventFaultRecordPurpose.

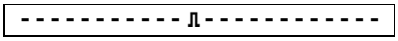
Le Littéral est un symbole littéral spécifique du fabricant de tachygraphe comportant au maximum 12 caractères.

Le CodeErreur est un code d'erreur spécifique du fabricant de tachygraphe comportant au maximum 12 caractères.

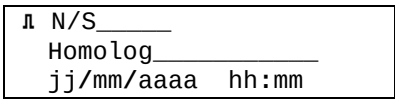
14 ***Identification de la VU***
Identificateur de bloc
Nom du fabricant de la VU
Adresse du fabricant de la VU
Numéro de référence de la VU
Numéro d'homologation de la VU
Numéro de série de la VU
Année de fabrication de la VU
Version du logiciel de la VU et date d'installation



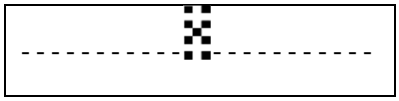
15 ***Identification des capteurs***
Identificateur de bloc



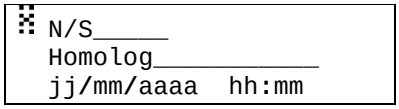
15.1 *Enregistrement de couplage*
Numéro de série du capteur
Numéro d'homologation du capteur
Date de couplage du capteur



16 ***Identification du GNSS***
Identificateur de bloc



16.1 *Enregistrement de couplage*
Numéro de série du dispositif GNSS externe
Numéro d'homologation du dispositif GNSS externe
Date de couplage du dispositif GNSS externe



17 ***Données relatives à l'étalonnage***

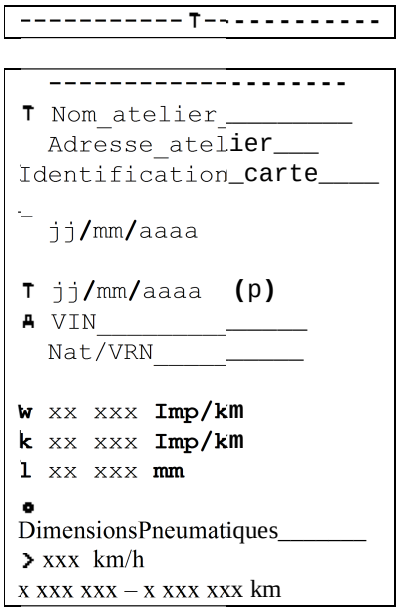
Identificateur de bloc

17.1 *Enregistrement d'étalonnage*

Identificateur d'enregistrement
Atelier responsable de 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 d'étalonnage + motif d'étalonnage
VIN
État membre dans lequel le véhicule est immatriculé et numéro d'immatriculation du véhicule (VRN)
Coefficient caractéristique du véhicule
Constante de l'équipement d'enregistrement
Circonférence effective des pneumatiques
Dimensions des pneumatiques montés

Réglage du dispositif limiteur de vitesse
Ancien et nouveau kilométrages indiqués au compteur



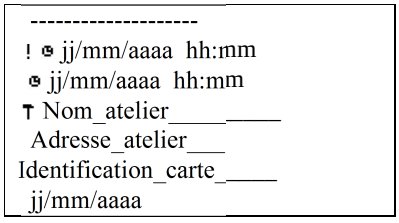
Le motif d'étalonnage (p) prend la forme d'un code numérique indiquant la raison pour laquelle ces paramètres d'étalonnage ont été enregistrés et codés en conformité avec l'élément d'information MotifÉtalonnage.

18 ***Remise à l'heure***

Identificateur de bloc

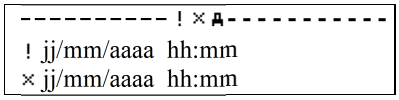
18.1 *Enregistrement de la remise à l'heure*

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



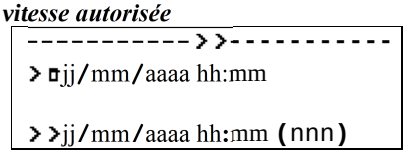
19 Événement et anomalie les plus récents enregistrés dans la VU

Identificateur de bloc
Date et heure de l'événement le plus récent
Date et heure de l'anomalie la plus récente



20 ***Informations relatives au contrôle de dépassement de la vitesse autorisée***

Identificateur de bloc
Date et heure du dernier CONTRÔLE DE DÉPASSEMENT DE LA VITESSE AUTORISÉE
Date/heure du premier dépassement de la vitesse autorisée et nombre des événements de cette nature enregistrés depuis lors



21 ***Enregistrement des dépassements de la vitesse autorisée***

21.1 Identificateur de bloc «Premier dépassement de la vitesse autorisée après le dernier étalonnage»

```
--------->>T---------
```

21.2 Identificateur de bloc «Les 5 dépassements les plus sérieux relevés au cours des 365 derniers jours écoulés»

```
-------->>(365)------
```

21.3 Identificateur de bloc «Le dépassement le plus sérieux pour chacune des périodes coïncidant avec les dix derniers jours de manifestation»

```
-------->>(10)-------
```

21.4 Identificateur d'enregistrement
Date, heure et durée
Vitesses maximale et moyenne, nombre d'événements similaires 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 est dépourvu de tout enregistrement de dépassement de la vitesse autorisée

```
>>---
```

22 ***Informations saisies manuellement***

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 saisies manuellement»; introduisez suffisamment de lignes vierges en amont de toute rubrique saisie manuellement afin de pouvoir rédiger les informations requises ou apposer une signature.

23 ***Cartes les plus récentes insérées dans la VU***

Identificateur de bloc
23.1 Carte insérée
Identificateur d'enregistrement
Type de carte, génération, version, fabricant*
Identification de carte
Numéro de série de la carte
Date et heure de la dernière insertion de carte

```
-------- ⊟▬◷ --------


----
T <gén> <version> <CF>
Identification de carte
Numéro de série de la carte
jj/mm/aaaa hh:mm
```

* (le tout sur une seule ligne)
avec
type de carte: pictogramme, un caractère + espace
gén: GEN1 ou GEN2, 4 caractères + espace
version: jusqu'à 10 caractères
CF: 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 quotidien des activités du conducteur extraites d'une carte

PRT_008 Le tirage quotidien des activités du conducteur extraites d'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 la VU)
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 la VU (à partir de laquelle le tirage est exécuté + GEN)
6	Dernier étalonnage de cette VU
7	Dernier contrôle auquel le conducteur inspecté a été soumis
8	Délimiteur des activités du conducteur
8a	Condition hors champ au début de cette journée
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
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 la VU
13.4	Enregistrements d'événements/anomalies (5 derniers événements ou anomalies enregistrés ou en cours dans la VU)
22.1	Lieu du contrôle
22.2	Signature du contrôleur
22.5	Signature du conducteur

3.2 Tirage quotidien des activités du conducteur extraites de la VU

PRT_009 Le tirage quotidien des activités du conducteur extraites de la VU doit respecter le format suivant:

1	Date et heure d'impression du document
2	Type de document imprimé
3	Identification du titulaire de la carte (pour toutes les cartes insérées dans la VU + GEN)
4	Identification du véhicule (à partir duquel le tirage est exécuté)
5	Identification de la VU (à partir de laquelle le tirage est exécuté + GEN)
6	Dernier étalonnage de cette VU
7	Dernier contrôle auquel ce tachygraphe a été soumis
9	Délimiteur des activités du conducteur
10	Délimiteur de lecteur de carte du conducteur (lecteur 1)

10a	Condition hors champ au début de cette journée
10.1 / 10.2 / 10.3 /10.3a / 10.4	Activités par ordre chronologique (lecteur conducteur)
10	Délimiteur de lecteur de carte du convoyeur (lecteur 2)
10a	Condition hors champ au début de cette journée
10.1 / 10.2 / 10.3 /10.3a / 10.4	Activités par ordre chronologique (lecteur convoyeur)
11	Délimiteur de synthèse quotidienne
11.1	Synthèse des périodes sans carte dans le lecteur du conducteur
11.4	Lieux saisis par ordre chronologique
11.5	Données du GNSS
11.6	Totaux par activité
11.2	Synthèse des périodes sans carte dans le lecteur du convoyeur
11.4	Lieux saisis par ordre chronologique
11.5	Données du GNSS
11.7	Totaux par activité
11.3	Synthèse des activités par conducteur, les deux lecteurs étant inclus
11.4	Lieux saisis par ce conducteur, par ordre chronologique
11.5	Données du GNSS
11.8	Totaux par activité pour ce conducteur
13.1	Délimiteur d'événements et d'anomalies
12.4	Enregistrements d'événements/anomalies (5 derniers événements ou anomalies enregistrés ou en cours dans la VU)
13.1	Lieu du contrôle
22.2	Signature du contrôleur
22.3	De (heure) (espace disponible pour un conducteur dépourvu de carte lui permettant d'indiquer
22.4	À (heure) les périodes qui correspondent à ses prestations)
22.5	Signature du conducteur

3.3 Tirage des anomalies et événements extraits d'une carte

PRT_010 Le tirage des anomalies et événements extraits d'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 la VU + 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 des anomalies et événements extraits de la VU

PRT_011 Le tirage des anomalies et événements extraits de la VU doit respecter le format suivant:

1	Date et heure d'impression du document
2	Type de document imprimé
3	Identification du titulaire de la carte (pour toutes les cartes insérées dans la VU + 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 la VU)
13.3	Délimiteur des anomalies
13.4	Enregistrements d'anomalies (toutes les anomalies enregistrées ou en cours dans la VU)
22.1	Lieu du contrôle
22.2	Signature du contrôleur
22.5	Signature du conducteur

3.5 Tirage 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 titulaire de la carte (pour toutes les cartes insérées dans la VU + GEN)
4	Identification du véhicule (à partir duquel le tirage est exécuté)
14	Identification de la VU
15	Identification des capteurs
15.1	Données relatives au couplage des capteurs (toutes les données disponibles, par ordre chronologique)
16	Identification du GNSS
16.1	Données relatives au couplage du dispositif GNSS externe (toutes les données disponibles, par ordre chronologique)
17	Délimiteur des données d'étalonnage
17.1	Enregistrements d'étalonnage (ensemble des enregistrements disponibles par ordre chronologique)
18	Délimiteur de la remise à l'heure
18.1	Enregistrement de la remise à l'heure (ensemble des enregistrements disponibles, extraits des enregistrements de la remise à l'heure et des données d'étalonnage)
19	Événement et anomalie les plus récents enregistrés dans la VU

3.6 Tirage des dépassements de la vitesse autorisée

PRT_013 Le tirage des dépassements de la vitesse autorisée doit respecter le format suivant:

1	Date et heure d'impression du document
2	Type de document imprimé
3	Identification du titulaire de la carte (pour toutes les cartes insérées dans la VU + GEN)
4	Identification du véhicule (à partir duquel le tirage est exécuté)

20	Informations relatives au contrôle de dépassement de la vitesse autorisée
21.1	Identificateur des données de dépassement de la vitesse autorisée
21.4 / 21.5	Premier dépassement de la vitesse autorisée après le dernier étalonnage
21.2	Identificateur des données de dépassement de la vitesse autorisée
21.4 / 21.5	Les 5 dépassements les plus sérieux relevés au cours des 365 derniers jours écoulés
21.3	Identificateur des données de dépassement de la vitesse autorisée
21.4 / 21.5	Le dépassement le plus sérieux pour chacune des périodes coïncidant avec les dix derniers jours de manifestation
22.1	Lieu du contrôle
22.2	Signature du contrôleur
22.5	Signature du conducteur

3.7 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	Identifications du titulaire de la carte (pour toutes les cartes insérées dans la VU)
23	Cartes les plus récentes insérées dans la VU
23.1	Cartes insérées (jusqu'à 88 enregistrements)
12.3	Délimiteur des anomalies

FR

APPENDICE 5. AFFICHAGE

Les conventions de présentation suivantes s'appliquent dans le présent appendice:

* les caractères **gras** indiquent le texte à afficher (l'affichage demeure en caractères normaux),
* les caractères normaux indiquent des variables (pictogrammes ou données) à remplacer par leurs valeurs respectives à l'affichage:
* 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 emploie 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 convoyeur	2 Jhh**h**mm
Condition hors limites	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 de pause cumulé du conducteur	1 ⊙hh**h**mm ▮▮hh**h**mm
Temps de conduite continue et temps de pause cumulé du convoyeur	2 ⊙hh**h**mm ▮▮hh**h**mm
Temps de conduite cumulé du conducteur, enregistré pendant la semaine en cours et la semaine précédente	1 ⊙▮ hhh**h**mm

Temps de conduite cumulé du convoyeur, enregistré pendant la semaine en cours et la semaine précédente	20 hhh**h**mm

FR

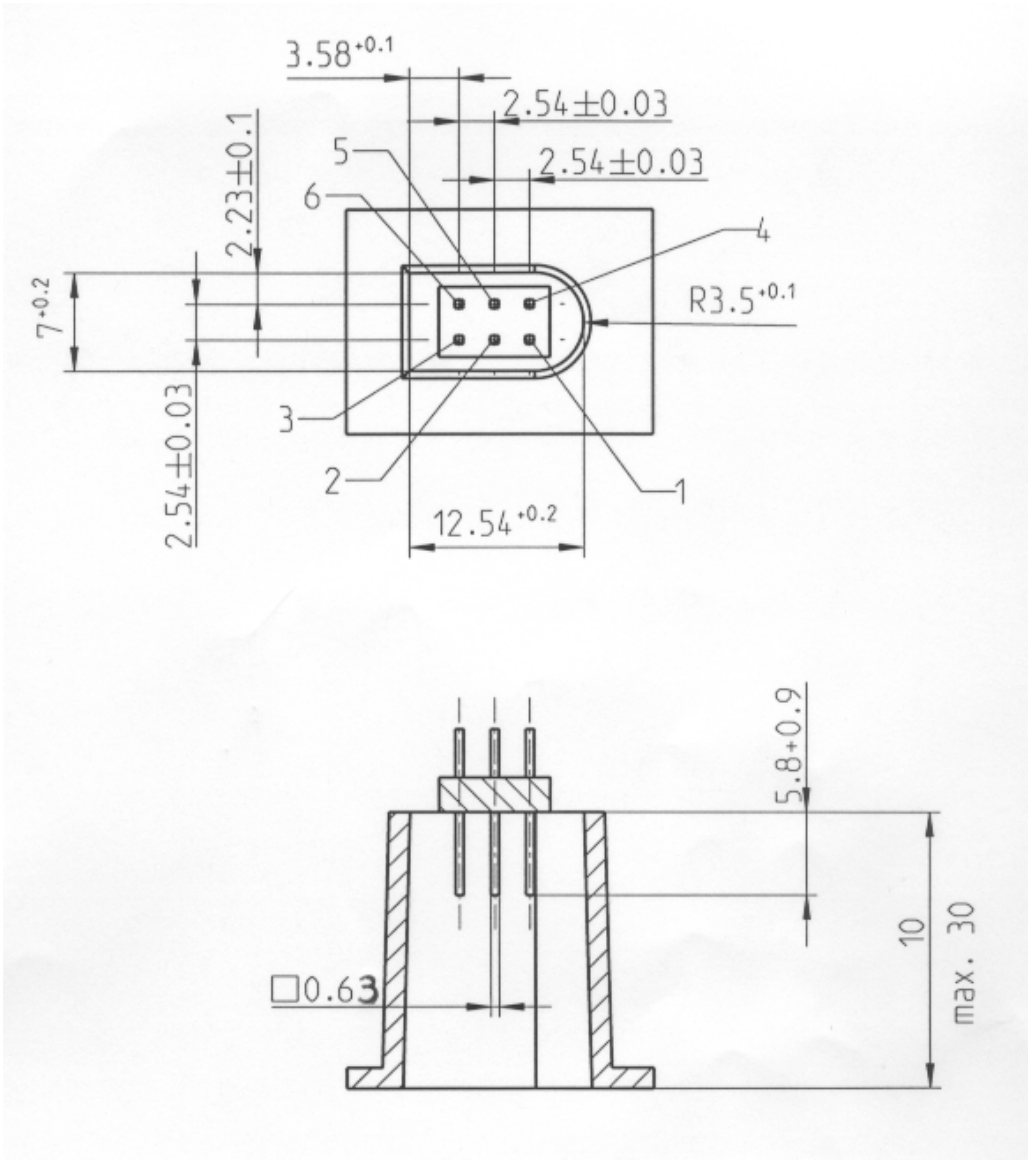
APPENDICE 6. CONNECTEUR FRONTAL POUR L'ETALONNAGE ET LE TELECHARGEMENT

TABLE DES MATIERES

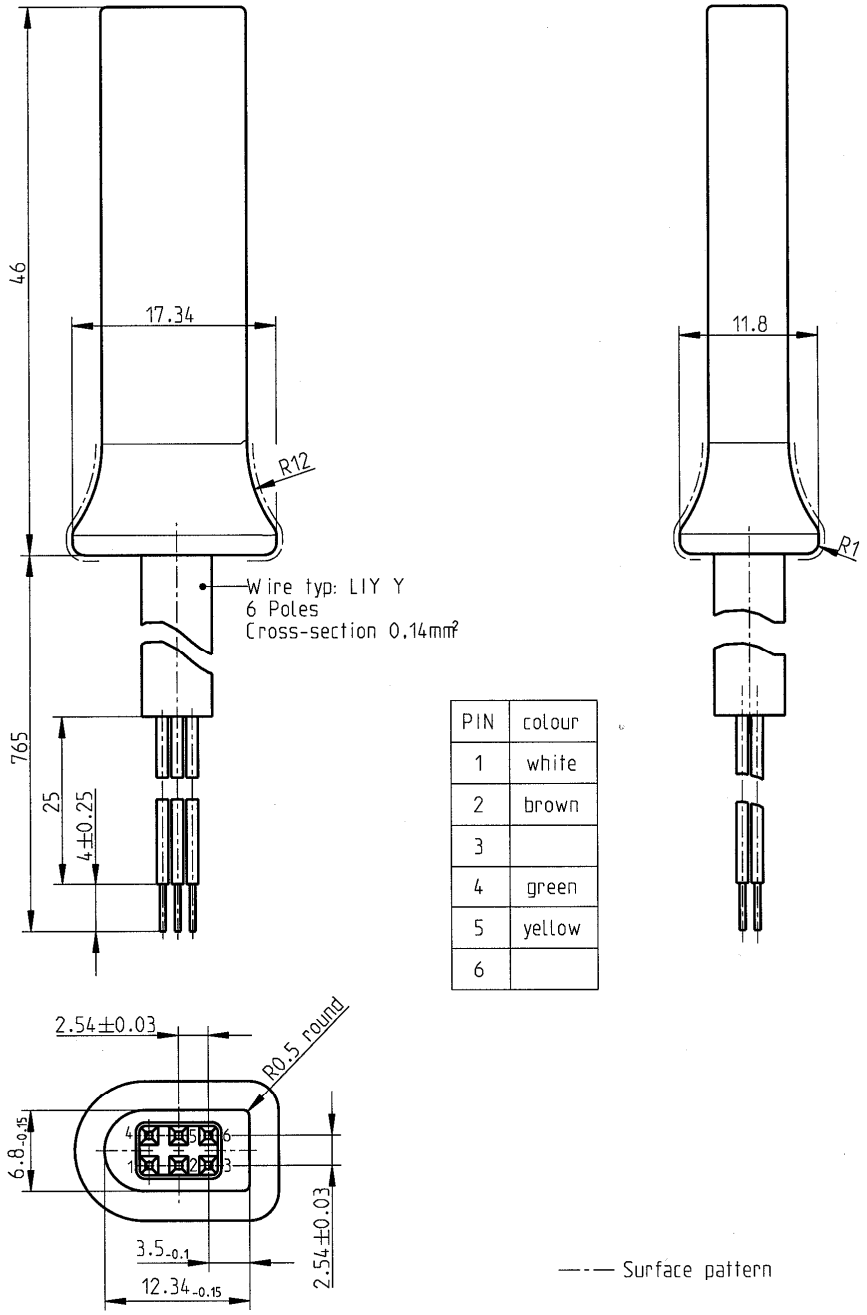
1. Matériel

1.1. Connecteur

INT_001 Le connecteur de téléchargement/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 plan suivant (toutes les cotes sont en millimètres):



Le schéma suivant illustre une fiche classique d'accouplement à 6 broches:



PIN	colour
1	white
2	brown
3	
4	green
5	yellow
6	

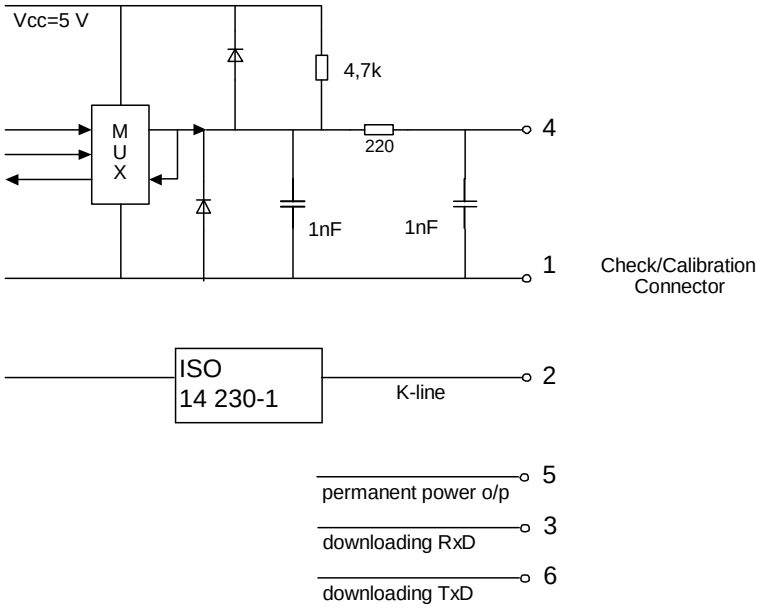
1.2. Affectation des contacts

INT_002 L'affectation des contacts doit être conforme au tableau suivant:

Pin	*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)
3	RxD — Téléchargement	Entrée de données dans le tachygraphe
4	Signal d'entrée/sortie	Étalonnage
5	Puissance de sortie permanente	La plage de tensions doit être identique à celle de l'alimentation électrique du véhicule diminuée de 3 V afin de tenir compte de la chute de tension inhérente au passage du courant à travers les circuits de protection Sortie 40 mA
6	TxD — Téléchargement	Sortie de données du tachygraphe

1.3. Schéma fonctionnel

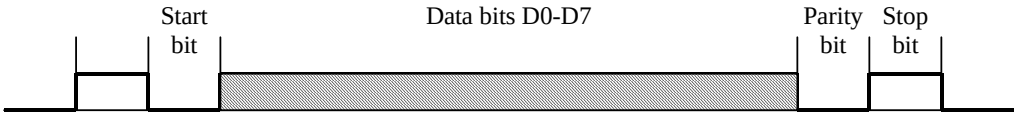
INT_003 Le schéma fonctionnel doit être conforme aux indications suivantes:



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 d'information

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 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 étant égal à 9 600 bits par seconde immédiatement après le début d'une communication.

3. Interface d'étalonnage

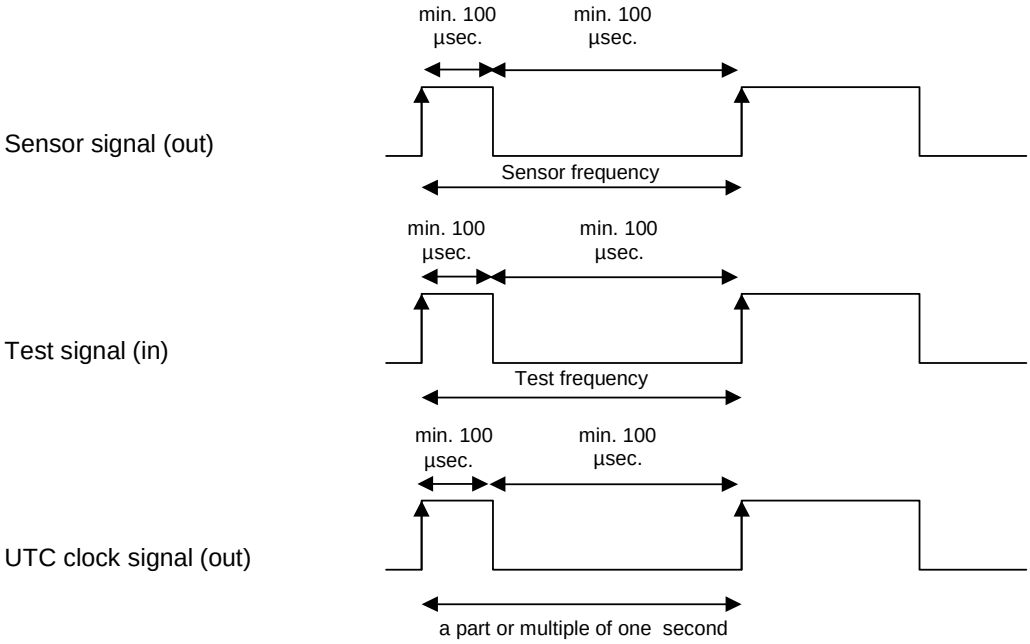
INT_007 La communication de données doit être conforme aux spécifications de la norme ISO 14230-1 Véhicules routiers — Systèmes de diagnostic — Protocole à mots clés 2000 — Partie 1: Couche physique. Première édition: 1999.

.

INT_008 Le signal d'entrée/sortie doit être conforme aux spécifications électriques suivantes:

Paramètre	Minimum	Caractéristique	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:


min. 100 µsec.
min. 100 µsec.
Sensor signal (out)
Sensor frequency
min. 100 µsec.
min. 100 µsec.
Test signal (in)
Test frequency
min. 100 µsec.
min. 100 µsec.
UTC clock signal (out)
a part or multiple of one second

FR

APPENDICE 7. PROTOCOLES DE TÉLÉCHARGEMENT DE DONNÉES

TABLE DES MATIERES

1. Introduction

Le présent appendice traite des procédures qu'il convient d'appliquer pour exécuter les différents types de téléchargement de données vers un support de mémoire externe. 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 en s'assurant de leur authenticité et de leur intégrité avant de procéder à leur analyse éventuelle.

1.1 Champ d'application

Certaines données sont susceptibles d'être téléchargées vers un support de mémoire externe (ESM):

- à partir d'une unité embarquée sur véhicule (VU) par l'intermédiaire d'un équipement spécialisé intelligent (IDE) raccordé à la VU,
- à partir d'une carte tachygraphique par l'intermédiaire d'un IDE équipé d'un périphérique de lecture de carte (IFD),
- à partir d'une carte tachygraphique par l'intermédiaire d'une unité embarquée sur véhicule et par le biais d'un IDE raccordé à la VU.

Afin de permettre la vérification de l'authenticité et de l'intégrité des données téléchargées qui auraient été sauvegardées sur un ESM, ces données s'accompagnent d'une signature conforme à l'appendice 11 (Mécanismes de sécurité communs). L'identification de l'équipement source (VU ou carte) et ses certificats de sécurité (État membre et équipement) sont également téléchargés. Le vérificateur doit être en possession d'une clé publique européenne sécurisée.

DDP_001 Les données téléchargées au cours d'une session de téléchargement doivent être enregistrées dans un seul et même fichier sur l'ESM.

1.2 Abréviations et notations

Les abréviations qui suivent apparaissent dans le présent appendice:

AID Identifiant d'application (*Application Identifier*)
ATR Réponse pour remise à zéro (*Answer To Reset*)
CS Octet de total de contrôle (*Checksum byte*)
DF Fichier spécialisé (*Dedicated File*)
DS_ Session de diagnostic (*Diagnostic Session*)
EF Fichier élémentaire (*Elementary File*)
ESM Support de mémoire externe (*External Storage Medium*)
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*)
IDE Équipement spécialisé intelligent: équipement servant à télécharger des données vers l'ESM (par exemple, le PC) (*Intelligent Dedicated Equipment*)
IFD Périphérique d'interface (*Interface Device*)
KWP Protocole à mots clés (*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 Longueur des balises (*Tag Length Value*)
TREP Paramètre de réponse du transfert (*Transfer Response Parameter*)
TRTP Paramètre de demande du transfert (*Transfer Request Parameter*)
VU Unité embarquée sur le véhicule (*Vehicle Unit*)

2. Téléchargement de données sur la VU

2.1 Procédure de téléchargement

Pour procéder au téléchargement de données sur la VU, l'opérateur doit exécuter les opérations suivantes:
- introduire la carte de tachygraphe qu'il détient dans la fente de l'un des lecteurs de carte de la VU(*);
- raccorder l'IDE au connecteur de téléchargement de la VU;
- établir la liaison entre l'IDE et la VU;
- sélectionner sur l'IDE les données à télécharger et envoyer la requête à la VU;
- 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 la VU 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'IDE jouant le rôle du maître et la VU celui de l'unité asservie.

La structure des messages, leur type et leur acheminement sont essentiellement basés sur le protocole à mots clés 2000 (KWP) (ISO 14230-2 Véhicules routiers - Systèmes de diagnostic - Protocole à mots clés 2000 - Partie 2: Couche de liaison de données).

La couche d'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'IDE et la VU se caractérisent par une structure à trois éléments.
- 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).
- Champ de données composé d'un octet d'identification de service (SID) et d'un nombre variable d'octets d'information qui peuvent comprendre un octet optionnel de session de diagnostic (DS_) ou un octet optionnel de paramètre de transfert (TRTP ou TREP).
- Total de contrôle composé d'un octet total de contrôle (CS).

En-tête				Champ 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 F0 Hex pour l'IDE et EE Hex pour la VU.

L'octet LEN indique la longueur du champ de données.

L'octet 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, DS_, TRTP et TREP font également l'objet d'une définition présentée 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 champ 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 TREP 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 le contrôle d'erreur et l'abandon éventuel d'un échange de données, l'IDE accuse réception de chaque sous-message. L'IDE est à même d'accepter le sous-message, d'en demander la réémission et de demander à la VU d'en reprendre ou d'en abandonner la transmission.

DDP_004 Si le champ de données du dernier sous-message contient exactement 255 octets, il est indispensable d'adjoindre à l'ensemble un sous-message final comportant un champ de données vide (à l'exception des SID, TREP et compteur de sous-messages) pour indiquer la fin du message.

Exemple:

En-tête	SID	TREP	Message	CS
4 octets	Longueur supérieure à 255 octets			

Transmis sous la forme suivante:

En-tête	SID	TREP	00	01	Sous-message 1	CS
4 octets	255 octets					

En-tête	SID	TREP	00	02	Sous-message 2	CS
4 octets	255 octets					

…

En-tête	SID	TREP	xx	yy	Sous-message n	CS
4 octets	Longueur inférieure à 255 octets					

ou comme:

En-tête	SID	TREP	00	01	Sous-message 1	CS
4 octets	255 octets					

En-tête	SID	TREP	00	02	Sous-message 2	CS
4 octets	255 octets					

…

En-tête	SID	TREP	xx	yy	Sous-message n	CS
4 octets	255 octets					

En-tête	SID	TREP	xx	yy+1	CS
4 octets	4 octets				

(1) Types de messages

Le protocole de communication qui s'applique au téléchargement de données entre la VU et l'IDE réclame l'échange de 8 types de messages distincts.

La table qui suit en présente une synthèse.

Structure du message	En-tête 4 octets max.				Données 255 octets max.			Total de contrôle 1 octet
IDE -> **<- VU**	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	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	**TREP**	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 Req	10	**CS**
Service incompatible	80	F0	EE	03	7F	Sid Req	11	**CS**
Sous-fonction incompatible	80	F0	EE	03	7F	Sid Req	12	**CS**
Longueur du message incorrecte	80	F0	EE	03	7F	Sid Req	13	**CS**

Conditions non correctes ou erreur affectant la séquence d'interrogation	80	F0	EE	03	7F	Sid Req	22	**CS**
Demande excessive	80	F0	EE	03	7F	Sid Req	31	**CS**
Téléchargement (upload) refusé	80	F0	EE	03	7F	Sid Req	50	**CS**
Réponse en suspens	80	F0	EE	03	7F	Sid Req	78	**CS**
Données indisponibles	80	F0	EE	03	7F	Sid Req	FA	**CS**

Remarques:

- SID Req = SID de la demande correspondante
- TREP = le TRTP de la demande correspondante.
- La présence de cellules noires indique une absence de transmission.
- L'utilisation du terme «upload» (considéré à partir de l'IDE) 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 la VU).
- Cette table ne présente pas de compteur potentiel de sous-messages de 2 octets.
- Le lecteur désigne le numéro de lecteur, soit «1» (carte sur le lecteur du conducteur) soit «2» (carte sur le lecteur du convoyeur).
- Si le lecteur n'est pas précisé, la VU sélectionne le lecteur 1 s'il contient une carte et le lecteur 2 uniquement si l'utilisateur le sélectionne.
-

Demande d'établissement de la communication (SID 81)

DDP_005 Ce message est émis par l'IDE pour établir la liaison d'intercommunication avec la VU. Les communications initiales sont toujours effectuées à 9 600 bauds (jusqu'à ce que ce débit soit modifié à l'aide des services appropriés de contrôle des liaisons).

Réponse positive à une demande d'établissement de la communication (SID C1)

DDP_006 La VU émet ce message pour répondre positivement à une demande d'établissement de la communication. Il 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.

Demande d'ouverture d'une session de diagnostic (SID 10)

DDP_007 L'IDE émet un message de demande d'ouverture d'une session de diagnostic dans le but de solliciter une nouvelle session de diagnostic avec la VU. La sous-fonction «session par défaut» (81 Hex) indique qu'une session de diagnostic standard va être ouverte.

Réponse positive à une demande d'ouverture de session de diagnostic (SID 50)

DDP_008 La VU émet un message de réponse positive à une demande de diagnostic pour répondre positivement à une demande d'ouverture d'une session de diagnostic.

Service de contrôle de liaison (SID 87)

DDP_052 Le service de contrôle de liaison est utilisé par l'IDE pour initier une modification du débit en bauds. Cette opération comporte deux étapes. Dans la première étape, l'IDE propose une modification du débit en bauds, en indiquant le nouveau débit. À la réception d'un message positif de la VU, l'IDE envoie la confirmation du changement du débit en bauds à la VU (deuxième étape). L'IDE passe alors au nouveau débit en bauds. Après réception de la confirmation, la VU passe au nouveau débit en bauds.

Réponse positive au contrôle de liaison (SID C7)

DDP_053 La réponse positive au contrôle de liaison est délivrée par la VU sur demande du service de contrôle de liaison (première étape). À noter qu'aucune réponse n'est donnée à la demande de confirmation (deuxième étape).

Demande de téléchargement (upload) (SID 35)

DDP_009 L'IDE émet un message de demande de téléchargement afin de préciser à la VU qu'il réclame l'exécution d'une opération de téléchargement. Afin de satisfaire aux exigences de la norme ISO 14229, des données sont incluses concernant l'adresse, la taille et les caractéristiques de format des données demandées. Ces informations n'étant pas connues de l'IDE avant le téléchargement, l'adresse de mémoire est mise à 0, la structure est non cryptée et non compressée et la taille de la mémoire est mise au maximum.

Réponse positive à une demande de téléchargement (SID 75)

DDP_010 La VU émet un message de réponse positive à une demande de téléchargement pour signifier à l'IDE que la VU 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'IDE que les messages ultérieurs de réponse positive à une demande de transfert de données comporteront au maximum 00FF hex octets.

Demande de transfert de données (SID 36)

DDP_011 L'IDE émet une demande de transfert de données afin de préciser à la VU la nature des données à télécharger. Un paramètre de demande de transfert (TRTP) d'un octet indique de quel type de transfert il s'agit.

Il existe six types de transfert de données:
- Récapitulatif (TRTP 01),
- Activités associées à une date précise (TRTP 02),
- Évènements et anomalies (TRTP 03),
- Vitesse instantanée (TRTP 04),
- Données techniques (TRTP 05),
- Téléchargement de carte (TRTP 06).

DDP_054 Il est obligatoire pour l'IDE de demander un transfert de données du type «récapitulatif» (TRTP 01) au cours d'une session de téléchargement, car cela seul garantit que les certificats de la VU sont enregistrés sur le fichier téléchargé (et permet ainsi la vérification de la signature numérique).

Dans le deuxième cas de figure (TRTP 02), le message de demande de transfert de données comporte l'indication du jour civil (format `TimeReal`) auquel le téléchargement est associé.

Réponse positive à une demande de transfert de données (SID 76)

DDP_012 La VU 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 réclamées ainsi qu'un paramètre de réponse à une demande de transfert (TREP) correspondant à celui de la demande.

DDP_055 Dans le premier cas (TREP 01), la VU enverra des données destinées à aider l'opérateur de l'IDE dans le choix des données qu'ils souhaitent télécharger. Les informations contenues dans ce message sont les suivantes:
- Certificats de sécurité,
- Identification du véhicule,
- Date et heure actuelles sur la VU,
- Date la plus précoce et la plus tardive pour le téléchargement (données de la VU),
- Indications concernant la présence de cartes dans la VU.
- Téléchargements antérieurs vers une entreprise,
- Verrouillages d'entreprise,
- Contrôles précédents.

Demande de fin de transfert (SID 37)

DDP_013 L'IDE émet un message de demande de fin de transfert pour informer la VU que la session de téléchargement est terminée.

Réponse positive à une demande de fin de transfert (SID 77)

DDP_014 La VU émet un message de réponse positive à une demande de fin de transfert pour accuser réception de la demande de fin de transfert.

Demande d'arrêt de la communication (SID 82)

DDP_015 L'IDE émet un message de demande d'arrêt de la communication dans le but de rompre la liaison d'intercommunication avec la VU.

Réponse positive à une demande d'arrêt de la communication (SID C2)

DDP_016 La VU 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.

Accusé de réception d'un sous-message (SID 83)

DDP_017 L'IDE émet un accusé de réception de sous-message pour confirmer la réception des différentes parties d'un message transmis sous forme de sous-messages. Le champ de données contient le SID transmis par la VU 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 la VU par l'IDE
- MsgC indique la manifestation d'un problème affectant la réception du sous-message numéro MsgC.
  Demande de renvoi du sous-message concerné adressée à la VU par l'IDE.
- FFFF réclame l'interruption du message en cours de transmission.
  L'IDE peut recourir à ce code pour mettre un terme à la transmission du message envoyé par la VU et ce, quelle qu'en soit la raison.

Le système permet d'accuser (ou non) réception du dernier sous-message d'un message quelconque (octet LEN < 255) en recourant ou non à l'un quelconque de ces codes.

Composée de plusieurs sous-messages, la réponse de la VU s'énonce comme suit:

- Réponse positive à une demande de transfert de données (SID 76)

Réponses négatives (SID 7F)

DDP_018 La VU émet le message de réponse négative en réponse aux messages ci-dessus si elle s'avère dans l'impossibilité de satisfaire à la demande transmise. Les champs 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 incompatible
  Le SID de la demande n'est pas intelligible à la VU.
- 12 sous-fonction incompatible
  Le DS_ ou le TRTP de la demande ne sont pas intelligibles à la VU 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 d'interrogation
  Le service demandé n'est pas disponible ou la séquence des messages de demande est incorrecte.
- 31 demande excessive
  Le relevé (champ de données) du paramètre de la demande n'est pas valable.
- 50 téléchargement (upload) refusé
  La demande ne peut être exécutée (la VU est exploitée dans un mode inapproprié ou elle présente une anomalie interne).
- 78 réponse en suspens
  L'action réclamée ne peut être achevée dans le temps imparti et la VU 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 la VU (p. ex. absence d'insertion de carte…).

(2) Acheminement des messages

Pendant une procédure de téléchargement normale, l'acheminement des messages s'effectue habituellement comme suit:

IDE		VU
Demande d'établissement de la communication	⇨	
	⇦	Réponse positive
Demande d'ouverture d'une session de diagnostict	⇨	
	⇦	Réponse positive
Demande de téléchargement (upload)	⇨	
	⇦	Réponse positive
Demande de transfert de données - Récapitulatif	⇨	
	⇦	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 (champ 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

(3) Synchronisation

DDP_019 Dans des conditions d'exploitation normales, les paramètres de synchronisation dont la figure ci-après fournit l'illustration sont d'application:

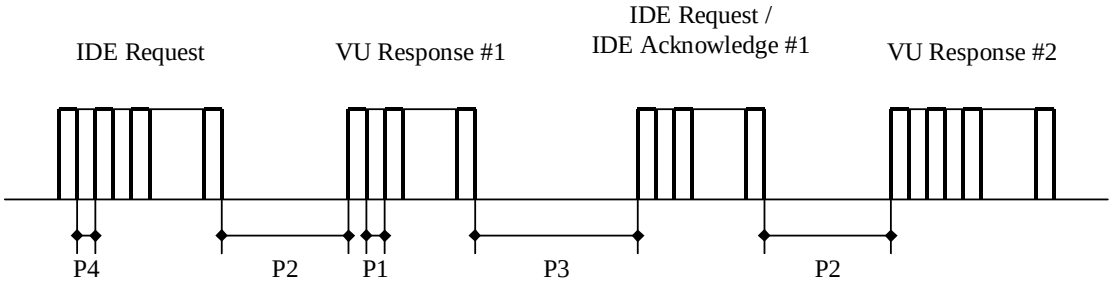


Figure 1 - Acheminement des messages, synchronisation

Où:
P1 = Temps interoctet caractérisant une réponse de la VU.
P2 = Temps ménagé entre la fin d'une demande de l'IDE et le début de la réponse de la VU ou entre la fin d'un accusé de réception de l'IDE et le début de la prochaine réponse de la VU.
P3 = Temps ménagé entre la fin d'une réponse de la VU et le début d'une nouvelle demande de l'IDE, entre la fin d'une réponse de la VU et le début d'un accusé de réception de l'IDE ou entre la fin d'une demande de l'IDE et le début d'une nouvelle demande de l'IDE dans l'éventualité où la VU manquerait à répondre.
P4 = Temps interoctet caractérisant une demande de l'IDE.
P5 = Valeur étendue de P3 pour le téléchargement de cartes.

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	1000 (*)
P3	10	5000
P4	5	20
P5	10	20 minutes

(*) Si la VU réagit en émettant une réponse négative contenant un code qui possède la signification suivante: «réception correcte de la demande, réponse en suspens», cette valeur est portée à la même limite supérieure que celle de P3.

(4) Traitement des erreurs

Si une erreur se manifeste pendant l'échange de messages, le plan d'acheminement des messages est modifié en fonction de l'équipement qui a décelé l'erreur et du message à l'origine de celle-ci.

Les figures 2 et 3 illustrent les procédures de traitement d'erreur appliquées respectivement à la VU et à l'IDE.

Phase d'établissement de la communication

DDP_020 Si l'IDE 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, celui-ci temporise alors pendant une période P3min avant d'émettre à nouveau la même demande.

DDP_021 Si la VU détecte une erreur dans la séquence provenant de l'IDE, celle-ci n'envoie aucune réponse; elle attend un autre message de demande d'établissement de la communication dans un délai P3max.

Phase de communication

Deux procédures de traitement d'erreur distinctes peuvent être définies:

1. La VU détecte une erreur de transmission de l'IDE

DDP_022 La VU procède à l'analyse de chaque message reçu afin de déceler toute erreur éventuelle de synchronisation, de structure des octets (p. ex. violations affectant les bits de départ et d'arrêt) ou de perte de verrouillage de trame (réception d'un nombre erroné d'octets, octet total de contrôle erroné).

DDP_023 Si la VU détecte l'une des erreurs susmentionnées, elle n'envoie aucune réponse et ne tient aucun compte du message reçu.

DDP_024 La VU peut détecter d'autres erreurs dans le format ou le contenu du message reçu (p. ex. un message incompatible), même si le message satisfait aux exigences de longueur et de contrôle du total; dans ce cas, la VU répond à l'IDE par un message de réponse négatif précisant la nature de l'erreur.

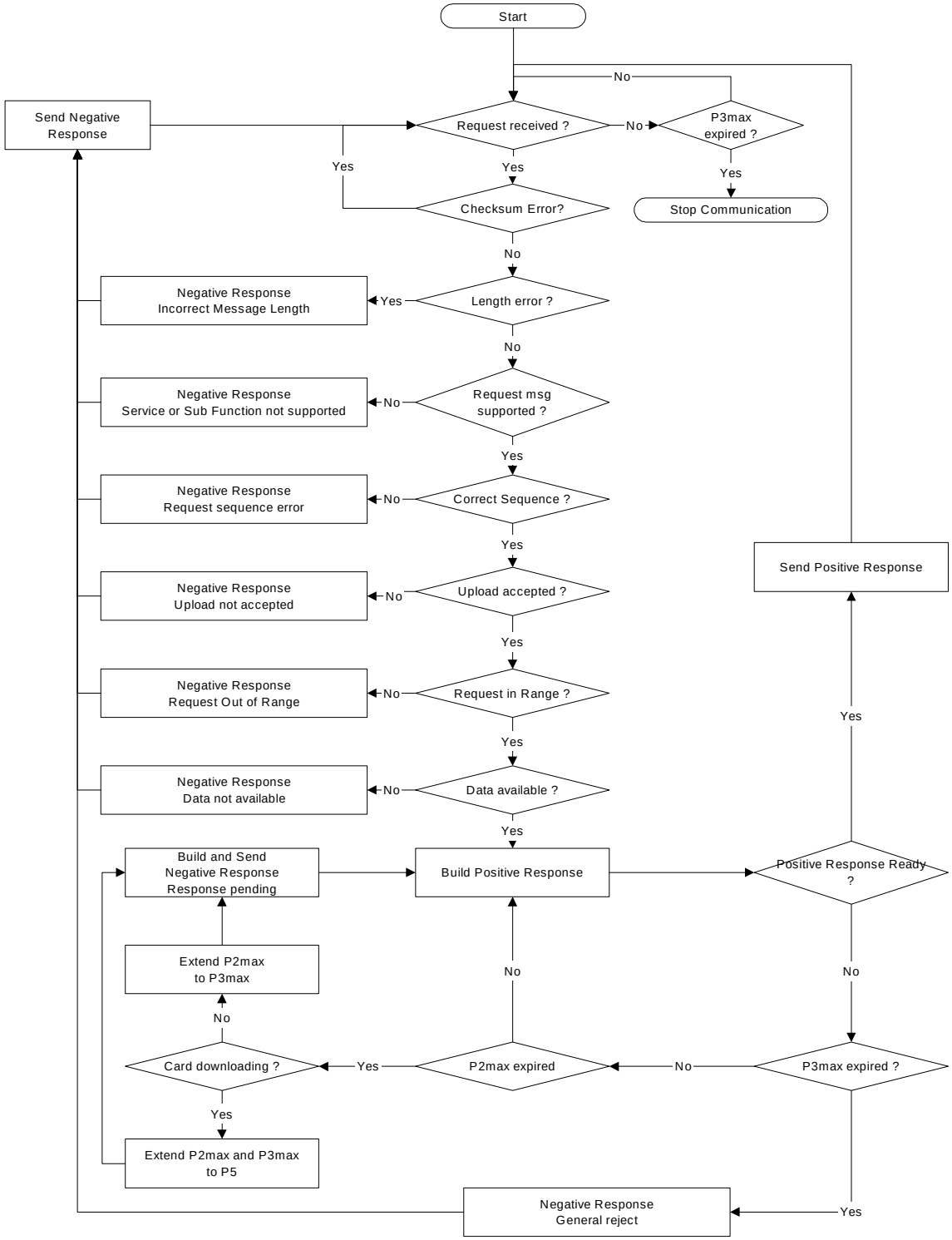


Figure 2 - Traitement d'erreur au niveau de la VU

2. L'IDE détecte une erreur de transmission de la VU

DDP_025 L'IDE procède à l'analyse de chaque message reçu afin de déceler toute erreur éventuelle de synchronisation, de structure des octets (p. ex. violations affectant les bits de départ et d'arrêt) ou de perte de verrouillage de trame (réception d'un nombre erroné d'octets, octet total de contrôle erroné).

DDP_026 L'IDE 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'IDE détecte une erreur ou si la VU ne lui envoie aucune réponse dans un délai 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 quelconque sera considéré comme une demande adressée à la VU.

DDP_028 L'IDE attend au moins une période de P3min avant d'entamer chaque transmission; la période d'attente se mesure depuis la dernière occurrence calculée d'un bit d'arrêt suivant la détection d'erreur.

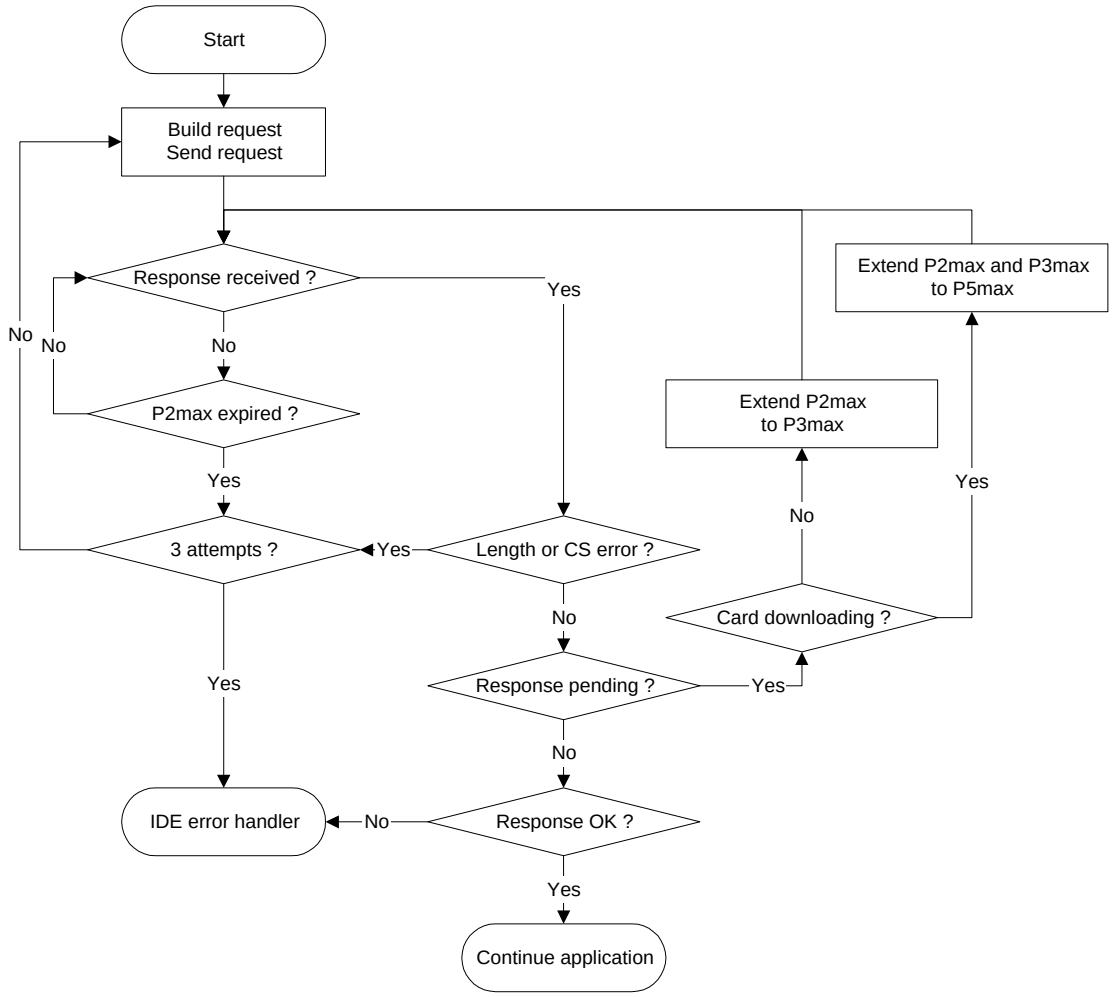


Figure3 - Traitement d'erreur au niveau de l'IDE

(5) Contenu des messages de réponse

Ce paragraphe traite du contenu des champs de données que comportent les différents messages de réponse positive.

Les éléments d'information sont définis dans l'appendice 1 (Dictionnaire de données).

Remarque: concernant les téléchargements de génération 2, toutes les données de niveau supérieur sont représentées dans un tableau des relevés, même s'il ne contient qu'un relevé. Un tableau de relevés débute avec un en-tête; cet en-tête contient le type de relevés, sa taille et le nombre total de relevés. Les tableaux de relevés sont intitulés «...RecordArray» (avec en-tête) dans les tableaux suivants.

Réponse positive à un récapitulatif de transfert de données

DDP_029 Le champ de données du message «Réponse positive à un récapitulatif de transfert de données» doit fournir les données ci-après dans l'ordre qui suit en vertu des SID 76 Hex, TREP 01 Hex et critères appropriés de séparation et de comptage des sous-messages:

Structure de données de génération 1

Élément de donnée	**Commentaire**
MemberStateCertificate VUCertificate	Certificats de sécurité de la VU
VehicleIdentificationNumber VehicleRegistrationIdentification	Identification du véhicule
CurrentDateTime	Date et heure actuelles sur la VU
VuDownloadablePeriod	Période téléchargeable
CardSlotsStatus	Catégorie de cartes insérées dans la VU
VuDownloadActivityData	Téléchargement précédent de la VU
VuCompanyLocksData	Tous les verrouillages d'entreprise mémorisés. Si cette section est vide, seule l'expression noOfLocks = 0 est envoyée.
VuControlActivityData	Tous les relevés de contrôle mémorisés dans la VU. Si cette section est vide, seule l'expression noOfControls = 0 est envoyée.

Signature	Signature RSA de toutes les données (hormis les certificats) à partir de VehicleIdentificationNumber jusqu'au dernier octet du dernier VuControlActivityData.

Structure de données de génération 2

Élément de donnée	**Commentaire**
MemberStateCertificateRecordArray	Certificat de l'État membre
VuCertificateRecordArray	Certificate de la VU
VehicleIdentificationNumberRecordArray	Identification du véhicule
VehicleRegistrationNumberRecordArray	Plaque minéralogique du véhicule
CurrentDateTimeRecordArray	Date et heure actuelles sur la VU
VuDownloadablePeriodRecordArray	Période téléchargeable
CardSlotsStatusRecordArray	Catégorie de cartes insérées dans la VU
VuDownloadActivityDataRecordArray	Téléchargement précédent de la VU
VuCompanyLocksRecordArray	Tous les verrouillages d'entreprise mémorisés. Si cette section est vide, un en-tête de tableau avec l'expression noOfRecords = 0 est envoyé .
VuControlActivityRecordArray	Tous les relevés de contrôle mémorisés dans la VU. Si cette section est vide, un en-tête de tableau avec l'expression noOfRecords = 0 est envoyé .
SignatureRecordArray	Signature ECC de toutes les données antérieures hormis les certificats.

Réponse positive à une demande de transfert de données relatives aux activités

DDP_030 Le champ de données du message «Réponse positive à une demande de transfert de données relatives aux activités» doit fournir les données ci-après dans l'ordre qui suit en vertu des SID 76 Hex, TREP 02 Hex et critères appropriés de séparation et de comptage des sous-messages:

Structure de données de génération 1

Élément de donnée	**Commentaire**
`TimeReal`	Date du jour de téléchargement
`OdometerValueMidnight`	Kilométrage à la fin de la journée téléchargée
`VuCardIWData`	Données relatives aux cycles d'insertion et de retrait des cartes. – Si cette section ne contient aucune donnée disponible, seule l'expression noOfVuCardIWRecords = 0 est envoyée. – Lorsque VuCardIWRecord figure à 00h00 (insertion de carte de la veille) ou à 24h00 (retrait de carte du lendemain), elle apparaît entièrement sur les deux jours concernés.
`VuActivityDailyData`	État des lecteurs à 00h00 et modifications d'activité mémorisés pour la journée téléchargée.
`VuPlaceDailyWorkPeriodData`	Données relatives aux emplacements mémorisés pour la journée téléchargée. Si cette section est vide, seule l'expression noOfPlaceRecords = 0 est envoyée.
`VuSpecificConditionData`	Données relatives aux conditions particulières mémorisées pour la journée téléchargée. Si cette section est vide, seule l'expression noOfSpecificConditionRecords = 0 est

		envoyée.
Signature		Signature RSA de toutes les données à partir de TimeReal jusqu'au dernier octet du dernier relevé de conditions particulières.

Structure de données de génération 2:

Élément de donnée	Commentaire
DateOfDayDownloadedRecordArray	Date du jour de téléchargement
OdometerValueMidnightRecordArray	Kilométrage à la fin de la journée téléchargée
VuCardIWRecordArray	Données relatives aux cycles d'insertion et de retrait des cartes. – Si cette section ne contient aucune donnée disponible, un en-tête de tableau avec l'expression noOfRecords = 0 est envoyé. – Lorsque VuCardIWRecord figure à 00h00 (insertion de carte de la veille) ou à 24h00 (retrait de carte du lendemain), elle apparaît entièrement sur les deux jours concernés.
VuActivityDailyRecordArray	État des lecteurs à 00h00 et modifications d'activité mémorisés pour la journée téléchargée.
VuPlaceDailyWorkPeriodRecordArray	Données relatives aux emplacements mémorisés pour la journée téléchargée. Si cette section est vide, un en-tête de tableau avec l'expression noOfRecords = 0 est envoyé.
VuGNSSCDRecordArray	Positions GNSS du véhicule si le temps de conduite continue du conducteur atteint un multiple de trois heures. Si cette section est vide, un en-tête de tableau avec l'expression noOfRecords = 0 est envoyé.
VuSpecificConditionRecordArray	Données relatives aux conditions particulières mémorisées pour la journée téléchargée. Si cette section est vide, un en-tête de tableau avec l'expression noOfRecords = 0 est envoyé.
SignatureRecordArray	Signature ECC de toutes les données antérieures.

Réponse positive à une demande de transfert de données relatives aux événements et anomalies

DDP_031 Le champ de données du message «Réponse positive à une demande de transfert de données relatives aux événements et anomalies» doit fournir les données ci-après dans l'ordre qui suit en vertu des SID 76 Hex, TREP 03 Hex et critères appropriés de séparation et de comptage des sous-messages:

Structure de données de génération 1

Élément de donnée	Commentaire
VuFaultData	Toutes les anomalies enregistrées ou en cours au sein de la VU. Si cette section est vide, seule l'expression noOfVuFaults = 0 est envoyée.
VuEventData	Tous les évènements enregistrés ou en cours au sein de la VU (hormis les dépassements de vitesse). Si cette section est vide, seule l'expression noOfVuEvents = 0 est envoyée.
VuOverSpeedingControlData	Données relatives au dernier contrôle de dépassement de vitesse (valeur par défaut en l'absence de données).
VuOverSpeedingEventData	Tous les évènements en matière de dépassements de vitesse enregistrés dans la VU. Si cette section est vide, seule l'expression noOfVuOverSpeedingEvents = 0 est envoyée.

VuTimeAdjustmentData	Tous les évènements de réglage horaire mémorisés dans la VU (hormis le cadre d'étalonnage complet). Si cette section est vide, seule l'expression noOfVuTimeAdjRecords = 0 est envoyée.
Signature	Signature RSA de toutes les données à partir de noOfVuFaults jusqu'au dernier octet du dernier relevé de réglage horaire.

Structure de données de génération 2:

Élément de donnée	**Commentaire**
VuFaultRecordArray	Toutes les anomalies enregistrées ou en cours au sein de la VU. Si cette section est vide, un en-tête de tableau avec l'expression noOfRecords = 0 est envoyé.
VuEventRecordArray	Tous les évènements enregistrés ou en cours au sein de la VU (hormis les dépassements de vitesse). Si cette section est vide, un en-tête de tableau avec l'expression noOfRecords = 0 est envoyé.
VuOverSpeedingControlDataRecordArray	Données relatives au dernier contrôle de dépassement de vitesse (valeur par défaut en l'absence de données).
VuOverSpeedingEventRecordArray	Tous les évènements en matière de dépassements de vitesse enregistrés dans la VU. Si cette section est vide, un en-tête de tableau avec l'expression noOfRecords = 0 est envoyé.
VuTimeAdjustmentRecordArray	Tous les évènements de réglage horaire mémorisés dans la VU (hormis le cadre d'étalonnage complet). Si cette section est vide, un en-tête de tableau avec l'expression noOfRecords = 0 est envoyé.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	Signature ECC de toutes les données antérieures.

Réponse positive à une demande de transfert de données relatives à la vitesse du véhicule

DDP_032 Le champ de données du message «Réponse positive à une demande de transfert de données relatives à la vitesse du véhicule» doit fournir les données ci-après dans l'ordre qui suit en vertu des SID 76 Hex, TREP 04 Hex et critères appropriés de séparation et de comptage des sous-messages:

Structure de données de génération 1

Élément de donnée	Commentaire
VuDetailedSpeedData	Toutes les données se rapportant à l'évolution de la vitesse du véhicule 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:

Élément de donnée	Commentaire
VuDetailedSpeedBlockRecordArray	Toutes les données se rapportant à l'évolution de la vitesse du véhicule pendant une minute au cours de laquelle le véhicule était en mouvement 60 valeurs de vitesse par minute (une par seconde).
SignatureRecordArray	Signature ECC de toutes les données antérieures.

Réponse positive à une demande de transfert de données techniques

DDP_033 Le champ de données du message «Réponse positive à une demande de transfert de données techniques» doit fournir les données ci-après dans l'ordre qui suit en vertu des SID 76 Hex, TREP 05 Hex et critères appropriés de séparation et de comptage des sous-messages:

Structure de données de génération 1

Élément de donnée	Commentaire
VuIdentification	
SensorPaired	
VuCalibrationData	Tous les relevés d'étalonnage mémorisés dans la VU.
Signature	Signature RSA de toutes les données à partir de vuManufacturerName jusqu'au dernier octet du dernier VuCalibrationRecord.

Structure de données de génération 2:

Élément de donnée	Commentaire
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Tous les couplages MS mémorisés dans la VU.
VuSensorExternalGNSSCoupledRecordArray	Tous les couplages du dispositif GNSS externe mémorisés dans la VU
VuCalibrationRecordArray	Tous les relevés d'étalonnage mémorisés dans la VU.
VuCardRecordArray	Toutes les données relatives à l'insertion de carte mémorisées dans la VU.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Signature ECC de toutes les données antérieures.

2. Archivage 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 la VU, l'IDE doit enregistrer au sein d'un seul et même fichier physique toutes les données transmises par la VU pendant cette session de téléchargement dans des messages de réponse positive concernant le transfert de données. La sauvegarde de ces données en exclut les en-têtes de message, compteurs de sous-messages, sous-messages vides et totaux de contrôle; mais elle inclut les SID et TREP (du premier sous-message dans l'éventualité où leur nombre serait supérieur à l'unité).

Protocole de téléchargement des cartes tachygraphiques

3. Champ d'application

Ce paragraphe comporte une description du téléchargement direct vers un IDE des données de carte mémorisées sur une carte tachygraphique. L'IDE n'appartient pas à l'environnement sécurisé; aucune authentification n'a donc lieu entre la carte et l'IDE.

4. Définitions

Session de téléchargement: chaque fois que le système procède à une opération de téléchargement des données enregistrées sur une carte à circuit(s) intégré(s). Cette session couvre l'ensemble de la procédure, de la réinitialisation de l'ICC par un IFD à la désactivation de l'ICC (retrait de la carte ou réinitialisation suivante).

Fichier de données signé: fichier enregistré sur l'ICC. Ce fichier est transféré en clair vers l'IFD. Sur l'ICC, le fichier est haché et signé; la signature est transférée vers l'IFD.

5. 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 `CI`. Ces informations à caractère facultatif ne sont protégées par aucune signature numérique.
- Téléchargement des EF Card_Certificate (ou CardSignCertificate) et CA_Certificate. Ces informations ne sont protégées par aucune signature numérique.
  Il faut impérativement télécharger ces fichiers lors de toute session de téléchargement.

- Téléchargement des autres EF de données d'application (dans le DF Tachygraphe et Tachograph_G2 DF le cas échéant) sauf l'EF Card_Download. Ces informations sont protégées par une signature numérique.
- Il y a lieu de télécharger au moins les EF Application_Identification et ID lors de toute session de téléchargement.
  - Lors du téléchargement d'une carte de conducteur, il faut également procéder obligatoirement au téléchargement des EF suivants:
    - Events_Data,
    - Faults_Data,
    - Driver_Activity_Data,
    - Vehicles_Used,
    - Places,
    - GNSS_Places (le cas échéant),
    - Control_Activity_Data,
    - Specific_Conditions.
- 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.
- Lors du téléchargement d'une carte d'atelier, il convient de réinitialiser le compteur d'étalonnage enregistré dans
- Lors du téléchargement d'une carte d'atelier, l'EF Sensor_Installation_Data n'est pas téléchargé.

(1) Séquence d'initialisation

DDP_036 L'IDE doit lancer la séquence en procédant comme suit:

Carte	*Sens*	*IDE/IFD*	*Signification/Remarques*
	⇦	Réinitialisation matérielle	
ATR	⇨		

L'utilisateur a l'option de recourir à la PPS pour passer à un débit supérieur à condition que l'ICC en assure la prise en charge.

(2) Séquence de téléchargement des fichiers de données non signés

DDP_037 La séquence de téléchargement des EF ICC, IC, Card_Certificate (ou CardSignCertificate) et CA_Certificate se présente comme suit:

Carte	*Sens*	*IDE/IFD*	*Signification/Remarques*
	⇦	**Select File**	Sélection par le biais d'identificateurs de fichier
OK	⇨		
	⇦	**Read Binary**	Si le volume des données que contient le fichier est supérieur à la capacité de la mémoire tampon du lecteur ou de la carte, la commande doit être réitérée jusqu'à ce que les données que contient ce fichier aient été extraites dans leur intégralité.
Données	⇨	Sauvegarder les données sur l'ESM	selon **6** Format d'archivage des données
OK			

Note 1: avant de sélectionner l'EF Card_Certificate (ou CardSignCertificate), il convient de sélectionner préalablement l'application tachygraphique (sélection opérée par IDA).

Note 2: la sélection et la lecture d'un fichier sont également réalisables en une étape à l'aide de la commande Read Binary et d'un identifiant EF court.

(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	Dir	IDE/IFD	Signification/Remarques
	⇦	**Select File**	
OK	⇨		
	⇦	**Procéder au hachage du fichier (Hash of File)**	Permet de calculer la valeur de hachage par rapport au contenu du fichier sélectionné en appliquant l'algorithme de hachage prescrit en conformité avec l'appendice 11. 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 le tampon ou la carte ne peut en contenir, la commande doit être réitérée jusqu'à ce que les données que contient ce fichier aient été extraites dans leur intégralité.
Données OK	⇨	Sauvegarder les données sur l'ESM	selon **6** Format d'archivage des données
	⇦	**PSO: Compute Digital Signature**	
Exécution 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 l'ESM	selon **6** Format d'archivage des données

Remarque: la sélection et la lecture d'un fichier sont également réalisables en une étape à l'aide de la commande Read Binary et d'un identifiant EF court. Dans ce cas, l'EF peut être sélectionné et lu avant d'exécuter la commande procédant au hachage du fichier.

(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	Dir	IDE/IFD	Signification/Remarques
	⇦	**Select File** EF Card_Download	Sélection par le biais d'identificateurs de fichier
OK	⇨		
	⇦	**Update Binary** NoOfCalibrationsSinceDownload = '00 00'	
réinitialise le nombre de téléchargements de la carte			
OK	⇨		

Remarque: la sélection et la mise à jour d'un fichier sont également réalisables en une étape à l'aide de la commande Update Binary et d'un identifiant EF court.

6. Format d'archivage des données

(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 d'archivage exécutée après leur transfert 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 l'ESM.

(2) Format des fichiers

DDP_041 Le format des fichiers se présente comme la concaténation de plusieurs objets TLV.

DDP_042 La balise associée à un EF doit prendre la forme du FDI du fichier assorti de l'appendice «00».

DDP_043 La balise associée à la signature d'un EF doit prendre la forme du FDI du fichier assorti de l'appendice «01».

DDP_044 La longueur correspond à une valeur exprimée par deux octets. Cette valeur détermine le nombre d'octets affectés au champ valeur. La valeur «FF FF» que contient le champ 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 que recèle le fichier concerné.

Définition	Signification	Longueur
FDI (2 octets) ||"00"	Balise pour EF (FDI)	3 octets
FDI (2 octets) ||"01"	Balise pour signature d'EF (FDI)	3 octets
xx xx	Longueur du champ valeur	2 octets

Exemple de données enregistrées dans un fichier de téléchargement sur un ESM:

Balise	Longueur	Valeur
00 02 00	00 11	Données du EF ICC
C1 00 00	00 C2	Données du EF Card_Certificate
		...
05 05 00	0A 2E	Données du EF Vehicles_Used
05 05 01	00 80	Signature du EF Vehicles_Used

- Téléchargement d'une carte tachygraphique par l'intermédiaire d'une unité embarquée sur véhicule.

DDP_047 La VU doit autoriser le téléchargement du contenu d'une carte de conducteur insérée dans le lecteur d'un IDE connecté.

DDP_048 Cet IDE doit envoyer un message «Demande de transfert de données du type téléchargement de carte» à la VU pour lancer ce mode de transmission (cf. □(1073774592)).

DDP_049 À ce stade, la VU doit procéder au téléchargement de la carte dans son intégralité, fichier par fichier, en conformité avec le protocole de téléchargement de carte défini au paragraphe 0 ainsi qu'à l'envoi à l'IDE de toutes les données extraites de la carte dans le format de fichier TLV approprié (cf. □6(2)) et encapsulées dans un message «Réponse positive à une demande de transfert de données».

DDP_050 L'IDE 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, TREP, compteurs de sous-messages et totaux de contrôle) et les enregistrer dans un seul et même fichier physique conformément à la description présentée au paragraphe □2.

DDP_051 Ensuite, la VU doit, selon le cas, procéder à une actualisation du fichier de données des activités de contrôle ou de téléchargement de cartes (Control_Activity_Data ou Card_Download) sur la carte du conducteur.

FR

APPENDICE 8. PROTOCOLE D'ETALONNAGE

TABLE DES MATIERES

1. Introduction

Le présent appendice traite des modalités d'échange des données entre un appareil d'essai et une unité embarquée sur véhicule par l'intermédiaire de la ligne K. Cette ligne fait partie intégrante de l'interface d'étalonnage décrite à l'appendice 6. Le présent appendice traite aussi du contrôle de la ligne de signalisation d'entrée/sortie exercé au niveau du connecteur d'étalonnage.

L'établissement de communications sur la ligne K est décrit à la section 4 «Services de communication de communication».

Le présent appendice s'appuie sur le concept de «sessions» de diagnostic pour déterminer la portée du contrôle de la ligne K au gré de l'évolution des modalités d'échange. La session par défaut est la «StandardDiagnosticSession», où toutes les données que contient une unité embarquée sur véhicule sont susceptibles d'en être extraites, mais aucune donnée ne peut être enregistrée sur cette unité.

La sélection de la session de diagnostic fait l'objet d'une description détaillée à la section 5 «Services de gestion de gestion».

Le présent appendice s'applique aux deux générations de VU et de cartes d'atelier, conformément aux exigences d'interopérabilité établies par le présent règlement.

CPR_001 La «ECUProgrammingSession» autorise l'entrée de données au sein de l'unité embarquée sur véhicule. En cas d'entrée de données d'étalonnage, l'unité embarquée sur véhicule doit en outre être exploitée en mode ÉTALONNAGE.

Le transfert de données par l'intermédiaire de la ligne K fait l'objet d'une description détaillée à la section □ «Services de transmission de données de transmission de données». Les formats des données transférées sont décrits en détail à la section 8 «Structures des dataRecords».

CPR_002 «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 fait l'objet d'une description à la section 7 «Contrôle des impulsions d'essai – Unité fonctionnelle de contrôle des entrées/sortiesrôle 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, la VU doit réagir correctement à toute adresse d'appareil d'essai. L'adresse physique de la VU s'énonce comme suit: 0xEE.

2. Terminologie, définitions et références

Les protocoles, messages et codes d'erreur sont principalement basés sur un projet de norme ISO 14229-1 (Véhicules routiers — Systèmes de diagnostic — Partie 1: services de diagnostic, version 6 du 22 février 2001).

Des codages d'octets et autres valeurs hexadécimales s'utilisent lors de la définition des identificateurs de service, de l'élaboration des demandes et réponses de service et de la configuration des paramètres standard.

Le terme «appareil d'essai» fait référence à l'équipement utilisé pour saisir des données de programmation/étalonnage dans la VU.

Les termes «client» et «serveur» font respectivement référence à l'appareil d'essai et à la VU.

Le terme ECU (*Electronic Control Unit*) signifie «unité de commande électronique» et s'applique à la VU.

Références:

ISO 14230-2: Véhicules routiers — Systèmes de diagnostic — Protocole à mots clés 2000 — Partie 2: Couche de 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 et auxquels doit pourvoir le tachygraphe.

CPR_004 Ce tableau indique quels sont les services disponibles lors d'une session de diagnostic active.

- La **1re colonne** répertorie les services disponibles.
- La **2e colonne** indique le numéro de section qui présente une description détaillée du service considéré dans le présent appendice.
- La **3e colonne** indique les valeurs affectées à l'identificateur de service dans les messages de demande de service.
- La **4e colonne** précise quels sont les services de la «**StandardDiagnosticSession**» (**SD**) dont la mise en œuvre dans la VU est indispensable.
- La **5e colonne** précise quels sont les services de la «**ECUAdjustmentSession**» (**ECUAS**) dont la mise en œuvre est indispensable 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 la VU.
- La **6e colonne** précise quels sont les services de la «**ECUProgrammingSession**» (**ECUPS**) dont la mise en œuvre est indispensable pour procéder à la programmation des paramètres d'exploitation dans la VU.

			Sessions de diagnostic		
Noms des services de diagnostic	**Section n°**	**Valeurs affectées aux identificateurs de service**	**SD**	**ECUAS**	**ECUPS**
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

Tableau 1 - Récapitulatif des valeurs affectées aux identificateurs de service

■ Ce symbole rappelle le caractère obligatoire du service correspondant pendant cette session de diagnostic.

Aucun symbole n'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-après:

Nom du service	*Description*
StartCommunication	Le client demande le lancement d'une session de communication avec un ou plusieurs serveur(s).
StopCommunication	Le client demande l'arrêt de la session de communication en cours.

Nom du service	*Description*
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 d'exploitation souhaité.

4.1. Service StartCommunication

CPR_006 À la réception d'une primitive d'indication StartCommunication, la VU vérifie si l'établissement de la liaison d'intercommunication requise est envisageable dans les conditions présentes. Les conditions d'établissement d'une liaison d'intercommunication font l'objet d'une description détaillée dans le document ISO 14230-2.

CPR_007 Ensuite, la VU 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 VU déjà initialisée (et entrée en session de diagnostic) reçoit une nouvelle demande StartCommunication (p.ex. en raison d'une reprise sur incident au niveau de l'appareil d'essai), cette demande doit être acceptée et la VU réinitialisée.

CPR_009 Si, pour une raison quelconque, l'établissement de la liaison d'intercommunication s'avère impossible, la VU doit continuer à fonctionner dans les mêmes conditions qu'immédiatement avant la tentative d'établissement d'une liaison d'intercommunication.

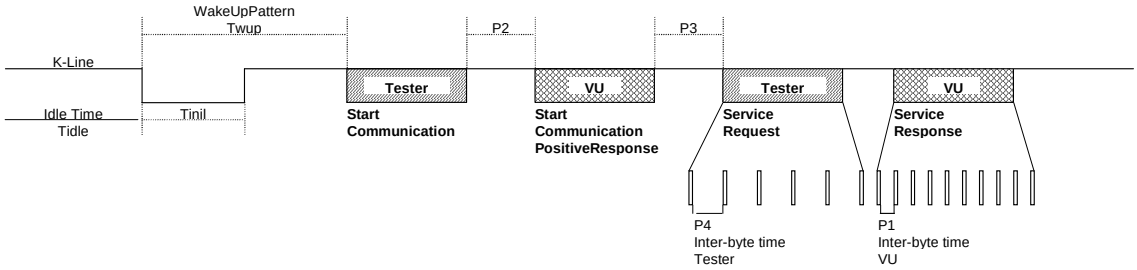
CPR_010 Le message de demande StartCommunication doit comporter une adresse physique.

CPR_011 L'initialisation de la VU pour les services est réalisée par la méthode d'initialisation rapide.
- Il existe un temps d'inoccupation préalable à toute activité.
- L'appareil d'essai envoie ensuite une configuration d'initialisation.
- Toutes les informations nécessaires à l'établissement d'une communication sont contenues dans la réponse de la VU.

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,
- la VU attend la première demande en provenance de l'appareil d'essai,
- la VU se trouve en mode de diagnostic par défaut, autrement dit le mode StandardDiagnosticSession;
- la ligne de signalisation d'entrée/sortie d'étalonnage est dans son état d'exploitation par défaut, à savoir, désactivée.

CPR_014 Le débit 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 (Wup) sur la ligne K. Cette trame débute au terme d'un délai d'inoccupation de la ligne K suivi d'un temps de Tinil. L'appareil d'essai émet le premier bit du service StartCommunication au terme d'un délai de Twup suivi du premier front descendant.



K-Line	*Ligne K*
Idle time Tidle	Temps d'inoccupation Tidle
WakeUp pattern Twup	Trame de réveil Twup
Tinil	Tinil

K-Line	*Ligne K*
Tester	Appareil d'essai
Start communication	Lancer la communication
VU	Unité embarquée sur le véhicule
Start communication positive response	Réponse positive pour le lancement de la communication
tester	Appareil d'essai
VU	Unité embarquée sur le véhicule
Service response	Réponse à la demande de service
Service request	Demande de service
P4 interbyte time tester	Appareil d'essai - Délai interoctet P4
P1 interbyte time VU	VU - Délai interoctet P1

CPR_017 Les valeurs de synchronisation propres à l'initialisation rapide et aux communications en général font l'objet d'une description détaillée dans les tableaux ci-après. Pour ce qui concerne le temps d'inoccupation, plusieurs possibilités sont envisageables:

- Première transmission après mise en marche, Tidle = 300 ms.
- Après achèvement du Service StopCommunication, Tidle = P3 min.
- Après interruption d'une communication pour cause de dépassement du temps imparti P3 max., Tidle = 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 propres à l'initialisation rapide

Paramètre de		*Valeurs minimales admises (ms)*	*Valeurs maximales admises (ms)*
synchronisation	**Description des paramètres**	**min.**	**max.**
P1	Délai interoctet à respecter dans l'attente d'une réponse de la VU	0	20
P2	Laps de temps entre une demande de l'appareil d'essai et une ou deux réponse(s) de la VU	25	250
P3	Laps de temps entre la fin des réponses de la VU et le début d'une nouvelle demande émise par l'appareil d'essai	55	5000
P4	Délai interoctet à respecter dans l'attente d'une demande émise par l'appareil d'essai	5	20

Tableau 4 - Valeurs de temporisation 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 de 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	**StartCommunication Request Service Id**	**81**	**SCR**
#5	Total de contrôle	00-FF	CS

Tableau 5 - Message StartCommunication Request

Octet #	*Nom de 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	**StartCommunication Positive Response Service Id**	**C1**	**SCRPR**
#6	Octet clé 1	EA	KB1
#7	Octet clé 2	8F	KB2
#8	Total de contrôle	00-FF	CS

Tableau 6 - Message StartCommunication Positive Response

CPR_019 Il n'y a pas de réponse négative au message StartCommunication Request. Faute de message de réponse positive à transmettre, la VU n'est pas initialisée, aucune donnée n'est émise et le système demeure en mode d'exploitation 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, la VU doit vérifier si les conditions en vigueur permettent d'interrompre la communication en cours. Si tel est le cas, la VU doit exécuter toutes les opérations requises pour mettre un terme à cette communication.

CPR_021 Si une interruption de la communication est envisageable, la VU 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 s'avère impossible d'interrompre la communication concernée, la VU doit émettre une primitive de réponse StopCommunication en recourant au paramètre de réponse négative sélectionné.

CPR_023 Si la VU détecte un dépassement du délai P3max, la communication est interrompue sans s'accompagner de l'émission d'aucune 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 de 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	**StopCommunication Request Service Id**	**82**	**SPR**
#6	Total de contrôle	00-FF	CS

Tableau 7 - Message StopCommunication Request

Octet #	*Nom de 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	**StopCommunication Positive Response Service Id**	**C2**	**SPRPR**
#6	Total de contrôle	00-FF	CS

Tableau 8 - Message StopCommunication Positive Response

Octet #	*Nom de 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	**negative Response Service Id**	**7F**	**NR**
#6	StopCommunication Request Service Identification	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Total de contrôle	00-FF	CS

Tableau 9 - Message StopCommunication Negative Response

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 ne coupe éventuellement la communication. Ce service, envoyé périodiquement, maintien en activité la session de diagnostic et la communication en remettant à zéro le compteur P3 à chaque demande de prestation.

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 de 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	**TesterPresent Request Service Id**	**3E**	**TP**
#6			RESPREQ_Y
	Sous-fonction = responseRequired = [oui	01	RESPREQ_N
	non]	02	O
#7	Total de contrôle	00-FF	CS

Tableau 10 - Message TesterPresent Request

CPR_080 Si le paramètre responseRequired est «oui», le serveur répondra par le message positif suivant. Si le paramètre est «non», le serveur n'envoie pas de réponse.

Octet #	*Nom de 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	**TesterPresent Positive Response Service Id**	**7E**	**TPPR**
#6	Total de contrôle	00-FF	CS

Tableau 11 - Message TesterPresent Positive Response

CPR_081 Le service accepte les codes de réponse négative suivants:

Octet #	*Nom de 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	**negative Response Service Id**	**7F**	**NR**
#6	TesterPresent Request Service Identification	3E	TP
#7	responseCode = [SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
	incorrectMessageLength]	13	RC_IML
#8	Total de contrôle	00-FF	CS

Tableau 12 - Message TesterPresent Negative Response

5. Services de gestion

Les services disponibles font l'objet d'une description détaillée dans le tableau ci-après:

Nom du service	*Description*
StartDiagnosticSession	Le client demande le lancement d'une session de diagnostic avec une VU.
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 permettre des services spécifiques du constructeur du véhicule qui ne font pas partie du 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 la VU,
- la VU doit toujours ouvrir la StandardDiagnosticSession lorsqu'elle est mise sous tension. Si aucune autre session de diagnostic n'est ouverte, la StandardDiagnosticSession doit rester ouverte aussi longtemps que la VU est sous tension,

- si une session de diagnostic déjà ouverte a été demandée par l'appareil d'essai, la VU envoie un message de réponse positive;
- lorsque l'appareil d'essai demande une nouvelle session de diagnostic, la VU envoie d'abord un message de réponse positive StartDiagnosticSession avant que la nouvelle session ne s'ouvre dans la VU. Si la VU n'a pu ouvrir la nouvelle session de diagnostic demandée, elle envoie un message de réponse négative à StartDiagnosticSession et la session en cours se poursuit.

CPR_026 Le lancement d'une session de diagnostic n'est envisageable qu'à la condition qu'une communication ait été préalablement établie entre le client et la VU.

CPR_027 Les paramètres de synchronisation définis dans le Tableau 4 deviendront actifs au terme de l'exécution réussie d'une StartDiagnosticSession, pour autant que le message de demande comporte le paramètre diagnosticSession défini sur «StandardDiagnosticSession» dans l'éventualité où une autre session de diagnostic aurait été préalablement 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 de 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	**StartDiagnosticSession Request Service Id**	**10**	**STDS**
#6	diagnosticSession = [une valeur extraite du Tableau 17]	xx	DS_…
#7	Total de contrôle	00-FF	CS

Tableau 14 - Message StartDiagnosticSession Request

Octet #	*Nom de 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	**StartDiagnosticSession Positive Response Service Id**	**50**	**STDSPR**
#6	diagnosticSession = [même valeur que l'octet 6 du Tableau 14]	xx	DS_…
#7	Total de contrôle	00-FF	CS

Tableau 15 - Message StartDiagnosticSession Positive Response

Octet #	*Nom de 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	**Negative Response Service Id**	**7F**	**NR**
#6	StartDiagnosticSession Request Service Id	10	STDS

Octet #		*Nom de paramètre*	*Valeur hex.*	*Mnémonique*
#7	ResponseCode =	[subFunctionNotSupported [a]	12	RC_SFNS
		incorrectMessageLength [b]	13	RC_IML
		conditionsNotCorrect [c]	22	RC_CNC
#8		Total de contrôle	00-FF	CS

Tableau 16 - Message StartDiagnosticSession Negative Response

[a] - La valeur introduite dans l'octet 6 du message de demande n'est pas prise en charge, c.-à-d. pas dans le Tableau 17,
[b] – la longueur du message est incorrecte,
[c] – les critères pour la demande StartDiagnosticSession ne sont pas remplis.

5.1.3 Définition du paramètre

CPR_029 Le service StartDiagnosticSession utilise le paramètre ***diagnosticSession (DS_)*** pour sélectionner le comportement particulier du ou des serveurs. Les sessions de diagnostic qui suivent sont précisées dans le présent document:

Hex.	*Description*	*Mnémonique*
81	**StandardDiagnosticSession**	**SD**
	Cette session de diagnostic permet d'activer tous les services indiqués dans le **Tableau 1 colonne 4 «SD».** Ces services autorisent l'extraction de données enregistrées sur un serveur (VU). Cette session de diagnostic ne devient active qu'après la réussite de la phase d'initialisation entre client (appareil d'essai) et serveur (VU). Cette session de diagnostic est susceptible d'être écrasée par d'autres sessions de diagnostic spécifiées dans ce chapitre.	
85	**ECUProgrammingSession**	**ECUPS**
	Cette session de diagnostic permet d'activer tous les services indiqués dans le **Tableau 1 colonne 6 «ECUPS».** Ces services prennent en charge la programmation de la mémoire d'un serveur (VU). Cette session de diagnostic est susceptible d'être écrasée par d'autres sessions de diagnostic spécifiées dans cette Section.	
87	**ECUAdjustmentSession**	**ECUAS**
	Cette session de diagnostic permet d'activer tous les services indiqués dans le **Tableau 1 colonne 5 «ECUAS».** Ces services prennent en charge le contrôle des entrées/sorties d'un serveur (VU). Cette session de diagnostic est susceptible d'être écrasée par d'autres sessions de diagnostic spécifiées dans ce chapitre.	

Tableau 17 - Définition des valeurs diagnosticSession

5.2. Service SecurityAccess

Il n'est possible d'écrire des données d'étalonnage que si la VU est en mode ÉTALONNAGE. Outre l'insertion d'une carte d'atelier valide dans le lecteur approprié de la VU, il est indispensable d'entrer le numéro d'identification individuel adéquat dans la VU pour avoir accès au mode ÉTALONNAGE.

Lorsque la VU est en mode ÉTALONNAGE ou CONTRÔLE, il est également possible d'accéder à la ligne E/S d'étalonnage.

Le service SecurityAccess permet d'introduire le numéro d'identification individuel et d'indiquer à l'appareil d'essai si la VU est exploitée ou non en mode ÉTALONNAGE.

Le système permet de recourir à d'autres méthodes pour entrer ce numéro d'identification individuel.

5.2.1 Description des messages

Le service SecurityAccess comporte l'exécution d'un message SecurityAccess «requestSeed» (demande de germe), suivi le cas échéant d'un message SecurityAccess «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 véhicule est prête à accepter un PIN (numéro d'identification individuel).

CPR_034 Si l'unité embarquée sur véhicule est déjà en mode ÉTALONNAGE, elle répond à la demande qui lui est adressée par l'envoi d'un «germe» de 0x0000 en utilisant le service SecurityAccess Positive Response.

CPR_035 Si l'unité embarquée sur 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 SecurityAccess Positive Response.

CPR_036 Si l'unité embarquée sur 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, parce que ce dernier n'en contient aucune ou que l'unité embarquée sur véhicule attend la transmission du PIN requis par une autre méthode, celle-ci doit répondre à la demande qui lui est adressée par l'envoi d'une réponse négative accompagnée d'un code de réponse conditionsNotCorrectOrRequestSequenceError.

CPR_037 En définitive, l'appareil d'essai devra recourir au message SecurityAccess "sendKey" pour transmettre un PIN à l'unité embarquée sur véhicule. Pour ménager le temps nécessaire à l'exécution du processus d'authentification de la carte, la VU devra recourir au code de réponse négative requestCorrectlyReceived-ResponsePending (demande bien reçue — réponse suit) afin de prolonger le temps de réponse. Le temps de réponse ne devra cependant pas dépasser 5 minutes. Dès que le service demandé est exécuté, la VU 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 la VU jusqu'à ce que le service demandé soit exécuté et le message de réponse finale envoyé.

CPR_038 L'unité embarquée sur véhicule ne doit répondre à cette demande en utilisant le service SecurityAccess Positive Response qu'à la condition d'être exploitée en mode ÉTALONNAGE.

CPR_039 Dans les cas énumérés ci-après, l'unité embarquée sur véhicule doit répondre à cette demande par une réponse négative accompagnée de l'un des codes de réponse suivants:

- subFunctionNot supported: format non valable pour le paramètre de la sous-fonction (accessType),
- conditionsNotCorrectOrRequestSequenceError: unité embarquée sur véhicule pas prête à accepter l'entrée 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 la tentative d'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 de 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	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – requestSeed	7D	AT_RSD
#7	Total de contrôle	00-FF	CS

Tableau 18 - Message SecurityAccess Request- requestSeed

Octet #	*Nom de 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	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – requestSeed	7D	AT_RSD
#7	Seed High	00-FF	SEEDH
#8	Seed Low	00-FF	SEEDL
#9	Total de contrôle	00-FF	CS

Tableau 19 - Message SecurityAccess - requestSeed Positive Response

Octet #	*Nom de 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	negativeResponse Service Id	7F	NR
#6	SecurityAccess Request Service Id	27	SA
#7	responseCode =		
	[conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
#8	Total de contrôle	00-FF	CS

Tableau 20 - Message SecurityAccess Negative Response

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 de 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	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – sendKey	7E	AT_SK
#7 à #m+6	Clé#1 (sup.)		
	…	xx	
	Clé #m (inf., la valeur de m doit être comprise entre 4 et	⋯	
	8 inclus)	xx	KEY
#m+7	Total de contrôle	00-FF	CS

Tableau 21 - Message SecurityAccess Request - sendKey

Octet #	*Nom de paramètre*	*Valeur hex.*	*Mnémonique*

Octet #	*Nom de 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	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – sendKey	7E	AT_SK
#7	Total de contrôle	00-FF	CS

Tableau 22 - Message SecurityAccess - sendKey Positive Response

Octet #	*Nom de 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	**NegativeResponse Service Id**	**7F**	**NR**
#6	SecurityAccess Request Service Id	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 SecurityAccess Negative Response

- Services de transmission de données

Les services disponibles font l'objet d'une description détaillée dans le tableau ci-après:

Nom du service	*Description*
ReadDataByIdentifier	Le client demande la transmission de la valeur actuelle d'un relevé avec accès par recordDataIdentifier.
WriteDataByIdentifier	Le client demande l'enregistrement d'un relevé avec accès par recordDataIdentifier.

Tableau 24 –

6. Services de transmission de données

6.1. Service ReadDataByIdentifier

6.1.1 Description des messages

CPR_050 Le message de demande ReadDataByIdentifier est utilisé par le client pour demander l'extraction de valeurs enregistrées sur un serveur. Les données sont identifiées par recordDataIdentifier. C'est au fabricant de la VU qu'incombe la responsabilité de s'assurer que les conditions d'exploitation normale du serveur sont 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 de 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	**ReadDataByIdentifier Request Service Id**	**22**	**RDBI**
#6 à #7	recordDataIdentifier = [une valeur extraite du Tableau 28]	xxxx	RDI_…
#8	Total de contrôle	00-FF	CS

Tableau 25 - Message ReadDataByIdentifier Request

Octet #	*Nom de 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	**ReadDataByIdentifier Positive Response Service Id**	**62**	**RDBIPR**
#6 et #7	recordDataIdentifier = [même valeur que les octets #6 et #7 Tableau 25]	xxxx	RDI_...
#8 à #m+7	dataRecord[] = [data#1 **:** data#m]	xx **:** xx	DREC_DATA1 **:** DREC_DATAm
#m+8	Total de contrôle	00-FF	CS

Tableau 26 - Message ReadDataByIdentifier Positive Response

Octet #	*Nom de 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	**NegativeResponse Service Id**	**7F**	**NR**

Octet #	*Nom de paramètre*	*Valeur hex.*	*Mnémonique*
#6	ReadDataByIdentifier Request Service Id	22	RDBI
#7	ResponseCode= [requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect]	22	RC_CNC
#8	Total de contrôle	00-FF	CS

Tableau 27 - Message ReadDataByIdentifier Negative Response

6.1.3 Définition des paramètres

CPR_052 Le paramètre ***recordDataIdentifier (RDI_)*** dans le message de demande ReadDataByIdentifier identifie un relevé de données.

CPR_053 Les valeurs recordDataIdentifier définies par le présent document figurent dans le tableau ci-après.

Ce tableau recordDataIdentifier se compose de quatre colonnes et d'un certain nombre de lignes.
- La **1re colonne (Hex.)** indique la «Valeur hex.» affectée à recordDataIdentifier spécifié dans la 3e colonne.
- **La 2e colonne (Élément de donnée)** indique l'élément de donnée de l'Appendice 1 sur lequel est basé recordDataIdentifier (un transcodage est parfois nécessaire).
- **La 3e colonne (Description)** spécifie le nom recordDataIdentifier correspondant.
- La **4e colonne (Mnémonique)** indique le mnémonique associé à ce recordDataIdentifier.

Hex.	*Élément de données*	*Nom du recordDataIdentifier (voir la structure indiquée à la Section 8.2)*	*Mnémonique*
F90B		TimeDate	RDI_TD
F912		HighResolutionTotalVehicleDistance	RDI_HRTVD
F918		Kfactor	RDI_KF
F91C		LfactorTyreCircumference	RDI_LF
F91D		WvehicleCharacteristicFactor	RDI_WVCF
F921		TyreSize	RDI_TS
F922		NextCalibrationDate	RDI_NCD
F92C		SpeedAuthorised	RDI_SA
F97D		RegisteringMemberState	RDI_RMS
F97E		VehicleRegistrationNumber	RDI_ VRN
F190		VIN	RDI_ VIN

Tableau 28 - Définition des valeurs recordDataIdentifier

CPR_054 Le paramètre ***dataRecord (DREC_)*** est utilisé par le message de réponse positive ReadDataByIdentifier pour fournir au client (appareil d'essai) la valeur du relevé de données identifiée par recordDataIdentifier. Les structures de données sont indiquées à la Section 8. D'autres dataRecords facultatifs, telles que les entrées propres à la VU ainsi que les données de sortie internes et externes, 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 procéder à l'enregistrement de valeurs associées aux relevés de données sur un serveur. Les données sont identifiées par recordDataIdentifier. C'est au fabricant de la VU qu'incombe la responsabilité de s'assurer que les conditions d'exploitation normale du serveur sont réunies lors de l'exécution de ce service. Pour procéder à l'actualisation des paramètres répertoriés au Tableau 28 , il faut que la VU soit exploitée 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 de 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	WriteDataByIdentifier Request Service Id	2E	WDBI
#6 à #7	recordDataIdentifier = [une valeur extraite du Tableau 28]	xxxx	RDI_…
#8 à m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Total de contrôle	00-FF	CS

Tableau 29 - Message WriteDataByIdentifier Request

Octet #	*Nom de 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	**WriteDataByIdentifier Positive Response Service Id**	**6E**	**WDBIPR**
#6 à #7	recordDataIdentifier = [même valeur que les octets #6 et #7 Tableau 29]	xxxx	RDI_...
#8	Total de contrôle	00-FF	CS

Tableau 30 - Message WriteDataByIdentifier Positive Response

Octet #	*Nom de 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

Octet #	*Nom de paramètre*	*Valeur hex.*	*Mnémonique*
#4	Octet de longueur supplémentaire	03	LEN
#5	**NegativeResponse Service Id**	**7F**	**NR**
#6	WriteDataByIdentifier Request Service Id	2E	WDBI
#7	ResponseCode= [requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect]	22	RC_CNC
#8	Total de contrôle	00-FF	CS

Tableau 31 - Message WriteDataByIdentifier Negative Response

6.2.3 Définition du paramètre

Le paramètre ***recordDataIdentifier (RDI_)*** est défini au Tableau 28 .

Le paramètre ***dataRecord (DREC_)*** est utilisé pour le message de demande WriteDataByIdentifier afin de fournir au serveur (VU) les valeurs de relevé identifiées par le recordDataIdentifier. Les structures de données sont indiquées à la section 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-après:

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 réalisée par l'intermédiaire du connecteur frontal permet de contrôler ou de surveiller les impulsions d'essai au moyen d'un testeur approprié.

CPR_058 Il est possible de configurer cette ligne de signalisation d'entrée/sortie par le biais d'une commande lancée sur la ligne K 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 de signalisation d'entrée/sortie est utilisée pour entrer un signal de vitesse (signal d'essai) en remplacement du signal de vitesse du détecteur de mouvement; cette fonction n'est pas disponible en mode CONTRÔLE,
- realTimeSpeedSignalOutputSensor, où la ligne de signalisation d'entrée/sortie est utilisée pour la sortie du signal de vitesse du détecteur de mouvement;
- RTCOutput, où la ligne de signalisation d'entrée/sortie d'étalonnage est utilisée pour la sortie du signal de l'horloge UTC; cette fonction n'est pas disponible en mode CONTRÔLE.

CPR_059 Pour être en mesure de configurer l'état de la ligne, il faut que l'unité embarquée sur véhicule soit entrée en session de réglage et qu'elle soit exploitée en mode ÉTALONNAGE ou CONTRÔLE. Lorsque la VU est en mode ÉTALONNAGE, les quatre états de la ligne peuvent être sélectionnés (désactivé; speedSignalInput; realTimeSpeedSignalOutputSensor; RTCOutput). Lorsque la VU est en mode CONTRÔLE , seuls deux états de lignes peuvent être sélectionnés (désactivé; realTimeSpeedOutputSensor). Lorsque l'opérateur décide de sortir du ÉTALONNAGE ou CONTRÔLE, l'unité embarquée sur véhicule doit s'assurer que la ligne de signalisation d'entrée/sortie 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 la VU alors que la ligne de signalisation d'E/S est exploitée en mode entrée, cette ligne de signalisation passera en mode sortie ou sera ramenée à son état de désactivation.

CPR_061 La séquence est:

- Établissement d'une liaison d'intercommunication par le biais du service StartCommunication.
- Entrée en session de réglage par le biais du service StartDiagnosticSession et passage en mode d'exploitation ÉTALONNAGE ou CONTRÔLE (l'ordre d'exécution de ces deux opérations est sans importance).
- Modification de l'état de la sortie par le biais 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 de 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	InputOutputControlByIdentifier Request Sid	2F	IOCBI
#6 et #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 ou	ControlOptionRecord = [		COR_...
#8 à #9	inputOutputControlParameter - une valeur extraite du Tableau 36	xx	IOCP_...
	controlState – une valeur extraite du Tableau 37 (cf. Note ci-dessous)]	xx	CS_…
#9 ou #10	Total de contrôle	00-FF	CS

Tableau 33 - Message InputOutputControlByIdentifier Request

Note: le paramètre controlState n'apparaît que dans certains cas (cf. 7.1.3).

Octet #	*Nom de 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	**inputOutputControlByIdentifier Positive Response SId**	**6F**	**IOCBIPR**
#6 et #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 ou	controlStatusRecord = [		CSR_
#8 à #9	inputOutputControlParameter (valeur identique à l'octet #8 Tableau 33)	xx	IOCP_...
	controlState (valeur identique à l'octet #9 Tableau 33)] (le cas échéant)	xx	CS_…
#9 ou #10	Total de contrôle	00-FF	CS

Tableau 34 - Message InputOutputControlByIdentifier Positive Response

Octet #	*Nom de 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	**negativeResponse Service Id**	**7F**	**NR**
#6	inputOutputControlByIdentifier Request SId	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 InputOutputControlByIdentifier Negative Response

7.1.3 Définition du paramètre

CPR_064 Le paramètre ***inputOutputControlParameter (IOCP_)*** est défini dans le tableau ci-après.

Hex.	*Description*	*Mnémonique*
00	ReturnControlToECU	RCTECU
	Cette valeur doit indiquer au serveur (VU) que l'appareil d'essai ne commande plus la ligne de signalisation d'E/S.	
01	ResetToDefault	RTD
	Cette valeur doit indiquer au serveur (VU) qu'il est tenu de ramener à son état initial la ligne de signalisation E/S.	
03	ShortTermAdjustment	STA
	Cette valeur doit indiquer au serveur (VU) qu'il est tenu de régler la ligne de signalisation E/S en lui attribuant la valeur incluse dans le paramètre controlState.	

Tableau 36 - Définition des valeurs inputOutputControlParameter

CPR_065 Le paramètre ***controlState*** n'apparaît que lorsque le inputOutputControlParameter est configuré comme ShortTermAdjustment et défini dans le tableau ci-après:

Mode	*Valeur hex.*	*Description*
Désactivé	00	Ligne d'E/S désactivée (par défaut)
Activé	01	Active la ligne E/S d'étalonnage comme speedSignalInput
Activé	02	Active la ligne E/S d'étalonnage comme realTimeSpeedSignalOutputSensor
Activé	03	Active la ligne E/S d'étalonnage comme RTCOutput

Tableau 37 - Définition des valeurs controlState

8. Structures des dataRecords

Le présent chapitre 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 à la section □.

CPR_067 Tous les paramètres indiqués sont pris en charge par la VU.

CPR_068 Les données transmises par la VU à l'appareil d'essai en réponse à une demande sont du type mesurées (c.-à-d. la valeur actuelle du paramètre demandé telle que mesurée ou observée par la VU).

8.1. 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 non disponible ou non pris en charge dans le module en cause. Les valeurs de la gamme «non demandé» permettent la transmission d'un message de commande et identifient 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.

Nom de la gamme	*1 octet (valeur hex.)*	*2 octets (valeur hex.)*	*4 octets (Hex Value)*	*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

Tableau 38 – Plages de dataRecords

CPR_073 Pour les paramètres encodés en ASCII, le caractère ASCII «*» est réservé comme délimiteur.

8.2. Structures des dataRecords

Les Tableau 39 à Tableau 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 identifié par son recordDataIdentifier:

Nom de paramètre	*Longueur des données (en octets)*	*Résolution*	*Gamme opérationnelle*
TimeDate	8		Cf. détails au 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, 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		Cf. détails au Tableau 41
SpeedAuthorised	2	gain 1/256 km/h/bit, décalage 0	0 à 250,996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14		Cf. détails au Tableau 42
VIN	17	ASCII	ASCII

Tableau 39 - 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 - 125 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 la note ci-après au Tableau 41)	0,25 à 31,75 jours
6	Année	gain 1 année/bit, décalage année + 1985 (voir note ci-dessous au Tableau 41)	années 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 40 - Structure détaillée de TimeDate (valeur de recordDataIdentifier # F90B)

CPR_076 Le Tableau 41 expose en détail la structure 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 note ci-après)	0,25 à 31,75 jours
3	Année	gain 1 année/bit, décalage année + 1985 (voir note ci-dessous)	années 1985 à 2235

Tableau 41 - Structure détaillée de NextCalibrationDate (valeur de recordDataIdentifier # F922)

Note 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 identifier le premier jour du mois; 5, 6, 7 et 8 identifient le deuxième jour du mois, etc.
2) Ce paramètre n'influence pas ni ne modifie le paramètre des heures précité.

Note concernant l'utilisation de l'octet du paramètre «Année»:
Une valeur «0» pour l'année identifie l'année 1985; une valeur «1» identifie 1986, etc

CPR_078 Le Tableau 42 expose en détail la structure des différents octets du paramètre VehicleRegistrationNumber:

Octet	*Définition du paramètre*	*Résolution*	*Gamme opérationnelle*
1	Page de code (telle que définie à l'appendice 1)	ASCII	01 à 0A
2 à 14	Numéro d'immatriculation du véhicule (tel que défini à l'appendice 1)	ASCII	ASCII

Tableau 42 - Structure détaillée du VehicleRegistrationNumber (valeur recordDataIdentifier # F97E)

FR

APPENDICE 9. HOMOLOGATION
LISTE DES ESSAIS MINIMAUX REQUIS

TABLE DES MATIERES

1. Introduction

2. Homologation

L'homologation CE destiné à un équipement (ou un composant) de contrôle ou à une carte tachygraphique repose sur:

- une **certification de sécurité** basée sur des spécifications de critères communs contre une cible de sécurité parfaitement conforme à l'appendice 10 de la présente annexe (à compléter ou à modifier),
- une **certification de fonctionnement** exécutée par les autorités compétentes d'un État membre certifiant que l'élément testé satisfait aux exigences de la présente annexe sur le plan des fonctions exécutées, de la précision des mesures et des caractéristiques environnementales,
- une c**ertification d'interopérabilité** exécutée par l'organisme compétent chargé de certifier l'interopérabilité de l'appareil de contrôle (ou la carte tachygraphique) visé avec la carte tachygraphique (ou l'appareil de contrôle) indispensable (cf. chapitre 8 de la présente annexe).

Le présent appendice précise les tests minimaux que les autorités compétentes d'un État membre doivent effectuer dans le cadre des essais de fonctionnement ainsi que les tests 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 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 appendice.

Les exigences numérotées font référence au corpus de l'annexe. Les autres exigences font référence aux autres appendices (p. ex. PIC_001 fait référence à l'exigence PIC_001 de l'appendice 3 Pictogrammes).

Le présent appendice traite séparément de l'homologation du détecteur de mouvement, de celle de l'unité embarquée sur le véhicule et du dispositif GNSS externe, respectivement considérés comme des composants distincts de l'appareil de contrôle. Chaque composant obtient son propre certificat d'homologation qui dresse la liste des autres composants compatibles. L'essai fonctionnel 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 vice versa.

3. Références

Le présent appendice fait référence aux documents suivants:

IEC 60068-2-1: Essais d'environnement - Partie 2-1: Essais - Essai A: Froid

IEC 60068-2-2: Procédures de base pour les essais d'environnement; partie 2: essais; essai B: chaleur sèche

(sinusoïdal).

IEC 60068-2-6: Essais d'environnement - Partie 2: Essais - Essai Fc: Vibrations (sinusoïdales)

IEC 60068-2-14: Essais d'environnement; Partie 2-14 : Essais; Essai N: Variation de température

IEC 60068-2-27: Essais d'environnement. Part 2: Essais. Essai Ea et guide: Chocs

IEC 60068-2-30: Essais d'environnement - Partie 2-30: Essais - Essai Db: Essai cyclique de chaleur humide (cycle de 12 h + 12 h)

IEC 60068-2-64: Essais d'environnement - Partie 2-64: Essais - Essai Fh: Vibrations aléatoires à large bande et guide

IEC 60068-2-78 Essais d'environnement - Part 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 + Rectificatif technique : 2010 + AMD1 :2014 Véhicules routiers - Méthodes d'essai des perturbations électriques provenant de décharges électrostatiques

ISO 7637-1 :2002 + AMD1 : 2008 Véhicules routiers - Perturbations électriques par conduction et par couplage - Partie 1: Définitions et généralités

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/IEC 7816-1 Cartes d'identification - Cartes à circuit intégré - Partie 1: Cartes à contacts - Caractéristiques physiques.

ISO/IEC 7816-2 Cartes d'identification - Cartes à circuit intégré - Partie 2: Dimensions et emplacements des contacts.

ISO/IEC 7816-3 Cartes d'identification - Cartes à circuit intégré - Partie 3: Interface électrique et protocoles de transmission.

ISO/IEC 10373-1 :2006 + AMD1 :2012 ICartes d'identification - Méthodes d'essai - Partie 1: Caractéristiques générales

ISO/IEC 10373-3 :2010 + Rectificatif technique :2013 ICartes d'identification - Méthodes d'essai - Partie 3: Cartes à circuit(s) intégré(s) à contacts et dispositifs d'interface assimilés

ISO 16844-3:2004, Cor 1:2006 Véhicules routiers - Systèmes tachygraphes - Partie 3: Interface de capteur de mouvement (avec les unités embarquées sur le véhicule).

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

UN ECE R10 Prescriptions uniformes relatives à l'homologation des véhicules en ce qui concerne la compatibilité électromagnétique (Commission économique pour l'Europe des Nations unies)

4. Essais fonctionnels de l'unité embarquée sur le véhicule

N°	Essai	Description	Exigences connexes
1	**Examen administratif**		
1.1	Documentation	Exactitude de la documentation	
1.2	Résultats des essais du 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 avec la documentation		
2.2	Identification/marquage		224 à 226
2.3	Matériaux		219 à 223
2.4	Scellements		398, 401 à 405
2.5	Interfaces externes		
3	**Essais de fonctionnement**		
3.1	Fonctions prévues		03, 04, 05, 07, 382,
3.2	Modes d'exploitation		09 à 11*, 132, 133
3.3	Droits d'accès aux fonctions et données		12* 13*, 382, 383, 386 à 389
3.4	Surveillance de l'insertion et du retrait des cartes		15, 16, 17, 18, 19*, 20*, 132
3.5	Mesure de la vitesse et de la distance		21 à 31
3.6	Chronométrage (essai exécuté à 20 °C)		38 à 43
3.7	Surveillance des activités du conducteur		44 à 53, 132
3.8	Surveillance de l'état de conduite		54, 55, 132
3.9	Entrées manuelles		56 à 62
3.10	Gestion des dispositifs de verrouillage de l'entreprise		63 à 68
3.11	Suivi des activités de contrôle		69, 70
3.12	Détection d'événements et/ou d'anomalies		71 à 88 132
3.13	Données d'identification des équipements		93*, 94*, 97, 100
3.14	Données d'insertion et de retrait de la carte du conducteur		102* à 104*
3.15	Données relatives aux activités du conducteur		105* à 107*
3.16	Données relatives aux lieux et aux emplacements		108* à 112*
3.17	Données relatives aux kilométrages		113* à 115*
3.18	Données détaillées relatives à la vitesse		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 de réglage de l'heure		124*, 125*
3.23	Données relatives aux activités de contrôle		126*, 127*
3.24	Données relatives aux dispositifs de verrouillage de l'entreprise		128*
3.25	Téléchargement de données relatives aux activités		129*
3.26	Données relatives aux conditions particulières		130*, 131*
3.27	Enregistrement et mémorisation sur les cartes tachygraphiques		134, 135,, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Affichage		90, 132, 149 à 166, PIC_001, DIS_001

3.29	Impression		90, 132, 167 à 179, PIC_001, PRT_001 à PRT_014
3.30	Avertissement		132, 180 à 189, PIC_001
3.31	Téléchargement de données à destination de supports externes		90, 132, 190 à 194
3.32	Communication à distance pour les contrôles routiers ciblés		195 à 197
3.33	Données de sortie à destination de dispositifs externes supplémentaires		198, 199
3.34	Étalonnage		202 à 206*, 383, 384, 386 à 391
3.35	Contrôles routiers d'étalonnage		207 à 209
3.36	Réglage de l'heure		210 à 212*
3.37	Absence d'interférence des fonctions supplémentaires		06, 425
3.38	Interface des capteurs de mouvement		02, 122
3.39	Dispositif GNSS externe		03, 123
3.40	Vérifier que la VU détecte, enregistre et stocke les événements et/ou anomalies défini(e)s par le fabricant de la VU lorsqu'un capteur de mouvement couplé réagit à des champs magnétiques qui perturbent la détection des mouvements du véhicule.		217
3.41	Suite de chiffrement et paramètres de domaines normalisés		CSM_48, CSM_50
4	**Essais environnementaux**		
4.1	Température	S'assurer de la fonctionnalité en exécutant les essais suivants: Essai conforme à la norme ISO 16750-4, Chapitre 5.1.1.2: Essai d'exploitation à basse température (72 h @ -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 d'exploitation à haute température (72 h à 70 °C) Cet essai satisfait à la norme CEI 60068-2-2: Procédures d'essai environnemental de base; partie 2: essais; essais 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 de maintien de 2h à chaque température). Il est possible de se livrer à un nombre limité d'essais (parmi ceux définis à la section 3 de ce tableau) aux températures minimale et maximale indiquées ainsi que pendant les cycles de variation de la température.	213
4.2	Humidité	S'assurer 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, comportant 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	1. 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 la satisfaction de cette exigence. La durée minimale de cet essai s'élève à 3 × 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. 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, y compris 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 aléatoires 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-avant 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	S'assurer 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	S'assurer 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	S'assurer que les signaux d'entrée et de sortie sont protégés contre les courts-circuits à l'alimentation électrique et à la terre (ISO 16750-2)	216
5	**Essais de compatibilité électromagnétique**		
5.1	Émissions rayonnées et sensibilité	Conformité avec le règlement CEE R10	218
5.2	Décharge électrostatique	Conformité avec la norme ISO 10605:2008 + Rectificatif technique:2010 + AMD1:2014: +/- 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 24 V: conformité avec la norme ISO 7637-2 + Règlement CEE n° 10 Rév. 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 + Règlement CEE n° 10 Rév. 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 testée que pour les unités 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

5. 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 avec la documentation		
2.2.	Identification/marquage		225, 226,
2.3	Matériaux		219 à 223
2.4.	Scellements		398, 401 à 405
3.	**Essais de fonctionnement**		
3.1	Données d'identification du capteur		95 à 97*
3.2	Appariement capteur de mouvement – unité embarquée sur véhicule		122*, 204
3.3	Détection de mouvement Exactitude de la mesure du mouvement		 30 à 35
3.4	Interface d'unité embarquée sur le véhicule		02
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 VU connectée puisse détecter, enregistrer et stocker les anomalies du capteur		217
4.	**Essais environnementaux**		
4.1	Température d'exploitation	S'assurer de la fonctionnalité de ce composant (telle qu'elle est définie dans le test n° 3.3) pour la plage de températures [− 40 °C + 135 °C] en exécutant les essais suivants: CEI 60068-2-1 essai Ad, en appliquant une durée d'essai de 96 heures à la température minimale To_{min} CEI 60068-2-2 essai Bd, en appliquant une durée d'essai de 96 heures à la température maximale Tomax Essai conforme à la norme ISO 16750-4: Chapitre 5.1.1.2: Essai d'exploitation à basse température (24 h @ -40 °C) Cet essai satisfait à la norme CEI 60068-2-1: Essais d'environnement — Partie 2-1: essais - essai A: CEI 68-2-2 essai froid Bd, en appliquant une durée d'essai de 96 heures à la température minimale de -40 °C. Essai conforme à la norme ISO 16750-4: Chapitre 5.1.2.2: Essai d'exploitation à haute température (96 h @ 135 °C) Cet essai satisfait à la norme CEI 60068-2-2: Procédures d'essai environnemental de base; partie 2: essais; essais 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 de maintien de 30 minutes à chaque température) IEC 60068-2-14: Essais d'environnement — Partie 2-14: essais - essai N: changement de température	213
4.3	Cycles humides	S'assurer de la fonctionnalité de ce composant (telle qu'elle est définie dans le test n° 3.3) en exécutant l'essai CEI 60068-2-30, essai Db, comportant 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

4.4	vibrations	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: Vibrations - Mode mixte	219
4.5	Chocs mécaniques	ISO 16750-3: Chapitre 4.2.3: Essai VI: Essai pour dispositifs dans ou sur l'engrenage Choc demi-sinusoïdal, accélération à convenir dans la plage entre 3 000...15 000 m/s², durées 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 (code IP) - Protection des équipements électriques contre les corps étrangers, l'eau et les contacts (Valeur cible IP 64)	220, 221
4.7	Protection contre les inversions de polarité	S'assurer que le détecteur de mouvement est capable de supporter une inversion de polarité au niveau de son alimentation électrique	216
4.8	Protection contre les courts-circuits	S'assurer que les signaux d'entrée et de sortie sont protégés contre les courts-circuits à l'alimentation électrique et à la terre	216
5.	**Essais de compatibilité électromagnétique**		
5.1	Émissions rayonnées et sensibilité	Contrôler la conformité avec le règlement CEE R10	218
5.2	Décharge électrostatique	Conformité avec la norme ISO 10605:2008 + Rectificatif technique:2010 + AMD1:2014: +/- 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 24 V: conformité avec la norme ISO 7637-2 + Règlement CEE n° 10 Rév. 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 + Règlement CEE n° 10 Rév. 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 testée que pour les unités 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 de fonctionnement des cartes tachygraphiques

Essais conformes à la présente Section 4,
n° 5 «Essais de protocole»,
n° 6 «Structure de la carte» et
n° 7 «Essais de fonctionnement»
peuvent être effectués par l'évaluateur ou le certificateur pendant la procédure de certification de la sécurité Critères communs (CC) du module avec circuit.

Les essais numéros 2.3 et 4.2 sont identiques. Il s'agit des essais mécaniques de la combinaison incluant le corps de la carte et le module du circuit. En cas de modification de l'un de ces composants (corps de la carte ou module du circuit), les essais deviennent nécessaires.

N°	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 1C, chapitre 4.1 «Données visibles», 227) La première page doit comporter: les mots «carte de conducteur» ou «carte de contrôleur» ou «carte d'atelier» ou «carte d'entreprise» imprimés en majuscules dans la ou les langue(s) officielle(s) de l'État membre qui a délivré la carte, selon le type de carte. [nom de l'État membre] Annexe 1C, chapitre 4.1 «Données visibles», 228) La première page doit comporter: le nom de l'État membre qui a délivré la carte (facultatif). [Signature] Annexe 1C, chapitre 4.1 «Données visibles», 229) La première page doit comporter: 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. [Énumération] Annexe 1C, chapitre 4.1 «Données visibles», 232 Le verso doit comporter: une légende des numéros indiqués au recto. [Couleur] Annexe 1C, chapitre 4.1 «Données visibles», 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.	227 à 229*, 232, 234 à 236

		[Sécurité] Annexe 1C, chapitre 4.1 «Données visibles», 235) Les cartes tachygraphiques présentent au minimum 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 1C, chapitre 4.1 «Données visibles», 236 Les États membres ajoutent des couleurs ou des marquages, comme des symboles nationaux et des caractéristiques de sécurité. [Marque d'homologation] Les cartes tachygraphiques contiennent une marque d'homologation. La marque d'homologation est composée: - 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, - d'un numéro d'homologation correspondant au numéro du certificat d'homologation établie 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 respecter 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 respecter 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 [Construction de la carte] Les cartes tachygraphiques doivent respecter la norme ISO/CEI 7810 Cartes d'identification - Caractéristiques physiques, [6] Construction de la carte [Matériaux des cartes] Les cartes tachygraphiques doivent respecter la norme ISO/CEI 7810 Cartes d'identification - Caractéristiques physiques, [7] Matériaux des cartes	240, 243 ISO/CEI 7810

		[Rigidité à la flexion] Les cartes tachygraphiques doivent respecter 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 respecter 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 respecter 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 respecter 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 respecter la norme ISO/CEI 7810 Cartes d'identification - Caractéristiques physiques, [8] Caractéristiques de la carte, [8.6] Lumière	
		[Durabilité] Annexe 1C, chapitre 4.4 «Spécifications environnementales et électriques», 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 respecter 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 respecter 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 respecter 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 respecter 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 respecter 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 respecter 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 respecter la norme ISO/CEI 7810:2003/Amd. 1:2009, Cartes d'identification – Caractéristiques physiques, Amendement 1: Critères des cartes contenant des circuits intégrés [9.2] Contraintes de flexion dynamique Nombre total de cycles de flexion: 4000.	ISO/CEI 7810
		[Torsion] Les cartes tachygraphiques doivent respecter la norme ISO/CEI 7810:2003/Amd. 1:2009, Cartes d'identification – Caractéristiques physiques, Amendement 1: Critères des cartes contenant des circuits intégrés [9.3] Contraintes de torsion dynamique Nombre total de cycles de torsion: 4000.	
3	**Module**		
3.1	**Module**	Le module désigne l'encapsulation du circuit et la plaque de contact.	ISO/CEI 7816
		[Profil de surface] Les cartes tachygraphiques doivent respecter 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 respecter 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 respecter la norme ISO/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 respecter 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 respecter 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.	
4	**Circuit**		
4.1	**Circuit**	[Température d'exploitation] Le circuit de la carte tachygraphique fonctionne dans une plage de température ambiante de -25℃ à +85 ℃.	241 à 244 CEE R10 ISO/CEI 7810 ISO/CEI 10373
		[Température et humidité] Annexe 1C, chapitre 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, et au minimum dans une gamme de température comprise entre -25 ℃ et +70 ℃, avec d es pointes occasionnelles à +85 ℃, «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 aux températures et hygrométries suivantes pendant une période donnée. Après chaque étape, la fonctionnalité électrique des cartes tachygraphiques fait l'objet d'essais. **1.** Température de -20 ℃ pendant 2 heures. **2.** Température de +/-0 ℃ pendant 2 heures. **3.** Température de +20 ℃, 50 % HR pendant 2 heures. **4.** Température de +50 ℃, 50 % HR pendant 2 heures. **5.** Température de +70 ℃, 50 % HR pendant 2 heures. La température augmente par intermittence à +85 ℃, 50 % HR, pendant 60 min. 6. Température de +70 ℃, 85 % HR pendant 2 heures. La température augmente par intermittence à +85 ℃, 85 % HR, pendant 30 min.	
		[Humidité] Annexe 1C, chapitre 4.4 «Spécifications environnementales et électriques», 242 Les cartes tachygraphiques doivent pouvoir fonctionner correctement dans une gamme d'humidité comprise entre 10 % et 90 %.	

		[Compatibilité électromagnétique - CEM] Annexe 1C, chapitre 4.4 «Spécifications environnementales et électriques», 244 En fonctionnement, les cartes tachygraphiques doivent satisfaire à la réglementation CEE R10, relative à la compatibilité électromagnétique.	
		[Électricité statique] Annexe 1C, chapitre 4.4 «Spécifications environnementales et électriques», 244 En fonctionnement, les cartes tachygraphiques doivent être protégées contre les décharges électrostatiques. Les cartes tachygraphiques doivent respecter la norme ISO/CEI 7810:2003/Amd. 1:2009, Cartes d'identification – Caractéristiques physiques, Amendement 1: Critères des 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 respecter la norme ISO/CEI 7810:2003/Amd. 1:2009, Cartes d'identification – Caractéristiques physiques, Amendement 1: Critères des 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 respecter 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 trois roues pour les CCI avec contacts	
		[Enveloppe] Les cartes tachygraphiques doivent respecter 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	Module de circuit intégré des essais mécaniques intégré dans le corps de la carte -> identique 2.3	[Flexion] Les cartes tachygraphiques doivent respecter la norme ISO/CEI 7810:2003/Amd. 1:2009, Cartes d'identification – Caractéristiques physiques, Amendement 1: Critères des cartes contenant des circuits intégrés [9.2] Contraintes de flexion dynamique Nombre total de cycles de flexion: 4000.	ISO/CEI 7810
		[Torsion] Les cartes tachygraphiques doivent respecter la norme ISO/CEI 7810:2003/Amd. 1:2009, Cartes d'identification – Caractéristiques physiques, Amendement 1: Critères des cartes contenant des circuits intégrés [9.3] Contraintes de torsion dynamique Nombre total de cycles de torsion: 4000.	
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		S'assurer de la conformité de la structure des fichiers enregistrée sur la carte en contrôlant la présence des fichiers obligatoires sur la carte ainsi que leurs conditions d'accès	TCS_22 à TCS_28 TCS_140 à TCS_179
7	**Essais de fonctionnement**		
7.1	Fonctionnement normal	Vérifier au moins une fois chaque usage autorisé de chaque commande. (ex: essayer la commande UPDATE BINARY avec CLA = ′00′, CLA = ′0C′ pour des paramètres P1, P2 et Lc distincts). S'assurer que les opérations voulues ont été correctement exécutées sur la carte (ex.: en extrayant le fichier sur lequel la commande considérée a été exécutée).	TCS_29 à TCS_139
7.2	Messages d'erreur	Il convient de tester une fois au moins chaque message d'erreur (comme indiqué à l'appendice 2) pour chaque commande. Tester une fois au moins chaque erreur générique (à l'exception des erreurs d'intégrité ′6400′ contrôlées pendant la phase de certification de sécurité).	
7.3	Suite de chiffrement et paramètres de domaines normalisés		CSM_48, CSM_50
8	**Personnalisation**		
8.1	Personnalisation optique	Annexe 1C, chapitre 4.1 «Données visibles», 230) La première page doit comporter: des indications particulières concernant la carte délivrée. Annexe 1C, chapitre 4.1 «Données visibles», 231) La première page doit comporter: Les dates sont indiquées sous la forme «jj/mm/aaaa» ou «jj.mm.aaaa» (jour, mois, année). Annexe 1C, chapitre 4.1 «Données visibles», 235) Les cartes tachygraphiques présentent au minimum 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

7. Essais du dispositif GNSS externe

N°	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 véhicule		123, 205
3.3	Position du GNSS		36, 37
3.4	Interface de l'unité embarquée sur véhicule lorsque le récepteur GNSS est externe à l'unité embarquée sur le véhicule		03
3.5	Suite de chiffrement et paramètres de domaines normalisés		CSM_48, CSM_50
4.	**Essais environnementaux**		
4.1	Température	S'assurer de la fonctionnalité en exécutant les essais suivants: Essai conforme à la norme ISO 16750-4, Chapitre 5.1.1.2: Essai d'exploitation à basse température (72 h @ -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 d'exploitation à haute température (72 h @ 70 °C) Cet essai satisfait à la norme CEI 60068-2-2: Procédures d'essai environnemental de base; partie 2: essais; essais 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 de maintien de 1 h à chaque température) Il est possible de se livrer à un nombre limité d'essais (parmi ceux définis à la section 3 de ce tableau) aux températures minimale et maximale indiquées ainsi que pendant les cycles de variation de la température	213
4.2	Humidité	S'assurer 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, comportant 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	1. 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 la satisfaction de cette exigence. La durée minimale de cet essai s'élève à 3 × 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. 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, y compris 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 aléatoires 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-avant 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 (code IP) - Protection des équipements électriques contre les corps étrangers, l'eau et les contacts (aucune modification des paramètres)	220, 221
4.5	Protection contre les surtensions	S'assurer 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, chapitre 4.3)	216
4.6	Protection contre les inversions de polarité	S'assurer que l'unité embarquée sur le véhicule est capable de supporter une inversion de polarité au niveau de son alimentation électrique (ISO 16750-2, chapitre 4.7)	216
4.7	Protection contre les courts-circuits	S'assurer que les signaux d'entrée et de sortie sont protégés contre les courts-circuits à l'alimentation électrique et à la terre (ISO 16750-2, chapitre 4.10)	216

5	**Essais de compatibilité électromagnétique**		
5.1	Émissions rayonnées et sensibilité	Conformité avec le règlement CEE R10	218
5.2	Décharge électrostatique	Conformité avec la norme ISO 10605:2008 + Rectificatif technique:2010 + AMD1:2014: +/- 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 24 V: conformité avec la norme ISO 7637-2 + Règlement CEE n° 10 Rév. 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 + Règlement CEE n° 10 Rév. 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 testée que pour les unités à installer sur des véhicules dépourvus de dispositif commun de protection externe contre la perte de charge. Pour la proposition de perte de charge, consulter la norme ISO 16750-2, 4e édition, chapitre 4.6.4.	218

8. Essais des équipements de communication à distance

N°	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	Matériaux		219 à 223
4.	**Essais environnementaux**		
4.1	Température	S'assurer de la fonctionnalité en exécutant les essais suivants: Essai conforme à la norme ISO 16750-4, Chapitre 5.1.1.2: Essai d'exploitation à basse température (72 h @ -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 d'exploitation à haute température (72 h @ 70 °C) Cet essai satisfait à la norme CEI 60068-2-2: Procédures d'essai d'environnement de base; partie 2: essais; essais 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 de maintien de 1 h (?) à chaque température). Il est possible de se livrer à un nombre limité d'essais (parmi ceux définis à la section 3 de ce tableau) aux températures minimale et maximale indiquées ainsi que pendant les cycles de variation de la température	213
4.4	Protection contre l'eau et les corps étrangers	Essai conforme à la norme ISO 20653: Véhicules routiers - Degrés de protection (code IP) - Protection des équipements électriques contre les corps étrangers, l'eau et les contacts (valeur ciblée IP40)	220, 221
5	**Essais de compatibilité électromagnétique**		
5.1	Émissions rayonnées et sensibilité	Conformité avec le règlement CEE R10	218
5.2	Décharge électrostatique	Conformité avec la norme ISO 10605:2008 + Rectificatif technique:2010 + AMD1:2014: +/- 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 24 V: conformité avec la norme ISO 7637-2 + Règlement CEE n° 10 Rév. 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 + Règlement CEE n° 10 Rév. 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 testée que pour les unités 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 sur le papier

N°	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 impressions.	172
2.2	Taille min. des caractères	Inspection visuelle des impressions 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 1.	174
2.4	Définition des impressions	Contrôle de l'homologation du type de tachygraphe et inspection visuelle des impressions	174
2.5	Lisibilité et identification des impressions	Inspection des impressions Étayé par des rapports d'essai et des protocoles d'essai 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	Contrôle visuel: la zone de signature du conducteur est disponible. D'autres zones de saisie manuscrites sont disponibles.	180

2.7	Détails complémentaires sur le recto et le verso du papier.	Le recto et le verso du papier peuvent fournir des détails et des informations supplémentaires. Ces détails et ces informations supplémentaires n'interfèrent pas systématiquement avec la lisibilité des impressions. Contrôle visuel	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'h.r. Récupération: 16 heures à +23 °C ± 2 °C/55 % ±3 % d'humidité relative	176, 178 CEI 60068-2-78-Cab
4	**Essais sur papier en circulation**		
4.1	Contexte de résistance à l'humidité (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'h.r. 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 16 heures à +23 °C ± 2 °C/55 % ±3 % d'humidité relative	176, 178
4.3	Thermorésistance	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 températures basses	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	Photorésistance	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 impressions est garantie si la densité optique respecte les contraintes suivantes:
Caractères imprimés: min. 1

Support (papier non imprimé): max 0,2
La mesure de densité optique des impressions produites respecte la norme DIN EN ISO 534.
Les impressions ne subissent aucune modification de dimension et demeurent parfaitement lisibles.

8. Essais d'interopérabilité

N°	Essai	Description
9.1 Essais d'interopérabilité entre unités embarquées sur véhicule et cartes tachygraphiques		
1	Authentification mutuelle	S'assurer de la bonne exécution de la procédure d'authentification mutuelle entre l'unité embarquée sur le véhicule et la carte tachygraphique.
2	Essais de lecture/écriture	Mettre à exécution un scénario d'activité classique sur l'unité embarquée sur le véhicule. Le scénario doit être adapté au type de carte testé et comporter l'exécution d'opérations d'écriture dans le plus grand nombre possible d'EF que présente la carte. Procéder à un téléchargement sur VU pour s'assurer de la bonne exécution de tous les enregistrements correspondants. Procéder à un téléchargement sur carte pour s'assurer de la bonne exécution de tous les enregistrements correspondants. Procéder à des impressions quotidiennes pour s'assurer de la bonne lisibilité des enregistrements correspondants.
9.2 Essais d'interopérabilité entre unités embarquées sur véhicule et capteurs de mouvement		
1	Appariement	S'assurer de la bonne exécution de l'appariement entre l'unité embarquée sur le véhicule 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'événement et d'anomalies aussi élevé que possible. Procéder à un téléchargement sur VU pour s'assurer de la bonne exécution de tous les enregistrements correspondants. Procéder à un téléchargement sur carte pour s'assurer de la bonne exécution de tous les enregistrements correspondants. Procéder à une impression quotidienne pour s'assurer de la bonne lisibilité des enregistrements correspondants.
9.3 Essais d'interopérabilité entre les VU 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 sur le véhicule 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'événement et d'anomalies aussi élevé que possible. Procéder à un téléchargement sur VU pour s'assurer de la bonne exécution de tous les enregistrements correspondants. Procéder à un téléchargement sur carte pour s'assurer de la bonne exécution de tous les enregistrements correspondants. Procéder à une impression quotidienne pour s'assurer de la bonne lisibilité des enregistrements correspondants.

FR

APPENDICE 10

EXIGENCES EN MATIÈRE DE SÉCURITÉ

Le présent appendice précise les exigences en matière de sécurité informatique concernant les 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 conforme aux 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 par un profil de protection du composant, conformément aux Critères communs.

SEC_003 La Commission européenne doit s'assurer que quatre profils de protection conformes à la présente annexe sont parrainés, développés, approuvés par les organismes gouvernementaux de certification de la sécurité informatique conjointement avec le groupe de travail d'interprétation conjointe (JIWG), qui encouragent la reconnaissance mutuelle des certificats sous l'égide européenne du SOG-IS MRA (accord sur la reconnaissance mutuelle des certificats d'évaluation de la sécurité en matière de technologie de l'information) et qu'ils font l'objet d'un enregistrement:

- profil de protection d'une unité embarquée sur le véhicule;
- profil de protection d'une carte tachygraphique;
- profil de protection d'un capteur de mouvement;
- profil de protection d'un dispositif GNSS externe.

Le profil de protection d'une unité embarquée sur le véhicule est destiné aux cas où l'unité embarquée sur le véhicule a été conçue pour être utilisée avec ou sans dispositif GNSS externe. Dans le premier cas, les exigences de sécurité du dispositif GNSS externe sont stipulées dans le profil de protection dédié.

SEC_004 Pour établir un objectif de sécurité en vue de l'obtention de certificats de sécurité du composant, les fabricants de composants habilités affineront et complèteront selon les besoins le profil de protection de composant approprié, sans supprimer ni modifier les spécifications concernant les menaces, les objectifs, les ressources procédurales et les fonctions de maintien de la sécurité.

SEC_005 La stricte conformité dudit objectif de sécurité avec le profil de protection correspondant doit être déclarée au cours du processus d'évaluation.

SEC_006 Le niveau de garantie exigé par chaque profil de protection est le niveau EAL4 augmenté des composants de garantie ATE_DPT.2 et AVA_VAN.5.

FR

APPENDICE 11 MECANISMES DE SECURITE COMMUNS

TABLE DES MATIERES

Préambule

Le présent appendice indique les mécanismes de sécurité garantissant

- l'authentification mutuelle entre les différents composants du tachygraphe.
- confidentialité, intégrité, authenticité et/ou non-répudiation des données transférées entre les différents composants du tachygraphe ou téléchargées vers un support de stockage externe.

Le présent appendice se compose de deux parties. La partie A définit les mécanismes de sécurité pour le tachygraphe de première génération (tachygraphe numérique). La partie B définit les mécanismes de sécurité pour le tachygraphe de deuxième génération (tachygraphe intelligent).

Les mécanismes spécifiés dans la partie A du présent appendice s'appliquent si au moins l'un des composants du tachygraphe concerné par une authentification mutuelle et/ou le processus de transfert des données est de première génération.

Les mécanismes spécifiés dans la partie B du présent appendice s'appliquent si les deux composants concernés par une authentification mutuelle et/ou le processus de transfert des données sont de deuxième génération.

L'appendice 15 fournit davantage d'informations à propos de l'utilisation des composants de première génération avec ceux de deuxième génération.

PARTIE A TACHYGRAPHE DE PREMIÈRE GÉNÉRATION

1 Introduction

1.1 Références

Le présent appendice 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 + 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 intersectorielles. Première édition: 1996 + Cor 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 tachygraphiques — Partie 3: Interface de capteur de mouvement.

1.2 Notations et abréviations

Les notations et abréviations qui suivent apparaissent dans le présent appendice:

(K_a, K_b, K_c)	Faisceau de clés destiné au triple algorithme de cryptage des données
CA	Organisme de certification
CAR	Références de l'organisme de certification
CC	Total de contrôle cryptographique
CG	Cryptogramme
CH	En-tête de commande
CHA	Autorisation d'un titulaire de certificat
CHR	Références d'un titulaire de certificat
D()	Décryptage avec DES (Data Encryption Standard)
DE	Élément de données
DO	Objet de données
d	Clé privée - Exposant privé RSA
e	Clé publique - Exposant public RSA
E()	cryptage avec DES
EQT	Équipement
Hash()	Valeur de hachage, en tant que sortie de *Hash*
Hash	Fonction Hash
KID	Identificateur de clé
Km	Clé TDES. Clé maîtresse définie dans ISO 16844-3
Km_{VU}	Clé TDES insérée dans les unités embarquées sur le véhicule
Km_{WC}	Clé TDES insérée dans les cartes d'ateliers
m	Représentant de message, nombre entier compris entre 0 et n-1
n	Clés RSA, modulo
PB	Octets de remplissage
PI	Octet indicateur de remplissage (employé dans les cryptogrammes destinés aux instructions DO de confidentialité)
PV	Valeur ordinaire
s	Représentant de signature, nombre entier compris entre 0 et n-1
SSC	Compteur de séquences d'émission
SM	Messagerie sécurisée
TCBC	Mode d ' exploitation par chaînage de blocs de données cryptées TDEA
TDEA	Triple algorithme d ' cryptage des données
TLV	Longueur des marqueurs
VU	Unité embarquée sur le véhicule
X.C	Certificat de l'utilisateur X, émis par un organisme de certification
X.CA	Organisme de certification de l'utilisateur X
X.CA.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'un organisme de certification et l'opérande de droite au certificat émis par ce même organisme. Nous obtenons en 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]	cryptage 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]	cryptage RSA de certaines 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 sur véhicule et les cartes tachygraphiques auront recours à un système cryptographique classique à clé publique RSA pour assurer les mécanismes de sécurité suivants:

- Authentification mutuelle entre unités embarquées sur véhicule et cartes tachygraphiques.
- Acheminement des clés triples de session DES (Data Encryption Standard) entre unités embarquées sur véhicule et cartes tachygraphiques.
- Signature numérique des données téléchargées sur des supports externes à partir d'unités sur véhicule ou de cartes tachygraphiques.

CSM_002 Les unités embarquées sur véhicule et les cartes tachygraphiques auront recours à un système cryptographique symétrique DES triple pour assurer un mécanisme garantissant l'intégrité des données lors des échanges de données utilisateur entre les unités embarquées sur véhicule et les cartes tachygraphiques et pour assurer, le cas échéant, la confidentialité des échanges de données entre les unités embarquées sur véhicule et les cartes tachygraphiques.

2.2 Algorithmes cryptographiques

2.2.1 Algorithme RSA

CSM_003 L'algorithme RSA est parfaitement défini par les relations suivantes:

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

Pour une description plus détaillée de la fonction RSA, reportez-vous au document de référence [PKCS1]. L'exposant public, e, pour les calculs de 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 auront recours à l'algorithme de hachage SHA-1 tel qu'il est défini dans le document de référence [SHA-1].

2.2.3 Algorithme de cryptage des données

CSM_005 Des algorithmes DES seront utilisés en mode chaînage de blocs de données cryptées.

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 seront générées à trois niveaux hiérarchiques fonctionnels:
- niveau européen,
- niveau État membre,
- niveau équipement.

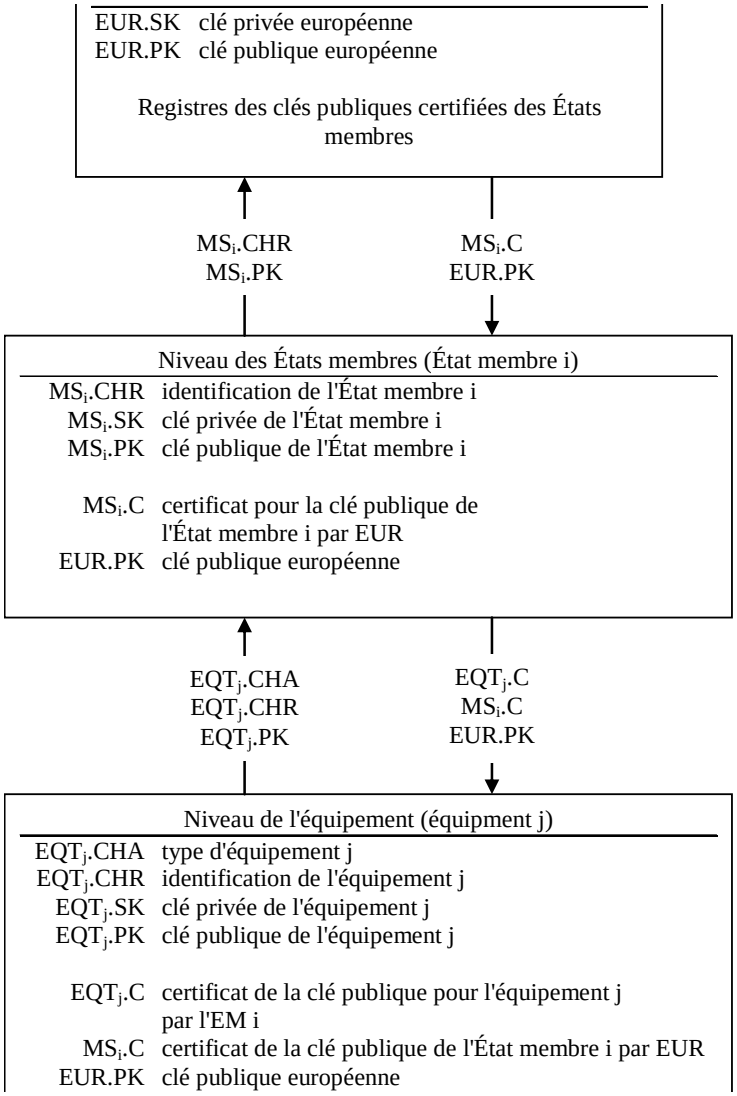
CSM_007 Au niveau européen, une seule paire de clés européenne (EUR.SK et EUR.PK) sera générée. La clé privée européenne permettra d'homologuer les clés publiques des États membres. Des registres de l'ensemble des clés certifiées seront conservés. Ces tâches seront exécutées par un organisme de certification européen, placé sous l'autorité et la responsabilité de la Commission européenne.

CSM_008 Au niveau État membre, une paire de clés par État membre (MS.SK et MS.PK) sera générée. Les clés publiques des États membres seront homologuées par l'organisme de certification européen. La clé privée de l'État membre permettra d'homologuer les clés publiques à introduire dans l'équipement (unité embarquée sur le véhicule ou carte tachygraphique). Des registres de l'ensemble des clés publiques certifiées seront conservés avec les données d'identification de l'équipement auquel elles sont destinées. Ces tâches seront exécutées par un organisme de certification national. Tout État membre est habilité à changer régulièrement de paire de clés.

CSM_009 Au niveau équipement, une seule paire de clés (EQT.SK et EQT.PK) sera générée et introduite dans chaque équipement. Les clés publiques d'équipement seront homologuées par un organisme de certification national. Ces tâches seront exécutées par les fabricants d'équipements, personnalisateurs d'équipement ou autorités compétentes à l'échelon national. Cette paire de clés sera utilisée par les services d'authentification, de signature numérique et de cryptage.

CSM_010 La confidentialité des clés privées doit être préservée durant leur génération, leur acheminement (éventuel) et leur archivage.

Le schéma fonctionnel qui suit représente une synthèse du cheminement des données caractérisant ce processus:



3.1.2 Clés de contrôle RSA

CSM_011 Aux fins d'essai des équipements (essais d'interopérabilité inclus), l'organisme de certification européen générera une paire de clés de contrôle européenne distincte et deux paires de clés de contrôle nationales au moins, dont les clés publiques seront homologuées conjointement avec la clé de contrôle privée européenne. Les fabricants introduiront, dans les équipements en cours de certification de type, des clés de test certifiées par l'une des clés de test nationales.

3.1.3 Clés du capteur de mouvement

La confidentialité des trois clés triple DES décrites ci-après est protégée de manière appropriée au cours de la génération, du transport (le cas échéant) et du stockage.

Afin de permettre l'utilisation de composants de tachygraphes conformes à la norme ISO 16844, l'autorité de certification européenne et les organismes de certification de l'État membre veilleront également aux aspects suivants:

CSM_036 L'organisme de certification européen génère les clés Km_{VU} et Km_{WC}, deux clés triple DES uniques et indépendantes, ainsi que la clé Km selon la formule: $Km = Km_{VU}$ XOR Km_{WC}. L'organisme de certification européen transmet ces clés, selon les procédures sécurisées appropriées, aux organismes de certification des États membres qui en font la demande.

CSM_037 Les organismes de certification des États membres:

- utilisent la clé Km pour chiffrer les données du capteur de mouvement demandées par les fabricants des capteurs de mouvement (les données à chiffrer avec la clé Km sont définies par la norme ISO 16844-3),
- transmettent la clé Km_{VU} aux fabricants d'unités embarquées sur le véhicule, selon les procédures sécurisées appropriées, afin qu'elles soient insérées dans les VU,
- veillent à ce que la clé Km_{WC} soit insérée dans toutes les cartes d'atelier (SensorInstallationSecData dans le fichier élémentaire Sensor_Installation_Data) lors de la personnalisation de la carte.

3.1.4 Génération et distribution de clés de session T-DES

CSM_012 Lors de leur processus d'authentification mutuelle, les unités embarquées sur véhicule et les cartes tachygraphiques généreront et échangeront les données nécessaires à l'élaboration d'une clé de session T-DES commune. La confidentialité de cet échange de données sera préservée par un mécanisme de cryptage RSA.

CSM_013 Cette clé sera utilisée lors de toutes les opérations cryptographiques ultérieures, en faisant appel à la messagerie sécurisée. Sa validité expirera à la fin de la session (retrait ou réinitialisation de la carte) et/ou après 240 usages (définition d'un usage de la clé: l'envoi d'une commande recourant à la messagerie sécurisée vers la carte appropriée et la réponse associée à cet envoi).

3.2 Clés

CSM_014 Les clés RSA ont les longueurs suivantes (indépendamment de leur niveau): modulo *n* 1024 bits, exposant public *e* 64 bits maximum, exposant privé *d* 1024 bits.

CSM_015 Les T-DES prendront la forme (K_a, K_b, K_a) , où K_a et K_b sont des clés indépendantes de 64 bits de long. Aucun bit de détection d'erreur de parité ne doit être établi.

3.3 Certificats

CSM_016 Les certificats associés aux clés publiques RSA seront du type «non self-descriptive» et «card verifiable» (Réf.: 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	ENTIER	1	Identificateur de profil du certificat ('01' pour cette version)
CAR	CHAÎNE D'OCTETS	8	Références de l'organisme de certification
CHA	CHAÎNE D'OCTETS	**7**	Autorisation d'un titulaire de certificat
EOV	TimeReal	4	Expiration du certificat. Optionnel, «FF» complété par des octets de remplissage en cas de non-utilisation.
CHR	CHAÎNE D'OCTETS	8	Références d'un titulaire de certificat
n	CHAÎNE D'OCTETS	128	Clé publique (module)
e	CHAÎNE D'OCTETS	8	Clé publique (exposant public)
		164	

Remarques:

1. «L'Identificateur de profil du certificat» (CPI) détermine la structure précise d'un certificat d'authentification. Il fait office d'identificateur interne d'équipement au sein d'une liste en-tête appropriée qui décrit la concaténation des éléments de données que comporte le certificat.

   La liste en-tête associée au contenu de ce certificat se présente comme suit:

‘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 CAR	Longueur CAR	Balise CHA	Longueur CHA	Balise EOV	Longueur EOV	Balise CHR	Longueur CHR	Balise de clé publique (construite)	Longueur des objets de données ultérieurs	Balise module	Longueur module	Balise exposant public	Longueur exposant public

2. Les «Références de l'organisme de certification» (CAR) permettent d'identifier l'organisme de certification émetteur du certificat de telle manière que l'élément de données puisse faire simultanément office d'identificateur de clé d'autorité renvoyant à la clé publique de l'organisme de certification (pour plus d'informations concernant le codage, reportez-vous à l'Identificateur de clé ci-après).

3. «L'Autorisation du titulaire de certificat» (CHA) permet d'identifier les droits du titulaire de certificat. Elle se compose de l'ID d'application du tachygraphe et du type d'équipement auquel est destiné le certificat considéré (en fonction de l'élément de données `EquipmentType`, '00' pour un État membre).

4. La «Référence du titulaire de certificat» (CHR) permet d'identifier exclusivement le titulaire de certificat de telle manière que l'élément de données puisse faire simultanément office d'identificateur de clé de sujet renvoyant à la clé publique du titulaire de certificat.

5. Les identificateurs de clé identifient uniquement les titulaires de certificat ou les organismes de certification. Ils sont codés comme suit:

   5.1. Équipement (VU ou carte):

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	Caractéristiques du fabricant	Code du fabricant

   S'il s'agit d'une VU, le fabricant est susceptible, lors de la demande de certificats, de 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'organisme de certification national compétent. Le certificat contiendra alors 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-avant.

   Dans le second cas de figure, le fabricant doit identifier individuellement chaque demande de certificat et envoyer les données d'identification correspondantes accompagnées de la clé publique à l'organisme de certification national compétent. Le certificat contiendra alors les données d'identification de la demande de certificat concernée. Le fabricant doit communiquer en retour à l'organisme de certification national compétent les données d'affectation des clés à l'équipement concerné (c.-à-d., les données d'identification de la demande de certificat et d'identification de l'équipement visé) après leur installation sur cet équipement. L'Identificateur de clé se présente sous la forme indiquée ci-après:

Données	*Numéro de série de la demande de certificat*	*Date*	*Type*	*Fabricant*

Données	*Numéro de série de la demande de certificat*	*Date*	*Type*	*Fabricant*
Longueur	4 octets	2 octets	1 octet	1 octet
Valeur	Entier	Codage DCB mm aa	'FF'	Code du fabricant

5.2 Organisme de certification:

Données	*Identification de l'organisme*	*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 la CA) '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 État membre, en cas de changement de clé.

6. Les vérificateurs de certificat sauront implicitement que la clé publique certifiée est une clé RSA propre à l'authentification, à la vérification et au cryptage de signatures numériques aux fins de confidentialité (le certificat ne contient aucun Identificateur d'objet permettant de le préciser).

3.3.2 Certificats émis

CSM_018 Le certificat émis se présente comme une signature numérique assortie d'une récupération partielle du contenu du certificat en conformité avec la norme ISO/CEI 9796-2 (annexe A.4 non comprise), les «Références de l'organisme de certification» clôturant le certificat.

$$X.C = X.CA.SK[\text{'6A'} \,||\, C_r \,||\, \mathit{Hash}(Cc) \,||\, \text{'BC'}] \,||\, C_n \,||\, X.CAR$$

Avec contenu de certificat $= Cc = C_r \,||\, C_n$ (106 octets, 58 octets)

Remarques:

1. Ce certificat comporte 194 octets.
2. Les CAR, masquées par la signature, s'ajoutent également à cette dernière, afin que la clé publique de l'organisme de certification puisse être sélectionnée pour procéder à la vérification du certificat.
3. Le vérificateur du certificat connaîtra implicitement l'algorithme employé par l'organisme de certification pour signer le certificat.

4. La liste en-tête associée à ce certificat émis se présente comme suit:

‘7F 21’	‘09’	‘5F 37’	’81 80’	‘5F 38’	‘3A’	‘42’	‘08’
Balise certificat CV (construite)	Longueur des objets de données ultérieurs	Balise signature	Longueur signature	Balise solde	Longueur solde	Balise CAR	Longueur CAR

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.CA.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 la Sign., C_n’ et CAR’: X.C = Sign || C_n’ || CAR’
  128 octets 58 octets 8 octets
– À partir de CAR′, sélectionner la clé publique de l'organisme de certification approprié (dans l'éventualité où cette opération n'aurait pas été exécutée par d'autres moyens).
– Ouvrir Sign avec la clé publique de la CA: Sr’= X.CA.PK [Sign].
– S'assurer que le Sr′ commence par ′6A′ et se termine par ′BC′.
– Calculer C_r’ et H’ d'après: 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’.

Vérifier la validité. À partir de C':

– Contrôler, le cas échéant, la date d'expiration.

Extraire et mémoriser la clé publique, l'identificateur de clé, l'autorisation du titulaire de certificat et la date d'expiration du certificat à partir du certificat C’:

– X.PK = *n* || *e*
– X.KID = CHR
– X.CHA = CHA
– X.EOV = EOV

4 Mécanisme d'authentification mutuelle

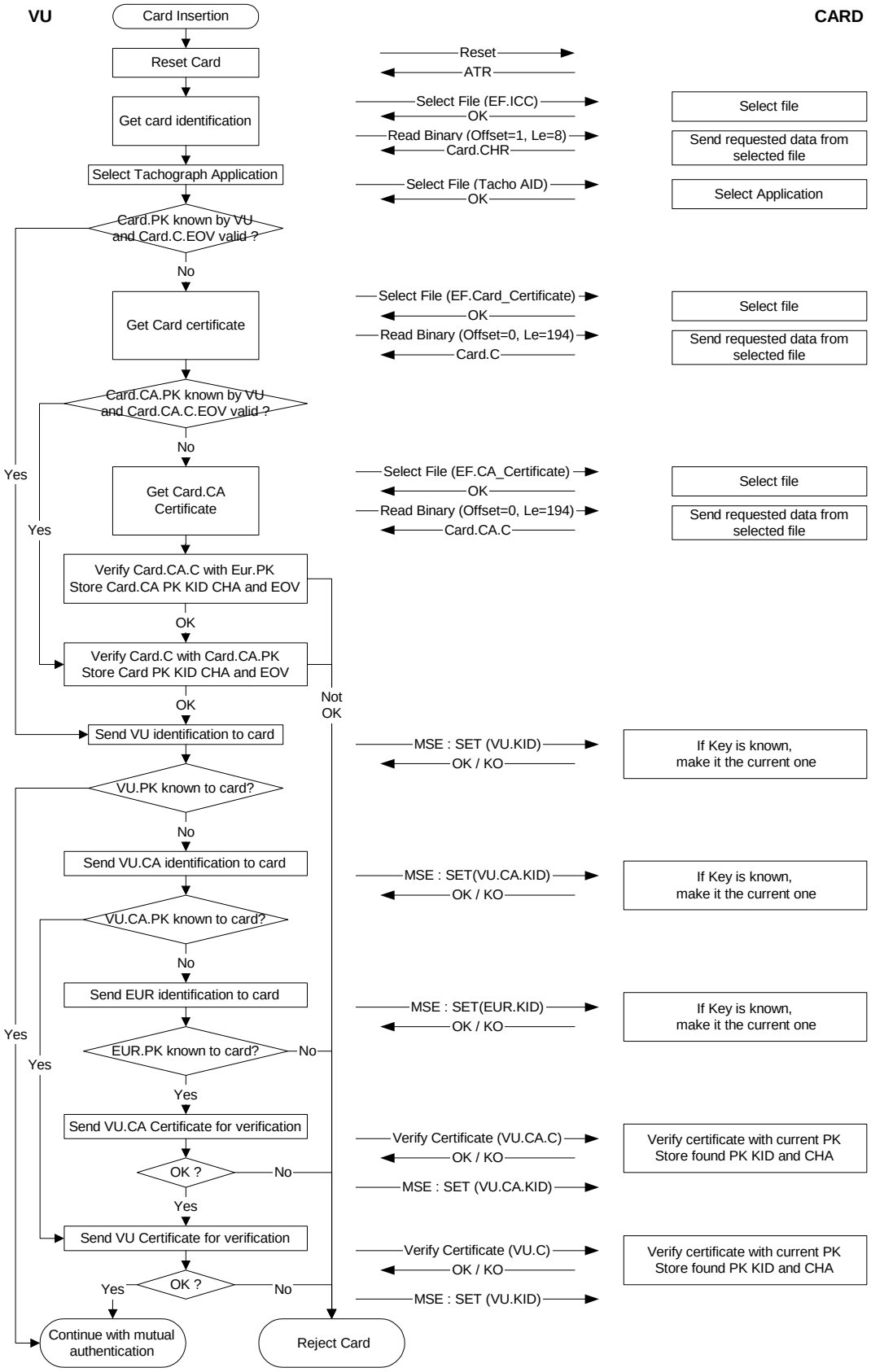
L'authentification mutuelle entre les cartes et les VU repose sur le principe suivant:

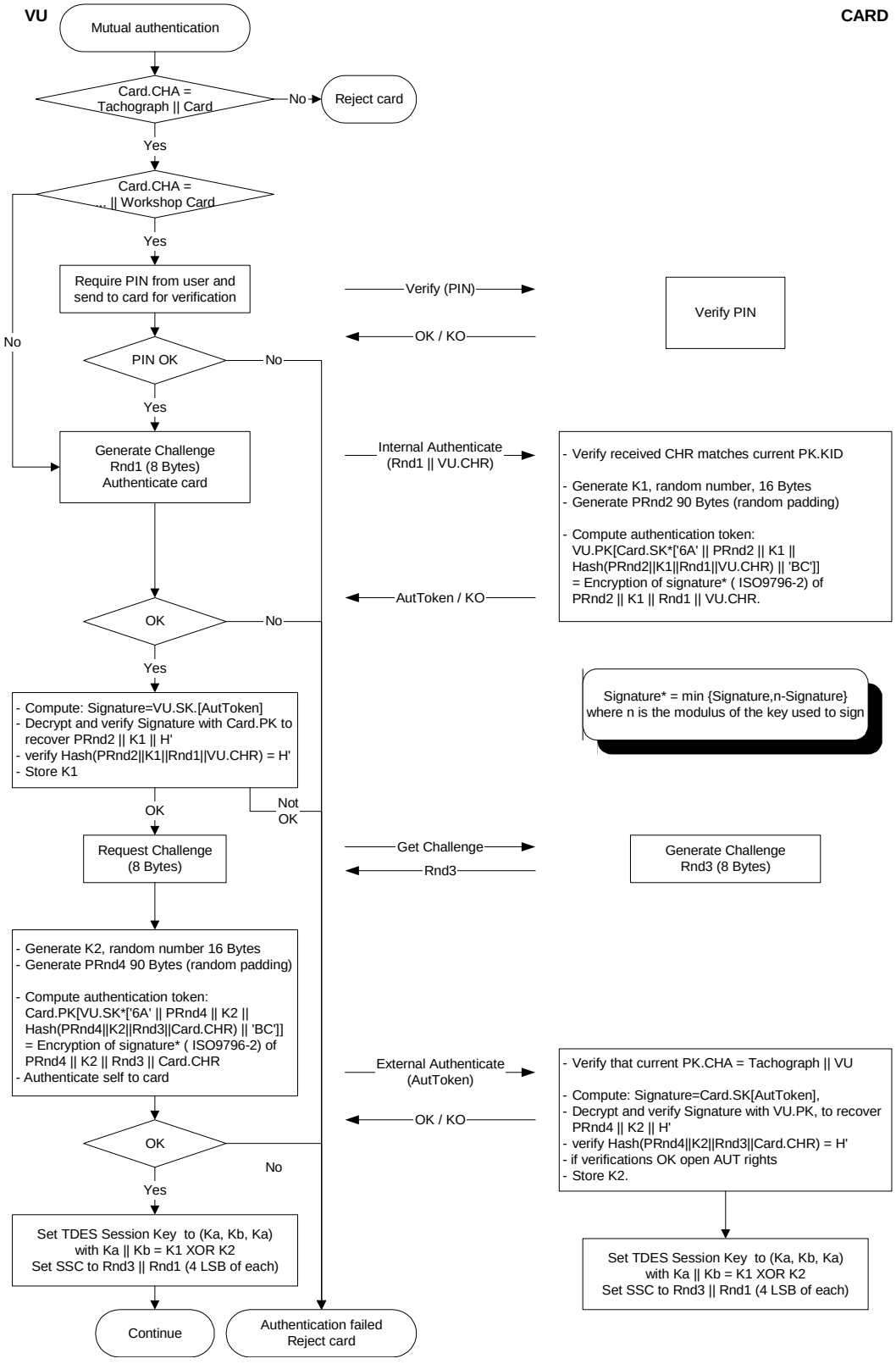
Chacune des parties doit démontrer à l'autre qu'elle possède une paire de clés valides, la clé publique qui aura permis leur homologation par l'organisme de certification national compétent étant elle-même homologuée par l'organisme de certification européen.

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.

La VU concernée déclenche le mécanisme d'authentification dès 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 Le protocole ci-après sera utilisé [les flèches indiquent les commandes et données échangées (voir 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
Not OK
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 VU et les cartes

5.1 Messagerie sécurisée

CSM_021 L'intégrité des transferts de données entre les VU et les cartes sera préservée par un dispositif de messagerie sécurisée, en conformité avec les 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 adjoindra un objet de données du type total de contrôle cryptographique aux objets de données transmis dans la commande ou la réponse. Le récepteur procédera à une vérification du total de contrôle cryptographique.

CSM_023 Le total de contrôle cryptographique des données transmises dans une commande intégrera l'en-tête de cette commande ainsi que la totalité des objets de données envoyés (= > CLA = ′0C′, et tous les objets de données seront encapsulés dans des balises au sein desquelles b1=1).

CSM_024 Les octets d'état/information transmis en réponse seront protégés par un total de contrôle cryptographique si cette réponse ne comporte aucun champ de données.

CSM_025 Les totaux de contrôle cryptographiques mesureront 4 octets de long.

Par conséquent, en cas de recours à la messagerie sécurisée, les commandes et réponses présentent la structure suivante:

Les instructions DO utilisées représentent un jeu partiel des DO de messagerie sécurisée décrites dans les dispositions de la norme ISO/CEI 7816-4:

Balise	*Mnémonique*	*Signification*
'81'	T_{PV}	Valeur simple non codée en BER-TLV (à protéger par CC)
'97'	$\mathbf{T_{LE}}$	Valeur de Le dans la commande non sécurisée (à protéger par CC)
'99'	T_{SW}	Infos d'état (à protéger par CC)
'8E'	T_{CC}	Total de contrôle cryptographique
'87'	$T_{PI\,CG}$	Octet indicateur de remplissage || Cryptogramme (valeur simple 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	[champ L_c]	[champ de données]	[champ L_e]
quatre octets				Octets L, indiquant B_1 à B_L		

Corps de la réponse	**En queue de réponse**
[champ de données]	SW1 SW2
Octets de données L_r	deux octets

La paire correspondante de réponses à une commande sécurisée se présente comme suit:

Commande sécurisée:

En-tête de commande (CH)				**Corps de la commande**										
CLA	INS	P1	P2	[nouveau champ L_c]	[nouveau champ de données]									[nouveau champ L_e]
					T_{PV}	L_{PV}	PV	$\mathbf{T_{LE}}$	L_{LE}	L_e	T_{CC}	L_{CC}	CC	
'OC'				Longueur du nouveau champ de données	'81'	L_c	Champ de données	'97'	'01'	L_e	'8E'	'04'	CC	'00'

Données à intégrer au total de contrôle = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB
PB = Octets de remplissage (80.. 00) en conformité avec les normes ISO-CEI 7816-4 et ISO 9797 méthode 2.
Les PV et LE des DO ne sont présents que si la commande non sécurisée comporte un certain nombre de données correspondantes.

Réponse sécurisée:

1. Cas où le champ de données de la réponse n'est pas vide et ne nécessite aucune protection aux fins de confidentialité:

Corps de la réponse						**En queue de réponse**
[nouveau champ de données]						Nouveau SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	Champ de données	'8E'	'04'	CC	

Données à intégrer dans le total de contrôle = T_{PV} || L_{PV} || PV || PB

2. Cas où le champ de données de la réponse n'est pas vide, mais nécessite une protection garantissant sa confidentialité:

Corps de la réponse						**En queue de réponse**
[nouveau champ de données]						Nouveau SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Données à transférer par CG: données non codées BER-TLV et octets de remplissage.
Données à intégrer dans le total de contrôle = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Cas où le champ de données de la réponse est vide:

Corps de la réponse						**En queue de réponse**
[nouveau champ de données]						Nouveau SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	Nouveaux SW1 et SW2	'8E'	'04'	CC	

Données à intégrer dans le total de contrôle = T_{SW} || L_{SW} || SW || PB

5.2 Traitement des erreurs de messagerie sécurisée

CSM_026 Si la carte tachygraphique reconnaît une erreur SM lors de l'interprétation d'une commande, les octets d'état doivent être renvoyés sans MS. Conformément à la norme ISO/CEI 7816-4, les octets d ' état suivants sont définis pour indiquer la manifestation d'erreurs de SM:

'66 88': Échec de la vérification du total de contrôle cryptographique,
'69 87': Absence d'objets de données SM prévus,
'69 88': Objets de données SM incorrects.

CSM_027 Si la carte tachygraphique renvoie des octets d'état sans DO SM ou avec une DO SM erronée, la VU doit mettre fin à la session en cours.

5.3 Algorithme de calcul des totaux de contrôle cryptographiques

CSM_028 La constitution des totaux de contrôle cryptographiques se fait à l'aide des contrôles d'accès au support (MAC) détaillés, en conformité avec la norme ANSI X9.19 à l'aide de DES:

- Phase initiale: le bloc de contrôle y0 est E(Ka, SSC).
- 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)).

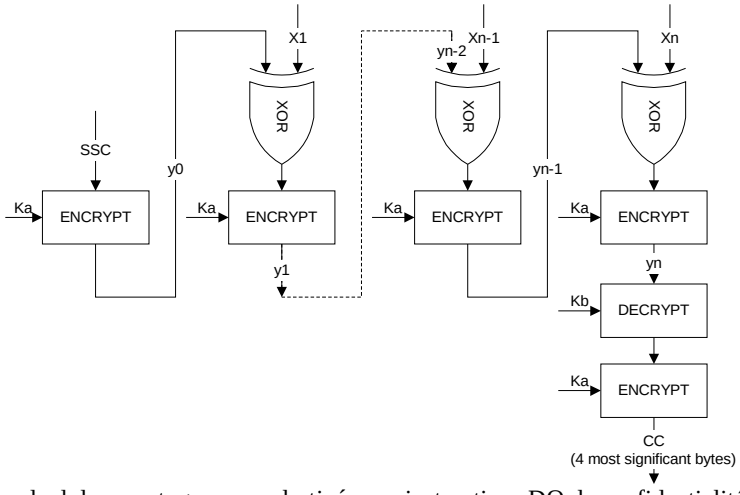
Où l'abréviation E() signifie le cryptage avec DES et l'abréviation D() le décryptage avec DES.

Les quatre octets les plus significatifs du total de contrôle cryptographique sont transférés.

CSM_029 Le compteur de séquences à l'émission (SSC) sera lancé pendant la procédure d'acceptation des clés:
SSC initial: Rnd3 (4 derniers octets significatifs) || Rnd1 (4 derniers octets significatifs).

CSM_030 Le compteur de séquences à l'émission sera incrémenté d'une unité avant le calcul de chaque MAC (en d'autres termes, le SSC associé à la première commande correspond au SSC initial + 1, tandis que le SSC associé à la première réponse correspond au SSC initial + 2).

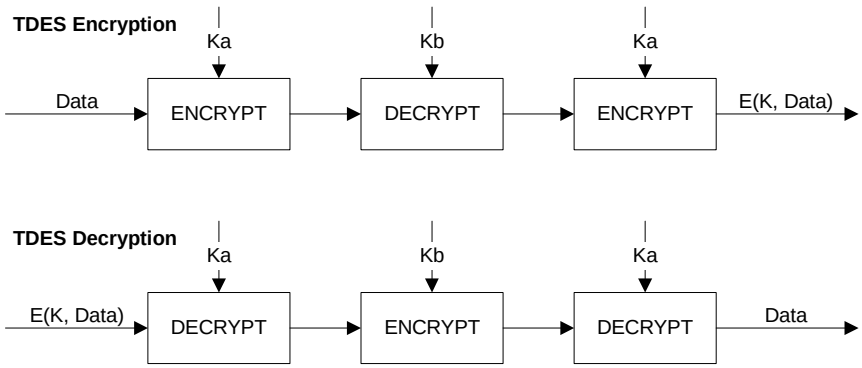
La figure ci-après illustre le calcul du MAC détaillé:



5.4 Algorithme de calcul des cryptogrammes destinés aux instructions DO de confidentialité

CSM_031 Ces cryptogrammes se calculent à l'aide du TDEA en mode d'exploitation TCBC, en conformité avec les [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 en TDES:



6 Mécanismes de signature numérique des téléchargements de données

CSM_032 L'équipement spécialisé intelligent (IDE) enregistre au sein d'un fichier de données physiques les données transmises à partir d'un équipement (VU ou carte) donné, pendant une session de téléchargement. Ce fichier doit contenir les certificats MS_i.C et EQT.C. Le fichier contient les signatures numériques associées de blocs de données conformément aux indications fournies dans l'appendice 7 (Protocoles de téléchargement des données).

CSM_033 Les signatures numériques des données téléchargées reposeront sur l'utilisation d'un schéma de signature numérique avec appendice permettant, le cas échéant, de lire des données téléchargées sans aucun décryptage.

6.1 Génération de signatures

CSM_034 La génération de signatures de données par l'équipement respectera le schéma de signature avec appendice, défini dans le document de référence [PKCS1] avec la fonction de hachage SHA-1:

Signature = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(Data))]

PS = Chaîne d'octets de remplissage de valeur ′FF′ dont la longueur équivaut à 128.

DER(SHA-1(*M*)) correspond à l'encodage de l'ID de l'algorithme pour la fonction de hachage et la valeur de hachage, dans une valeur ASN.1 de type `DigestInfo` (règles d'encodage distinctes):

‘30’||‘21’||‘30’||‘09’||‘06’||‘05’||‘2B’||‘0E’||‘03’||‘02’||‘1A’||‘05’||‘00’||‘04’||‘14’||Valeur de hachage

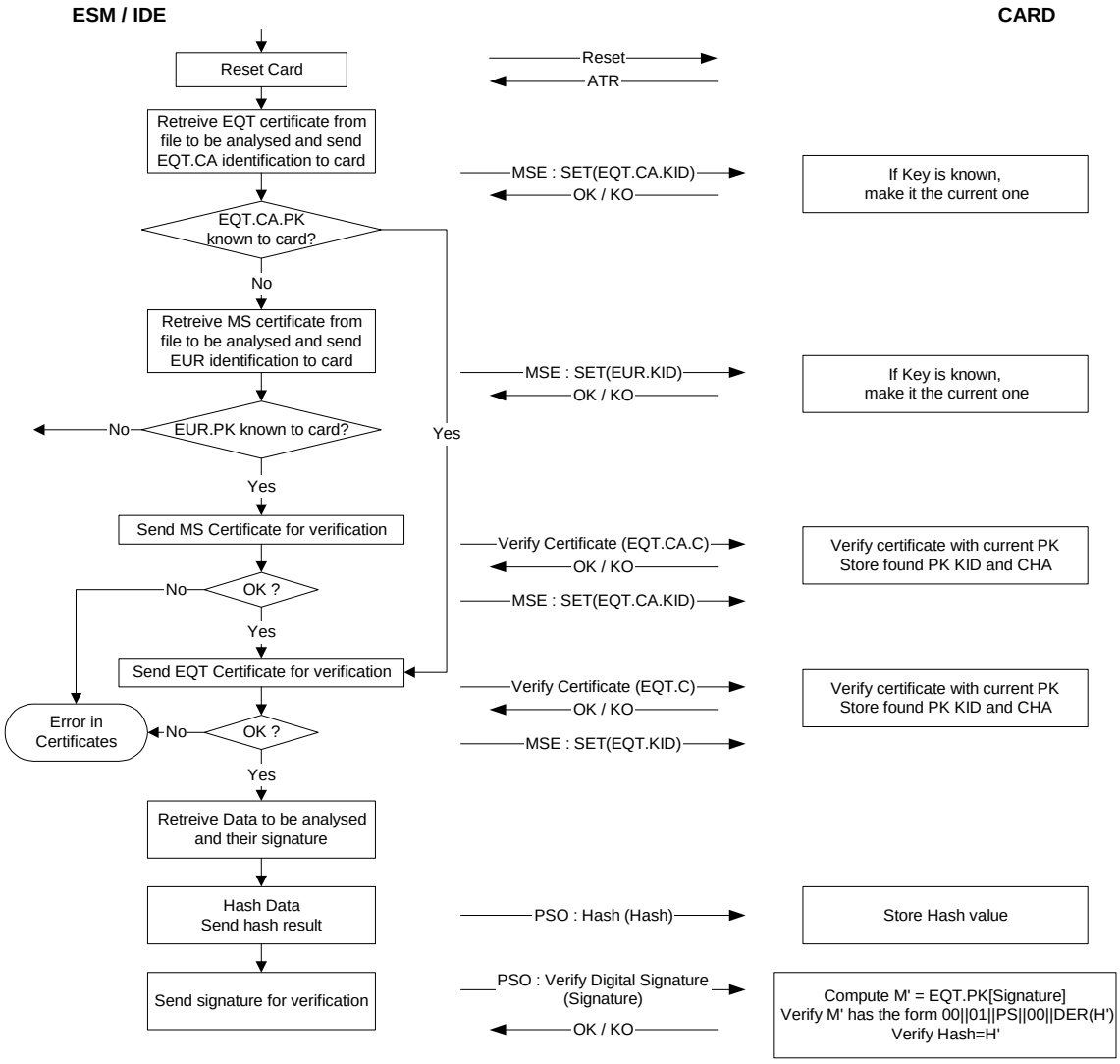
6.2 Vérification de signatures

CSM_035 La vérification de signatures de données, à laquelle sont soumises les données téléchargées, respectera le schéma de signature avec appendice, défini dans le document de référence [PKCS1] avec la fonction de hachage SHA-1.

Le vérificateur doit connaître (et approuver) la clé publique européenne EUR.PK.

Le tableau qui suit illustre le protocole qu'un équipement IDE doté d'une carte de contrôle est susceptible de respecter pour vérifier l'intégrité des données téléchargées et enregistrées sur l'ESM (support de mémoire externe). La carte de contrôle permet de procéder au décryptage des signatures numériques. Dans le cas présent, cette fonction n'est pas nécessairement implémentée au sein de l'IDE.

L'équipement qui a participé au téléchargement et à la signature des données à analyser est désigné par l'abréviation EQT.


ESM / IDE
CARD
Reset Card
Reset
ATR
Retreive EQT certificate from file to be analysed and send EQT.CA identification to card
MSE : SET(EQT.CA.KID)
OK / KO
If Key is known, make it the current one
EQT.CA.PK known to card?
No
Retreive MS certificate from file to be analysed and send EUR identification to card
MSE : SET(EUR.KID)
OK / KO
If Key is known, make it the current one
No
EUR.PK known to card?
Yes
Yes
Send MS Certificate for verification
Verify Certificate (EQT.CA.C)
OK / KO
Verify certificate with current PK Store found PK KID and CHA
No
OK ?
MSE : SET(EQT.CA.KID)
Yes
Send EQT Certificate for verification
Verify Certificate (EQT.C)
OK / KO
Verify certificate with current PK Store found PK KID and CHA
Error in Certificates
No
OK ?
MSE : SET(EQT.KID)
Yes
Retreive Data to be analysed and their signature
Hash Data
Send hash result
PSO : Hash (Hash)
Store Hash value
Send signature for verification
PSO : Verify Digital Signature (Signature)
OK / KO
Compute M' = EQT.PK[Signature]
Verify M' has the form 00||01||PS||00||DER(H')
Verify Hash=H'

PARTIE B TACHYGRAPHE DE DEUXIÈME GÉNÉRATION

1 Introduction

1.1 Références

Le présent appendice fait référence aux références suivantes:

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 2013-04-15
ISO 7816-8	ISO/CEI 7816-8 Cartes d'identification - Cartes à circuit intégré - Partie 8 Commandes pour des opérations de sécurité. Seconde édition: 2004-06-01
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, 2008-12-15
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 cryptage par blocs. Seconde édition: 2011-03-01
ISO 10116	ISO/CEI 10116,Technologies de l'information - Techniques de sécurité - Modes opératoires pour un cryptage par blocs de *n* bits. Troisième édition 2006-02-01
ISO16844-3	ISO/CEI 16844-3 Véhicules routiers – Systèmes tachygraphiques – Partie 3: Interface de capteur de mouvement. Première édition 2004, comprenant le rectificatif technique 1 2006
RFC 5480	Informations relatives à la clé publique soumise à cryptographie à courbe elliptique, mars 2009
RFC 5639	Cryptographie à courbe elliptique (ECC) - Génération de courbes et de courbes standard Brainpool, 2010
RFC 5869	Fonction de dérivation de clé par extraction et expansion basée sur HMAC (HKDF), mai 2010
SHS	National Institute of Standards and Technology (NIST), FIPS PUB 180-4: Norme de hachage sécurisé, mars 2012
SP 800-38B	National Institute of Standards and Technology (NIST), Special Publication 800-38B: Recommandation pour les modes d'exploitation de cryptage par blocs: Mode CMAC d'authentification, 2005
TR-03111	BSI Technical Guideline TR-03111, Cryptographie à courbe elliptique, version 2.00, 2012-06-28

1.2 Notations et abréviations

Les notations et abréviations qui suivent apparaissent dans le présent appendice:

AES Norme de cryptage avancé (Advanced Encryption Standard)
CA Organisme de certification
CAR Références de l ' organisme de certification
CBC Mode d'exploitation par chaînage de blocs de données cryptées TDEA
CH En-tête de commande
CHA Autorisation d'un titulaire de certificat

CHR Références d'un titulaire de certificat
CV Vecteur constant
DER Règles de codage distinctes
DO Objet de données
DSRC Communication dédiée de courte portée
ECC Cryptographie à courbe elliptique
ECDSA Algorithme de signature numérique à courbe elliptique
ECDH Courbe elliptique de Diffie-Hellman (algorithme de concordance de clé)
EGF Dispositif GNSS externe
EQT Équipement
IDS identificateur de service
K_M Clé maîtresse du capteur de mouvement permettant de coupler une unité embarquée sur véhicule avec un capteur de mouvement
K_{M-VU} Clé insérée dans les unités embarquées sur véhicule permettant à une VU d'extraire la clé maîtresse du capteur de mouvement si une carte d'atelier est insérée dans la VU
K_{M-WC} Clé insérée dans les cartes d'atelier permettant à une VU d'extraire la clé maîtresse du capteur de mouvement si une carte d'atelier est insérée dans la VU
MAC Code d'authentification du message
MoS Capteur de mouvement
MSB Octet le plus significatif
PKI Infrastructure à clé(s) publique(s) (ICP) ou infrastructure de gestion de clés (IGC)
RCF Équipement de communication à distance
SSC Compteur de séquences d ' émission
MS Messagerie sécurisée
TDES Triple Data Encryption Standard (norme relative au cryptage triple des données)
TLV Longueur des marqueurs
VU Unité embarquée sur le véhicule
X.C Certificat de clé publique d'un utilisateur X
X.CA Organisme de certification qui a émis le certificat d'un utilisateur X
X.CAR Référence de l'organisme de certification mentionnée dans le certificat d'un utilisateur X
X.CHR Référence du titulaire 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

1.3 Définitions

Les définitions des termes utilisés dans le présent appendice figurent à la section 1 de l'annexe 1C.

2 Systèmes et algorithmes cryptographiques

2.1 Systèmes cryptographiques

TCS_180 Les unités embarquées sur véhicule et les cartes tachygraphiques auront recours à un système cryptographique classique à clé publique à courbe elliptique pour assurer les mécanismes de sécurité suivants:
- authentification mutuelle entre une unité embarquée sur véhicule et une carte,
- concordance des clés de session AES entre une unité embarquée sur véhicule et une carte,
- assurer l'authenticité, l'intégrité et la non- répudiation des données téléchargées depuis les unités embarquées sur véhicule ou depuis les cartes tachygraphiques vers un support de stockage externe.

TCS_181 Les unités embarquées sur véhicule et les dispositifs GNSS externes auront recours à un système cryptographique à clé publique à courbe elliptique pour assurer les mécanismes de sécurité suivants:
- couplage d'une unité embarquée sur véhicule et d'un dispositif GNSS externe,
- authentification mutuelle entre une unité embarquée sur véhicule et un dispositif GNSS externe,
- concordance d'une session de clé AES entre une unité embarquée sur véhicule et un dispositif GNSS externe.

TCS_182 Les unités embarquées sur véhicule et les cartes tachygraphiques auront recours à un système cryptographique AES symétrique pour assurer les mécanismes de sécurité suivants:
- assurer l'authenticité et l'intégrité des données échangées entre une unité embarquée sur véhicule et une carte tachygraphique,
- le cas échéant, assurer la confidentialité des données échangées entre une unité embarquée sur véhicule et une carte tachygraphique.

TCS_183 Les unités embarquées sur véhicule et les dispositifs GNSS externes auront recours à un système cryptographique AES symétrique pour assurer les mécanismes de sécurité suivants:
- assurer l'authenticité et l'intégrité des données échangées entre une unité embarquée sur véhicule et un dispositif GNSS externe.

TCS_184 Les unités embarquées sur véhicule et les capteurs de mouvement auront recours à un système cryptographique AES symétrique pour assurer les mécanismes de sécurité suivants:
- couplage d'une unité embarquée sur véhicule et d'un capteur de mouvement,
- authentification mutuelle entre une unité embarquée sur véhicule et un capteur de mouvement,
- assurer la confidentialité des données échangées entre une unité embarquée sur véhicule et un capteur de mouvement.

TCS_185 Les unités embarquées sur véhicule et les cartes de contrôle auront recours à un système cryptographique AES symétrique pour assurer les mécanismes de sécurité suivants:
- assurer la confidentialité, l'authenticité et l'intégrité des données transmises par une unité embarquée sur véhicule à une carte de contrôle.

Remarques:
- Pour être précis, les données sont transmises par une unité embarquée sur véhicule vers un interrogateur distant sous le contrôle d'un agent de contrôle, qui se sert d'un dispositif de communication à distance interne ou externe à la VU; cf. appendice 14. Cependant, l'interrogateur distant adresse les données reçues à une carte de contrôle qui les déchiffre et valide leur authenticité. Du point de vue de la sécurité, le dispositif de communication distant et l'interrogateur distant sont entièrement transparents.
- Une carte d'atelier offre les mêmes services de sécurité au regard de l'interface DSRC qu'une carte de contrôle. Cela permet à un atelier de valider le fonctionnement satisfaisant de l'interface de communication à distance d'une VU, y compris la sécurité. Consulter la section 3.2.2 pour toute information complémentaire.

2.2 Algorithmes cryptographiques

2.2.1 Algorithmes symétriques

TCS_186 Les unités embarquées sur véhicule, cartes tachygraphiques, capteurs de mouvement et dispositifs GNSS externes devront être compatibles avec l'algorithme AES défini dans [AES] en respectant les longueurs de clés de 128, 192 et 256 bits.

2.2.2 Algorithmes asymétriques et paramètres de domaine normalisés

TCS_187 Les unités embarquées sur véhicule, cartes tachygraphiques et dispositifs GNSS externes devront être compatibles avec la cryptographie à courbe elliptique et respecter les longueurs de clés de 256, 384 et 512/521 bits.

TCS_188 Les unités embarquées sur véhicule, cartes tachygraphiques et dispositifs GNSS externes devront être compatibles avec l'algorithme de signature ECDSA défini dans [DSS].

TCS_189 Les unités embarquées sur véhicule, cartes tachygraphiques et dispositifs GNSS externes devront être compatibles avec l'algorithme de concordance avec les clés ECKA-EG défini dans [TR 03111].

TCS_190 Les unités embarquées sur véhicule, cartes tachygraphiques et dispositifs GNSS externes devront être compatibles avec tous les paramètres de domaines normalisés définis au Tableau 43 ci-après se rapportant à la cryptographie à courbe elliptique.

Nom	*Tailles (en bits)*	*Référence*	*Identificateur d'objet*
NIST P-256	256	[DSS], [RFC 5480]	secp256r1
BrainpoolP256r1	256	[RFC 5639]	brainpoolP256r1
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

Tableau 43Paramètres de domaines normalisés

Note: les identificateurs d'objet mentionnés dans la dernière colonne du Tableau 43 sont spécifiés dans [RFC 5639] pour les courbes Brainpool et dans [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}.
Ou en notation par point: 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}.
Ou en notation par point: 1.3.132.0.34.

2.2.3 Algorithmes de hachage

TCS_191 Les unités embarquées sur véhicule et les cartes tachygraphiques devront être compatibles avec les algorithmes SHA-256, SHA-384 et SHA-512 définis dans [SHS].

2.2.4 Méthodes de cryptage

TCS_192 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 (quasiment) égale. Le Tableau 44 montre les méthodes de cryptage autorisées:

ID Suite cryptée	*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

ID Suite cryptée	*Taille de clé ECC (en bits)*	*Longueur de clé AES (en bits)*	*Algorithme de hachage*	*Longueur MAC (en octets)*
CS#3	512/521	256	SHA-512	16

Tableau 44 Méthodes de cryptage autorisées

Remarque: les tailles de clés ECC de 512 et 521 bits sont considérées de force égale quelle que soit leur utilisation dans le cadre du présent appendice.

3 Clés et certificats

3.1 Paires de clés asymétriques et certificats de clé publique

3.1.1 Généralités

Note: les clés décrites dans cette section servent à l'authentification mutuelle et à la messagerie sécurisée entre les unités embarquées sur véhicule et les cartes tachygraphiques, ainsi qu'entre les unités embarquées sur véhicule et les dispositifs GNSS externes. Ces processus sont décrits en détail dans les chapitres 4 et 5 du présent appendice.

TCS_193 Au sein du système de tachygraphie intelligente européenne, les paires de clés ECC et leurs certificats sont générés et gérés selon trois niveaux hiérarchiques fonctionnels:

- niveau européen,
- niveau État membre,
- niveau équipement.

TCS_194 Au sein du système de tachygraphie intelligente européenne, les clés privées et publiques ainsi que les certificats sont générés, gérés et communiqués au moyen de méthodes sécurisées et normalisées.

3.1.2 Niveau européen

TCS_195 Au niveau européen, il est généré une seule paire de clés ECC, appelées EUR. Elle se compose d'une clé privée (EUR.SK) et d'une clé publique (EUR.PK). Cette paire de clés forment la paire racine de la PKI de tachygraphie intelligente européenne. Ces tâches sont exécutées par une Autorité de certification racine européenne (ERCA), placée sous l'autorité et la responsabilité de la Commission européenne.

TCS_196 L'ERCA utilise la clé privée européenne pour signer un certificat racine (autosigné) de la clé publique européenne et communique ce certificat racine européen à tous les États membres.

TCS_197 L'ERCA utilise la clé privée européenne pour signer les certificats des clés publiques dans les États membres sur demande. L'ERCA conserve les relevés de tous les certificats de clé publique signés délivrés aux États membres.

TCS_198 Comme le montre la Figure 1 de la section 3.1.7, l'ERCA génère une nouvelle paire de clés racine européenne tous les 17 ans. Dès lors que l'ERCA génère une nouvelle paire de clés racine européenne, l'organisme crée un nouveau certificat racine autosigné destiné à la nouvelle clé publique européenne. 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; cf. sections 3.2.1.2 et 3.2.2.2.

TCS_199 Avant de générer une nouvelle paire de clés racine européenne, l'ERCA mène une analyse de la force cryptographique nécessaire pour la nouvelle paire de clés, sachant qu'elle doit rester sécurisée pendant les 34 prochaines années. Si cela se révèle nécessaire, l'ERCA adopte une méthode de cryptage plus puissante que l'actuelle, comme le prévoit TCS_192.

TCS_200 Dès lors que l'ERCA génère une nouvelle paire de clés racine européenne, l'organisme crée un nouveau certificat de lien destiné à la nouvelle clé publique européenne et le signe avec la clé privée européenne précédente. La durée de validité du certificat de lien est de 17 ans. La Figure 1 de la section 3.1.7 l'illustre également.

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 à l'équipement de génération *X-1*, une méthode permettant de se fier à l'équipement de génération *X*.

TCS_201 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.

TCS_202 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 valides,
- les certificats de lien de toutes les générations de certificats EUR à l'exception du premier.

3.1.3 Niveau État membre

TCS_203 Au niveau de l'État membre, tous les États membres devant signer les certificats de carte tachygraphique génèrent une ou plusieurs paires de clés ECC unique, appelée MSCA_Card. Tous les États membres devant signer les certificats des unités embarquées sur véhicule ou des dispositifs GNSS externes génèrent en plus une ou plusieurs paires de clés ECC unique, appelée MSCA_VU-EGF.

TCS_204 La tâche de la génération des paires de clés de l'État membre incombe à l'autorité de certification de l'État membre (MSCA). Dès lors qu'une MSCA génère une paire de clés pour un État membre, elle doit adresser la clé publique à l'ERCA afin d'obtenir un certificat propre à l'État membre correspondant, signé par l'ERCA.

TCS_205 Une MSCA choisit la force de la paire de clés de l'État membre égale à celle de la paire de clés racine européenne servant à signer le certificat de l'État membre correspondant.

TCS_206 Une paire de clés MSCA_VU-EGF, le cas échéant, se compose d'une clé privée MSCA_VU-EGF.SK et d'une clé publique MSCA_VU-EGF.PK. Une MSCA utilise la clé privée MSCA_VU-EGF.SK exclusivement pour signer les certificats de clé publique des unités embarquées sur véhicule et des dispositifs GNSS externes.

TCS_207 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.

TCS_208 Une MSCA conserve des archives de tous les certificats de VU signés, de tous les certificats de dispositifs GNSS externes signés et de tous les certificats de cartes ainsi que l'identification de l'équipement auquel est destiné chacun de ces certificats.

TCS_209 La durée de validité d'un certificat MSCA_VU-EGF est de 17 ans plus trois mois. La durée de validité d'un certificat MSCA_Card est de 7 ans plus un mois.

TCS_210 Comme l'illustre la Figure 1 à la section 3.1.7, la clé privée d'une paire de clés MSCA_VU-EGF et la clé privée d'une paire de clé MSCA_Card possèdent une durée d'utilisation de deux années.

TCS_211 Une MSCA n'utilise pas la clé privée d'une paire de clés MSCA_VU-EGF à quelque fin que ce soit après l'expiration de sa période d'utilisation. De même, une MSCA n'utilise pas la clé privée d'une paire de clés MSCA_Card à quelque fin que ce soit après l'expiration de sa période d'utilisation.

TCS_212 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 valides.

TCS_213 Si une MSCA doit signer des certificats pour des unités embarquées sur véhicule ou pour des dispositifs GNSS externes, la MSCA doit également avoir à disposition les clés et certificats suivants:

- la paire de clés MSCA_VU-EGF en vigueur et le certificat correspondant,
- toutes les clés publiques MSCA_VU-EGF antérieures à utiliser pour vérifier les certificats des VU ou des dispositifs GNSS externes toujours valides.

3.1.4 Niveau équipement: unités embarquées sur véhicule

TCS_214 Deux paires de clés ECC uniques sont générées pour chaque unité embarquée sur véhicule, appelées VU_MA et VU_Sign. Cette tâche incombe aux fabricants de VU. Dès lors qu'une paire de clés VU est générée, la partie qui la génère doit adresser la clé publique à la MSCA de son pays de résidence afin d'obtenir un certificat VU correspondant, signé par la MSCA. La clé privée sert uniquement à une unité embarquée sur véhicule.

TCS_215 Les certificats VU_MA et VU_Sign attribués à une unité embarquée sur véhicule donnée possèdent la même date d'entrée en vigueur de certificat.

TCS_216 Un fabricant de VU choisit la force d'une paire de clés VU égale à celle de la paire de clés MSCA servant à signer le certificat VU correspondant.

TCS_217 Une unité embarquée sur véhicule utilise sa paire de clés VU_MA, composée d'une clé privée VU_MA.SK et d'une clé publique VU_MA.PK, exclusivement pour effectuer des opérations d'authentification de VU avec les cartes tachygraphiques et les dispositifs GNSS externes, comme le prévoient les sections 4.3 et 5.4 du présent appendice.

TCS_218 Une unité embarquée sur véhicule doit pouvoir générer des paires de clés ECC éphémères et utiliser une paire de clés éphémères exclusivement pour effectuer la concordance de clés de session avec une carte tachygraphique ou un dispositif GNSS externe, comme le prévoient les sections 4.4 et 5.4 du présent appendice.

TCS_219 Une unité embarquée sur véhicule utilise la clé privée VU_Sign.SK de sa paire de clés VU_Sign exclusivement pour signer des fichiers de données téléchargés, comme le prévoit le chapitre 8 du présent appendice. La clé publique VU_Sign.PK correspondante sert exclusivement à vérifier les signatures créées par la VU.

TCS_220 Comme le montre la Figure 1 de la section 3.1.7, la durée de validité d'un certificat VU_MA est de 15 ans et trois mois. La durée de validité d'un certificat VU_Sign est également de 15 ans et trois mois.

Remarques:

- La durée de validité étendue d'un certificat VU_Sign permet à une unité embarquée sur véhicule de créer des signatures valides par rapport à 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 VU_MA est nécessaire pour permettre à la VU d'authentifier une carte de contrôle ou une carte d'entreprise pendant les trois premiers mois qui suivent sa date d'expiration, de manière à pouvoir effectuer des téléchargements de données.

TCS_221 Une VU n'utilise pas la clé privée d'une paire de clés VU à quelque fin que ce soit après l'expiration du certificat correspondant.

TCS_222 Les paires de clés VU (hormis les paires de clés éphémères) et les certificats correspondants pour une VU donnée ne sont ni remplacés ni renouvelés sur le terrain une fois que la VU 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 la VU à chaque exécution d'une authentification de circuit et à chaque concordance de clé de session; cf. section 4.4. Remarque: les paires de clés éphémères ne possèdent pas de certificats correspondants.
- Cette exigence n'interdit pas la possibilité de remplacer les paires de clés VU statiques lors d'une maintenance ou d'une réparation dans un environnement contrôlé et sécurisé par le fabricant de VU.

TCS_223 Lorsqu'elle est mise en service, la VU contient les clés et les certificats cryptographiques suivants:

- la clé privée VU_MA et le certificat correspondant;

- la clé privée VU_Sign et le certificat correspondant;
- le certificat MSCA_VU-EGF comprenant la clé publique MSCA_VU-EGF.PK à utiliser pour vérifier les certificats VU_MA et VU_Sign;
- le certificat EUR comprenant la clé publique EUR.PK à utiliser pour vérifier le certificat MSCA_VU-EGF;
- le certificat EUR dont la durée de validité précède directement celle du certificat EUR à utiliser pour vérifier le certificat MSCA_VU-EGF, le cas échéant;
- le certificat de lien reliant ces deux certificats EUR, le cas échéant.

TCS_224 Outre les clés et les certificats cryptographiques listés en TCS_223, les VU contiennent également les clés et les certificats précisés à la partie A du présent appendice, permettant à une VU d'interagir avec les cartes tachygraphiques de première génération.

3.1.5 Niveau équipement: cartes tachygraphiques

TCS_225 Une paire de clés ECC unique appelée Card_MA est générée pour chaque carte tachygraphique. Une deuxième paire de clés ECC unique, appelé Card_Sign, est générée en plus pour chaque carte de conducteur et chaque carte d'atelier. Cette tâche incombe aux fabricants et aux personnalisateurs de cartes. Dès lors qu'une paire de clés pour carte est générée, la partie la générant doit adresser la clé publique à la MSCA de son pays de résidence afin d'obtenir un certificat pour carte correspondant, signé par la MSCA. La clé privée sert uniquement à la carte tachygraphique.

TCS_226 Les certificats Card_MA et Card_Sign attribués à une carte de conducteur ou d'atelier donnée possèdent la même date d'entrée en vigueur de certificat.

TCS_227 Un fabricant ou un personnalisateur de carte choisit la force d'une paire de clés pour carte égale à celle de la paire de clés MSCA servant à signer le certificat pour carte correspondant.

TCS_228 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 des clés de session avec les VU, comme le prévoient les sections 4.3 et 4.4 du présent appendice.

TCS_229 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 le prévoit le chapitre 8 du présent appendice. La clé publique Card_Sign.PK correspondante sert exclusivement à vérifier les signatures créées par la carte.

TCS_230 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 ans
- Pour les cartes de contrôle: 2 ans
- Pour les cartes d'atelier: 1 an

TCS_231 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

Note: la durée de validité étendue d'un certificat Card_Sign permet à une carte de conducteur de créer des signatures valides par rapport à 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.

TCS_232 Les paires de clés et les certificats correspondants d'une carte tachygraphique donnée ne sont ni remplacés ni renouvelés après l'émission de ladite carte.

TCS_233 Une fois émises, les cartes tachygraphiques contiennent 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.

TCS_234 Outre les clés et les certificats cryptographiques listés en TCS_233, les cartes tachygraphiques contiennent également les clés et les certificats précisés à la partie A du présent appendice, leur permettant d'interagir avec les VU de première génération.

3.1.6 Niveau équipement: dispositifs GNSS externes

TCS_235 Une paire de clés ECC unique appelée EGF_MA est générée pour chaque dispositif GNSS externe. Cette tâche incombe aux fabricants des dispositifs GNSS externes. Dès lors qu'une paire de clés EGF_MA est générée, la clé publique doit être adressée à la MSCA du pays de résidence afin d'obtenir un certificat EGF_MA correspondant, signé par la MSCA. La clé privée sert uniquement au dispositif GNSS externe.

TCS_236 Un fabricant d'EGF choisit la force d'une paire de clés EGF_MA égale à celle de la paire de clés MSCA servant à signer le certificat EGF_MA correspondant.

TCS_237 Un dispositif GNSS externe utilise sa paire de clés EGF_MA, composée d'une clé privée EGF_MA.SK et d'une clé publique EGF_MA.PK, exclusivement pour effectuer des opérations d'authentification mutuelle et de concordance des clés de session avec les VU, comme le prévoient les sections 5.4 et 5.4 du présent appendice.

TCS_238 La durée de validité d'un certificat EGF_MA est de 15 ans.

TCS_239 Un dispositif GNSS externe n'utilise pas la clé privée d'une paire de clés EGF_MA pour se coupler à une VU après l'expiration du certificat correspondant.

Note: comme l'explique la section 5.3.3, un EGF peut utiliser sa clé privée pour procéder à une authentification mutuelle avec la VU à laquelle il est couplé, y compris après l'expiration du certificat correspondant.

TCS_240 La paire de clés EGF_MA et les certificats correspondants pour un dispositif GNSS externe donné ne sont ni remplacés ni renouvelés sur le terrain une fois que l'EGF entre en opération.

Remarque: cette exigence n'interdit pas la possibilité de remplacer les paires de clés EGF lors d'une maintenance ou d'une réparation dans un environnement contrôlé et sécurisé par le fabricant d'EGF.

TCS_241 Lorsqu'il entre en opération, le dispositif GNSS externe contient les clés et les certificats cryptographiques suivants:

- la clé privée EGF_MA et le certificat correspondant;
- le certificat MSCA_VU-EGF comprenant la clé publique MSCA_VU-EGF.PK à utiliser pour vérifier le certificat EGF_MA;
- le certificat EUR comprenant la clé publique EUR.PK à utiliser pour vérifier le certificat MSCA_VU-EGF;
- le certificat EUR dont la durée de validité précède directement celle du certificat EUR à utiliser pour vérifier le certificat MSCA_VU-EGF, le cas échéant;
- le certificat de lien reliant ces deux certificats EUR, le cas échéant.

3.1.7 Généralités: certificat de substitution

La Figure 1 ci-après montre comment différentes générations de certificats racine ERCA, de certificats de lien ERCA, de certificats MSCA et d'équipement (VU et carte) sont émis et utilisés au fil du temps:

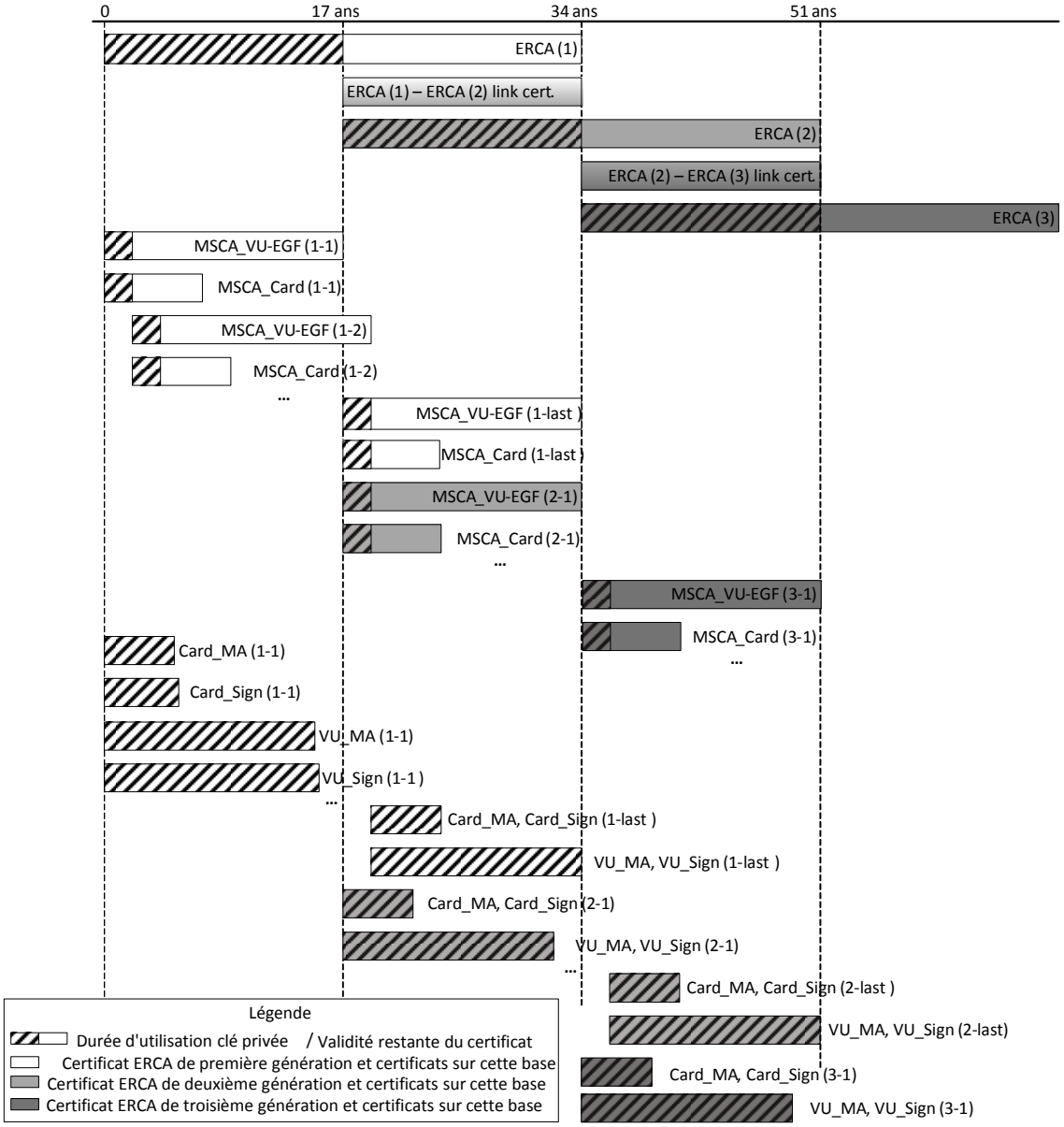


Figure 1 Émission et utilisation de différentes générations de certificats racine ERCA, de certificats de lien ERCA, de certificats MSCA et d'équipement

Légende

Notes relatives à la Figure 1:

1. Le nombre entre parenthèses indique les différentes générations du certificat racine. P. ex. ERCA (1) désigne le certificat racine ERCA de première génération; ERCA (2) désigne celui de deuxième génération; etc.
2. D'autres certificats sont repérés par deux nombres entre parenthèses. Le premier indique la génération du certificat racine dont relève leur émission, le deuxième indique la génération du certificat lui-même. P. ex. MSCA_Card (1-1) désigne le premier certificat MSCA_Card émis sous ERCA (1); MSCA_Card (2-1) désigne

le premier certificat MSCA_Card émis sous ERCA (2); MSCA_Card (2-last) désigne le dernier certificatMSCA_Card émis sous ERCA (2); Card_MA(2-1) désigne le premier certificat Card pour l'authentification mutuelle émis sous 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 ERCA (2) peu de temps après MSCA_Card (1-last), le dernier certificat MSCA_Card sous ERCA (1).
4. Comme l'illustre la figure, les premiers certificats VU et Card émis sous ERCA (2) apparaissent presque deux ans avant que n'apparaissent les derniers certificats VU et Card émis sous ERCA (1). Cela s'explique par le fait que les certificats VU et Card sont émis sous un certificat MSCA, pas directement sous le certificat ERCA. Le certificat MSCA (2-1) est émis immédiatement après l'entrée en validité d'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 présentent à peu de chose près la même durée de validité, malgré le fait qu'ils sont de générations différentes.
5. La durée de validité indiquée sur ces cartes est 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 VU_MA et VU_Sign n'est précisée que pour la première génération.

3.2 Clés symétriques

3.2.1 Clés de sécurisation de la communication du capteur de mouvement de la VU

3.2.1.1 Généralités

Note: les lecteurs de la présente section doivent maîtriser le contenu de la norme [ISO 16844-3] qui décrit l'interface entre une VU et un capteur de mouvement. La procédure de couplage entre une VU et un capteur de mouvement est décrite en détail au chapitre 6 du présent appendice.

TCS_242 Un nombre de clés symétriques donné est nécessaire pour coupler des VU 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. 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 (anticipée), comme le prévoit le TCS_192.

Légende	*Symbole*	*Produit par*	*Méthode de génération*	*Mémorisé par*
Clé maîtresse du capteur de mouvement - partie VU	KM-VU	ERCA	Aléatoire	ERCA, MSCA impliquées dans l'émission des certificats VU, fabricants de VU, VU
Clé maîtresse du capteur de mouvement - partie atelier	KM-WC	ERCA	Aléatoire	ERCA, MSCA, fabricants de cartes, cartes d'atelier
Clé maîtresse du capteur de mouvement	KM	Généré de manière non indépendante	Calculé comme KM = KM-VU XOR KM-WC	ERCA, MSCA impliquées dans l'émission des clés de capteurs de mouvement (facultatif)*
Clé d'identification	KID	Généré de manière non indépendante	Calculé comme KID = KM XOR CV, où CV est défini par le TCS_248	ERCA, MSCA impliquées dans l'émission des clés de capteurs de mouvement (facultatif)*
Clé de	KP	Fabricant des capteurs de	Aléatoire	Un capteur de

Légende	*Symbole*	*Produit par*	*Méthode de génération*	*Mémorisé par*
couplage		mouvement		mouvement
Clé de session	KS	VU (durant le couplage de la VU et du capteur de mouvement)	Aléatoire	Une VU et un capteur de mouvement

Tableau 45 Clés de sécurisation de la VU - communication du capteur de mouvement

*Le stockage de K_M et K_{ID} est facultatif, car ces clés peuvent être calculées selon K_{M-VU}, K_{M-WC} et CV.

TCS_243 L'autorité de certification racine européenne génère K_{M-VU} et K_{M-WC}, deux clés AES aléatoires et uniques dont dérive le calcul de la clé maîtresse du capteur de mouvement K_M comme K_{M-VU} XOR K_{M-WC}. L'ERCA communique $K_{M,}$ K_{M-VU} et K_{M-WC} aux organismes de certification de l'État membre sur leur demande.

TCS_244 L'ERCA attribue à chaque clé maîtresse du capteur de mouvement K_M un numéro de version unique, qui s'applique également à la constitution des clés K_{M-VU} et K_{M-WC} ainsi qu'à l'identification du K_{ID} de la clé qui y est associée. L'ERCA informe les MSCA du numéro de version lorsqu'elle leur adresse K_{M-VU} et K_{M-WC}.

Remarque: le numéro de version sert à distinguer les générations de ces clés, comme l'explique en détail la section 3.2.1.2.

TCS_245 Les organismes de certification de l'État membre transmettent $K_{M-VU,}$ et son numéro de version aux fabricants de VU sur leur demande. Les fabricants de VU insèrent K_{M-VU}et son numéro de version dans toutes les VU fabriquées.

TCS_246 Les organismes de certification de l'État membre vérifient que K_{M-WC} 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` dans l'appendice 2.
- Comme l'explique la section 3.2.1.2, il s'avère possible de devoir insérer plusieurs générations de K_{M-WC} dans une même carte d'atelier.

TCS_247 Outre la clé AES spécifiée au TCS_246, la MSCA garantit que la clé TDES $Km_{WC,}$ spécifiée par le CSM_037 dans la partie A du présent appendice, est 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 VU de première génération.
- Une carte d'atelier de deuxième génération contient deux applications distinctes. L'une se conforme à la partie B du présent appendice et l'autre à la partie A. Cette dernière contient la clé TDES Km_{WC}.

TCS_248 Une MSCA impliquée dans l'émission 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, CV. La valeur du vecteur constant est la suivante:

- Pour les clés maîtresses du capteur de mouvement sur 128 bits: CV = ‘B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83’
- Pour les clés maîtresses du capteur de mouvement sur 192 bits: CV = ‘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 sur 256 bits: CV = ‘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’

Note: les vecteurs constants sont générés de la manière suivante:
Pi_10 = 10 premiers octets de la portion décimale de la constante mathématique π = ‘24 3F 6A 88 85 A3 08 D3 13 19’
CV_128-bits = 16 premiers octets de SHA-256(Pi_10)
CV_192-bits = 24 premiers octets de SHA-384(Pi_10)
CV_256-bits = 32 premiers octets de SHA-512(Pi_10)

TCS_249 Les fabricants de capteurs de mouvement génèrent une clé de couplage aléatoire unique K_P pour chaque capteur de mouvement et communiquent chaque clé de couplage aux organismes de certification de l'État membre. La MSCA chiffre chaque clé de couplage séparément à l'aide de la clé maîtresse du capteur de mouvement K_M et retourne la clé cryptée au fabricant de capteurs de mouvement. Pour chaque clé cryptée, la MSCA avertit le fabricant de capteurs de mouvement du numéro de version de la K_M. associée.

Note: comme l'explique la section 3.2.1.2, il se peut qu'un fabricant de capteurs de mouvement doive générer plusieurs clés de couplage uniques pour un même capteur de mouvement.

TCS_250 Les fabricants de capteurs de mouvement génèrent un numéro de série unique pour chaque capteur de mouvement et communiquent tous les numéros de série aux organismes de certification de l'État membre. La MSCA chiffre chaque numéro de série séparément à l'aide de la clé d'identification K_{ID} et retourne le numéro de série crypté au fabricant de capteurs de mouvement. Pour chaque numéro de série crypté, la MSCA avertit le fabricant de capteurs de mouvement du numéro de version du K_{ID} associé.

TCS_251 En ce qui concerne les exigences TCS_249 et TCS_250, la MSCA a recours à l'algorithme AES dans le mode d'exploitation par chaînage de blocs de données cryptées, tel que le définit la norme [ISO 10116], en respectant 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 s'avère nécessaire, la MSCA utilise la méthode de remplissage numéro deux définie par la norme [ISO 9797-1].

TCS_252 Le fabricant de capteurs de mouvement stocke la clé de couplage et le numéro de série cryptés dans le capteur de mouvement auquel ils sont destinés. Il y stocke également les valeurs de texte en clair correspondantes et le numéro de version de K_M et de K_{ID} qui a servi au cryptage.

Note: comme l'explique la section 3.2.1.2, il se peut qu'un fabricant de capteurs de mouvement doive enregistrer plusieurs clés de couplage uniques cryptées et plusieurs numéros de série cryptés pour un même capteur de mouvement.

TCS_253 Outre le matériel cryptographique AES spécifié en TCS_252, le fabricant de capteurs de mouvement peut également stocker dans chaque capteur de mouvement le matériel cryptographique TDES spécifié dans l'exigence CSM_037 dans la partie A du présent appendice.

Note: ce faisant, il permet à un capteur de mouvement de deuxième génération de se coupler avec une VU de première génération.

TCS_254 La longueur de la clé de session K_S générée par une VU pendant le couplage avec un capteur de mouvement est liée à la longueur de son $K_{M\text{-}VU,}$ comme décrit au TCS_192.

3.2.1.2 Remplacement de la clé maîtresse du capteur de mouvement dans un équipement de deuxième génération

TCS_255 Toutes les clés maîtresses des capteurs de mouvement et toutes les clés associées (cf. Tableau 45) 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.

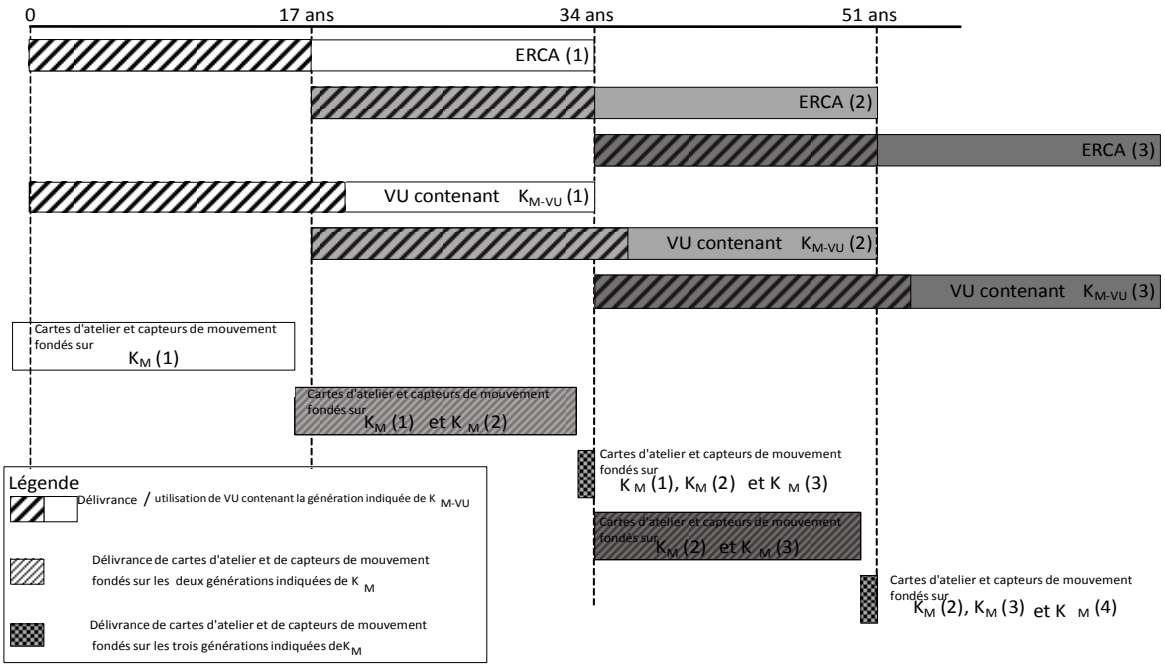


Figure 2 Émission et utilisation de diverses générations de clés maîtresses de capteurs de mouvement sur des VU, des capteurs de mouvement et des cartes d'ateliers

TCS_256 Au moins un an avant la génération d'une nouvelle paire de clés racine européenne, conformément au TCS_198, l'ERCA génère une nouvelle clé maîtresse de capteur de mouvement K_M en générant de nouvelles $K_{M\text{-}VU}$ et $K_{M\text{-}WC}$. 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 au TCS_192. L'ERCA communique les nouvelles K_M, $K_{M\text{-}VU}$ et $K_{M\text{-}WC}$ ainsi que leur numéro de version aux MSCA sur leur demande.

TCS_257 Les MSCA s'assurent que toutes les générations valides de $K_{M\text{-}WC}$ sont stockées dans chaque carte d'atelier émise sous leur autorité, de même que leurs numéros de version, comme illustré à la Figure.

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 $K_{M\text{-}WC}$, comme l'illustre la Figure 2.

TCS_258 À propos de la procédure décrite par lesTCS_249 et TCS_250 ci-dessus: la MSCA chiffre chaque paire de clés de couplage K_P reçue des fabricants de capteurs de mouvement séparément selon chaque génération valide 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 valide de clé d'identification K_{ID}. Le fabricant de capteurs de mouvement stocke tous les cryptages de clé de couplage et de numéro de série dans le capteur de mouvement auquel ils sont destinés. Il y stocke également les valeurs de texte en clair correspondantes et le ou les numéro(s) de version de K_M et K_{ID} qui ont servi au cryptage.

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 cryptées selon trois générations de $K_{M,}$, comme l'illustre la Figure 2.

TCS_259 À propos de la procédure décrite par le TCS_249 ci-dessus: du fait que la longueur de la clé de couplage K_P doit être liée à celle de K_M (cf. TCS_242), 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 adresse chaque clé de couplage à la MSCA. La MSCA vérifie que chaque clé de couplage est cryptée 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 (cf. TCS_253), il indique à la MSCA que la clé maîtresse du capteur de mouvement TDES doit servir à 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 leurs longueurs respectives.

TCS_260 Les fabricants de VU insèrent uniquement une génération de $K_{M\text{-}VU}$ dans chaque VU, accompagnée de son numéro de version. Cette génération de $K_{M\text{-}VU}$ est liée au certificat ERCA dont découlent les certificats VU.

Remarques:

- Une VU liée à un certificat ERCA de génération *X* contient uniquement une $K_{M\text{-}VU,}$ 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 VU de génération *X* ne peut pas se coupler avec un capteur de mouvement de génération *X-1*.
- Du fait que les cartes d'atelier présentent une validité d'un an, les exigences TCS_255 - TCS_260 font que toutes les cartes d'atelier contiennent le nouveau $K_{M\text{-}WC}$ à l'émission de la première VU contenant le nouveau $K_{M\text{-}VU}$. Par conséquent, une telle VU pourra toujours calculer la nouvelle K_M. De plus, pendant ce temps, la plupart des nouveaux capteurs de mouvement contiendront des données codées basées sur la nouvelle K_M, également.

3.2.2 Clés de sécurisation de la communication DSRC

3.2.2.1 Généralités

TCS_261 L'authenticité et la confidentialité des données communiquées par la VU aux autorités de contrôle à l'aide d'un canal de communication distant DSRC sont garanties par un jeu de clés AES propres à la VU découlant d'une unique clé maîtresse DSRC, KM_{DSRC}.

TCS_262 La clé maîtresse DSRC KM_{DSRC} est une clé AES générée, stockée et diffusée 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, conformément au TCS_192.

TCS_263 L'ERCA communique la clé maîtresse DSRC aux organismes de certification de l'État membre sur leur demande et de manière sécurisée. Cela leur permet de calculer les clés DSRC propres aux VU et de s'assurer que la clé maîtresse DSRC est insérée dans toutes les cartes de contrôle et d'atelier émises sous leur responsabilité.

TCS_264 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 adresse la clé maîtresse DSRC.

Remarque: le numéro de version sert à distinguer les générations de ces clés maîtresses DSRC, comme l'explique en détail la section 3.2.2.2.

TCS_265 Pour chaque VU, le fabricant de VU crée un numéro de série VU unique qu'il adresse aux organismes de certification de l'État membre en vue d'obtenir un jeu de deux clés DSRC propre aux VU. Le numéro de série VU relève du type de données `VuSerialNumber` et les règles de codage distinctes (DER) conformes à la norme [ISO 8825-1] servent à son cryptage.

TCS_266 Dès réception d'une demande de clés DSRC propres aux VU, la MSCA calcule deux clés AES pour la VU, appelées K_VU_{DSRC}_ENC et K_VU_{DSRC}_MAC. Ces clés propres aux VU sont de longueur identique à celle de la clé maîtresse DSRC. La MSCA utilise la fonction de dérivation de clé définie au [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 TCS_192. La fonction de dérivation de clé figurant au [RFC 5869] sert 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)*, avec
  T(1) = HMAC-Hash (*PRK*, *T(0)* || *info* || ‘01’) et
  - *T(0)* = chaîne vide (‘’)
  - *info* = numéro de série VU conforme au TCS_265
- K_VU_{DSRC}_ENC = premiers *L* octets de *OKM* et
  K_VU_{DSRC}_MAC = derniers *L* octets de *OKM*
  où *L* de la longueur requise de K_VU_{DSRC}_ENC et K_VU_{DSRC}_MAC en octets.

TCS_267 La MSCA communique K_VU_{DSRC}_ENC et K_VU_{DSRC}_MAC aux fabricants de VU de manière sécurisée en vue de leur insertion dans les VU auxquelles ils sont destinés.

TCS_268 Après leur émission, la VU enregistre K_VU_{DSRC}_ENC et K_VU_{DSRC}_MAC dans sa mémoire sécurisée, de façon à pouvoir assurer l'intégrité, l'authenticité et la confidentialité des données envoyées au moyen du canal de communication distant. La VU mémorise également le numéro de version de la clé maîtresse DSRC servant à calculer les clés propres aux VU.

TCS_269 Après leur émission, les cartes de contrôles et d'atelier enregistrent KM_{DSRC} dans leur mémoire sécurisée, de façon à pouvoir vérifier l'intégrité et l'authenticité des données envoyées par la VU par le canal de communication distant et de façon à pouvoir décrypter ces données. Les cartes de contrôle et d'atelier mémorisent également le numéro de version de la clé maîtresse DSRC.

Note: comme l'explique la section 3.2.2.2, il s'avère possible de devoir insérer plusieurs générations de KM_{DSRC} dans une même carte d'atelier ou de contrôle.

TCS_270 La MSCA archive toutes les clés DSRC propres aux VU qu'elle a générées, ainsi que leur numéro de version et l'identificateur de la VU destinés à chaque jeu de clés.

3.2.2.2 Substitution de clé maîtresse DSRC

TCS_271 Toutes les clés maîtresses DSRC sont liées à une génération donnée de paire de clés racine ERCA. L'ERCA remplace donc 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.

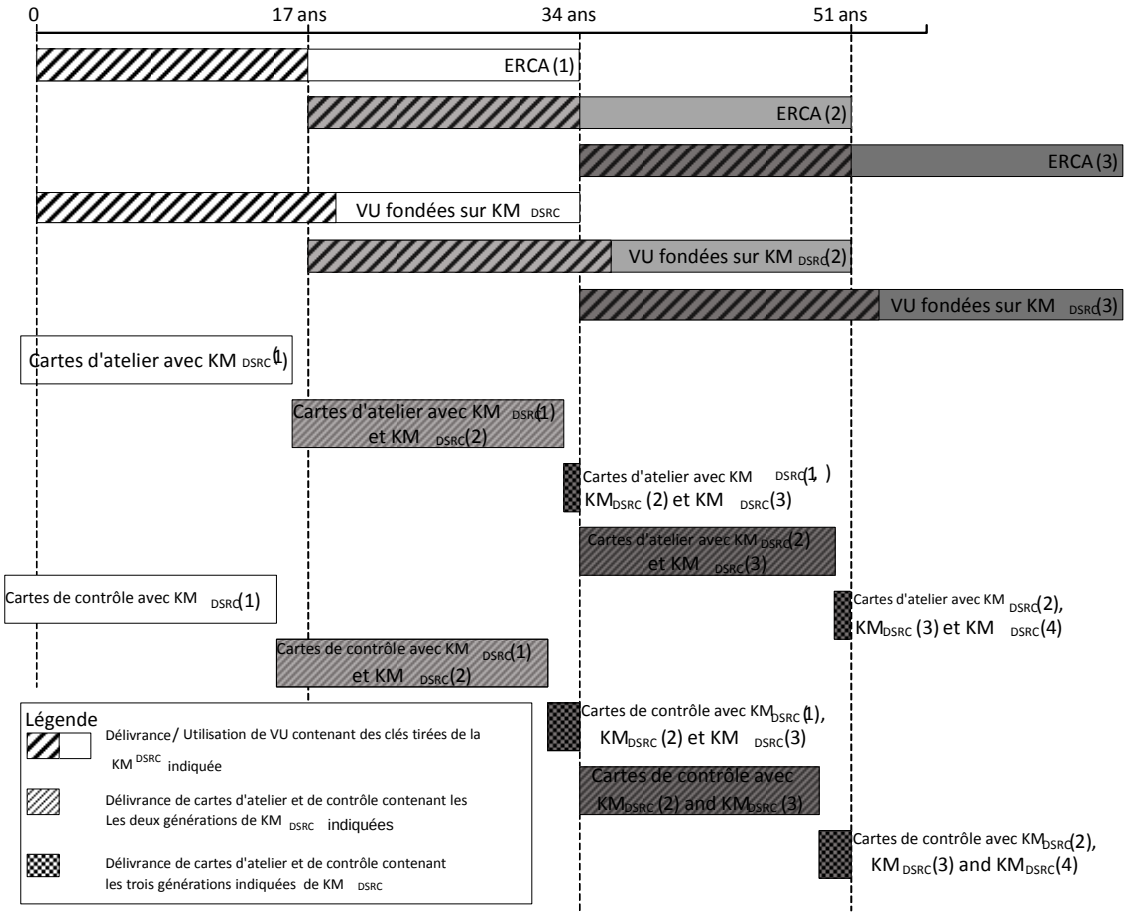


Figure 3 Émission et utilisation de diverses générations de clés maîtresses DSRC sur des VU, des cartes d'ateliers et de contrôle

TCS_272 Au moins deux ans avant la génération d'une nouvelle paire de clés racine européenne, conformément au TCS_198, 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 TCS_192. L'ERCA communique la nouvelle clé maîtresse DSRC ainsi que son numéro de version aux MSCA sur leur demande.

TCS_273 Les MSCA s'assurent que toutes les générations valides de KM_{DSRC} sont stockées dans chaque carte de contrôle émise sous leur autorité, de même que leurs numéros de version, comme illustré à la Figure 2.

Note: cela implique qu'au cours des deux dernières années de validité d'un certificat ERCA, les cartes de contrôle sont émises avec trois générations de KM_{DSRC}, comme l'illustre la Figure 2.

TCS_274 Les MSCA s'assurent que toutes les générations de KM_{DSRC} valides depuis au moins un an et toujours en cours de validité sont stockées dans chaque carte d'atelier émise sous leur autorité, de même que leurs numéros de version, comme illustré à la Figure 2.

Note: 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 l'illustre la Figure 2.

TCS_275 Les fabricants de VU insèrent uniquement un jeu de clés DSRC propres aux VU dans chaque VU, accompagné de son numéro de version. Ce jeu de clés résulte de la génération KM_{DSRC} liée au certificat ERCA dont découlent les certificats VU.

Remarques:

- Cela implique qu'une VU liée à un certificat ERCA de génération *X* contient uniquement une K_VU_{DSRC}_ENC et une K_VU_{DSRC}_MAC, de génération *X* même si la VU est émise après le début de la durée de validité du certificat ERCA de génération *X+1*. La Figure 3 illustre ce principe.
- Du fait que les cartes d'atelier présentent une validité d'un an et les cartes de contrôle une validité de deux ans, les exigences TCS_273 - TCS_275 font que toutes les cartes d'atelier et de contrôle contiennent la nouvelle clé maîtresse DSRC à l'émission de la première VU contenant les clés propres aux VU relevant de cette clé maîtresse.

3.3 Certificats

3.3.1 Généralités

TCS_276 Tous les certificats inscrits dans le système de tachygraphie intelligente européenne sont de type autodescriptifs et vérifiables par carte (VC) conformément aux normes [ISO 7816-4] et [ISO 7816-8].

TCS_277 Les règles de codage distinctes (DER) conformes à la norme [ISO 8825-1] servent à encoder les structures de données ASN.1 et (selon l'application) les objets de données au sein des certificats.

Note: cet cryptage produit la structure Tag-Length-Value (TLV) suivante:

- Balise: la balise est cryptée sur un ou deux octet(s) et indique le contenu.
- Longueur: la longueur est cryptée comme un entier non signé sur un, deux ou trois octet(s), soit une longueur maximale de 65 535 octets. On utilise le nombre minimal d'octets.
- Valeur: la valeur est cryptée sur zéro octet ou plus.

3.3.2 Contenu du certificat

TCS_278 Tous les certificats possèdent une structure présentée dans le profil de certificat du Tableau 46.

Champ	**ID de champ**	**Balise**	**Longueur (en octets)**	**Type de données ASN.1 (voir appendice 1)**
Certificat ECC	C	‘7F 21’	var	
Corps du certificat ECC	B	‘7F 4E’	var	
Identificateur de profil du certificat	CPI	‘5F 29’	‘01’	INTEGER(0..255)
Référence de l'organisme de certification	CAR	‘42’	‘08’	KeyIdentifier
Autorisation du titulaire de certificat	CHA	‘5F 4C’	‘07’	CertificateHolder Authorisation
Clé publique	PK	‘7F 49’	var	
Paramètres de domaines	DP	‘06’	var	OBJECT IDENTIFIER
Point public	PP	‘86’	var	CHAÎNE D'OCTETS
Référence du titulaire de certificat	CHR	‘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	CHAÎNE D'OCTETS

Tableau 46Profil de certificat version 1

Note: l'ID de champ sert dans les sections ultérieures du présent appendice à indiquer les zones individuelles d'un certificat, p. ex. X.CAR désigne la référence des organismes de certification mentionnée dans le certificat d'un utilisateur X.

3.3.2.1 Certificate Profile Identifier

TCS_279 Les certificats adoptent un identificateur de profil de certificat pour indiquer le profil de certificat utilisé. La version 1, comme précisé au Tableau 46, est identifiée par une valeur de '00'.

3.3.2.2 Certificate Authority Reference

TCS_280 La référence des organismes de certification sert à identifier la clé publique à utiliser pour vérifier la signature du certificat. La référence des organismes de certification doit donc être identique à celle du titulaire de certificat dans le certificat des organismes de certification correspondants.

TCS_281 Un certificat racine ERCA est autosigné, c'est-à-dire que la référence des organismes de certification et la référence du titulaire du certificat figurant sur le certificat sont identiques.

TCS_282 Pour un certificat de lien ERCA, la référence du titulaire du certificat est identique au CHR du nouveau certificat racine ERCA. La référence des organismes de certification d'un certificat de lien est identique au CHR du certificat racine ERCA antérieur.

3.3.2.3 Certificate Holder Authorisation

TCS_283 L'autorisation du titulaire de certificat permet d'identifier le type de certificat. Elle se compose des six octets principaux de l'ID de l'application tachygraphique concaténée avec le type d'équipement auquel est destiné le certificat.

3.3.2.4 Public Key

La clé publique héberge deux éléments de données: les paramètres du domaine normalisé à utiliser avec la clé publique du certificat et la valeur du point public.

TCS_284 L'élément de données Paramètres de domaine contient l'un des identificateurs d'objet précisé au Tableau 43 en vue de référencer un jeu de paramètres de domaines normalisés.

TCS_285 L'élément de données Public Point contient le point public. Les points publics de la courbe elliptique sont convertis en chaînes d'octets comme le précise le [TR-03111]. On utilise la structure cryptée non compressée. Les validations décrites au [TR-03111] s'appliquent toujours lorsque l'on décode un point de la courbe elliptique.

3.3.2.5 Certificate Holder Reference

TCS_286 La référence du titulaire de certificat sert d'identificateur pour la clé publique fournie avec le certificat. Elle sert à référencer cette clé publique dans d'autres certificats.

TCS_287 Concernant les certificats de cartes et de dispositifs GNSS externes, la référence du titulaire de certificat relève du type de données `ExtendedSerialNumber` comme précisé en appendice 1.

TCS_288 Concernant les VU, le fabricant, lorsqu'il demande un certificat, connaît ou non le numéro de série propre au fabricant de la VU à laquelle s'adresse ce certificat et la clé privée associée. Dans le premier cas, la référence du titulaire de certificat relève du type de données `ExtendedSerialNumber` comme précisé en appendice 1. Dans le dernier cas, la référence du titulaire de certificat relève du type de données `CertificateRequestID` comme précisé en appendice 1.

TCS_289 Concernant les certificats ERCA et MSCA, la référence du titulaire de certificat relève du type de données `CertificationAuthorityKID` comme précisé en appendice 1.

3.3.2.6 Certificate Effective Date

TCS_290 La date d'entrée en vigueur du certificat indique la date et l'heure de début de la durée de validité du certificat. La date d'entrée en vigueur du certificat correspond à la date de génération du certificat.

3.3.2.7 Certificate Expiration Date

TCS_291 La date d'expiration du certificat indique la date et l'heure de fin de la durée de validité du certificat.

3.3.2.8 Certificate Signature

TCS_292 La signature du certificat est créée en fonction du corps de certificat codé, y compris la balise et la longueur de ce dernier. Les [DSS] préconisent d'adopter l'algorithme de signature ECDSA et le TCS_192 préconise d'utiliser l'algorithme de hachage associé à la taille de la clé des autorités de signature. La structure de la signature est en clair, conformément au [TR-03111].

3.3.3 Certificats de demande

TCS_293 Lors de la demande d'un certificat, le demandeur adresse les données suivantes à ses organismes de certification:

- l'identificateur de profil de certificat du certificat demandé,
- la référence des organismes de certification attendue pour signer le certificat,
- la clé publique à signer.

TCS_294 Outre les données dans le TCS_293, une MSCA envoie les données suivantes dans une demande de certificat à l'ERCA, ce qui permet à l'ERCA de créer la référence du titulaire de certificat du nouveau certificat MSCA:

- le code numérique national des organismes de certification (type de données `NationNumeric` défini à l'appendice 1),
- le code numérique national des organismes de certification (type de données `NationAlpha` défini à l'appendice 1),
- le numéro de série sur un octet permettant de faire la distinction entre les différentes clés de l'organisme de certification si certaines clés font l'objet de modifications,
- le champ de deux octets contenant les informations complémentaires spécifiques à l'organisme de certification.

TCS_295 Outre les données dans le TCS_293, un fabricant d'équipement envoie les données suivantes dans une demande de certificat à une MSCA, ce qui lui permet de créer la référence du titulaire de certificat du nouvel équipement:

- un identificateur propre au fabricant pour le type d'équipement considéré;
- s'il est connu (cf. TCS_296), un 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.

TCS_296 Concernant les VU, le fabriquant, lorsqu'il demande un certificat, connaît ou non le numéro de série propre au fabricant de la VU à laquelle s'adresse ce certificat et la clé privée associée. S'il est connu, le fabricant de VU adresse le numéro de série à la MSCA. S'il n'est pas connu, le fabricant identifie de manière distincte chaque demande de certificat et adresse le numéro de série de la demande de certificat à la MSCA. Le certificat produit contient le numéro de série de la demande de certificat. Après insertion du certificat dans une VU donnée, le fabricant communique la connexion entre le numéro de série de la demande de certificat et l'identificateur de la VU à la MSCA.

4 Authentification mutuelle de la carte et de la VU et messagerie sécurisée

4.1 Généralités

TCS_297 À haut niveau, la sécurité des communications échangées entre une VU et une carte tachygraphique repose sur les étapes suivantes:

- D'abord, chaque partie montre à l'autre qu'elle détient un certificat de clé publique valide, signé par l'organisme de certification d'un État membre. En retour, le certificat de clé publique MSCA doit être signé par l'organisme de certification racine européen. Cette étape correspond à la vérification de la chaîne de certification et fait l'objet d'une spécification détaillée à la section 4.2
- Deuxièmement, la VU 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, la VU est authentifiée. Cette étape correspond à l'authentification de la VU et fait l'objet d'une spécification détaillée à la section 4.3.
- Troisièmement, les deux parties calculent indépendamment deux clés de session AES à l'aide d'un algorithme de concordance de clé asymétrique. En utilisant l'une de ces clés de session, la carte crée un code d'authentification de message (MAC) en fonction de certaines données envoyées par la VU. La VU 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 spécification détaillée à la section 4.4.
- Quatrièmement, la VU 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 spécification détaillée à la section 4.5.

TCS_298 Le mécanisme décrit au TCS_297 est déclenché par la VU dès lors qu'une carte est insérée dans l'un de ses lecteurs de carte.

4.2 Vérification mutuelle de la chaîne de certificat

4.2.1 Vérification de la chaîne de certificat de la carte par la VU

TCS_299 Les VU adoptent le protocole prévu à la Figure 4 pour vérifier la chaîne de certificat d'une carte tachygraphique.

Notes relatives à la Figure 4:

- Les certificats et les clés publiques associés à la carte mentionnés sur cette Figure sont ceux de l'authentification mutuelle. La section 3.1.5 précise leur intitulé: Card_MA.
- Les certificats Card.CA et les clés publiques mentionnées dans la figure sont ceux destinés à la signature des certificats de carte; cela est indiqué dans le CAR du certificat Card. La section 3.1.3 précise leur intitulé: MSCA_Card.
- Le certificat Card.CA.EUR mentionné sur cette figure est le certificat racine européen indiqué dans le CAR du certificat Card.CA.
- Le certificat Card.Link mentionné sur cette figure est le certificat de lien de la carte, le cas échéant. Comme le précise la section 3.1.2, 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 européenne.
- Le certificat Card.Link.EUR est le certificat racine européen indiqué dans le CAR du certificat Card.Link.

TCS_300 Comme illustré sur la Figure 4, la vérification du certificat de la carte commence dès l'insertion de la carte. La VU lit la référence du titulaire de la carte (`cardExtendedSerialNumber`) à partir du EF ICC. La VU vérifie si elle connaît la carte, c'est-à-dire si elle a vérifié la chaîne de certificat de la carte dans le passé et si elle l'a stockée pour la réutiliser à l'avenir. Si tel est le cas et que le certificat de la carte est toujours valide, la procédure se poursuit avec la vérification de la chaîne de certificat de la VU. Sinon, la VU lit successivement depuis la carte le certificat MSCA_Card à utiliser pour vérifier le certificat de la carte, Card.CA. 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 un tel certificat est reconnu, la VU utilise ce certificat pour vérifier les certificats de carte sous-jacents lus à partir de la carte. En cas de réussite, la procédure se poursuit avec la vérification de la chaîne de certificat de la VU. En cas d'échec, la VU ignore la carte.

Remarque: la VU peut connaître le certificat Card.CA.EUR pour trois raisons:

- le certificat Card.CA.EUR est identique à celui de la VU;

- le certificat Card.CA.EUR précède celui de la VU et la VU contient ce certificat dès son émission (cf. CSM_81);
- le certificat Card.CA.EUR succède à celui de la VU et la VU a reçu un certificat de lien d'une autre carte tachygraphique, l'a vérifié et mémorisé pour une utilisation ultérieure.

TCS_301 Comme l'indique la Figure 4, une fois que la VU a vérifié l'authenticité et la validité d'un certificat encore inconnu, elle le mémorise pour l'utiliser ultérieurement, de manière à ne pas devoir le vérifier à nouveau s'il lui est représenté. Au lieu de mémoriser la totalité du certificat, une VU peut choisir de ne mémoriser que le contenu du corps du certificat, conformément à la section 3.3.2.

TCS_302 La VU vérifie la validité temporelle de tout certificat lu depuis la carte ou mémorisé et refuse les certificats expirés. Pour vérifier la validité temporelle d'un certificat présenté par la carte, une VU utilise son horloge interne.

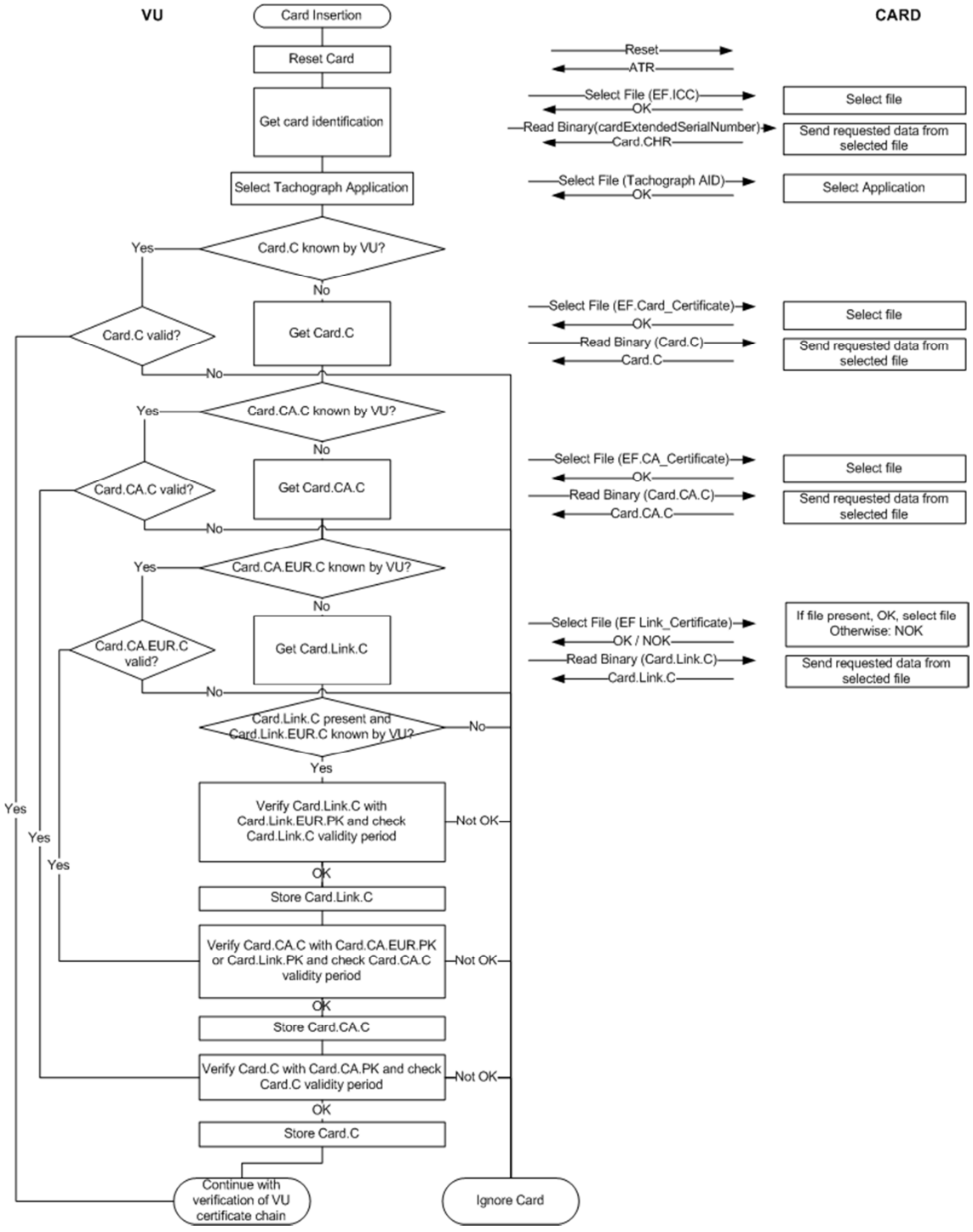


Figure 4Protocole de vérification de la chaîne de certificat de la carte par la VU

4.2.2 Vérification de la chaîne de certificat de la VU par la carte

TCS_303 Les cartes tachygraphiques adoptent le protocole prévu à la Figure 5 pour vérifier la chaîne de certificat d'une VU.

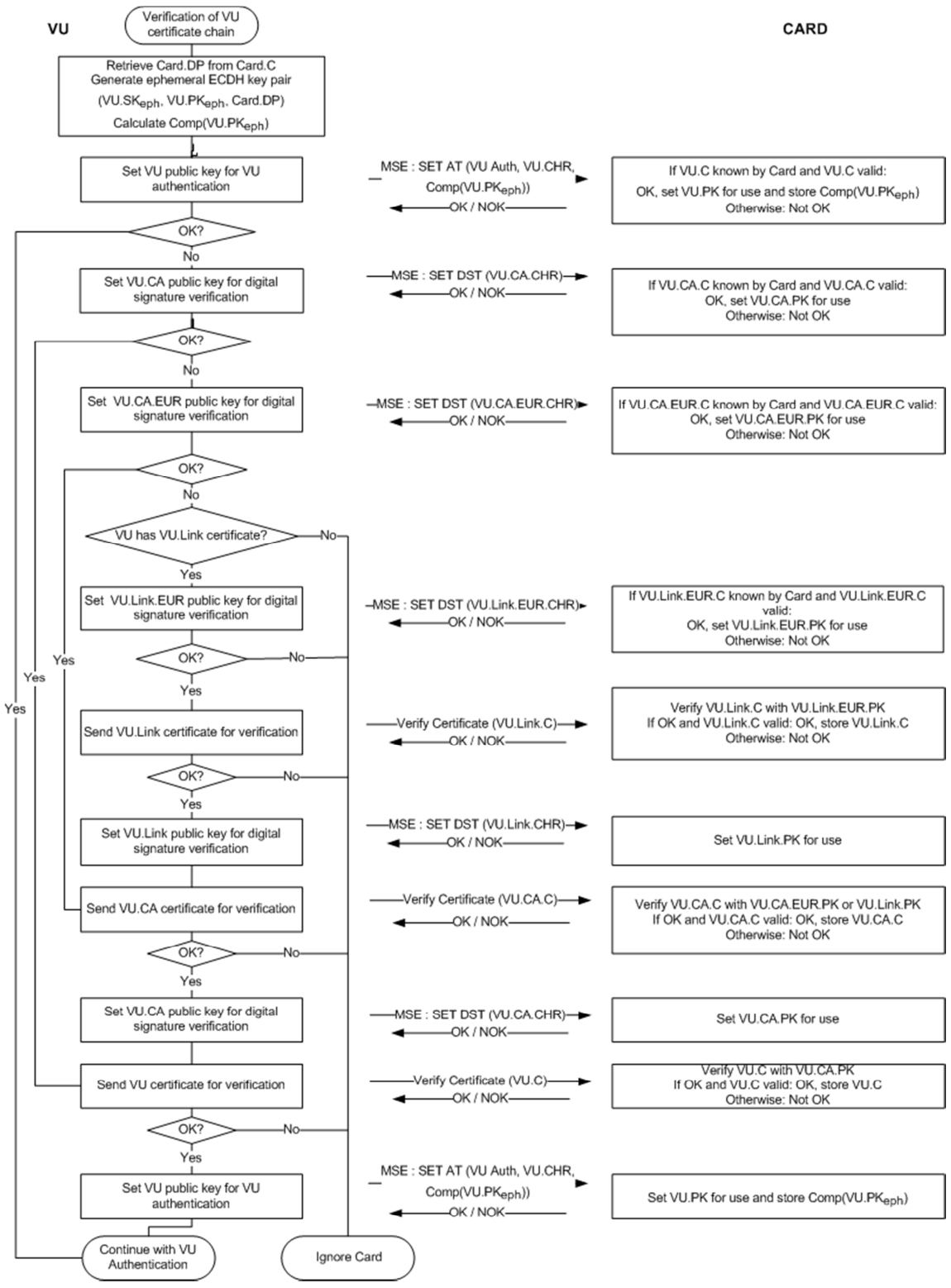


Figure 5 Protocole de vérification de la chaîne de certificat de la VU par la carte

Notes relatives à la Figure 5:

- Les certificats et les clés publiques associés à la VU mentionnés sur cette figure sont ceux de l'authentification mutuelle. La section 3.1.4 précise leur intitulé: VU_MA.
- Les certificats et les clés publiques VU.CA mentionnés sur cette figure sont ceux de la signature des certificats de la VU et du dispositif GNSS externe. La section 3.1.3 précise leur intitulé: MSCA_VU-EGF.
- Le certificat VU.CA.EUR mentionné sur cette figure est le certificat racine européen indiqué dans le CAR du certificat VU.CA.
- Le certificat VU.Link mentionné sur cette Figure est le certificat de lien de la VU, le cas échéant. Comme le précise la section 3.1.2, 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 européenne.
- Le certificat VU.Link.EUR est le certificat racine européen indiqué dans le CAR du certificat VU.Link.

TCS_304 Comme l'illustre la Figure 5, la vérification de la chaîne de certificat de la VU commence avec la tentative de la VU de fixer sa propre clé publique afin de l'utiliser dans la carte tachygraphique. En cas de réussite, cela signifie que la carte a déjà vérifié la chaîne de certificat de la VU par le passé et a mémorisé le certificat de la VU pour l'utiliser ultérieurement. Dans ce cas, le certificat de la VU est prêt à servir et la procédure se poursuit avec l'authentification de la VU. Si la carte ne reconnaît par le certificat de la VU, la VU présente successivement le certificat MSCA_VU afin de vérifier le certificat de la VU, le certificat VU.CA.EUR afin de vérifier le certificat MSCA_VU et éventuellement le certificat de lien dans le but d'identifier un certificat que la carte connaisse. Si un tel certificat est reconnu, la carte utilise ce certificat pour vérifier les certificats VU sous-jacents qui lui sont présentés. En cas de réussite, la VU définit finalement sa clé publique pour l'utiliser dans la carte tachygraphique. En cas d'échec, la VU ignore la carte.

Remarque: la carte peut connaître le certificat VU.CA.EUR pour trois raisons:

- le certificat VU.CA.EUR est identique à celui de la VU;
- le certificat VU.CA.EUR précède celui de la VU et la carte contient ce certificat dès son émission (cf. CSM_91);
- le certificat VU.CA.EUR succède à celui de la carte, et la carte a reçu un certificat de lien d'une autre VU, l'a vérifié et mémorisé pour une utilisation ultérieure.

TCS_305 La VU utilise la commande MSE: Set AT pour définir sa clé publique et l'utiliser dans la carte tachygraphique. Comme spécifié dans l'appendice 2, cette commande contient une indication du mécanisme cryptographique qui servira avec la clé définie. Ce mécanisme correspond à l'authentification de la VU utilisant l'algorithme ECDSA, en combinaison avec l'algorithme de hachage associé à la taille de clé de la paire de clés VU_MA de la VU, comme le spécifie le TCS_192.

TCS_306 La commande MSE: Set AT contient également une indication de la paire de clés éphémères qu'utilise la VU pendant la concordance des clés de session (cf. section 4.4). Par conséquent, avant d'envoyer la commande MSE: Set AT, la VU génère une paire de clés ECC éphémères. Pour la génération de la paire de clés éphémères, la VU utilise les paramètres de domaine normalisés indiqués par le certificat de la carte. La paire de clés éphémères est notée ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). La VU utilise l'abscisse du point public éphémère ECDH comme identification de clé; il s'agit de la représentation comprimée de la clé publique appelée $Comp(VU.PK_{eph})$.

TCS_307 Si la commande MSE: Set AT aboutit, la carte définit le VU.PK indiqué pour une utilisation ultérieure pendant l'authentification de la VU et mémorise temporairement $Comp(VU.PK_{eph})$. Si plusieurs commandes MSE: Set AT aboutissent, elles sont adressées avant de procéder à la concordance des clés de session. La carte mémorise uniquement le dernier $Comp(VU.PK_{eph})$ reçu.

TCS_308 La carte vérifie la validité temporelle de tout certificat présenté par la VU ou référencé par la VU pendant qu'il était en mémoire dans la carte et refuse les certificats expirés.

TCS_309 Pour vérifier la validité temporelle d'un certificat présenté par la VU, chaque carte tachygraphique stocke en interne des données représentant le temps actuel. Ces données ne sont pas directement actualisables par une VU. Enfin, l'heure actuelle d'une carte est définie comme étant la date effective du certificat Card_MA de la carte. Une carte actualise son heure actuelle si la Date effective d'un certificat authentique représentant une «source d'heure valide» présenté par une VU est plus récente que l'heure actuelle de la carte. Dans ce cas, la carte définit son heure actuelle sur la date effective dudit certificat. La carte accepte uniquement les certificats suivants comme source d'heure valide:

- certificats de lien ERCA de deuxième génération;
- certificats MSCA de deuxième génération;
- certificats de VU de deuxième génération émis par le même pays que le ou les certificat(s) de carte de ladite carte.

Note: la dernière exigence implique qu'une carte doit pouvoir reconnaître le CAR du certificat de la VU, p. ex. le certificat MSCA_VU-EGF. Il ne s'agit pas du même que le CAR de son propre certificat, qui est le certificat MSCA_Card.

TCS_310 Comme l'indique la Figure 5, une fois que la carte a vérifié l'authenticité et la validité d'un certificat encore inconnu, elle le mémorise pour l'utiliser ultérieurement, de manière à ne pas devoir le vérifier à nouveau s'il lui est représenté. Au lieu de mémoriser la totalité du certificat, une carte peut choisir de ne mémoriser que le contenu du corps du certificat, conformément à la section 3.3.2.

4.3 Authentification de VU

TCS_311 Les unités embarquées sur véhicule et les cartes adoptent le protocole d'authentification de VU illustré sur la Figure 6 pour authentifier la VU par rapport à la carte. L'authentification de la VU permet à la carte tachygraphique de vérifier explicitement l'authenticité de la VU. Pour ce faire, la VU utilise sa clé privée pour signer un défi généré par la carte.

TCS_312 La VU inclut à proximité du défi de la carte, la signature de la référence du titulaire de la carte extraite du certificat de la carte.

Remarque: cela garantit que la carte auprès de laquelle la VU s'authentifie est la même que celle dont la VU a préalablement vérifié la chaîne de certificat.

TCS_313 La VU insère également dans la signature l'identificateur de la clé publique éphémère Comp(VU.PK_{eph}) que la VU utilise pour définir la messagerie sécurisée pendant la procédure d'authentification de circuit, conformément aux spécifications de la section 4.4.

Remarque: cela garantit que la VU avec laquelle une carte communique pendant une session de messagerie sécurisée est la même VU que celle authentifiée par la carte.

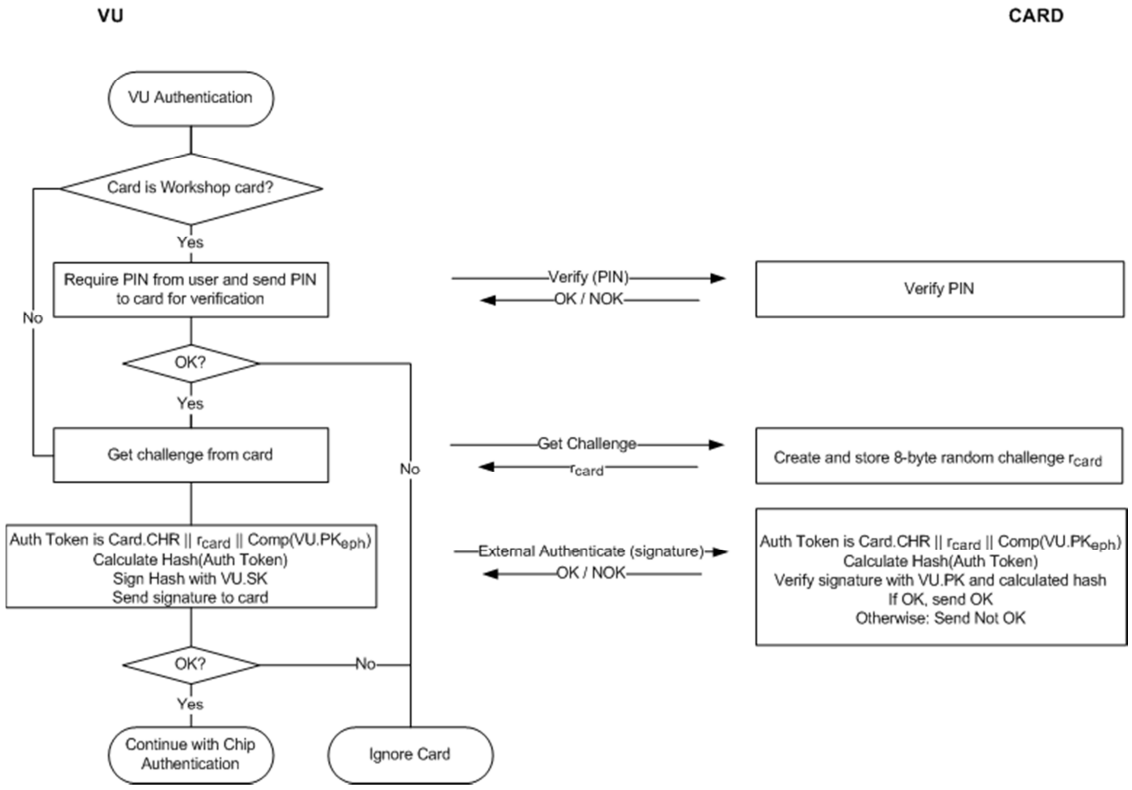


Figure 6 Protocole d'authentification de la VU

TCS_314 Si la VU envoie plusieurs commandes GET CHALLENGE pendant son authentification, la carte renvoie un nouveau défi aléatoire sur 8 octets à chaque fois, mais mémorise uniquement le dernier.

TCS_315 L'algorithme de signature utilisé par la VU pour authentifier la VU est l'ECDSA préconisé par les [DSS], en combinaison avec l'algorithme de hachage associé à la taille de clé de la paire de clés VU_MA de la VU, conformément au TCS_192. La structure de la signature est en clair, conformément au [TR-03111]. La VU adresse la signature produite à la carte.

TCS_316 À réception de la signature de la VU dans une commande EXTERNAL AUTHENTICATE, la carte:

- calcule le jeton d'authentification en concaténant Card.CHR, le lanceur de défis de la carte r_{card} et l'identificateur de la clé publique éphémère de la VU Comp(VU.PK_{eph});
- calcule le hachage en fonction du jeton d'authentification, à l'aide de l'algorithme de hachage associé à la taille de clé de la paire de clés VU_MA de la VU, conformément au TCS_192;
- vérifie la signature de la VU à l'aide de l'algorithme ECDSA combiné au VU.PK et au hachage calculé.

4.4 Authentification du circuit et concordance des clés de session

TCS_317 Les unités embarquées sur véhicule et les cartes adoptent le protocole d'authentification de circuit illustré sur la **Figure 7** pour authentifier la carte par rapport à la VU. L'authentification du circuit permet à l'unité embarquée sur véhicule de vérifier explicitement l'authenticité de la carte.

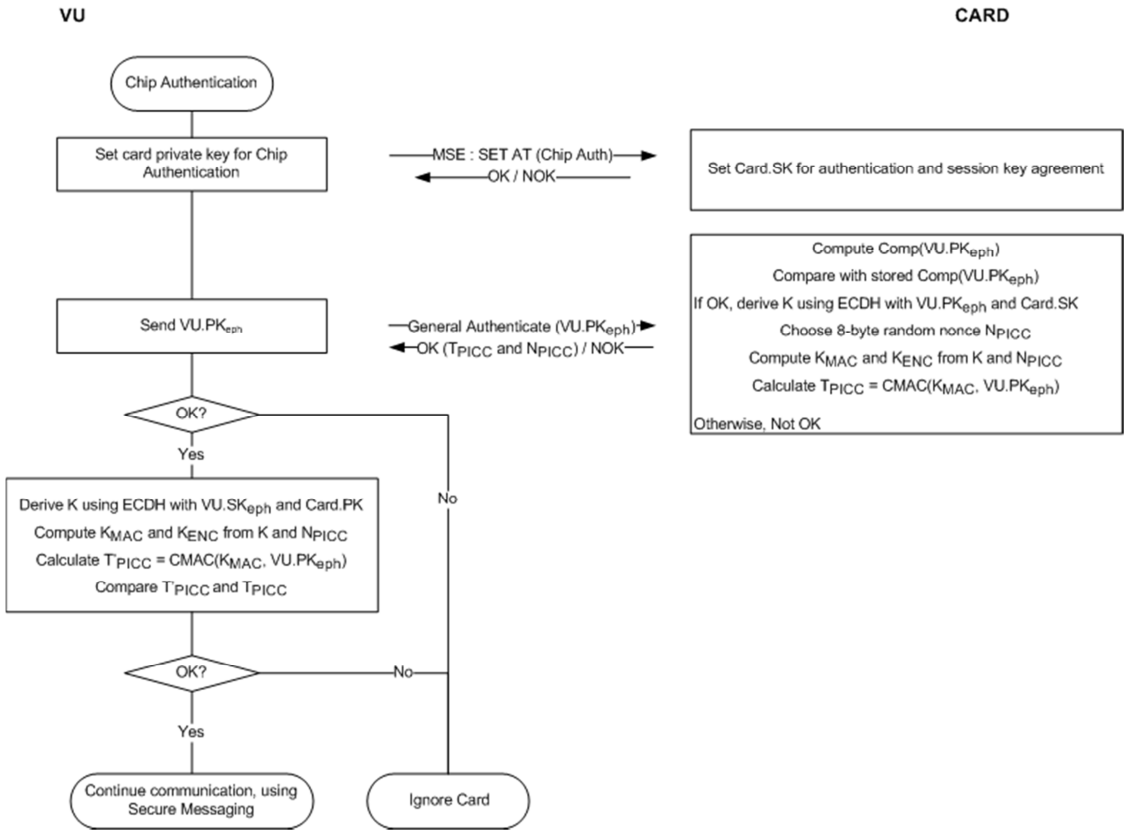


Figure 7 Authentification du circuit et concordance des clés de session

TCS_318 La VU et la carte suivent les étapes suivantes:

1. La VU lance la procédure d'authentification du circuit en adressant 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 au TCS_192». La VU détermine la taille de clé de la paire de clés de la carte d'après le certificat de la carte.
2. La VU adresse le point public $VU.PK_{eph}$ de sa paire de clés éphémères à la carte. Conformément au TCS_306, la VU génère cette paire de clés éphémères avant de vérifier la chaîne de certificat de la VU. La VU a envoyé l'identificateur de la clé publique éphémère $Comp(VU.PK_{eph})$ à la carte qui l'a mémorisé.
3. La carte calcule $Comp(VU.PK_{eph})$ d'après $VU.PK_{eph}$ et compare le résultat avec la valeur mémorisée de $Comp(VU.PK_{eph})$.
4. À l'aide de l'algorithme ECDH combiné à la clé privée statique de la carte et la clé publique éphémère de la VU, la carte calcule un K secret.
5. La carte choisit un mot aléatoire forgé pour l'occasion sur 8 octets N_{PICC} et l'utilise pour calculer les deux clés de session AES K_{MAC} et K_{ENC} d'après K. Cf. TCS_321.
6. En utilisant K_{MAC}, la carte calcule un jeton d'authentification en fonction de l'identificateur de la clé publique éphémère de la VU: $T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})$. La carte envoie N_{PICC} et T_{PICC} à l'unité embarquée sur véhicule.
7. À l'aide de l'algorithme ECDH combiné à la clé publique statique de la carte et la clé privée éphémère de la VU, la VU calcule le même K secret que la carte à l'étape 4.
8. La VU calcule les clés de session K_{MAC} et K_{ENC} d'après K et N_{PICC}; cf. TCS_321
9. La VU vérifie le jeton d'authentification T_{PICC}.

TCS_319 À l'étape 3 ci-dessus, la carte calcule Comp(VU.PKeph) comme l'abscisse du point public dans VU.PKeph.

TCS_320 Aux étapes 4 et 7 ci-dessus, la carte et l'unité embarquée sur véhicule utilisent l'algorithme ECKA-EG défini au [TR-03111].

TCS_321 Aux étapes 5 et 8 ci-dessus, la carte et l'unité embarquée sur véhicule utilisent la fonction de dérivation de clé pour les clés de session AES définie au [TR-03111], en respectant les précisions et modifications suivantes:

- 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 *r* est 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, conformément au TCS_192.

TCS_322 Aux étapes 6 et 9 ci-dessus, la carte et l'unité embarquée sur véhicule utilisent l'algorithme AES en mode CMAC, conformément au [SP 800-38B]. La longueur de T_{PICC} est liée à la longueur des clés de session AES, conformément au TCS_192.

4.5 Messagerie sécurisée

4.5.1 Généralités

TCS_323 Toutes les commandes et réponses échangées entre une unité embarquée sur véhicule et une carte tachygraphique après authentification réussie du circuit et jusqu'à la fin de la session sont protégées par la messagerie sécurisée.

TCS_324 Hormis la lecture d'un fichier avec les règles d'accès SM-R-ENC-MAC-G2 (cf. appendice 2, section 4), la messagerie sécurisée sert uniquement en mode d'authentification. 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.

TCS_325 Lors de la lecture de données provenant d'un fichier soumis aux règles d'accès SM-R-ENC-MAC-G2, la messagerie sécurisée est utilisée en mode chiffrer-puis-authentifier. Cela signifie que les données de réponse sont d'abord cryptées pour assurer la confidentialité du message, puis qu'un MAC est calculé par rapport aux données cryptées formatées pour garantir l'authenticité et l'intégrité.

TCS_326 La messagerie sécurisée utilise AES comme défini en [AES] avec les clés de session K_{MAC} et K_{ENC} convenues pendant l'authentification du circuit.

TCS_327 Un entier non signé sert de compteur de séquences à l'émission (SSC) pour empêcher les attaques par relecture. La taille du SSC est égale à la taille du bloc AES, soit 128 bits. Le SSC respecte la structure MSB-First. Le compteur de séquences d'envoi est initialisé 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 SSC est incrémenté avant chaque commande ou réponse APDU générée, c'est-à-dire que la valeur de départ du SSC dans une session de SM est égale à zéro et qu'à la première commande, la valeur du SSC est égale à un. La valeur du SSC pour la première réponse est égale à deux.

TCS_328 En ce qui concerne le cryptage des messages, K_{ENC} est utilisé avec l'AES dans le mode d'exploitation par chaînage de cryptage par blocs (CBC), tel que le définit la norme [ISO 10116], en respectant un paramètre d'entrelacement de $m = 1$ et un vecteur d'initialisation $SV = E(K_{ENC}\ SSC)$, c'est-à-dire la valeur actuelle du compteur de séquences d'envoi cryptée avec K_{ENC}.

TCS_329 En ce qui concerne l'authentification de message, K_{MAC} est utilisé avec AES en mode CMAC conformément au [SP 800-38B]. La longueur de MAC est liée à la longueur des clés de session AES, conformément au TCS_192. Le compteur de séquence d'envoi est inclus dans le MAC en le préfixant avant le datagramme à authentifier.

4.5.2 Structure de message sécurisé

TCS_330 La messagerie sécurisée n'utilise que des objets de données de messagerie sécurisée (cf. [ISO 7816-4]) au Tableau 47. Dans tous les messages, ces objets de données servent dans l'ordre défini par ce tableau.

Nom de l'objet de données	*Balise*	*Présence Obligatoire (M), Conditionnelle (C) ou Interdite (F) dans* **Commandes**	**Réponses**
Valeur en clair non codée en BER-TLV	'81'	C	C
Valeur en clair codée BER-TLV sans SM-DO	'B3'	C	C
Indicateur de contenu de remplissage par cryptogramme, valeur en clair non codée en BER-TLV	'87'	C	C
Le protégé	'97'	C	F
État de traitement	'99'	F	M
Total de contrôle cryptographique	'8E'	M	M

Tableau 47Objets de données de messagerie sécurisée

Remarque: comme le précise l'appendice 2, les cartes tachygraphiques sont compatibles avec les commandes READ BINARY et UPDATE BINARY avec un octet impair INS ('B1' resp. 'D7'). Ces variantes de commande sont nécessaires pour lire et actualiser des fichiers de 32 768 octets et davantage. Dans ce cas, on utilise la variante suivante: un objet de données avec la balise 'B3' plutôt qu'un objet avec la balise '81'. Cf. appendice 2 pour toute information complémentaire.

TCS_331 Tous les objets de données de SM sont codés DER-TLV conformément à la norme [ISO 8825-1]. Ce cryptage produit la structure Tag-Length-Value (TLV) suivante:

- Balise: la balise est cryptée sur un ou deux octet(s) et indique le contenu.
- Longueur: la longueur est cryptée comme un entier non signé sur un, deux ou trois octet(s), soit une longueur maximale de 65 535 octets. On utilise le nombre minimal d'octets.
- Valeur: la valeur est cryptée sur zéro octet ou plus.

TCS_332 Les APDU protégés par la messagerie sécurisée sont créés de la manière suivante:

- L'entête de commande est inclus dans le calcul MAC, par conséquent la valeur '0C' sert pour l'octet de classe CLA.
- Comme le précise l'appendice 2, tous les octets INS sont pairs, hormis 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 SM.
- Dans la commande protégée APDU, le nouvel octet Le est défini à '00'. Si nécessaire, un objet de données '97' est inclus dans le champ de données afin de transmettre la valeur initiale de Le.

TCS_333 Tout objet de données à chiffrer doit être complété conformément à la norme [ISO 7816-4] en utilisant l'indicateur '01' de contenu de remplissage. Concernant le calcul du MAC, chaque objet de données de l'APDU est également complété séparément conformément à la norme [ISO 7816-4].

Remarque: le remplissage destiné à la messagerie sécurisée est toujours affecté à la couche de messagerie sécurisée, jamais aux algorithmes CMAC ou CBC.

Résumé et exemples

Une commande APDU de la messagerie sécurisée appliquée respecte la structure suivante, selon le cas de chaque commande non sécurisée (DO correspond à l'objet de données):

Cas 1: CLA INS P1 P2 || Lc' || DO '8E' || Le

Cas n° 2: CLA INS P1 P2 || Lc' || DO '97' || DO'8E' || Le

Cas n° 3 (octet INS pair): CLA INS P1 P2 || Lc' || DO '81' || DO'8E' || Le

Cas 3 (octet INS impair): CLA INS P1 P2 || Lc' || DO 'B3' || DO'8E' || Le

Cas n° 4 (octet INS pair): CLA INS P1 P2 || Lc' || DO '81' || DO'97' || DO'8E' || Le

Cas 4 (octet INS impair): CLA INS P1 P2 || Lc' || DO 'B3' || DO'97' || DO'8E' || Le

où Le = '00' ou '00 00' selon que l'on utilise des zones de longueur courte ou étendue; cf. [ISO 7816-4].

Une réponse APDU de la messagerie sécurisée appliquée respecte la structure suivante, selon le cas de chaque réponse non sécurisée:

Cas 1 ou 3: DO '99' || DO '8E' || SW1SW2
Cas n° 2 ou n° 4 (octet INS pair) avec codage: DO '81' || DO '99' || DO '8E' || SW1SW2
Cas 2 ou 4 (octet INS pair) sans cryptage: DO '87' || DO '99' || DO '8E' || SW1SW2
Cas 2 ou 4 (octet INS impair) sans cryptage: DO 'B3' || DO '99' || DO '8E' || SW1SW2

Remarque: Les cas 2 ou 4 (octet INS impair) avec cryptage ne servent jamais pour la communication entre une VU et une carte.

Ci-après suivent trois exemples de transformations APDU pour des commandes avec un code INS pair. La Figure 8 illustre une commande APDU authentifiée relevant du cas 4, la Figure 9 illustre une réponse APDU authentifiée relevant des cas 2 ou 4 et la Figure 10 indique une réponse APDU cryptée et authentifiée relevant des cas 2 ou 4.

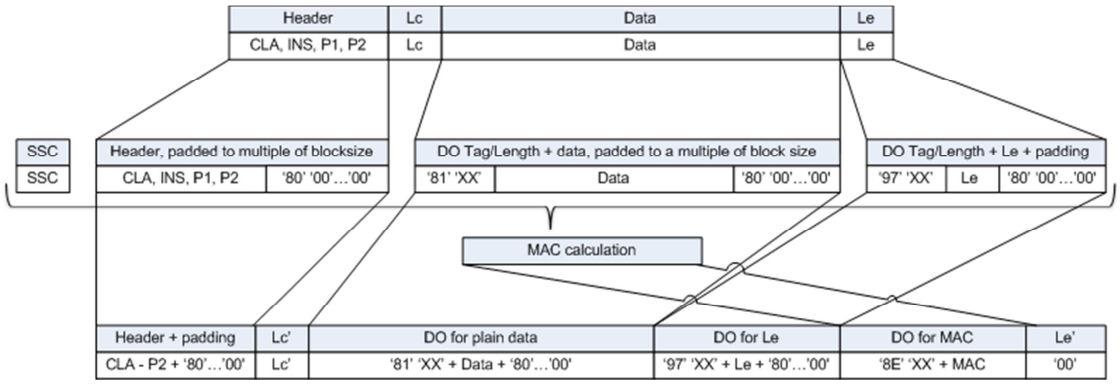


Figure 8 Transformation d'une commande APDU authentifiée relevant du cas 4

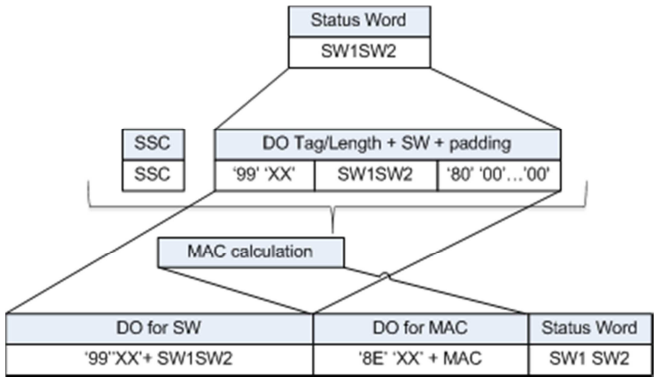


Figure 9 Transformation d'une réponse APDU authentifiée relevant des cas 1 ou 3

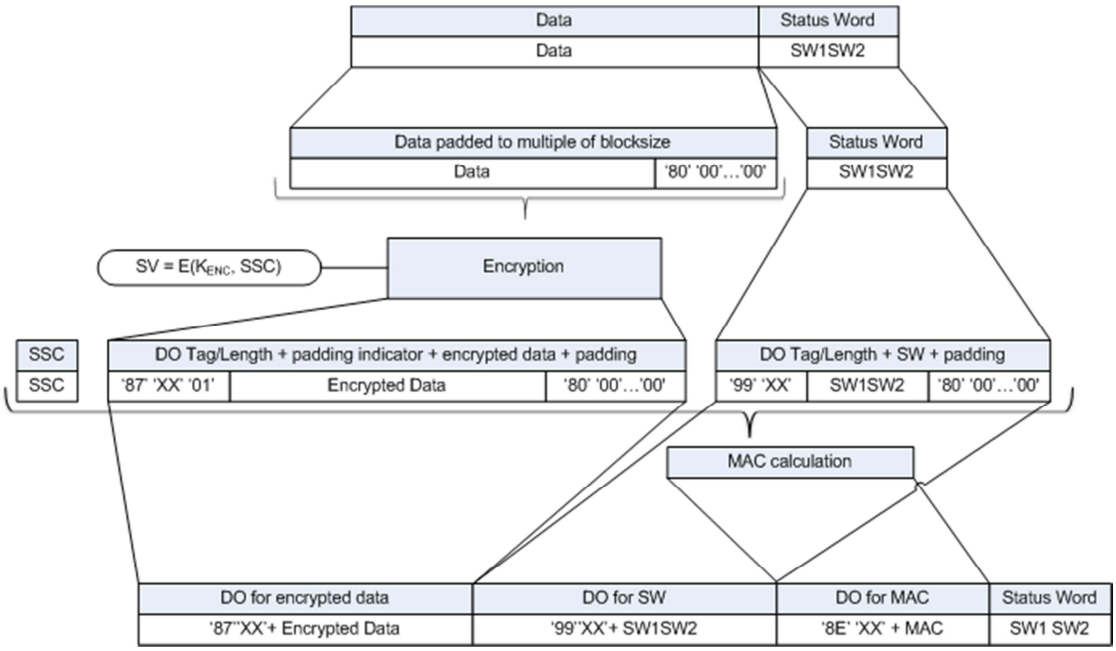


Figure 10 Transformation d'une réponse APDU cryptée et authentifiée relevant des cas 2 ou 4

4.5.3 Abandon de la session de messagerie sécurisée

TCS_334 Une unité embarquée sur véhicule abandonne une session de messagerie sécurisée en cours si et seulement si l'une des conditions suivantes survient:

- elle reçoit une réponse APDU en clair,
- elle détecte une erreur de messagerie sécurisée dans une réponse APDU:
  - un objet de données de messagerie sécurisée manque, l'ordre des objets de données est erroné ou un objet de données inconnu est présent.
  - un objet de données de la messagerie sécurisée est erroné, p. ex. la valeur MAC est erronée, la structure TLV est erronée ou l'indicateur de remplissage de la balise '87' est égal à '01'.
- la carte adresse un octet d'état indiquant qu'il a détecté une erreur de SM (cf. TCS_336),
- la limite pour le nombre de commandes et de réponses associées de la session actuelle est atteinte. Pour une VU donnée, cette limite est définie par son fabricant et tient compte des exigences de sécurité du matériel utilisé, avec une valeur maximale de 240 commandes et réponses associées de SM par session.

TCS_335 Une carte tachygraphique abandonne une session de messagerie sécurisée en cours si et seulement si l'une des conditions suivantes survient:

- elle reçoit une réponse APDU en clair,
- elle détecte une erreur de messagerie sécurisée dans une commande APDU:
  - un objet de données de messagerie sécurisée manque, l'ordre des objets de données est erroné ou un objet de données inconnu est présent.
  - un objet de données de la messagerie sécurisée est erroné, p. ex. la valeur MAC est erronée ou la structure TLV est erronée.
- l'alimentation est coupée ou la carte est réinitialisée,
- la VU sélectionne une application sur la carte,
- la VU entame la procédure d'authentification de la VU,
- la limite pour le nombre de commandes et de réponses associées de la session actuelle est atteinte. Pour une carte donnée, cette limite est définie par son fabricant et tient compte des exigences de sécurité du matériel utilisé, avec une valeur maximale de 240 commandes et réponses associées de SM par session.

TCS_336 Concernant la gestion des erreurs de SM par une carte tachygraphique:

- si dans une commande APDU, certains objets de données de messagerie sécurisée attendus manquent, l'ordre des objets de données est erroné ou des objets de données inconnus sont présents, une carte tachygraphique répond au moyen des octets d'état '69 87'.
- si un objet de données de messagerie sécurisée dans une commande APDU est erroné, une carte tachygraphique répond au moyen des octets d'état '69 88'.

Dans ce cas, les octets d'état sont renvoyés sans utiliser la SM.

TCS_337 Si une session de Messagerie sécurisée entre une VU et une carte tachygraphique est abandonnée, la VU et la carte tachygraphique:

- détruisent de façon sécurisée les clés de sessions mémorisées;
- établissent immédiatement une nouvelle session de messagerie sécurisée, conformément aux dispositions des sections 4.2 à 4.5.

TCS_338 Si pour une raison quelconque, la VU décide de redémarrer une authentification mutuelle vis-à-vis d'une carte insérée, la procédure est relancée avec la vérification de la chaîne de certification de la carte, conformément aux dispositions de la section 4.2 et continue conformément aux dispositions des sections 4.2 à 4.5.

5 couplage de l'UV et du dispositif GNSS, authentification mutuelle et messagerie sécurisée

5.1 Généralités

TCS_339 Le dispositif GNSS qu'utilise une VU pour déterminer sa position peut être interne (c'est-à-dire intégré au boîtier de la VU et non extractible) ou externe (module indépendant). Dans le premier cas, il n'est pas nécessaire de normaliser la communication interne entre le dispositif GNSS et la VU. Les exigences du présent chapitre ne s'appliquent donc pas. Dans le deuxième cas, il est nécessaire de normaliser la communication entre le dispositif GNSS et la VU. Les exigences de protection du présent chapitre s'appliquent donc.

TCS_340 La sécurisation des communications échangées entre une unité embarquée sur véhicule et un dispositif GNSS externe passe par les mêmes exigences que la communication sécurisée entre une unité embarquée sur véhicule et une carte tachygraphique. Le dispositif GNSS externe (EGF) joue le rôle de la carte tachygraphique. Toutes les exigences mentionnées au chapitre 4 pour les cartes tachygraphiques sont satisfaites par l'EGF et tiennent compte des écarts, clarifications et ajouts mentionnés au présent chapitre. En particulier, la vérification de la chaîne de certification mutuelle, l'authentification de la VU et l'authentification du circuit sont menées conformément aux dispositions des sections 5.3et 5.4.

TCS_341 La communication entre une unité embarquée sur véhicule et un EGF se distingue de la communication entre une unité embarquée sur véhicule et une carte tachygraphique en cela qu'une unité embarquée sur véhicule et un EGF doivent être couplés une fois dans l'atelier avant que la VU et l'EGF puissent échanger des données basées GNSS en fonctionnement normal. Le processus de couplage fait l'objet d'une description détaillée à la section 5.2.

TCS_342 Concernant la communication entre une unité embarquée sur véhicule et un EGF, 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 en appendice 2 de la présente Annexe.

5.2 couplage d'une VU et d'un dispositif externe GNSS

TCS_343 Une unité embarquée sur véhicule et un EGF sont couplés par un atelier. Seuls une unité embarquée sur véhicule et un EGF couplés peuvent communiquer en fonctionnement normal.

TCS_344 Le couplage d'une unité embarquée sur véhicule et d'un EGF n'est possible que si la VU est en mode étalonnage. Le couplage est lancé par l'unité embarquée sur le véhicule.

TCS_345 Un atelier peut coupler de nouveau une unité embarquée sur véhicule à un autre EGF ou au même EGF, et ce, à tout moment. Pendant le nouveau couplage, la VU détruit efficacement le certificat EGF_MA existant mémorisé et enregistre le certificat EGF_MA de l'EGF auquel elle vient d'être couplée.

TCS_346 Un atelier peut coupler de nouveau un EGF à une autre unité embarquée sur véhicule ou à la même, et ce, à tout moment. Pendant le nouveau couplage, l'EGF détruit efficacement le certificat VU_MA existant mémorisé et enregistre le certificat VU_MA de la VU à laquelle il vient d'être couplé.

5.3 Vérification mutuelle de la chaîne de certificat

5.3.1 Généralités

TCS_347 La vérification de la chaîne de certification mutuelle entre une VU et un EGF prend place uniquement durant le couplage d'une VU et d'un EGF par un atelier. Pendant le fonctionnement normal d'une VU et d'un EGF couplés, aucun certificat n'est vérifié. La VU et l'EGF font confiance aux certificats mémorisés pendant le couplage, après avoir vérifié leur validité dans le temps. La VU et l'EGF ne font confiance à aucun autre certificat pour protéger la communication entre la VU et l'EGF en fonctionnement normal.

5.3.2 Pendant le couplage VU - EGF

TCS_348 Pendant le couplage à un EGF, une unité embarquée sur véhicule utilise le protocole décrit à la Figure 4 (section 4.2.1) pour vérifier la chaîne de certification de l'EGF.

Notes relatives à la Figure 4 dans ce contexte:

- Le contrôle de la communication sort du champ d'application du présent appendice. Cependant, un EGF n'est pas une carte intelligente. La VU n'enverra donc vraisemblablement pas une Réinitialisation pour lancer la communication et ne recevra pas d'ATR.
- Les certificats et les clés publiques associés à la carte mentionnés sur cette Figure sont ceux de l'EGF en vue de l'authentification mutuelle. La section 3.1.6 précise leur intitulé: EGF_MA.
- Les certificats et les clés publiques Card.CA mentionnés sur cette Figure sont ceux du MSCA en vue de la signature des certificats EGF. La section 3.1.3 précise leur intitulé: MSCA_VU-EGF.
- Le certificat Card.CA.EUR mentionné sur cette Figure est le certificat racine européen indiqué dans le CAR du certificat MSCA_VU-EGF.
- Le certificat Card.Link mentionné sur cette Figure correspond au certificat de lien de l'EGF, le cas échéant. Comme le précise la section 3.1.2, 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 européenne.
- Le certificat Card.Link.EUR est le certificat racine européen indiqué dans le CAR du certificat Card.Link.
- Au lieu du `cardExtendedSerialNumber`, la VU lit le `sensorGNSSserialNumber` depuis l'EF ICC.
- Au lieu de sélectionner l'AID de la carte tachygraphique, la VU sélectionne l'AID de l'EGF.
- «Ignorer la carte» devient «Ignorer l'EGF».

TCS_349 Une fois le certificat EGF_MA vérifié, l'unité embarquée sur véhicule mémorise ce certificat pour l'utiliser en fonctionnement normal; cf. section 5.3.3.

TCS_350 Pendant le couplage à une VU, un dispositif GNSS externe utilise le protocole décrit à la Figure 5 (section 4.2.2) pour vérifier la chaîne de certification de la VU.

Notes relatives à la Figure 5 dans ce contexte:

- La VU génère une nouvelle paire de clés éphémères en utilisant les paramètres de domaine du certificat EGF.
- Les certificats et les clés publiques associés à la VU mentionnés sur cette Figure sont ceux de l'authentification mutuelle. La section 3.1.4 précise leur intitulé: VU_MA.
- Les certificats et les clés publiques VU.CA mentionnés sur cette Figure sont ceux de la signature des certificats de la VU et du dispositif GNSS externe. La section 3.1.3 précise leur intitulé: MSCA_VU-EGF.
- Le certificat VU.CA.EUR mentionné sur cette Figure est le certificat racine européen indiqué dans le CAR du certificat VU.CA.
- Le certificat VU.Link mentionné sur cette Figure est le certificat de lien de la VU, le cas échéant. Comme le précise la section 3.1.2, 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 européenne.
- Le certificat VU.Link.EUR est le certificat racine européen indiqué dans le CAR du certificat VU.Link.

TCS_351 À titre d'exception par rapport à l'exigence du TCS_309, un EGF utilise le temps GNSS pour vérifier la validité dans le temps de tout certificat présenté.

TCS_352 Une fois le certificat VU_MA vérifié, le dispositif GNSS externe mémorise ce certificat pour l'utiliser en fonctionnement normal; cf. section 5.3.3.

5.3.3 Pendant le fonctionnement normal

TCS_353 En fonctionnement normal, une unité embarquée sur véhicule et un EGF respectent le protocole décrit sur la Figure 11 pour vérifier la validité dans le temps des certificats EGF_MA et VU_MA mémorisés et pour définir la clé publique VU_MA en vue de l'authentification ultérieure de la VU. Aucune autre vérification mutuelle des chaînes de certificats n'a lieu en fonctionnement normal.

Note: la Figure 11 illustre essentiellement les premières étapes indiquées sur les Figure 4 et Figure 5. Cependant, un EGF n'étant pas une carte intelligente, la VU n'enverra donc vraisemblablement pas une réinitialisation pour lancer la communication et ne recevra pas d'ATR. Dans tous les cas, cela sort du champ d'application du présent appendice.

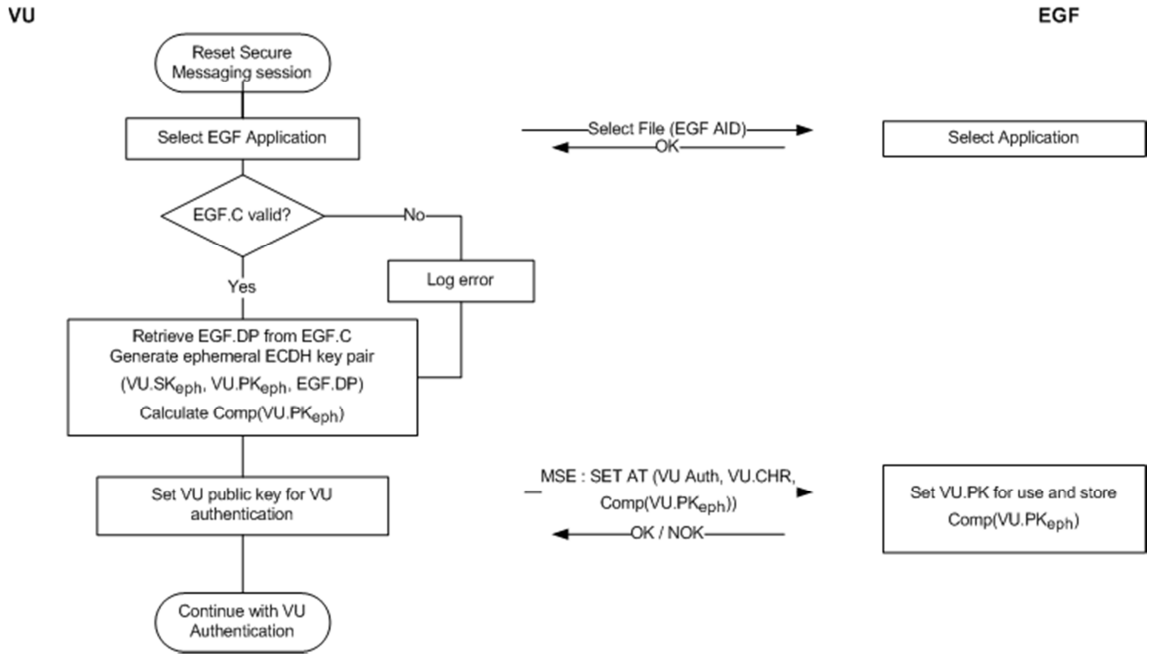


Figure 11 Vérification mutuelle de la validité dans le temps du certificat en fonctionnement normal entre la VU et l'EGF

TCS_354 Comme l'illustre la Figure 11, l'unité embarquée sur véhicule enregistre une erreur si le certificat EGF_MA n'est plus valide. Cependant, l'authentification mutuelle, la concordance des clés et la communication ultérieure au moyen de la messagerie sécurisée se déroulent normalement.

5.4 Authentification de la VU, Authentification du circuit et concordance des clés de session

TCS_355 L'authentification de la VU, l'authentification du circuit et la concordance des clés de la session entre une VU et un EGF ont lieu pendant le couplage et dès qu'une session de messagerie sécurisée est réétablie en fonctionnement normal. La VU et l'EGF exécutent les procédures décrites aux sections 4.3 et 4.4. Toutes les exigences prévues dans ces sections s'appliquent.

5.5 Messagerie sécurisée

TCS_356 Toutes les commandes et réponses échangées entre une unité embarquée sur véhicule 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 dans la section 4.5 s'appliquent.

TCS_357 Si une session de messagerie sécurisée entre une VU et un EGF est abandonnée, la VU établit immédiatement une nouvelle session de messagerie sécurisée, comme le prévoient les sections 5.3.3 et 5.4.

6 Couplage et communication de la VU et du capteur de mouvement

6.1 Généralités

TCS_358 Une unité embarquée sur véhicule et un capteur de mouvement communiquent à l'aide du protocole d'interface prévu par la norme [ISO 16844-3] pendant le couplage et le fonctionnement normal. Cela inclut les changements prévus au présent chapitre et à la section 3.2.1.

Note: les lecteurs de la présente section sont censés maîtriser le contenu de la norme [ISO 16844-3].

6.2 Couplage de la VU et du capteur de mouvement à l'aide de générations de clés différentes

Comme expliqué à la section 3.2.1, la clé maîtresse du capteur de mouvement et toutes les clés associées sont régulièrement remplacées. Cela entraîne la présence de trois clés AES K_{M-WC} liées au capteur de mouvement, au maximum, (de générations de clés consécutives) sur les cartes d'atelier. De même, un maximum de trois différents cryptages de données de type AES (sur la base de générations consécutives de clé maîtresse K_M du capteur de mouvement) peuvent être présents sur les capteurs de mouvement. Une unité embarquée sur véhicule contient une seule clé K_{M-VU} associée au capteur de mouvement.

TCS_359 Une VU et un capteur de mouvement de deuxième génération sont couplés comme suit (comparer au tableau 6 de la norme [ISO 16844-3]):

1. Une carte d'atelier de deuxième génération est insérée dans la VU et cette dernière est raccordée au capteur de mouvement.
2. La VU lit toutes les clés K_{M-WC} disponibles sur la carte d'atelier, inspecte leur numéro de version de clé et choisit celui qui correspond au numéro de version de la clé VU K_{M-VU}. Si la clé K_{M-WC} correspondante est absente de la carte d'atelier, la VU abandonne la procédure de couplage et affiche le message d'erreur approprié pour le titulaire de la carte d'atelier.
3. La VU calcule la clé maîtresse du capteur de mouvement K_M à partir de K_{M-VU} et de $K_{M-WC,}$ et calcule la clé d'identification K_{ID} à partir de K_M, comme le prévoit la section 3.2.1.
4. La VU envoie les instructions pour lancer la procédure de couplage par rapport au capteur de mouvement, comme le prévoit la norme [ISO 16844-3] et chiffre le numéro de série reçu du capteur de mouvement avec la clé d'identification $K_{ID.}$ génération. En retour, la VU envoie le numéro de série crypté au capteur de mouvement.
5. Le capteur de mouvement compare le numéro de série crypté consécutivement avec les cryptages des numéros de série dont il dispose en interne. S'il identifie une correspondance, la VU est authentifiée. Le capteur de mouvement prend note de la génération de K_{ID} qu'utilise la VU et renvoie la version codée correspondante de sa clé de couplage; c'est-à-dire que le codage a été créé avec la même génération de K_M.
6. La VU déchiffre la clé de couplage à l'aide de K_M, génère une clé de session $K_{S,}$, la chiffre à l'aide d'une clé de couplage et envoie le résultat au capteur de mouvement. Le capteur de mouvement déchiffre K_S.
7. La VU assemble les informations de 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 reçue et les renvoie à la VU. La VU vérifie que les informations de couplage sont identiques à celles qu'elle a adressées au capteur de mouvement à l'étape précédente. Dans l'affirmative, cela prouve que le capteur de mouvement utilise la même K_S que la VU. Par conséquent, à l'étape 5, il adresse sa clé de couplage cryptée avec la bonne génération de K_M. Le capteur de mouvement est ainsi authentifié.

Note: les étapes 2 et 5 divergent de la procédure normalisée [ISO 16844-3]; les autres étapes restent standard.

Exemple: imaginons qu'un couplage ait lieu durant la première année de validité du certificat ERCA (3); cf. Figure 2 de la section 3.2.1.2. En outre,

- Imaginons que le capteur de mouvement ait été émis pendant la dernière année de validité du certificat ERCA(1). Il contient alors les clés et les données suivantes:
  - N_s[1]: son numéro de série crypté avec K_{ID} de génération 1,

- N_s[2]: son numéro de série crypté avec K_{ID} de génération 2,
- N_s[3]: son numéro de série crypté avec K_{ID} de génération 3,
- K_P[1]: sa clé de couplage[12] de génération 1, cryptée avec K_M de génération 1,
- K_P[2]: sa clé de couplage de génération 2, cryptée avec K_M de génération 2,
- K_P[3]: sa clé de couplage de génération 3, cryptée avec K_M de génération 3,

- Imaginons que la carte d'atelier ait été émise pendant la première année de validité du certificat ERCA (3). Elle contient donc les générations 2 et 3 de la clé K_{M-WC}.
- Imaginons que la VU est de génération 2 et contient K_{M-VU} de génération 2.

Dans ce cas, voici le déroulement des étapes 2 à 5:

- Étape 2: la VU lit la K_{M-WC} de génération 2 et de génération 3 depuis la carte d'atelier et inspecte leur numéro de version.
- Étape 3: la VU combine la K_{M-WC} de génération 2 avec sa K_{M-VU} afin de calculer K_M et $K_{ID.}$
- Étape 4: la VU chiffre le numéro de série reçu du capteur de mouvement avec $K_{ID.}$
- 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 identifie une correspondance. Il conclut que la VU est de génération 2 et renvoie donc la K_P[2].

6.3 couplage et communication de la VU et du capteur de mouvement en utilisant AES

TCS_360 Comme le précise le Tableau 45 de la section 3.2.1, toutes les clés impliquées dans le couplage d'une VU et d'un capteur de mouvement de deuxième génération et dans leur communication ultérieure sont des clés AES, plutôt que des clés TDES de double longueur, comme le prévoit la norme [ISO 16844-3]. La longueur de ces clés AES peuvent être de 128, 192 ou 256 bits. La taille des blocs AES étant de 16 octets, la longueur d'un message crypté doit être un multiple de 16 octets, comparé aux 8 octets des clés TDES. Par ailleurs, certains de ces messages servent au transport des clés AES, dont la longueur peut être de 128, 192 ou 256 bits. Par conséquent, le nombre d'octets de données par instruction figurant dans le tableau 5 de la norme [ISO 16844-3] peuvent évoluer vers celui figurant au Tableau 48.

Instruction	*Demande/Réponse*	*Description des données*	*nbre d'octets de données en clair selon [ISO 16844-3]*	*nbre d'octets de données en clair utilisant des clés AES*	*nbre d'octets de données cryptées utilisant des clés AES d'une longueur de*		
					128	**192**	**256**
10	demande	Données d'authentification + numéro de fichier	8	8	16	16	16
11	réponse	Données d'authentification + contenu de fichier	16 bits ou 32 bits selon le fichier	16 bits ou 32 bits selon le fichier	16 / 32	16 / 32	16 / 32
41	demande	numéro de série MoS	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

[12] Note: les clés de couplage de génération 1, 2 et 3 peuvent être identiques ou peuvent toutes être de longueur différentes, comme le prévoit le TCS_259.

Instruction	*Demande/Réponse*	*Description des données*	*nbre d'octets de données en clair selon [ISO 16844-3]*	*nbre d'octets de données en clair utilisant des clés AES*	*nbre d'octets de données cryptées utilisant des clés AES d'une longueur de*		
					128	**192**	**256**
70	demande	Données d'authentification	8	8	16	16	16
80	réponse	Valeur du compteur MoS + données d'authen.	8	8	16	16	16

Tableau 48 Nombre d'octets de données cryptées et en clair par instruction comme le prévoit la norme [ISO 16844-3]

TCS_361 Les informations relatives au couplage envoyées dans les instructions 43 (demande de la VU) et 50 (réponse du MoS) sont assemblées comme le prévoit la section 7.6.10 de la norme [ISO 16844-3], hormis l'utilisation de l'algorithme AES au lieu de l'algorithme TDES dans la procédure de cryptage des données de couplage. Cela entraine donc deux cryptages AES et l'adoption du remplissage prévu au TCS_362 pour correspondre à la taille des blocs AES. La clé K'_p servant à cet cryptage est générée comme suit:

- Dans le cas où la clé de couplage K_P est de 16 octets: $K'_p = K_P$ XOR $(N_s||N_s)$
- Dans le cas où la clé de couplage K_P est de 24 octets: $K'_p = K_P$ XOR $(N_s||N_s||N_s)$
- Dans le cas où la clé de couplage K_P est 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.

TCS_362 Si la longueur des données en clair (utilisant les clés AES) n'est pas un multiple de 16 octets, la méthode de remplissage n° 2 définie par la norme [ISO 9797-1] est utilisée.

Note: la norme [ISO 16844-3] prévoit un nombre d'octets de données en clair multiples de 8 de sorte que le remplissage n'est pas nécessaire lorsque des clés TDES sont utilisées. Le présent appendice ne modifie pas la définition des données et des messages prévue par la norme [ISO 16844-3]. Il reste donc nécessaire de procéder au remplissage.

TCS_363 Concernant l'instruction 11 et lorsque plusieurs blocs de données doivent être cryptés, il convient d'utiliser le mode d'exploitation par chaînage de cryptage par blocs comme le prévoit la norme [ISO 10116], avec un paramètre d'entrelacement $m = 1$. L'IV à utiliser est:

- Concernant 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 n° 2 définie par la norme [ISO 9797-2]; cf. sections 7.6.5. et 7.6.6. de la norme [ISO 16844-3].
- Concernant toutes les autres instructions dont plus de 16 octets sont transférés, comme le spécifie le Tableau 48: '00' {16}, c'est-à-dire 16 octets de valeur binaire égale à 0.

Remarque: comme indiqué aux sections 7.6.5 et 7.6.6 de la norme [ISO 16844-3], lorsque le MoS 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 cryptage en mode CBC des fichiers de données; et
- crypté et inclus comme premier bloc dans les données envoyées à la VU.

6.4 couplage de la VU et du capteur de mouvement pour des équipements de générations différentes

TCS_364 Comme l'explique la section 3.2.1, un capteur de mouvement de deuxième génération contient le cryptage TDES des données de couplage (comme le définit la partie A du présent appendice), qui permet de coupler le capteur de mouvement avec une VU de première génération. Dans ce cas, une VU de première génération et un capteur de mouvement de deuxième génération sont couplés comme le prévoient la partie A du présent appendice et la norme [ISO 16844-3]. Concernant la procédure de couplage, une carte d'atelier de première ou de deuxième génération peut être utilisée indifféremment.

Remarques:

- Il n'est pas possible de coupler une VU 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 VU de deuxième génération avec capteur de mouvement.

7 Sécurité des communications distantes utilisant DSRC

7.1 Généralités

Comme le prévoit l'appendice 14, une VU génère régulièrement des données de surveillance du tachygraphe à distance (RTM) qu'elle envoie au dispositif (interne ou externe) de communication à distance (RCF). 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 14. L'appendice 1 spécifie que les données RTM résultent de la concaténation de:

- **Données utiles cryptées du tachygraphe** le cryptage des données utiles en clair du tachygraphe
- **Données de sécurité DSRC** décrites ci-dessous

Les 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 1.

TCS_365 Les données en clair `tachographPayload` communiquées par une VU à un dispositif de communication à distance (si le RCF est externe à la VU) ou par une VU à l'interrogateur distant au moyen de l'interface DSRC (si le RCF est interne à la VU) sont protégées en mode chiffrer-puis-authentifier. Cela signifie que les données utiles du tachygraphe sont d'abord cryptées pour protéger la confidentialité du message, puis qu'un MAC est calculé pour garantir l'authenticité et l'intégrité des données.

TCS_366 Les données relatives à la sécurité DSRC correspondent à une concaténation des éléments de données suivants dans l'ordre indiqué; cf. Figure 12

- **Date et heure actuelles** la date et l'heure actuels de la VU (type de données **`TimeReal`).**
- **Compteur** un compteur sur trois octets, cf.TCS_367**.**
- **Numéro de série de la VU** le numéro de série de la VU (type de données **`VuSerialNumber`).**
- **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 la VU; cf. section 3.2.2**.**
- **MAC** le MAC calculé en fonction de tous les octets précédents dans les données RTM.

TCS_367 Le compteur sur trois octets dans les données relatives à la sécurité DSRC respecte la structure MSB-first. La première fois qu'une VU calcule un jeu de données RTM après son entrée en production, elle définit la valeur du compteur à zéro. La VU incrémente le compteur d'une unité avant chaque nouveau calcul du jeu de données RTM suivant.

7.2 Cryptage des données utiles du tachygraphe et génération du MAC

TCS_368 En partant d'un élément de données en clair de type TachographPayload tel que décrit à l'appendice 14, une VU chiffre ces données comme illustré à la Figure 12: la clé DSRC de la VU pour codage $K\_VU_{DSRC}\_ENC$ (cf. section 3.2.2) avec AES, en mode d'exploitation par chaînage de cryptage par blocs (CBC), tel que défini par la norme [ISO 10116], selon un paramètre d'entrelacement m = 1. Le vecteur d'initialisation est égal à *IV = date et heure actuelles* || *'00 00 00 00 00 00 00 00'* || où *la date et l'heure actuelles* ainsi que *le compteur* sont spécifiés en TCS_366*. Les données à chiffrer sont complétées par un contenu de remplissage à l'aide de la méthode n° 2 définie par la norme [ISO 9797-1]*.

TCS_369 Une VU calcule le MAC dans les données de sécurité DSRC comme illustré sur 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. La VU utilise sa clé DSRC d'authentification $K\_VU_{DSRC}\_MAC$ (cf. section 3.2.2) avec l'algorithme AES en mode CMAC comme spécifié au [SP 800-38B]. La longueur de MAC est liée à la longueur des clés de DSRC propres à la VU, conformément au TCS_192.

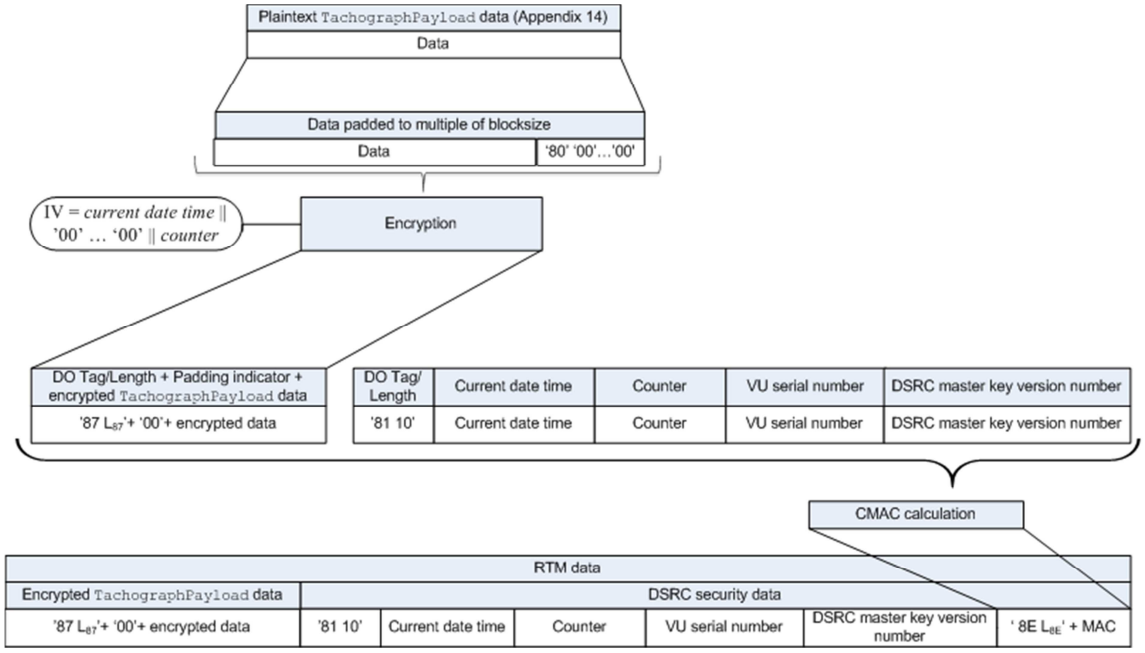


Figure 12cryptage des données utiles du tachygraphe et génération du MAC

7.3 Vérification et décryptage de la charge du tachygraphe

TCS_370 Lorsqu'un interrogateur reçoit les données RTM d'une VU, il envoie la totalité des données RTM à une carte de contrôle dans le champ de données d'une commande PROCESS DSRC MESSAGE, conformément à l'appendice 2. Puis:

1. la carte de contrôle inspecte le numéro de version de la clé maîtresse DSRC dans les données relatives à la sécurité DSRC. Si la carte de contrôle ne connaît pas la clé maîtresse DSRC indiquée, elle envoie une erreur conformément à l'appendice 2 et abandonne la procédure.
2. la carte de contrôle utilise la clé maîtresse DSRC indiquée en combinaison avec le numéro de série de la VU dans les données relatives à la sécurité DSRC pour calculer les clés DSRC propres à la VU K_VU_{DSRC}_ENC et K_VU_{DSRC}_MAC, comme le précise le TCS_266.
3. la carte de contrôle utilise K_VU_{DSRC}_MAC pour vérifier le MAC dans les données relatives à la sécurité DSRC, conformément au TCS_369. Si le MAC est erroné, la carte de contrôle envoie une erreur conformément à l'appendice 2 et abandonne la procédure.
4. la carte de contrôle utilise K_VU_{DSRC}_ENC pour décrypter les données utiles cryptées du tachygraphe, comme le précise TCS_368. La carte de contrôle supprime le remplissage et envoie les données utiles du tachygraphe décryptées à l'interrogateur distant.

TCS_371 Pour éviter les attaques par relecture, l'interrogateur distant vérifie la récence des données RTM en contrôlant que le *current date time* dans les données relatives à la sécurité DSRC ne diffère pas trop de ses propres date et heure actuelles.

Remarques:

- Cela impose à l'interrogateur distant de disposer d'une source horaire exacte et fiable.
- L'appendice 14 exigeant qu'une VU calcule un nouveau jeu de données RTM toutes les 60 secondes, d'une part et l'horloge de la VU intégrant une marge d'erreur autorisée d'une minute par rapport à l'heure exacte, d'autre part, la limite basse de récence des données RTM est fixée à deux minutes. La récence exigée varie également selon le degré de précision de l'horloge de l'interrogateur distant.

TCS_372 Lorsqu'un atelier vérifie le fonctionnement correct de la fonctionnalité DSRC d'une VU, il envoie la totalité des données RTM reçues de la VU à une carte d'atelier dans la zone de données d'une commande PROCESS DSRC MESSAGE, conformément à l'appendice 2. La carte d'atelier effectue tous les contrôles et toutes les actions spécifiés au TCS_370.

8 Signature des téléchargement de données et contrôle des signatures

8.1 Généralités

TCS_373 L'équipement spécialisé intelligent (IDE) enregistre les données reçues d'une VU ou d'une carte donnée pendant une session de téléchargement au sein d'un fichier de données physiques. Les données peuvent être mémorisées sur un support de stockage externe. Ce fichier contient les signatures numériques en fonction des blocs de données, comme le spécifie l'appendice 7. Ce fichier contient également les certificats suivants (cf. section 3.1):

- en cas de téléchargement depuis une VU:
  - le certificat VU_Sign;
  - le certificat MSCA_VU-EGF comprenant la clé publique à utiliser pour vérifier le certificat VU_Sign.
- en cas de téléchargement depuis une carte:
  - le certificat Card_Sign;
  - le certificat MSCA_Card comprenant la clé publique à utiliser pour vérifier le certificat Card_Sign.

TCS_374 L'IDE dispose également des éléments suivants:

- en cas d'utilisation d'une carte de contrôle pour vérifier la signature, comme illustré sur la Figure 13: le certificat de lien reliant le plus récent certificat EUR à celui dont la validité le précède immédiatement, le cas échéant.
- S'il vérifie la signature: tous les certificats racines européens valides.

Note: la méthode qu'utilise l'IDE pour extraire ces certificats ne figure pas au présent appendice.

8.2 Génération de signatures

TCS_375 L'algorithme de signature pour créer des signatures numériques en fonction des données téléchargées doit être de type ECDSA conformément aux règles [DSS], en ayant recours à l'algorithme de hachage associé à la taille de clé de la VU ou de la carte, conformément au TCS_192. La structure de la signature est en clair, conformément au [TR-03111].

8.3 Vérification de signatures

TCS_376 Un IDE peut procéder à la vérification d'une signature par rapport aux données téléchargées lui-même ou utiliser une carte de contrôle à cette fin. S'il utilise une carte de contrôle, la vérification de la signature respecte l'illustration de la Figure 13. S'il procède lui-même à la vérification de la signature, l'IDE vérifie l'authenticité et la validité de tous les certificats dans la chaîne de certificats contenue dans le fichier de données ainsi que la signature par rapport aux données conformément à la procédure relative aux signatures définie par les [DSS].

Notes relatives à la Figure 13:

- L'équipement qui a participé à la signature des 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 VU_Sign ou Card_Sign.
- Les certificats et les clés publiques EQT.CA mentionnés sur la Figure sont ceux destinés à la signature des certificats VU ou Card, selon le cas.
- Le certificat EQT.CA.EUR mentionné sur cette Figure est le certificat racine européen indiqué dans le CAR du certificat EQT.CA
- Le certificat EQT.Link mentionné sur cette Figure est le certificat de lien de l'EQT, le cas échéant. Comme le précise la section 3.1.2, 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 européenne.
- Le certificat EQT.Link.EUR désigne le certificat racine européen indiqué dans le CAR du certificat EQT.Link.

TCS_377 Pour calculer le M de hachage envoyé à la carte de contrôle dans la commande PSO:hash, l'IDE utilise l'algorithme de hachage associé à la taille de la clé de la VU ou de la carte depuis laquelle les données sont téléchargées, conformément au TCS_192.

TCS_378 Pour vérifier la signature EQT, la carte de contrôle respecte la procédure relative aux signatures définies par les règles [DSS].

Remarque: le présent document ne spécifie aucune action à entreprendre s'il est impossible de vérifier une signature associée à un fichier de données téléchargé ou si cette vérification échoue.

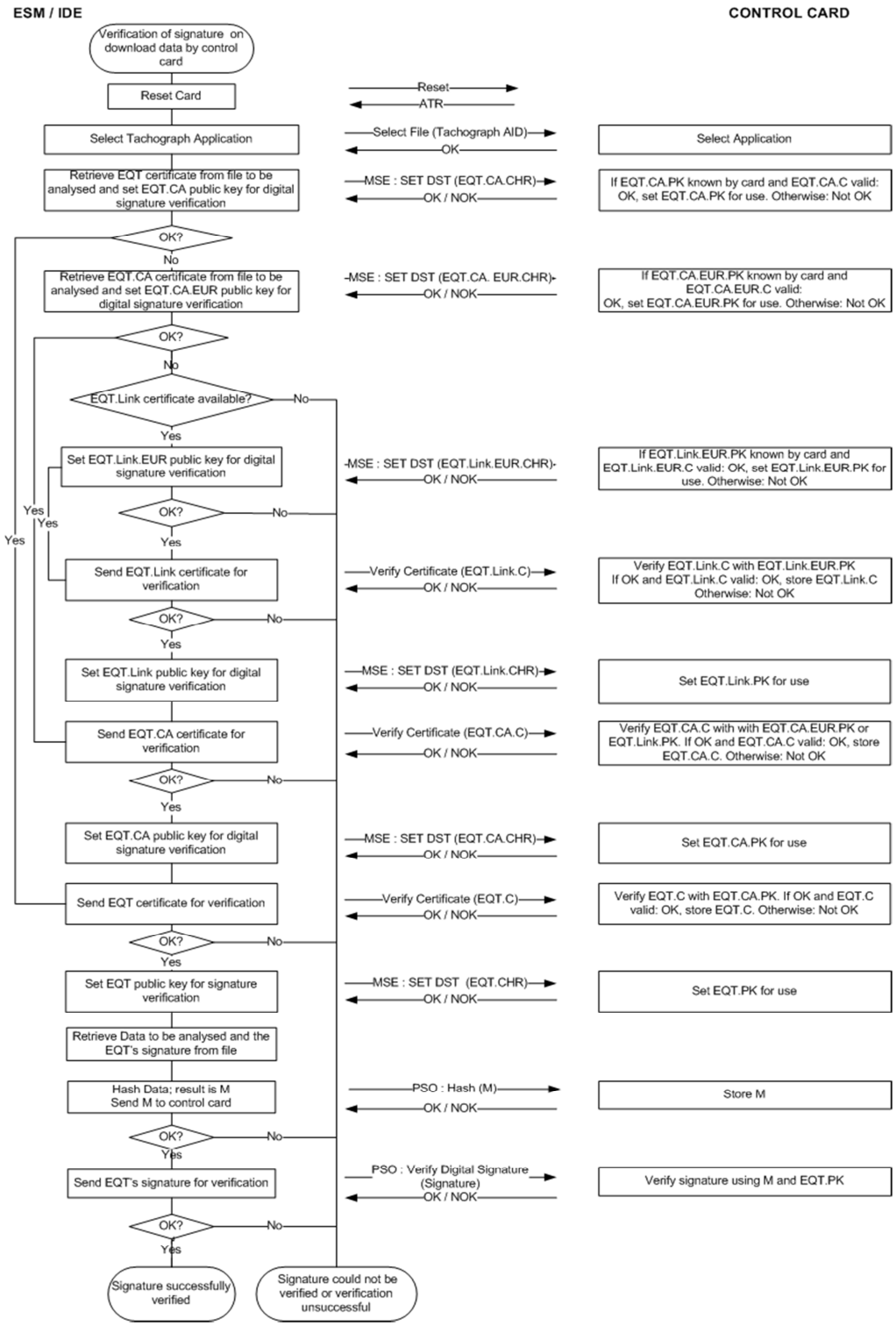


Figure 13Protocole de vérification de la signature associée à un fichier de données téléchargé

FR

APPENDICE 12 POSITIONNEMENT BASÉ SUR UN SYSTÈME MONDIAL DE NAVIGATION PAR SATELLITE (GNSS)

TABLE DES MATIERES

1. Introduction

Le présent appendice présente les exigences techniques associées 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 des informations 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

TCS_379 L'unité embarquée sur le véhicule recueille les données de localisation d'au moins un 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 14:

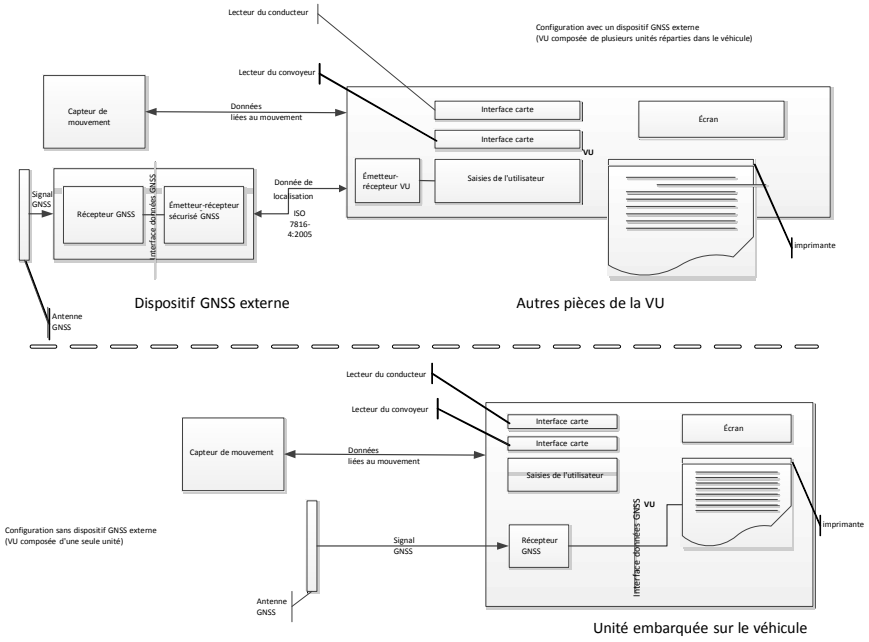


Figure 14 Différentes configurations du récepteur GNSS

1.2 Abréviations et notations

Dans le présent appendice, sont utilisées les abréviations suivantes:

DOP Affaiblissement de la précision
EGF Fichier élémentaire de dispositif GNSS
EGNOS Système européen de navigation par recouvrement géostationnaire
GNSS Global navigation satellite system (système mondial de radionavigation par satellite)
GSA DOP du GPS et satellites actifs
HDOP Affaiblissement de la précision horizontale
ICD Document de contrôle des interfaces
NMEA National Marine Electronics Association
PDOP Affaiblissement de la précision de position
RMC Minimum spécifique recommandé

SIS Signal dans l'espace
VDOP Affaiblissement de la précision verticale
VU Unité embarquée sur le véhicule

2. Spécifications 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[13]. 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).

TCS_380 Les constructeurs veillent à ce que les récepteurs GNSS des tachygraphes intelligents soient compatibles avec les services de positionnement fournis par les systèmes Galileo et EGNOS. Les fabricants ont également la possibilité de choisir, en plus, d'assurer la compatibilité avec d'autres systèmes de navigation par satellite.

TCS_381 Le récepteur GNSS prend en charge l'authentification sur le service ouvert Galileo lorsque ledit service est fourni par le système Galileo et pris en charge par les fabricants de récepteurs GNSS.

3. Phrases NMEA

La présente section décrit les phrases NMEA utilisées pendant le fonctionnement du tachygraphe intelligent. Cette section est applicable à la configuration du tachygraphe intelligent avec et sans dispositif GNSS externe.

TCS_382 Les données de localisation reposent sur les données GNSS du minimum spécifique recommandé (RMC) de la phrase NMEA, 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 RMC est la suivante (d'après la norme NMEA V4.1):

1 2 3 4 5 6 7 8 9 10 11 12

$--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

[13] 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).

Figure 15 Structure de la phrase RMC

L'état indique la disponibilité du signal GNSS. Tant que la valeur de l'état n'est pas fixée à A, les données reçues (c'est-à-dire l'heure ou la latitude ou la longitude) ne peuvent pas servir à enregistrer la position du véhicule dans la VU.

La résolution de la position repose sur la structure de la phrase RMC décrite ci-dessus. La première partie des zones 3) et 5) 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).

TCS_383 L'unité embarquée sur le véhicule mémorise dans la base de données de la VU les informations relatives au positionnement en termes de latitude et de longitude selon une résolution d'1/10 minute ou 1/600 degré, comme le décrit l'appendice 1 pour les coordonnées géographiques type.

La VU peut utiliser la commande GPS DOP et satellites actifs (GSA) pour déterminer et enregistrer la disponibilité et l'exactitude du signal. En particulier, HDOP sert à fournir une indication sur le degré d'exactitude des données de localisation enregistrées (cf. 4.2.2). La VU 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 Satellite-Based Augmentation System (SBAS).

1234 14 15161718

$--GSA,a,a,x,x,x,x,x,x,x,x,x,x,x,x,x.x,x.x,x.x*hh :

1) Mode de sélection
2) Mode
3) ID du premier satellite utilisé pour les points de repère
4) ID du deuxième satellite utilisé pour les points de repère
...
14) ID du douzième satellite utilisé pour les points de repère
15) PDOP exprimé en mètres
16) HDOP exprimé en mètres
17) VDOP exprimé en mètres
18) Identificateur du système GNSS
19) Total de contrôle

Figure 16 Structure de la phrase GSA

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).

TCS_384 La phrase GSA est mémorisée avec le numéro d'enregistrement '06'.

TCS_385 La taille maximale des phrases NMEA (p. ex. RMC, GSA ou d'autres), qui peut servir à étalonner la commande Read Record, est de 85 octets (cf. tTableau 49).

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.

TCS_386 Le dispositif GNSS externe doit être alimenté par une interface de véhicule spécifique.

TCS_387 Le dispositif GNSS externe se compose des éléments suivants (cf. Figure 17):

a) Un récepteur GNSS commercial pour fournir les données de positionnement à l'aide de l'interface de données GNSS. Par exemple, l'interface de données GNSS peut être la norme NMEA V4.10 selon laquelle le récepteur GNSS tient le rôle de l'émetteur et transmet les phrases NMEA à l'émetteur-récepteur sécurisé GNSS sur une fréquence d'1 Hz pour le jeu prédéfini de phrases NMEA, lequel doit comprendre au moins les phrases RMC et GSA. Le choix de la mise en œuvre de l'interface de données GNSS revient aux fabricants du dispositif GNSS externe.
b) Une unité d'émetteur-récepteur (émetteur-récepteur sécurisé GNSS) compatible avec la norme ISO/IEC 7816-4:2013 (cf. 0) pour communiquer avec l'unité embarquée sur le véhicule et prendre en charge l'interface de données GNSS s'adressant au récepteur GNSS. L'unité est dotée d'une mémoire qui enregistre les 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 intègre le récepteur GNSS et l'émetteur-récepteur sécurisé GNSS. La fonction de détection des fraudes met en pratique les mesures de protection de la sécurité comme le définit le profil de protection du tachygraphe intelligent.
d) Une antenne GNSS installée sur le véhicule et connectée au récepteur GNSS à l'aide du système clos.

TCS_388 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.

TCS_389 Dans la VU, l'émetteur-récepteur sécurisé de la VU constitue l'autre extrémité de la communication sécurisée avec l'émetteur-récepteur sécurisé GNSS. Il respecte la norme ISO/IEC 7816-4:2013 relative à la connexion au dispositif GNSS externe.

TCS_390 Pour la couche de communication avec le dispositif GNSS externe, la VU respecte la norme ISO/IEC 7816-12:2005 ou toute autre norme compatible avec la norme ISO/IEC 7816-4:2013. (cf. 0).

4.1.2 État du dispositif GNSS externe à la fin de la production

TCS_391 Le dispositif GNSS externe mémorise les valeurs suivantes dans la mémoire non volatile de l'émetteur-récepteur sécurisé GNSS lorsqu'il quitte l'usine:

- la paire de clé EGF_MA et son certificat,
- le certificat MSCA_VU-EGF comprenant la clé publique MSCA_VU-EGF.PK à utiliser pour vérifier le certificat EGF_MA,
- le certificat EUR comprenant la clé publique EUR.PK à utiliser pour vérifier le certificat MSCA_VU-EGF,
- le certificat EUR dont la durée de validité précède directement celle du certificat EUR à utiliser pour vérifier le certificat MSCA_VU-EGF, 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

TCS_392 Le protocole de communication entre le dispositif GNSS externe et l'unité embarquée sur le véhicule remplit trois fonctions:

1. la collecte et la distribution des données GNSS (p. ex. la position, l'heure et la vitesse),
2. la collecte des données de configuration du dispositif GNSS externe,
3. le protocole de gestion à l'appui de l'appariement, de l'authentification mutuelle et de la concordance de clés de session entre le dispositif GNSS externe et la VU.

TCS_393 Le protocole de communication repose sur la norme ISO/IEC 7816-4:2013 où l'émetteur-récepteur sécurisé de la VU tient le rôle du maître et l'émetteur-récepteur sécurisé du GNSS, le rôle de l'esclave. La connexion physique entre le dispositif GNSS externe et la VU repose sur la norme ISO/IEC 7816-12:2005 ou toute autre norme compatible avec la norme ISO/IEC 7816-4:2013

TCS_394 Le protocole de communication ne doit pas prendre en charge les zones de longueur étendue.

TCS_395 Le protocole de communication de la norme ISO 7816 (*-4:2013 et *-12:2005) entre le dispositif GNSS externe et la VU est fixé à T = 1.

TCS_396 Concernant les fonctions 1) de collecte et de diffusion des données GNSS, 2) de collecte des données de configuration du dispositif GNSS externe et 3) du protocole de gestion, l'émetteur-récepteur sécurisé GNSS simule une carte intelligente dont l'architecture du système de fichiers comprend un fichier maître (MF), un fichier spécialisé (DF) doté de l'identificateur d'application spécifié en Appendice 1, chapitre 6.2 ('FF 44 54 45 47 4D'), trois fichiers élémentaires contenant des certificats et un fichier élémentaire unique (EF.EGF) dont l'identificateur de fichier correspond à ‘2F2F’ comme le prévoit le Tableau 49.

TCS_397 L'émetteur-récepteur sécurisé GNSS mémorise les données provenant du récepteur GNSS et la configuration dans le fichier EF.EGF. Il s'agit d'un fichier d'enregistrement d'une longueur variable et linéaire dont l'identificateur correspond à '2F2F' au format hexadécimal.

TCS_398 L'émetteur-récepteur sécurisé GNSS doit utiliser une mémoire pour enregistrer les données et pouvoir effectuer au moins 20 millions de cycles d'écriture et de lecture. Hormis cet aspect, la conception interne et la mise en œuvre de l'émetteur-récepteur sécurisé GNSS incombent aux fabricants.

Le Tableau 49 fournit la modélisation des numéros d'enregistrement et des données. Remarque: il existe quatre phrases GSA correspondant aux quatre systèmes de satellite et au SBAS (Satellite-Based Augmentation System).

TCS_399 Le Tableau 49 présente la structure de fichier. Concernant les règles d'accès (ALW, NEV, SM-MAC), cf. appendice 2, chapitre 3.5.

Tableau 49 Structure de fichier

		Conditions d'accès		
Fichier	**ID de fichier**	**Lire**	**Actualiser**	**Codé**
MF	3F00			
EF.ICC	0002	ALW	NEV (par la VU)	Non
DF GNSS Facility	0501	ALW	NEV	Non
EF EGF_MACertificate	C100	ALW	NEV	Non
EF CA_Certificate	C108	ALW	NEV	Non

		Conditions d'accès		
EF Link_Certificate	C109	ALW	NEV	Non
EF.EGF	2F2F	SM-MAC	NEV (par la VU)	Non

Fichier/Élément d'information	*Numéro de l'enregistrement*	*Taille (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				
RMC NMEA Sentence	'01'	85	85	
1st GSA NMEA Sentence	'02'	85	85	
2nd GSA NMEA Sentence	'03'	85	85	
3rd GSA NMEA Sentence	'04'	85	85	
4th GSA NMEA Sentence	'05'	85	85	
5th GSA NMEA Sentence	'06'	85	85	
Numéro de série étendu du dispositif GNSS externe défini à l'appendice 1 comme SensorGNSSSerialNumber.	'07'	8	8	
Identificateur du système d'exploitation de l'émetteur-récepteur sécurisé GNSS défini à l'appendice 1 comme SensorOSIdentifier.	'08'	2	2	
Numéro d'homologation du dispositif GNSS externe défini à l'appendice 1 comme SensorExternalGNSSApprovalNumber.	'09'	16	16	
Identificateur du composant de sécurité du dispositif GNSS externe défini à l'appendice 1 comme SensorExternalGNSSSCIdentifier	'10'	8	8	
RFU – Reserved for Future Use	De '11' à 'FD'			

4.2.2 Transfert sécurisé de données GNSS

TCS_400 Le transfert sécurisé des données de positionnement GNSS est autorisé uniquement dans les conditions suivantes:

1. La procédure d'appariement a abouti conformément aux dispositions de l'appendice 11. Mécanismes de sécurité communs.
2. L'authentification mutuelle régulière et la concordance de clés de session entre la VU et le dispositif GNSS externe également décrites à l'appendice 11. Les mécanismes de sécurité communs sont appliqués à la fréquence indiquée.

TCS_401 Toutes les T secondes, où T est une valeur inférieure ou égale à 10, sauf pendant le déroulement de l'appariement, de l'authentification mutuelle et de la concordance de clés de session, la VU demande au dispositif GNSS externe les informations de positionnement selon la séquence suivante:

1. La VU demande les données de localisation et les données relatives à l'affaiblissement de la précision (provenant de la phrase GSA NMEA) au dispositif GNSS externe. L'émetteur-récepteur sécurisé de la VU utilise les commandes SELECT et READ RECORD(S) conformément à la norme ISO/IEC 7816-4:2013 en mode authentification uniquement de la messagerie sécurisée, tel que le prévoit l'appendice 11, section 11.5, avec l'identificateur de fichier «2F2F» et le nombre de RECORD égal à «01» pour la phrase NMEA RMC et '02','03','04','05','06' pour la phrase GSA NMEA.
2. Les dernières données de localisation reçues sont mémorisées dans l'EF avec l'identificateur '2F2F' et les enregistrements décrits au Tableau 49 dans l'émetteur-récepteur sécurisé GNSS car ce dernier reçoit les données NMEA du récepteur GNSS, sur une fréquence d'au moins 1 Hz, par l'interface de données GNSS.
3. L'émetteur-récepteur sécurisé GNSS envoie la réponse à l'émetteur-récepteur sécurisé de la VU à l'aide du message de réponse UDPA en mode authentification uniquement de la messagerie sécurisée, comme le décrit l'appendice 11, section 11.5.
4. L'émetteur-récepteur sécurisé de la VU contrôle l'authenticité et l'intégrité de la réponse reçue. En cas de résultat positif, les données de localisation sont transférées au processeur de la VU par l'interface de données GNSS.
5. Le processeur de la VU vérifie les données reçues en extrayant les informations (p. ex. la latitude, la longitude ou l'heure) de la phrase RMC NMEA. Cette dernière inclut les informations si le positionnement est valide. Si tel n'est pas 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 la VU extrait également les valeurs HDOP des phrases GSA NMEA et calcule la valeur moyenne d'après les systèmes de satellites disponibles (p. ex., lorsque les points de repère sont disponibles).
6. Le processeur de la VU mémorise les informations reçues et traitées comme la latitude, la longitude, l'heure et la vitesse dans la VU, selon la structure définie à l'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.

4.2.3 Structure de la commande Read Record

La présente section décrit en détail la structure de la commande Read Record (lecture des enregistrements). La messagerie sécurisée (mode authentification uniquement) est ajoutée conformément aux dispositions de l'appendice 11 Mécanismes de sécurité communs.

TCS_402 La commande est compatible avec le mode authentification uniquement de la messagerie sécurisée; cf. appendice 11.

TCS_403 Message de commande

Octet	*Longueur*	*Valeur*	*Description*
CLA	1	'0Ch'	Messagerie sécurisée demandée.
INS	1	'B2h'	Lire l'enregistrement.
P1	1	'XXh'	Nombre d'enregistrements ('00' indique l'enregistrement en cours).
P2	1	'04h'	Lire l'enregistrement avec le nombre d'enregistrements indiqué en P1.

Octet	*Longueur*	*Valeur*	*Description*
Le	1	‘XXh’	Longueur de données prévisible. Nombre d'octets à extraire.

TCS_404 L'enregistrement référencé en P1 devient l'enregistrement en cours.

Octet	*Longueur*	*Valeur*	*Description*
#1-#X	X	‘XX..XXh’	Données extraites
SW	2	‘XXXXh’	Mots d'état (ME1, ME2)

- Si la commande aboutit, l'émetteur-récepteur sécurisé GNSS renvoie ‘**9000**’.
- Si le fichier en cours n'est pas orienté enregistrement, l'émetteur-récepteur sécurisé GNSS renvoie **'6981'**.
- Si la commande est utilisée avec P1 = '00', mais sans aucun EF en cours, l'émetteur-récepteur sécurisé GNSS renvoie **'6986'** (commande interdite).
- Si l'enregistrement est introuvable, l'émetteur-récepteur sécurisé GNSS renvoie **'6A 83'**.
- Si le dispositif GNSS externe détecte une fraude, il renvoie les mots d'état **’66 90’**.

TCS_405 L'émetteur-récepteur sécurisé GNSS est compatible avec les commandes suivantes de la deuxième génération de tachygraphes, définies à l'appendice 2:

Commande	*Référence*
Select	Appendice 2 chapitre 3.5.1
Read Binary	Appendice 2 chapitre 3.5.2
Get Challenge	Appendice 2 chapitre 3.5.4
PSO: Verify Certificate	Appendice 2 chapitre 3.5.7
External Authenticate	Appendice 2 chapitre 3.5.9
General Authenticate	Appendice 2 chapitre 3.5.10
MSE:SET	Appendice 2 chapitre 3.5.11

4.3 Appariement, authentification mutuelle et concordance de clés de session du dispositif GNSS externe avec la VU

L'appariement, l'authentification mutuelle et la concordance de clés de session du dispositif GNSS externe avec la VU sont décrits à l'appendice 11. Mécanismes de sécurité communs, chapitre 11.

4.4 Traitement des erreurs

La présente section décrit comment des conditions d'erreur potentielles du dispositif GNSS externe sont traitées et enregistrées dans la VU.

4.4.1 Erreur de communication avec le dispositif GNSS externe

TCS_406 Si la VU ne parvient pas à gérer la communication avec le dispositif GNSS externe apparié pendant plus de 20 minutes consécutives, la VU génère et enregistre dans la VU un évènement de type EventFaultType avec la valeur enum *‘53’H External GNSS communication fault* assorti d'un horodatage indiquant l'heure actuelle. L'évènement 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 circule. Dans ce contexte, une erreur de communication survient lorsque l'émetteur-récepteur sécurisé de la VU ne reçoit pas de message de réponse après un message de demande, au sens de la section 4.2.

4.4.2 Atteinte à l'intégrité physique du dispositif GNSS externe

TCS_407 En cas d'atteinte au dispositif GNSS externe, l'émetteur-récepteur sécurisé GNSS efface toute sa mémoire, y compris le matériel cryptographique. Comme le prévoient GNS_25 et GNS_26, la VU détecte les infractions si la réponse possède l'état '6690'. La VU génère ensuite un évènement de type EventFaultType enum *'55'H Tamper detection of GNSS*.

4.4.3 Absence d'informations de positionnement en provenance du récepteur GNSS

TCS_408 Si l'émetteur-récepteur sécurisé GNSS ne reçoit aucune donnée du récepteur GNSS pendant plus de trois heures successives, il génère un message de réponse à la commande READ RECORD où le nombre RECORD est égal à '01' et contenant une zone de données de 12 octets tous définis sur 0xFF. Dès réception du message de réponse avec cette valeur de zone de données, la VU génère et mémorise un évènement de type EventFaultType enum *'52'H external 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.

4.4.4 Expiration du certificat du dispositif GNSS externe

TCS_409 Si la VU détecte que le certificat EGF utilisé pour l'authentification mutuelle n'est plus valide, la VU génère et enregistre une anomalie de l'équipement d'enregistrement de type EventFaultType enum *'56'H External GNSS facility certificate expired* assorti d'un horodatage indiquant l'heure actuelle. La VU utilise encore les données de positionnement GNSS reçues.

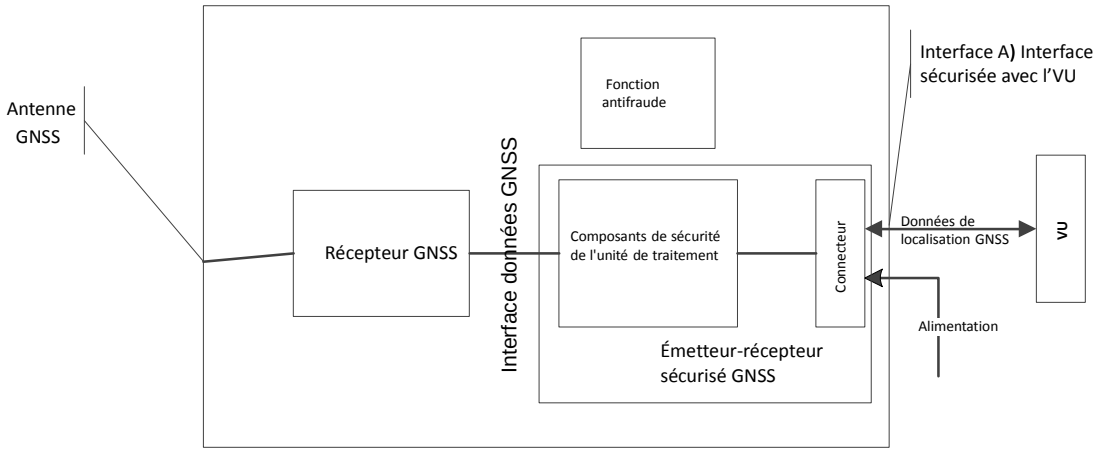


Figure 17 Schéma du dispositif GNSS externe

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 la VU tel qu'illustré à la Figure 14.

TCS_410 Le récepteur GNSS tient le rôle de l'émetteur qui transmet les phrases NMEA au processeur de la VU, 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.

TCS_411 Une antenne GNSS externe installée sur le véhicule ou une antenne GNSS interne doit être connectée à la VU.

5.2 Traitement des erreurs

5.2.1 Absence d'informations de positionnement en provenance du récepteur GNSS

TCS_412 Si la VU ne reçoit aucune donnée du récepteur GNSS pendant plus de trois heures successives, la VU génère et mémorise un évènement 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. Conflit temporel GNSS

Si la VU 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, la VU mémorise un évènement 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», la VU 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.

7. Conflit concernant le mouvement du véhicule

TCS_413 La VU déclenche et mémorise un évènement de conflit de mouvement du véhicule (cf. exigence 84 de l'annexe 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 ou le dispositif GNSS externe. Pour détecter ces conflits, on utilise la valeur médiane des écarts de vitesse entre ces sources, comme précisé ci-dessous:

- toutes les dix secondes, la valeur absolue de l'écart 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 dernières cinq minutes de mouvement servent à calculer la valeur médiane.

- la valeur médiane est calculée comme la moyenne des 80 % de valeurs restantes après élimination des plus élevées en valeur absolue.

L'évènement de conflit de mouvement du véhicule est déclenché si la valeur médiane 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: utiliser la valeur médiane des cinq dernières minutes limite le risque d'aberrations de mesure et de valeurs transitoires.) Cet évènement 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.

FR

Appendice 13 - Interface ITS

TABLE DES MATIERES

1. Introduction

Le présent appendice précise la conception et les procédures à respecter pour mettre en œuvre l'interface avec le système de transport intelligent (ITS) tel que le préconise l'article 10 du règlement (UE) n° 165/2014 (*le règlement*).

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;

(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 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 de mettre en œuvre d'autres interfaces (p. ex. au moyen d'un bus CAN) afin de transmettre les données de la VU à d'autres unités de traitement sur véhicule.

Le présent 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 présente annexe ne précise pas:

- la collecte de l'opération et de la gestion des *données* au sein de la VU (qui sera spécifiée ailleurs dans le *Règlement* 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* [Appendice 10 - Mécanismes de sécurité communs]).

- Les protocoles Bluetooth® qu'utilise l'interface ITS.

2.1. Abréviations, définitions et notations

Les abréviations et définitions qui suivent apparaissent dans le présent 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
TRTP	Paramètre de demande du transfert
TREP	Paramètre de réponse du transfert
VU	Unité embarquée sur le véhicule

3. Règlement et normes référents

La spécification définie au présent 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 appendice. En cas de conflit, les clauses du présent appendice prévalent.

Les règlements et normes mentionnés au présent 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 prérequises pour le transfert de données au moyen de l'interface ITS

La VU est responsable de l'actualisation et de la mémorisation des données dans la VU sans impliquer l'interface ITS. Les moyens pour y parvenir sont internes à la VU. Ils sont précisés ailleurs dans le règlement et pas au présent Appendice.

2.1.1 Les données fournies grâce à l'interface ITS

La VU est responsable de l'actualisation des données qui seront disponibles grâce à l'interface ITS selon une fréquence déterminée par les procédures de la VU, sans impliquer l'interface ITS. Les données de la VU sont utilisées comme base d'alimentation et d'actualisation des *données*. Les moyens pour y parvenir sont précisés ailleurs dans le *règlement*. En l'absence de précision, il s'agit d'une fonction liée à la conception du produit non spécifiée dans le présent Appendice.

2.1.2 Contenu des données

Le contenu des *données* est spécifié en Annexe 1 du présent Appendice.

2.1.3 Applications ITS

Les applications ITS utilisent les données mises à disposition par l'interface ITS, par exemple, dans le but d'optimiser la gestion des activités du conducteur tout en respectant le Règlement 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 Appendice.

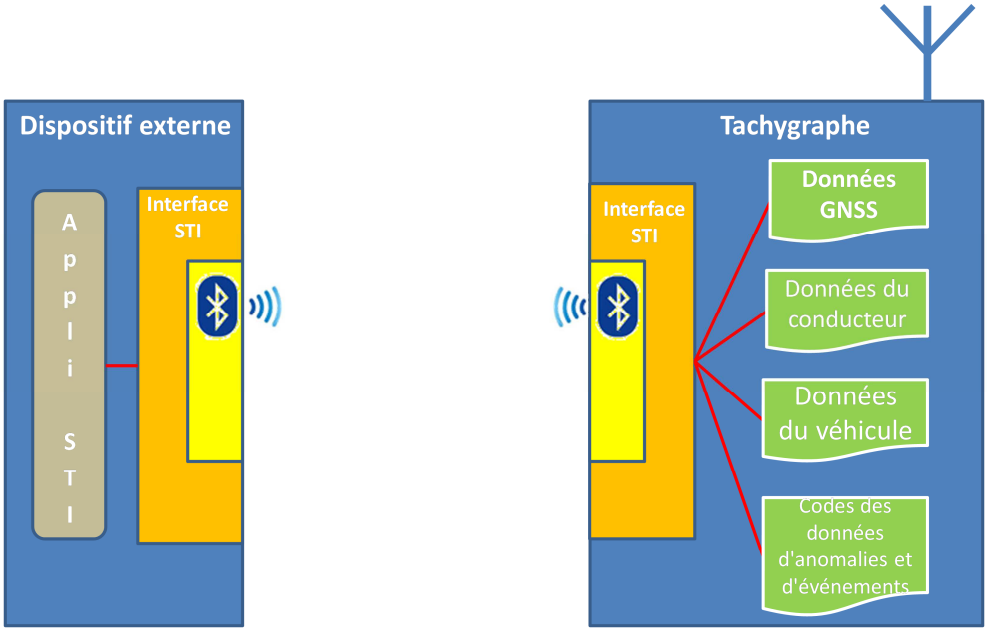
2.2 Technologie de communication

L'échange de *données* à l'aide de l'interface ITS 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 la VU 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 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 la VU à destination du dispositif externe.

2.3 Autorisation PIN

Pour des raisons de sécurité, la VU exécute un système d'autorisation de code PIN distinct du couplage Bluetooth®. Chaque VU 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 la VU, 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 la VU 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.

Nombre d'échecs successifs	*Durée du verrouillage*
3	30 secondes
6	5 minutes

Nombre d'échecs successifs	*Durée du verrouillage*
9	1 heure
12	24 heures
15	Permanents

Tableau50: Durée du verrouillage selon le nombre d'échecs successifs à renseigner le code PIN correct

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 la VU. Après dix tentatives infructueuses successives à fournir le code PUC, l'unité ITS est définitivement verrouillée et placée en liste noire.

Il arrive que le fabricant permette à titre facultatif de modifier le code PIN directement sur la VU; toutefois, le code PUC n'est pas modifiable. La modification du code PIN, le cas échéant, requiert de renseigner le code PIN directement sur la VU.

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 la VU ou par d'autres moyens). Procéder de la sorte permet de supprimer les unités ITS perdues ou volées de la liste autorisée. De même, toutes les unités ITS sortant de la portée de connexion Bluetooth® plus de vingt-quatre heures doivent être automatiquement supprimées de la liste autorisée de la VU, 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 la VU et la VU 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 ITS et l'interface de la VU 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.

2.4 Structure des messages

Tous les messages échangés entre l'unité ITS et la VU 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.

données			*Zone de données*					*Total de contrôle*
TGT	SRC	LEN	**SID**	TRTP	CC	CM	données	CS
3 octets			255 octets max.					1 octet

Tableau51: Structure générale des messages.

En-tête

TGT et SRC: ID des dispositifs cible (TGT) et source (SRC) du message. L'interface VU porte par défaut l'ID «EE». Cet ID n'est pas modifiable. L'unité ITS utilise l'ID «A0» par défaut pour son premier message de session de communication. L'interface de la VU assigne alors un ID unique à l'unité ITS 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 VU 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 ITS 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 (TRTP) 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*	*TRTP*	*CC*	*CM*	*données*	*CS*
3 octets	Longueur supérieure à 255 octets					1 octet

est transmis ainsi:

EN-TÊTE	*SID*	*TRTP*	*01*	*n*	*données*	*CS*
3 octets	255 octets					1 octet

EN-TÊTE	*SID*	*TRTP*	*02*	*n*	*données*	*CS*
3 octets	255 octets					1 octet

…

EN-TÊTE	*SID*	*TRTP*	*N*	*N*	*données*	*CS*
3 octets	255 octets max.					1 octet

Le tableau 3 présente les messages que la VU et l'unité ITS 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.

Message	En-tête			DONNÉES			Total de contrôle
	TGT	SRC	LEN	**SID**	TRTP	DONNÉES	
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	Temps	
RequestData							
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	**TREP**	Résultats	
DataUnavailable							
Chiffres non disponibles	*ITSID*	EE	02	0A	**TREP**	10	

données à caractère personnel non partagées	*ITSID*	EE	02	0A	**TREP**	11	
NegativeAnswer							
Téléchargement refusé	*ITSID*	EE	02	0B	SID Req	10	
Service incompatible	*ITSID*	EE	02	0B	SID Req	11	
Sous-fonction incompatible	*ITSID*	EE	02	0B	SID Req	12	
Longueur du message incorrecte	*ITSID*	EE	02	0B	SID Req	13	
Conditions non correctes ou erreur affectant la séquence d'interrogation	*ITSID*	EE	02	0B	SID Req	22	
Demande excessive	*ITSID*	EE	02	0B	SID Req	31	
Réponse en suspens	*ITSID*	EE	02	0B	SID Req	78	
Décalage ITSID	*ITSID*	EE	02	0B	SID Req	FC	
ITSID introuvable	*ITSID*	EE	02	0B	SID Req	FB	

Tableau52: Contenu détaillé des messages.

RequestPIN (SID 01)

Ce message est émis par l'interface de la VU si une unité ITS ni verrouillée ni autorisée lui adresse une demande de données.

SendITSID (SID 02)

Ce message est émis par l'interface de la VU 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 ITS pour que la VU 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 la VU pour informer l'unité du ITS 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 ITS pour que la VU 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 la VU pour informer l'unité du ITS 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 la VU en réponse à tout message émis par une unité ITS verrouillée hormis «SendPUC». Ce message comporte la durée restante de verrouillage de l'unité ITS, selon la structure séquentielle «chronologique» définie à l'annexe 3.

RequestData (SID 08)

Ce message d'accès aux données est émis par l'unité ITS. Un paramètre de demande de transfert (TRTP) d'un octet indique de quelle catégorie de données il s'agit. Il existe plusieurs catégories de données:

- standardTachData (TRTP 01): données disponibles en provenance du tachygraphe classées non personnelles.
- personalTachData (TRTP 02): données disponibles en provenance du tachygraphe classées personnelles.
- gnssData (TRTP 03): données du dispositif GNSS, toujours personnelles.
- standardEventData (TRTP 04): données relatives aux événements mémorisés classées non personnelles.
- personalEventData (TRTP 05): données relatives aux événements mémorisés classées personnelles.
- standardFaultData (TRTP 06): anomalies mémorisées classées non personnelles.
- manufacturerData (TRTP 07): données mises à disposition par le fabricant.

Cf. Annexe 3 du présent Appendice pour toute information complémentaire relative à chaque catégorie de données.

Cf. l'appendice 12 pour tout complément d'information à propos de la structure et du contenu des données du dispositif GNSS.

Cf. les annexes 1B et 1C pour tout complément d'information à propos du code et des anomalies relatifs aux données liées aux évènements.

ResquestAccepted (SID 09)

Ce message est émis par l'interface de la VU si un message «RequestData» émanant d'une unité ITS a été accepté. Ce message comporte un octet TREP, qui correspond à l'octet TRTP du message RequestData associé et toutes les données de la catégorie demandée.

DataUnavailable (SID 0A)

Ce message est émis par l'interface de la VU si, pour une raison quelconque, il est impossible d'envoyer les données demandées à une unité ITS autorisée. Ce message comporte un octet TREP, qui correspond au TRTP 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 la VU ne parvient pas à accéder aux données de la VU pour des raisons non précisées.
- Données à caractère personnel non partagées (11): L'unité ITS tente d'extraire des données à caractère personnel non partagées.

NegativeAnswer (SID 0B)

Ces messages sont émis par l'interface de la VU 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, ITSID...), sans s'y limiter. Le TRTP 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 TRTP 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 la VU 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.

2.5 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 ITS facultative. (cf. Annexe 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 ITS. 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.

2.6 Retrait de données standard

La figure 3 de l'annexe 2 représente le schéma de la séquence d'une demande valable adressée par l'unité ITS pour accéder aux données standard. L'unité ITS 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 standard:

- standardTachData (TRTP 01)
- standardEventData (TRTP 04)
- standardFaultData (TRTP 06)

2.7 Récupération de données à caractère personnel

La Figure 4 de l'annexe 2 représente le schéma séquentiel du traitement d'une demande de données à caractère personnel. Comme précédemment expliqué, l'interface de la VU adresse des données à caractère personnel uniquement si le conducteur a donné son accord explicite (cf. 4.5). Dans le cas contraire, la demande doit être automatiquement rejetée.

Parmi les données disponibles, les données suivantes sont considérées comme personnelles:

- personalTachData (TRTP 02)
- gnssData (TRTP 03)
- personalEventData (TRTP 05)
- manufacturerData (TRTP 07)

2.8 Récupération de données associées aux évènements et aux anomalies

Les unités ITS sont en mesure de demander des données associées aux évènements comportant la liste de tous les évènements imprévus. Ces données sont considérées comme étant des données standard ou personnelles, cf. annexe 3. Le contenu de chaque évènement varie selon la documentation fournie en annexe 1 du présent Appendice.

ANNEXE 1

LISTE DES données DISPONIBLES GRÂCE À L'interface ITS

Data	Source	Recommended classification
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
Driver1CumulatedDrivingTimePreviousAndCurrent Week	Driver Card	personal
Driver2CumulatedDrivingTimePreviousAndCurrent Week	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
Driver1NumberOfTimes9hDailyDrivingTimesExceed ed	Driver Card	personal
Driver2NumberOfTimes9hDailyDrivingTimesExceec ed	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
GNSS position	Vehicle Unit	personal

2°) DONNÉES ÉMANANT DU DISPOSITIF GNSS CONTINU APRÈ S ACCORD DU CONDUCTEUR

Cf. Appendice 12: GNSS

3°) CODES LIÉS AUX ÉVÈNEMENTS DISPONIBLES SANS L'AC CORD DU CONDUCTEUR

Événement	*Règles de stockage*	*données à enregistrer pour chaque événement*
Insertion d'une carte non valable	- les 10 événements les plus récents	- la date et l'heure de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de la carte à l'origine de l'événement, - le nombre d'événements semblables survenus le même jour.
Conflit de carte	- les 10 événements les plus récents	- la date et l'heure du début de l'événement, - la date et l'heure de la fin de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de chacune des deux cartes à l'origine du conflit.
Clôture incorrecte de la dernière session	- les 10 événements les plus récents	- la date et l'heure de l'insertion, - le type et le numéro de la ou des cartes, l'État membre de délivrance et la génération, - les données relatives à la dernière session telles qu'elles figurent sur la carte: - la date et l'heure de l'insertion, - le numéro d'immatriculation, l'État membre d'immatriculation et la génération de la VU.

Événement	*Règles de stockage*	*données à enregistrer pour chaque événement*
Interruption de l'alimentation électrique (2)	- l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence, - les 5 événements les plus longs enregistrés au cours des 365 derniers jours.	- la date et l'heure du début de l'événement, - la date et l'heure de la fin de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, - le nombre d'événements semblables survenus le même jour.
Erreur de communication avec l'équipement de communication à distance	- l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence, - les 5 événements les plus longs enregistrés au cours des 365 derniers jours.	- la date et l'heure du début de l'événement, - la date et l'heure de la fin de l'événement, - le type et le numéro de la ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, - le nombre d'événements semblables survenus le même jour.
Absence d'informations de position en provenance du récepteur GNSS	- l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence, - les 5 événements les plus longs enregistrés au cours des 365 derniers jours.	- la date et l'heure du début de l'événement, - la date et l'heure de la fin de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, - le nombre d'événements semblables survenus le même jour.
Erreur au niveau des données de mouvement	- l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence, - les 5 événements les plus longs enregistrés au cours des 365 derniers jours.	- la date et l'heure du début de l'événement, - la date et l'heure de la fin de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, - le nombre d'événements semblables survenus le même jour.

Événement	*Règles de stockage*	*données à enregistrer pour chaque événement*
Conflit concernant le mouvement du véhicule	- l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence, - les 5 événements les plus longs enregistrés au cours des 365 derniers jours.	- la date et l'heure du début de l'événement, - la date et l'heure de la fin de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, - le nombre d'événements semblables survenus le même jour.
Tentative d'atteinte à la sécurité	- les 10 événements les plus récents pour chaque type d'événements.	- la date et l'heure du début de l'événement, - la date et l'heure de la fin de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, - le type d'événement.
Conflit temporel	- l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence, - les 5 événements les plus longs enregistrés au cours des 365 derniers jours.	- la date et l'heure de l'appareil de contrôle, - la date et l'heure du GNSS, - le type et le numéro de la ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, - le nombre d'événements semblables survenus le même jour.

4) CODES LIÉS AUX ÉVÈNEMENTS DISPONIBLES SANS L'AC CORD DU CONDUCTEUR

Événement	*Règles de stockage*	*données à enregistrer pour chaque événement*
Conduite sans carte appropriée	- l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence, - les 5 événements les plus longs enregistrés au cours des 365 derniers jours.	- la date et l'heure du début de l'événement, - la date et l'heure de la fin de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'événement, - le nombre d'événements semblables survenus le même jour.
Insertion d'une carte en cours de route	- le dernier événement pour chacun des 10 derniers jours d'occurrence,	- la date et l'heure de l'événement, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération, - le nombre d'événements semblables survenus le même jour.
Excès de vitesse (1)	- l'événement le plus grave (c.-à.-d. celui présentant la vitesse moyenne la plus élevée) des 10 derniers jours d'occurrence, - les 5 événements les plus graves au cours des 365 derniers jours. - le premier événement survenu après le dernier étalonnage,	- la date et l'heure du début de l'événement, - la date et l'heure de la fin de l'événement, - la vitesse maximale mesurée au cours de l'événement, - la vitesse moyenne arithmétique mesurée au cours de l'événement, - le type et le numéro de carte, l'État membre de délivrance et la génération de la carte de conducteur (le cas échéant), - le nombre d'événements semblables survenus le même jour.

5) CODES LIÉS AUX données RELATIVES AUX ANOMALIES DISPONIBLES SANS L'ACCORD DU CONDUCTEUR

Faute	*Règles de stockage*	*données à enregistrer pour chaque anomalie*
Anomalie de la carte	- les dix dernières anomalies de la carte de conducteur.	- la date et l'heure du début de l'anomalie, - la date et l'heure de la fin de l'anomalie, - le type et le numéro de la carte ou des cartes, l'État membre de délivrance et la génération.
Anomalies de l'appareil de contrôle	- les 10 anomalies les plus récentes pour chaque type d'anomalie, - la première anomalie après le dernier étalonnage,	- la date et l'heure du début de l'anomalie, - la date et l'heure de la fin de l'anomalie, - la type de l'anomalie, - le type et le numéro de la ou des cartes, l'État membre de délivrance et la génération de toute carte insérée au début et/ou à la fin de l'anomalie.

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

- Défaillance interne de la VU
- anomalie de l'imprimante,
- anomalie de l'affichage,
- anomalie de téléchargement,
- anomalie du capteur,
- anomalie du récepteur GNSS ou du dispositif GNSS externe,
- anomalie de l'équipement de communication à distance.

6) ÉVÈNEMENTS ET ANOMALIES PARTICULIERS SE RAPPORT ANT AU FABRICANT SANS ACCORD 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 SÉQUENTIELS DES ÉCHANGES DE MESSAGES AVEC L'unité ITS.

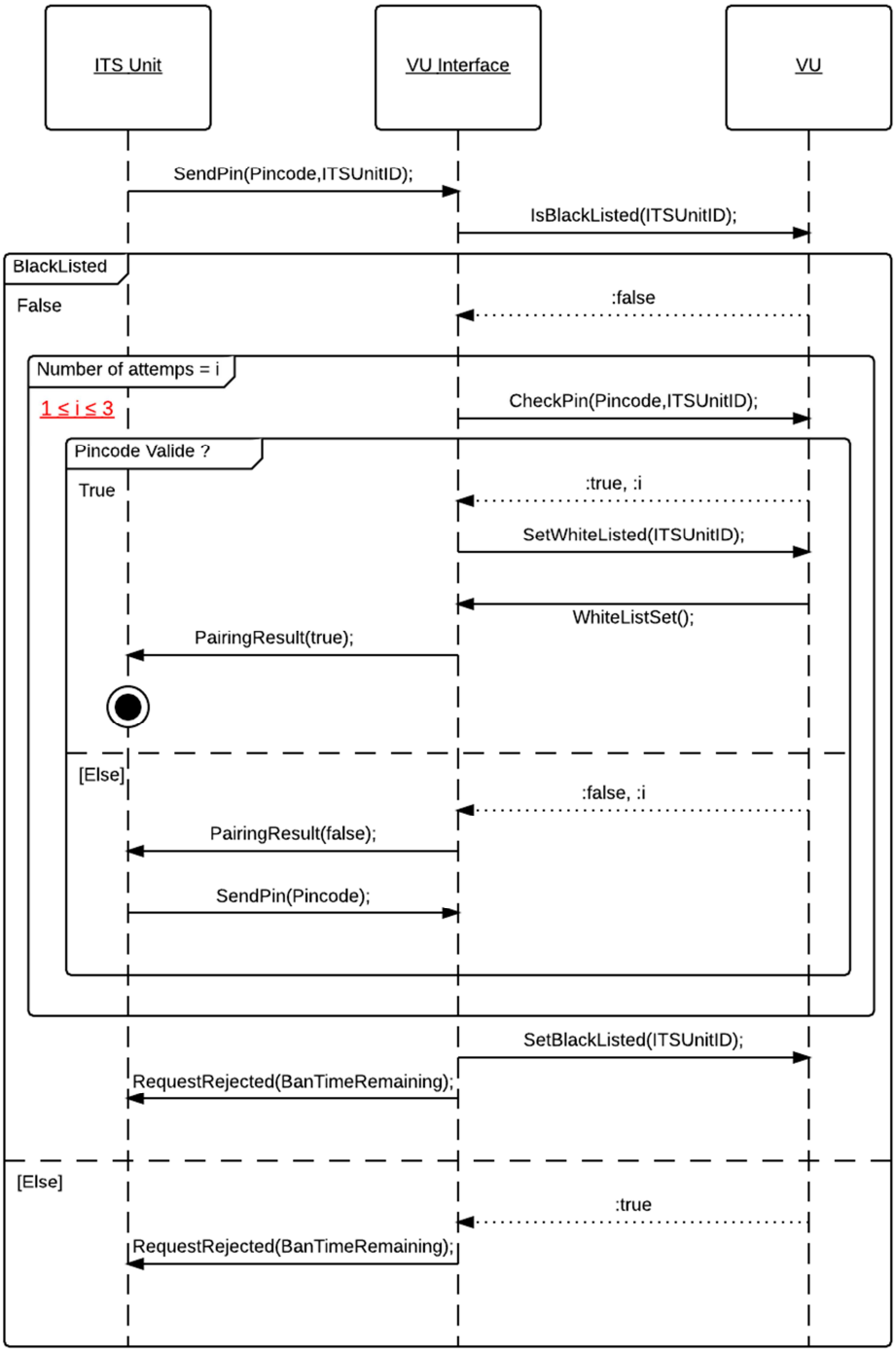


Figure 18. Schéma séquentiel de la tentative de validation du PIN

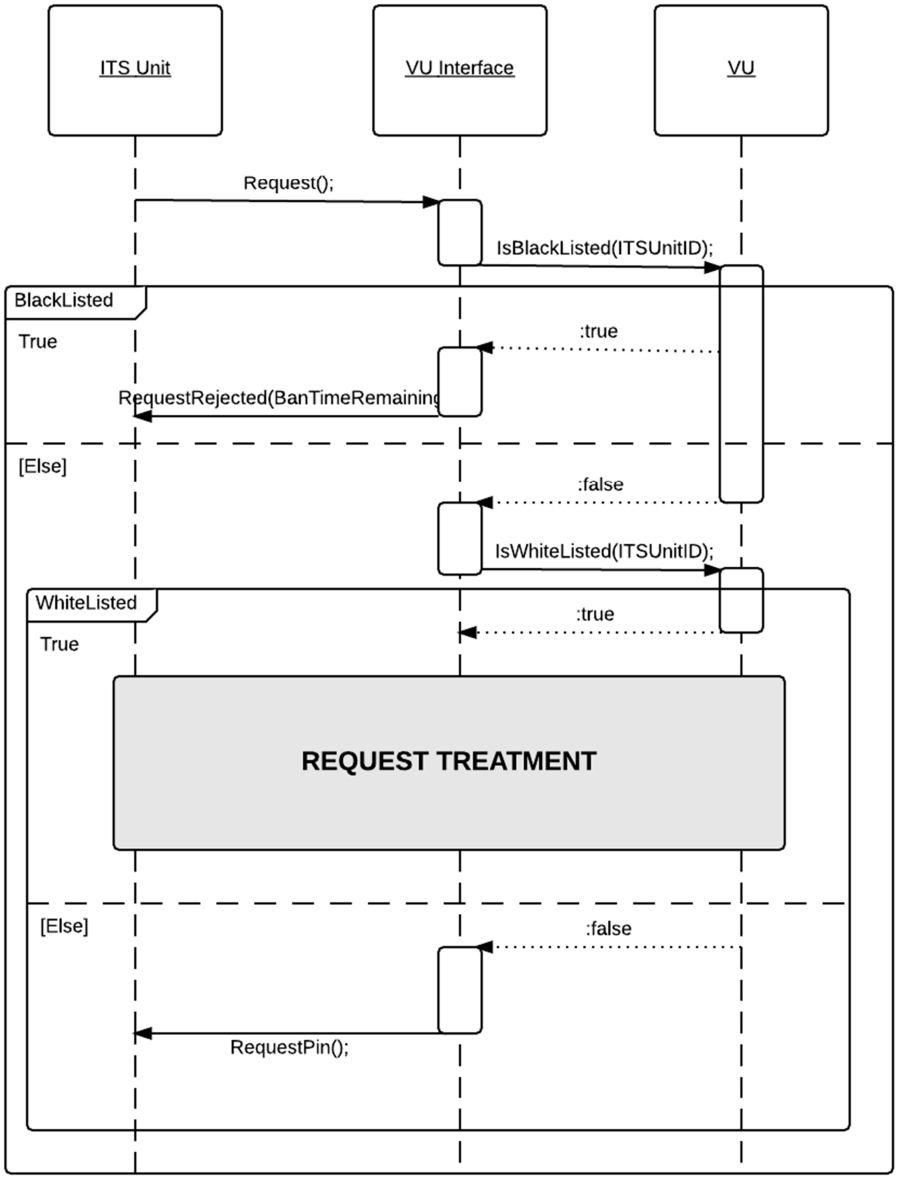


Figure 19. Schéma séquentiel de la vérification d'autorisation par l'unité ITS

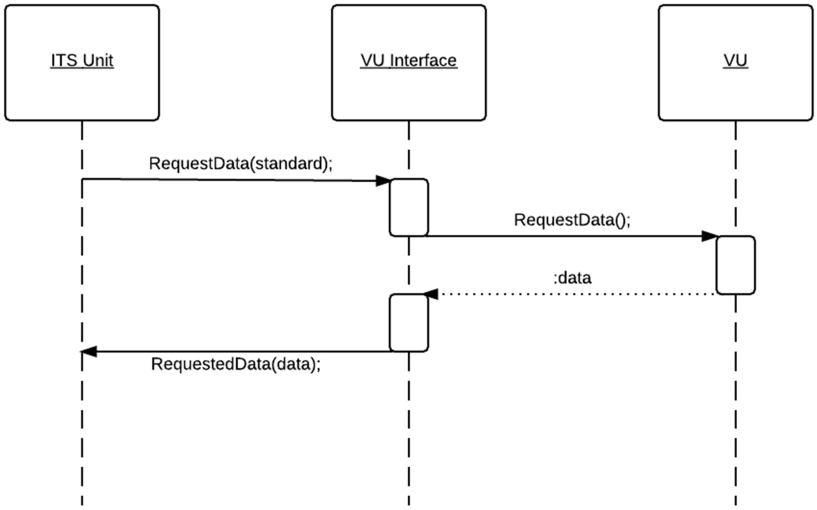


Figure 20. Schéma séquentiel du traitement d'une demande de données non personnelles (après accès PIN correct)

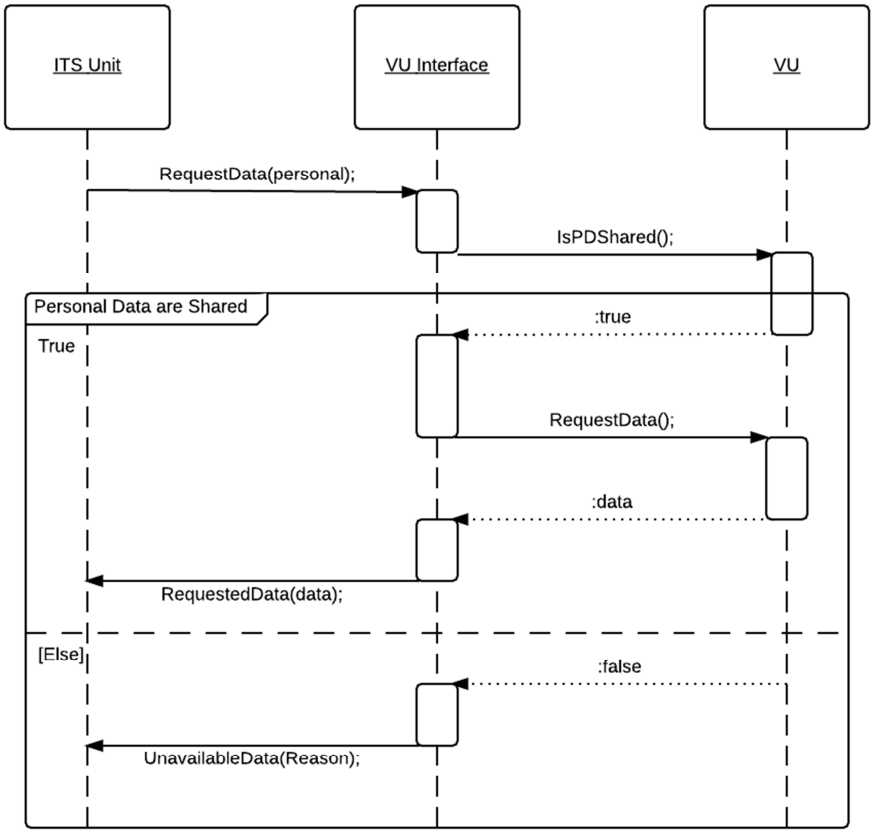


Figure 21. Schéma séquentiel du traitement d'une demande de données à caractère personnel (après accès PIN correct)

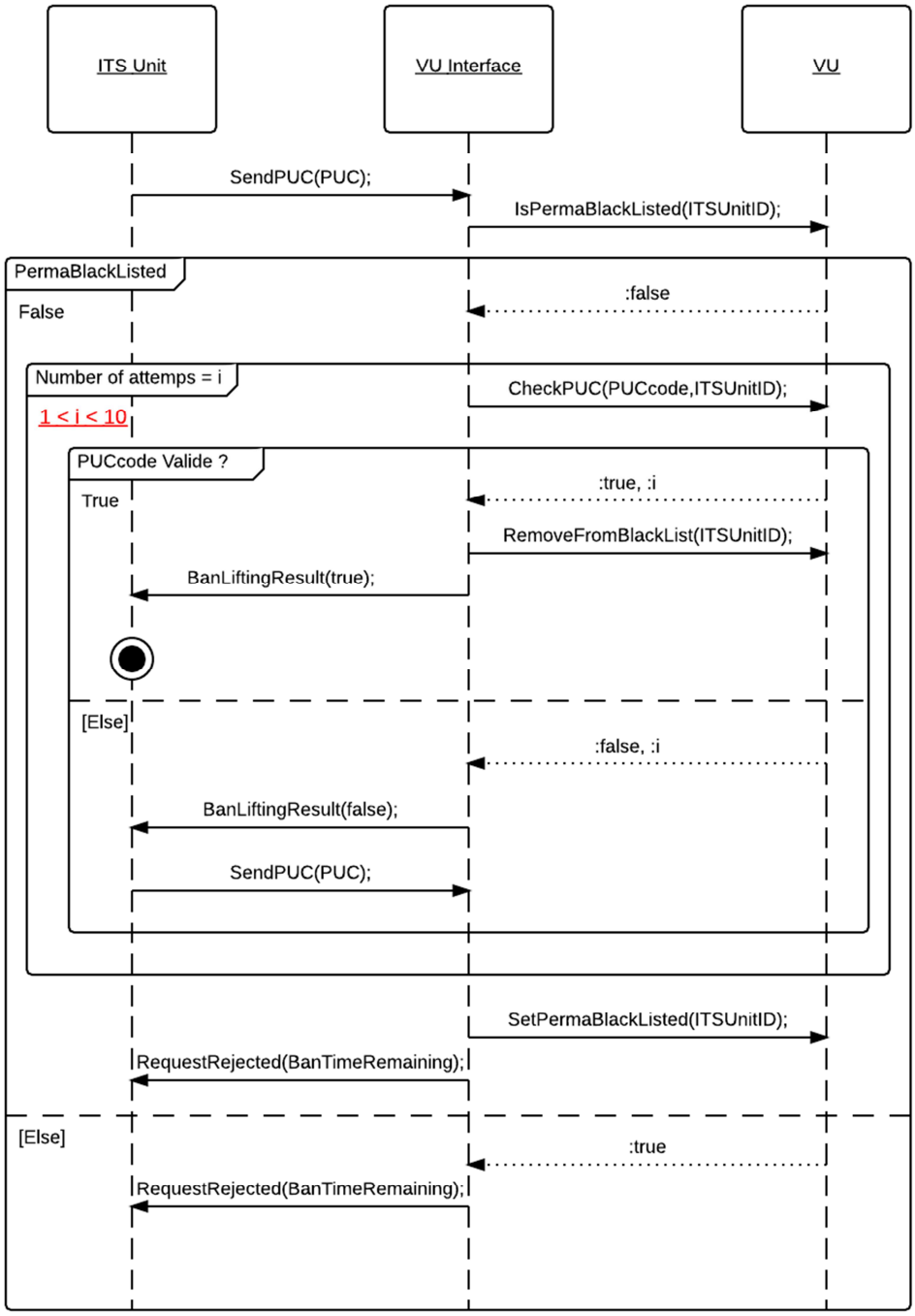


Figure 22. Schéma séquentiel de la tentative de validation du PUC

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,
          trtp 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/IEC 8859--
          surname UTF8String,
          codePageFirstname UTF8String, --See ISO/IEC 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 {
          --See Appendix 12 of this directive for more info about GNSS data format.--
     }

     StandardEventDataSheet ::= SEQUENCE{
```

```
          events SEQUENCE OF StandardEvent
     }

     PersonalEventDataSheet ::= SEQUENCE{
          events SEQUENCE OF PersonalEvent
     }
END

EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
     EXPORTS ALL;
     IMPORTS NationAlpha FROM Appendix1; --See Appendix 1 for more information about
NationAlpha--

          SecurityBreachEvent ::=SEQUENCE{
               --See Annex 1B for more information--
               }

          RecordingEquipmentFaultType ::= SEQUENCE{
               --See Annex 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 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
```

FR

APPENDICE 14. FONCTION DE COMMUNICATION À DISTANCE

TABLE DES MATIÈRES

1 Introduction

Le présent appendice spécifie la conception et les procédures à respecter pour mettre en œuvre la fonction de communication à distance (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 le tachygraphe est équipé d'une fonctionnalité de communication à distance qui permet aux autorités chargées du contrôle compétentes de lire les informations du tachygraphe embarqué sur les véhicules en circulation à l'aide d'un équipement d'interrogation à distance (lecteur de communication à distance à des fins de détection précoce, REDCR). Il s'agit notamment d'un équipement 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 fonctionnalité sert uniquement de préfiltre pour sélectionner les véhicules qui feront l'objet d'un contrôle plus approfondi. Cette fonctionnalité 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 à l'aide de *la communication* qui désigne un appareil sans fil utilisant la bande de fréquences de 5,8 GHz pour communiquer à distance, conforme à cet appendice, et validé en fonction des 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 à l'aide de l'équipement de communication uniquement lorsque l'équipement de l'autorité de contrôle compétent en fait la demande, à l'aide des moyens de radiocommunication compatibles (*lecteur de communication de détection précoce à distance, REDCR*).

DSC_4 *Les données* sont protégées pour assurer 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 fonctionnement satisfaisant 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* résultent de la sécurisation des *données* dans l'unité embarquée sur le véhicule (VU) combinée à l'utilisation exclusive du support de communication à distance sans fil DSRC sur la bande 5,8 GHz pour transférer les données utiles sécurisées et les données relatives à la sécurité (cf. 5.4.4). Cela implique 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. Cf. appendice 11 – Mécanismes communs de sécurité.

DSC_8 *Les données* contiennent un timbre horodateur indiquant l'heure de leur dernière mise à jour.

DSC_9 Le contenu des données relatives à la sécurité est uniquement connu des autorités de contrôle compétentes qui le régissent et des parties avec lesquelles elles partagent ces informations et ne relève pas des

dispositions de la *communication*, faisant l'objet du présent appendice, hormis en ce que la *communication* prévoit le transfert d'un paquet de données relatives à la sécurité avec chaque paquet de données utiles.

DSC_10 La même architecture et le même équipement servent à extraire d'autres concepts de données (comme le poids à bord) en adoptant l'architecture spécifiée aux présentes.

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 appendice vise à préciser la manière dont les agents des autorités de contrôle compétentes utilisent une communication sans fil DSRC spécifiée sur la bande des 5,8 GHz pour obtenir à distance des données (*les données*) provenant d'un véhicule ciblé, ces données devant servir à déterminer si ce véhicule est éventuellement en infraction avec le règlement (UE) n° 165/2014 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 identifient une infraction éventuelle ou qui s'y apportent, conformément à l'article 9 du règlement (UE) n° 165/2014.

Ce cas de figure prévoit une durée de communication 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 assurant le contrôle à distance des tachygraphes (RTM) pour d'autres applications, comme le poids maximal et les 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 appendice spécifie:

— L'équipement, les procédures et les protocoles de communication à utiliser pour *la communication.*
— Les normes et règlements que l'équipement radio doit respecter.
— 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 potentielle *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* (REDCR) peut demander plusieurs concepts de données relatifs au fret et à la flotte.

Pour plus de précision, le présent appendice ne spécifie pas:

— La collecte et la gestion des *données* dans la VU (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). Par souci de précision: *la communication* se limite à mettre *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 cryptage) concernant le contenu *des données* (spécifiées à l'appendice 11 Mécanismes communs de sécurité).

— Le détail de tous les concepts de données autres que RTM pouvant être obtenus à l'aide de la même architecture et du même équipement.

— Les détails du comportement et de la gestion entre la VU et la DSRC-VU ou le comportement au sein de la DSRC-VU (autre que dans le but de fournir les *données* en réponse à la demande d'un REDCR).

3 Abréviations, définitions et notations

Dans le présent appendice, sont utilisées les abréviations et définitions suivantes:

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, qu'amplifie un récepteur.
Communication	Échange d'informations et de données entre un DSRC-REDCR et une DSRC-VU conformément à la section 5 et selon une relation maître-esclave en vue d'obtenir les données.
Données	Données sécurisées adoptant une structure définie (cf. 5.4.4) demandées par le *DSRC-REDCR* et fournies par la *DSRC-VU* à l'aide d'une liaison DSRC sur la bande de 5,8 GHz, comme défini au point 5 ci-après.
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	Table de service de balise (Beacon Service Table)
CIWD	Insertion d'une carte en cours de conduite
CRC	Contrôle de redondance cyclique
DSC (n)	Identificateur d'une exigence pour un appendice DSRC donné
DSRC	communication spécialisée à courte portée
DSRC-REDCR	Lecteur de communication à distance à des fins de détection précoce DSRC
DSRC-VU	Unité embarquée sur le véhicule DSRC Il s'agit du «dispositif de détection précoce à distance» défini à l'annexe 1C.
DWVC	Conduite sans carte en cours de validité
EID	Identificateur d'élément
LLC	Contrôle de liaison logique
LPDU	Unité de données de protocole LLC
OWS	Système de pesage embarqué
PDU	Unité de données de protocole
REDCR	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 1C.
RTM	Contrôle à distance du tachygraphe
SM-REDCR	Lecteur de communication à distance à des fins de détection précoce, module de sécurité
TARV	Applications télématiques collaboratives pour véhicules de fret commercial réglementé (série de normes ISO 15638)
VU	Unité embarquée sur le véhicule
VUPM	Mémoire utile de la VU
VUSM	Module de sécurité de la VU
VST	Table de service de véhicule
WIM	Poids en mouvement
WOB	Poids à bord

La spécification définie au présent appendice renvoie aux règlements et normes suivants, et dépend d'eux en tout ou en partie. Les normes ou leurs clauses applicables figurent dans le présent appendice. En cas de conflit, les dispositions du présent appendice prévalent. En cas de conflit qu'aucune spécification du présent appendice ne résout, le fonctionnement conformément à la recommandation ERC 70-03 (et testé selon les paramètres pertinents de la norme EN 300 674-1) prévaut, suivi, dans l'ordre, par les normes EN 12795, EN 12253, EN 12834 et EN 13372, 6.2, 6.3, 6.4 et 7.1.

Les règlements et normes mentionnés au présent appendice sont les suivants:

[1] 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.

[2] 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).

[3] ERC 70-03 CEPT: Recommandation CCE 70-03 relative à l'utilisation des dispositifs à courte portée (DCP).

[4] Norme ISO 15638 Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV).

[5] 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).

[6] Norme EN 12253 Road transport and traffic telematics - Dedicated short-range communication - Physical layer using microwave at 5.8 GHz..

[7] Norme EN 12795 Road transport and traffic telematics - Dedicated short-range communication - Data link layer: medium access and logical link control.

[8] Norme EN 12834 Road transport and traffic telematics - Dedicated short-range communication - Application layer.

[9] Norme EN 13372 Road transport and traffic telematics - Dedicated short-range communication - Profiles for RTTT applications

[10] Norme ISO 14906 Electronic fee collection — Application interface definition for dedicated short-range communication

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 scénarios pris en charge sont les suivants:

«Profil de communication 1: contrôle routier utilisant un lecteur de communication à distance à des fins de détection précoce, sans fil et à courte portée afin de procéder à des contrôles routiers physiques (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 prérequises pour le transfert de données au moyen de l'interface DSRC 5,8 GHz

NOTE: pour comprendre le contexte des conditions prérequises, le lecteur se référera à la figure 14.3 ci-dessous.

4.1.1.1 Données détenues par la VU

DSC_12 La VU est responsable de l'actualisation et de la mémorisation des données qu'elle stocke selon une fréquence de 60 secondes sans impliquer la fonction de communication DSRC. Les moyens pour y parvenir sont internes à la VU, spécifiés par le règlement (UE) n° 165/2014, annexe 1 C, section 3.19 *«communication à distance pour les contrôles routiers ciblés»* et ne sont pas spécifiés au présent appendice.

4.1.1.2 Données communiquées au dispositif DSRC-VU

DSC_13 La VU est responsable de l'actualisation des données tachygraphiques DSRC (*les données*) dès lors qu'elle actualise les données qu'elle stocke selon une fréquence définie à la section 4.1.1.1 (DSC_12), sans impliquer la fonction de communication DSRC.

DSC_14 Les données de la VU sont utilisées comme base d'alimentation et d'actualisation des *données*. Les moyens pour y parvenir sont précisés dans l'annexe 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 appendice. En ce qui concerne la conception de la connexion entre le dispositif DSRC-VU et la VU, 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 décryptés, ils sont structurés et mis à disposition selon la forme et la structure spécifiées à la section 5.4.4 du présent appendice (Structures de 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, sont sécurisées avant d'être présentées à la *VU-DSRC*, sont présentées comme une valeur de concept de données sécurisées et enfin stockées temporairement dans la *VU-DSRC* en tant que version actuelle des *données*. Ces données sont transférées du *VUSM* à la fonction DSRC *VUPM*. Le *VUSM* et la *VUPM* désignent des fonctions, pas nécessairement des entités physiques. La forme des instanciations physiques exécutant ces fonctions est affaire de conception de produit, sauf indication dans une autre partie du règlement UE n° 165/2014.

4.1.1.5 Données de sécurité

DSC 17 Les données de sécurité (*securityData*), comprenant les données requises par le *REDCR* pour décrypter les *données*, sont communiquées conformément à l'appendice 11 Mécanismes communs de sécurité et sont présentées comme une valeur de concept de données en vue de leur stockage temporaire dans la *DSRC-VU* comme étant la version actuelle des *securityData*, selon la structure définie par le présent appendice, section 5.4.4.

4.1.1.6 Données VUPM disponibles pour le transfert à l'aide de l'interface DSRC

DSC 18 Le concept de données qui doit toujours être disponible dans la fonction DSRC VUPM en vue de son transfert immédiat sur demande du *REDCR* est défini à la section 5.4.4, qui contient les spécifications complètes du module ASN.1.

Récapitulatif 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 selon les paramètres pertinents de la norme EN 300 674-1 comme décrit à la section 5) (le *REDCR*) pour identifier 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 qui est 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 *REDCR* 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 utilise les interfaces DSRC 5,8 GHz fonctionnant conformément à la recommandation ERC 70-03 et testées selon les paramètres pertinents de la norme EN 300 674-1, décrite à la section 5. Cf. figure 14.1 (cas de figure n° 1).

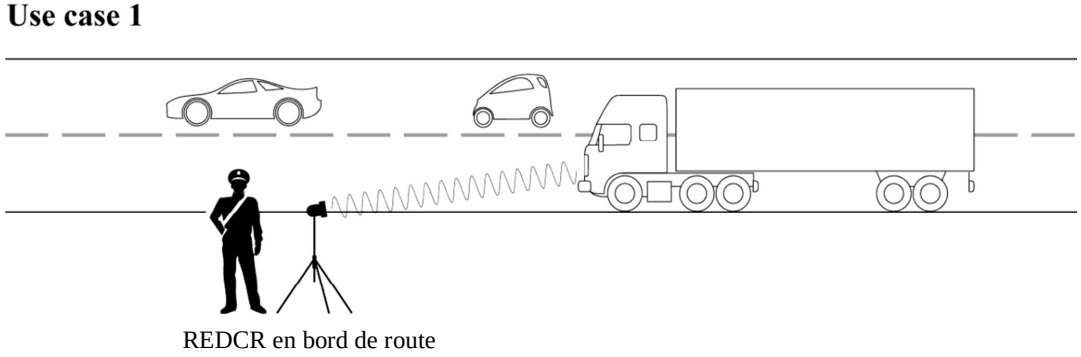


Figure 14.1 — Interrogation en bord de route avec DSRC 5,8 GHz

4.1.3 Profil 1b: à l'aide d'un lecteur de communication à distance à des fins de détection précoce (REDCR) qui est installé et dirigé dans un véhicule

Dans ce cas, l'agent des autorités de contrôle compétentes se trouve dans un véhicule en circulation et soit il utilise un *REDCR* manuel et portable depuis le véhicule en le pointant vers le centre du pare-brise du véhicule ciblé, soit le *REDCR* 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 REDCR est dans une position particulière par rapport au véhicule ciblé (par exemple directement en amont dans un flux de circulation). L'interrogation utilise les interfaces DSRC 5,8 GHz fonctionnant conformément à la recommandation ERC

70-03 et testées selon les paramètres pertinents de la norme EN 300 674-1, décrite à la section 5. Cf. figure 14.2. (Cas de figure n° 2).

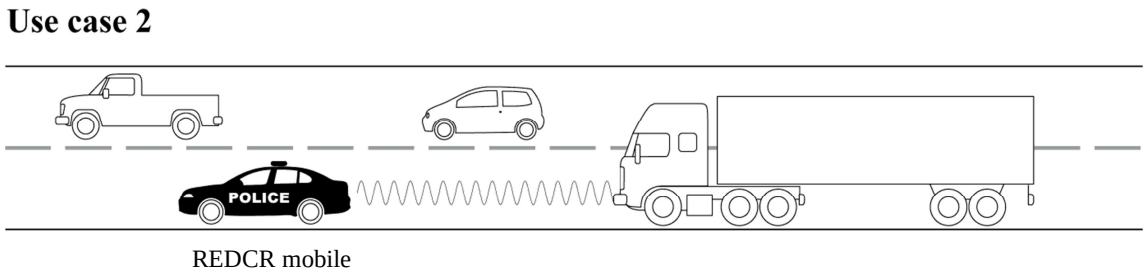


Figure 14.2 — Interrogation depuis un véhicule avec DSRC 5,8 GHz

4.2 Sécurité/Intégrité

Afin de permettre la vérification de l'authenticité et de l'intégrité des données téléchargées à l'aide de la communication à distance, ces *données* sécurisées font l'objet d'une vérification et d'un décryptage conformément à l'appendice 11 Mécanismes communs de sécurité.

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.

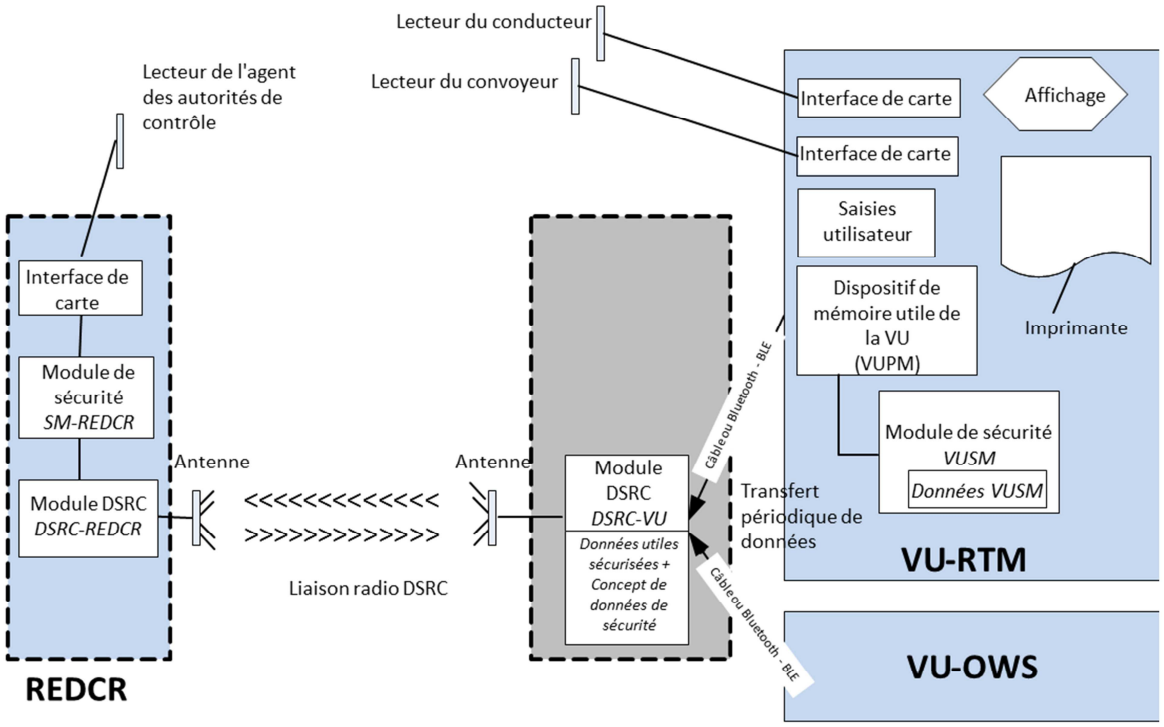


Figure 14.3 — Conception de la fonction de communication à distance

DSC_19 Les fonctions suivantes sont situées dans la VU:

- Module de sécurité (*VUSM*). Cette fonction présente dans la VU est responsable de la sécurisation des *données* à transmettre depuis la *DSRC-VU* à l'agent des autorités de contrôle compétentes par communication à distance.
- Les données sécurisées sont enregistrées dans la mémoire VUSM. La section 4.1.1.1 (DSC_12) prévoit la fréquence à laquelle la VU crypte et renouvelle le concept RTMdata (qui inclut les valeurs de concept des données utiles et des données de sécurité déterminées ci-après au présent appendice) détenu dans la mémoire de la DSRC-VU. L'exploitation du module de sécurité est définie à l'appendice 11 Mécanismes communs de sécurité et est exclue de la portée du présent appendice, hormis le fait que toute modification des données du VUSM doit entraîner la mise à jour du dispositif de communication de la VU.
- La communication entre la VU et la DSRC-VU peut être filaire ou de type Bluetooth Low Energy (BLE). La DSRC-VU peut soit être intégrée physiquement sur le pare-brise du véhicule avec l'antenne, soit être interne à la VU, soit être située à tout point intermédiaire.
- La DSRC-VU dispose d'une source d'alimentation électrique fiable à tout moment. Les moyens d'alimentation relèvent de la décision conceptuelle.
- La mémoire de la DSRC-VU est non volatile, afin de préserver les données dans la DSRC-VU y compris lorsque le contact du véhicule est coupé.
- Si la communication entre la VU et la DSRC-VU s'établit par BLE et que l'alimentation provient d'une batterie non rechargeable, l'alimentation de la DSRC-VU doit être remplacée lors de chaque inspection périodique. En outre, il incombe au fabricant de la DSRC-VU de vérifier que l'alimentation électrique perdure

d'une inspection périodique à l'autre. Il doit maintenir l'accès normal aux données au moyen d'un REDCR durant toute la période sans anomalie ni interruption.

- Dispositif de «mémoire utile» RTM VU (*VUPM*). Il incombe à cette fonction présente dans la VU de fournir et d'actualiser *les données.* Le contenu des *données* («TachographPayload») est défini aux sections 5.4.4/5.4.5 ci-après et mis à jour selon la fréquence précisée à la section 4.1.1.1 (DSC_12).
- DSRC-VU. Il s'agit de la fonction intégrée à l'antenne ou connectée à celle-ci, qui communique avec la VU grâce à une connexion filaire ou sans fil (BLE), qui détient les données actuelles (*données VUPM*) et gère la réponse à une interrogation par 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.
- Le module de sécurité (REDCR) (*SM-REDCR*) désigne la fonction servant à décrypter et à vérifier l'intégrité des données provenant de la VU. Les moyens pour y parvenir sont déterminés à l'appendice 11 Mécanismes communs de sécurité. Ils ne sont pas précisés au présent appendice.

- La fonction du dispositif DSRC (REDCR) (*DSRC-REDCR*) inclut un émetteur-récepteur de 5,8 GHz ainsi que le progiciel et le logiciel associés qui gèrent *la communication* avec la *DSRC-VU* conformément au présent appendice.
- Le *DSRC-REDCR* interroge la *DSRC-VU* du véhicule ciblé et obtient *les données* (les *données VUPM* actuelles du véhicule ciblé) grâce à la liaison et aux procédures DSRC et enregistre les données reçues dans son *SM-REDCR.*
- L'antenne DSRC-VU est placée de manière à optimiser la communication DSRC entre le véhicule et l'antenne en bord de route (en général, au centre ou à proximité du centre du pare-brise du véhicule). Pour les véhicules légers, une installation sur la partie supérieure du pare-brise convient.
    - Aucun objet métallique (ex.: porte-badge, autocollant, bande (teintée) anti-reflets, pare-soleil, essuie-glace au repos) ne doit se trouver à proximité ou devant l'antenne, car ils pourraient interférer avec la communication.
    - L'antenne est installée de sorte que son axe de visée est 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 selon les paramètres pertinents de la norme EN 300 674-1, comme décrit à la section 5. L'antenne et la communication peuvent mettre en œuvre des techniques d'atténuation contre le risque d'interférence sans fil comme décrit au rapport ECC 228, en utilisant notamment des filtres dans la communication CEN DSRC 5,8 GHz.

DSC_21 L'antenne DSRC est connectée à la DSRC-VU soit directement au sein du module installé sur ou à proximité du pare-brise, soit à l'aide d'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. Le masquage délibéré ou tout autre agissement qui nuit à la performance opérationnelle de l'antenne constitue une infraction au règlement (UE) n° 165/2014.

DSC_22 Le format de l'antenne n'est pas défini et demeure une décision commerciale, à condition que la DSRC-VU installée satisfasse aux exigences de conformité définies à la section 5 ci-dessous. L'antenne est positionnée comme défini au point DSC_19 et comme illustré à la figure 14.4 (ligne ovale) et elle prend efficacement en charge les cas d'usage décrits en 4.1.2 et en 4.1.3.

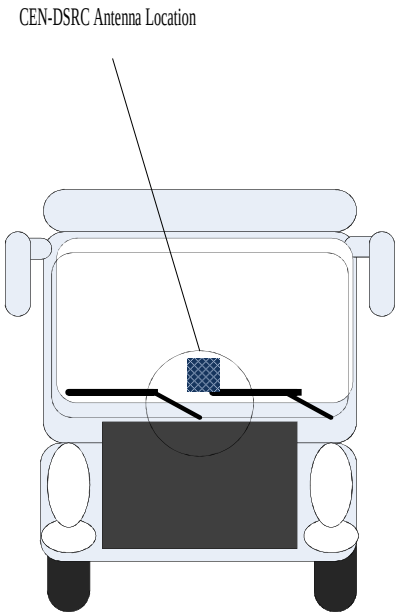


Figure 14.4 — Exemple de positionnement de l'antenne DSRC 5,8 GHz sur le pare-brise de véhicules réglementés

Le format du *REDCR* et de son antenne varie selon les caractéristiques du lecteur (installé sur un tripode, tenu à la main, installé dans un véhicule, etc.) et le mode opératoire adopté par l'agent des autorités de contrôle compétentes.

Une fonction d'affichage et/ou de notification sert à présenter les résultats de la fonction de communication à distance à l'agent des autorités de contrôle compétentes. Il est possible de disposer d'un affichage sur écran ou sous forme 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 au présent appendice.

DSC_23 La conception et le format du *REDCR* dépendent de la conception commerciale dans le cadre de la recommandation ERC 70-03 et des spécifications de conception et de performance définies au présent appendice (5.3.2). Le marché dispose de fait d'une souplesse optimale pour concevoir et fournir les équipements nécessaires dans le but de répondre à l'ensemble des cas de figure d'interrogation propres à toute autorité de contrôle compétente.

DSC_24 La conception et le format de la *DSRC-VU* et son positionnement à l'intérieur ou à l'extérieur de la VU varient selon la conception commerciale, dans le cadre de la recommandation ERC 70-03, et selon les spécifications de conception et de performance définies dans cet appendice à la section 5.3.2 et dans la présente section (5.1).

DSC_25 Cependant, la *DSRC-VU* doit raisonnablement être en mesure d'accepter les valeurs de concept de données provenant d'autres équipements de véhicule intelligent (tel qu'un équipement 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/noms de dossiers d'application connus et uniques et à condition que les instructions d'exploitation desdits protocoles soient mises à la disposition de la Commission européenne et disponibles sans frais pour les fabricants des équipements pertinents.

5.2 Déroulement des opérations

5.2.1 Opérations

Le déroulement des opérations est illustré sur la figure 14.5.

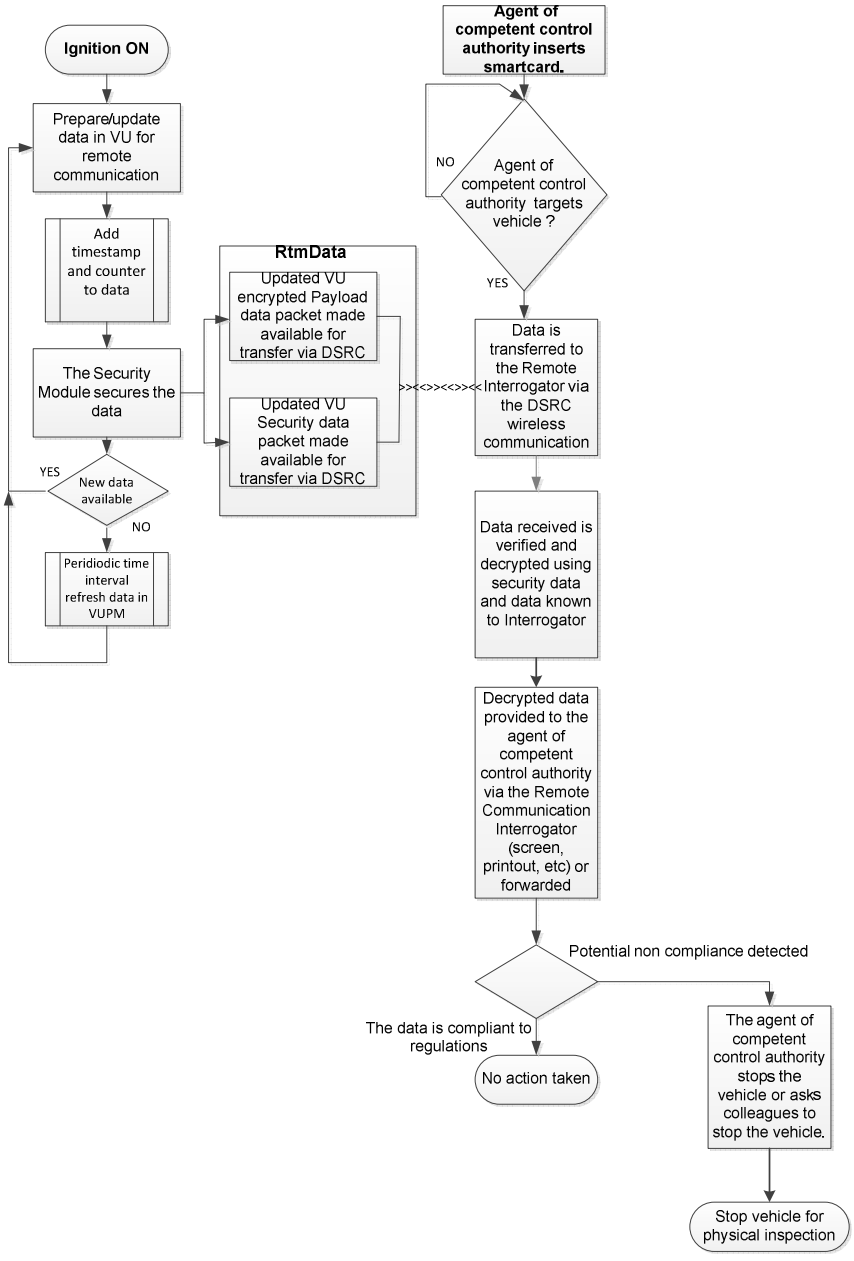


Figure 14.5 — Déroulement des opérations de la fonction de communication à distance

Les étapes sont décrites ci-après:

a. Dès lors que le véhicule est en marche (mis sous contact), le tachygraphe fournit des données à la fonction VU. La fonction VU prépare *les données* pour la fonction de communication à distance (cryptée) et actualise la *VUPM* mémorisée dans la *DSRC-VU* (comme défini aux sections 4.1.1.1 - 4.1.1.2). *Les données* collectées sont formatées comme défini aux sections 5.4.4 – 5.4.5 ci-dessous.
b. À chaque fois que *les données* sont actualisées, le timbre horodateur défini dans le concept de données de sécurité doit être actualisé.
c. La fonction *VUSM* protège les données conformément aux procédures déterminées à l'appendice 11.
d. À chaque mise à jour des *données* (cf. sections 4.1.1.1 - 4.1.1.2), *les données* sont transférées à la *DSRC-VU* où elles remplacent toutes les données antérieures afin que les données actualisées (*les données*) demeurent toujours disponibles en cas d'interrogation par un *REDCR*. *Lorsqu'elles sont fournies par la VU à la DSRC-VU, les données sont identifiables par le nom de fichier RTMData ou par l'identificateur d'application et les identificateurs d'attribut.*
e. Si un agent des autorités de contrôle compétentes souhaite cibler un véhicule et recueillir *les données* émanant du véhicule ciblé, l'agent des autorités de contrôle compétentes insère d'abord sa carte intelligente dans *le REDCR* pour établir *la communication* et permettre au *SM-REDCR* de vérifier son authenticité et de décrypter les données.
f. L'agent des autorités de contrôle compétentes vise ensuite un véhicule et procède à la demande de données par l'intermédiaire de la communication à distance. *Le REDCR* ouvre une session d'interface DSRC 5,8 GHz avec la *DSRC-VU* du véhicule ciblé et procède à la demande des *données*. *Les données* sont transférées vers *le REDCR* grâce au système de communication sans fil en tant qu'attribut DSRC utilisant le service d'application GET, comme défini à la section 5.4. L'attribut contient les valeurs de données utiles chiffrées et les données relatives à la sécurité DSRC.
g. Le *REDCR* procède à l'analyse des données qui sont ensuite communiquées à l'agent des autorités de contrôle compétentes.
h. L'agent des autorités de contrôle compétentes utilise les données pour prendre la décision d'arrêter ou non le véhicule en vue d'une inspection plus détaillée ou pour demander à un autre agent des autorités de contrôle compétentes d'intercepter le véhicule.

5.2.2 Interprétation des données reçues au moyen de la communication DSRC

DSC_26 Les données reçues via l'interface 5,8 GHz incluent la signification et le format définis aux sections 5.4.4 et 5.4.5 ci-dessous et uniquement ceux-là et doivent être interprétés au regard des objectifs qui y sont définis. Conformément aux dispositions du règlement (UE) n° 165/2014, *les données* servent uniquement à fournir les informations pertinentes à une autorité de contrôle compétente pour l'aider à déterminer quel véhicule intercepter pour un contrôle physique et sont détruites par la suite conformément à l'article 9 du règlement (UE) n° 165/2014.

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 avec l'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 du tachygraphe à distance doit être conforme à la recommandation ERC 70-03 et fonctionner selon celle-ci. Il doit également satisfaire aux paramètres définis aux tableaux 14.1 et 14.2 ci-dessous.

DSC_29 Par ailleurs, pour garantir la compatibilité avec les paramètres opérationnels d'autres systèmes DSRC 5,8 GHz normalisés, l'équipement utilisé pour le contrôle du tachygraphe à distance doit être conforme aux paramètres des 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 REDCR dispose de quatre possibilités: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	Dans les limites de 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 être connues au niveau de la DSRC-VU (conforme à EN 12253, EN 13372)
D1a (*)	Tolérance de fréquence des porteuses	□ 5 ppm	**(**conforme à EN 12253**)**
D2(*)	Masque spectral d'émission de la RSU (REDCR)	Dans les limites de ERC 70-03. Le REDCR doit correspondre à la classe B,C telle que définie dans la norme EN 12253 . Pas d'autre exigence spécifique dans la présente annexe	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 OBU(DSRC-VU)	5,795 – 5,815 GHz	(conforme à EN 12253)
D4 (*)	P.I.R.E. maximale	Dans les limites de ERC 70-03 (sans autorisations) et de la réglementation nationale Maximum +33 dBm	(conforme à EN 12253)
D4a	Masque angulaire p.i.r.e.	Conformément à la spécification déclarée et publiée du concepteur de l'interrogateur	**(**conforme à EN 12253**)**
D5	Polarisation	Circulaire anti-horaire	**(**conforme à EN 12253**)**
D5a	Polarisation croisée	XPD: Dans l'axe de visée: (REDCR) RSU t □□15 dB (DSRC-VU) OBU	**(**conforme à EN 12253**)**

Point	*Paramètre*	*Valeur(s)*	*Remarque*
		r □□10 dB Dans la zone -3 dB: (REDCR) RSU t □□10 dB (DSRC-VU) OBU r □□6 dB	
D6 (*)	Modulation	Modulation d'amplitude à deux niveaux	**(**conforme à EN 12253**)**
D6a (*)	Indice de modulation	0,5 ... 0,9	**(**conforme à EN 12253**)**
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 du bit. Le bit "0" présente une transition supplémentaire au milieu de l'intervalle du bit par rapport au bit "1".	**(**conforme à EN 12253**)**
D8 (*)	Débit binaire	500 kBit/s	**(**conforme à EN 12253**)**
D8a	Tolérance de l'horloge bit	mieux que □□□□□ ppm	**(**conforme à EN 12253**)**
D9(*)	Taux d'erreur binaire (B.E.R.) pour la communication	≤10^{-6} si la puissance incidente à l'OBU (DSRC-VU) se situe dans la plage donnée par [D11a à D11b].	**(**conforme à EN 12253**)**
D10	Signal déclenchant le réveil de l' OBU (DSRC-VU)	L'OBU (DSRC-VU) est réveillé à la réception d'une trame comportant 11 octets ou plus (préambule compris)	Aucune structure particulière n'est nécessaire pour le signal de réveil. La DSRC-VU peut s'éveiller à la réception d'une trame comportant moins de 11 octets (conforme à EN 12253)
D10a	Temps de démarrage maximal	≤ 5 ms	**(**conforme à EN 12253**)**

Point	*Paramètre*	*Valeur(s)*	*Remarque*
D11	Zone de communication	Région spatiale dans laquelle un B.E.R. conforme à D9a est atteint	**(**conforme à EN 12253**)**
D11a (*)	Limite de puissance (supérieure) pour la communication.	-24dBm	**(**conforme à EN 12253**)**
D11b (*)	Limite de puissance (inférieure) pour la communication.	Puissance incidente: -43 dBm (axe de visée) -41 dBm (dans la plage -45° - +45° correspondant au plan parallèle à la surface de la route, lorsque la DSRC-VU est installée ultérieurement dans le véhicule (Azimuth))	**(**conforme à EN 12253**)** Exigence supérieure pour des angles horizontaux jusqu'à ±45°, compte tenu des cas de figure définis dans la présente annexe.
D12(*)	Niveau de puissance de coupure de (DSRC-VU)	-60 dBm	(conforme à EN 12253)
D13	Préambule	Préambule obligatoire.	**(**conforme à EN 12253**)**
D13a	Longueur et structure du préambule	16 bits □ 1 bit "1" codé en FM0	**(**conforme à EN 12253**)**
D13b	Forme d'onde du préambule	Séquence alternant les niveaux faible et élevé, avec une durée d'impulsion de 2 µs. La tolérance est donnée par D8a	**(**conforme à EN 12253**)**
D13c	Bits non significatifs	La RSU (REDCR) peut émettre au maximum 8 bits après le drapeau de fin. Un OBU (DSRC-VU) n'est pas tenu de tenir compte de ces bits supplémentaires.	**(**conforme à 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

Tableau 14.2 — Paramètres de liaison montante

Point	*Paramètre*	*Valeur(s)*	*Remarque*
U1 (*)	Fréquences sous-porteuses	Un OBU (DSRC-VU) prend en charge les fréquences 1,5 MHz et 2,0 MHz Une RSU (REDCR) 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 de fréquence des sous-porteuses	□□□□□□□	(conforme à EN 12253)
U1b	Utilisation de bandes latérales	Mêmes données des deux côtés	(conforme à EN 12253)
U2 (*)	Masque spectral d'émission de l'OBU (DSRC-VU)	conformément à EN12253 1) Puissance hors bande: voir ETSI EN 300674-1 2) Puissance dans la bande: [U4a] dBm à 500 kHz 3) Émission dans toute autre voie montante: U2(3)-1 = -35 dBm à 500 kHz	(conforme à EN 12253)
U4a (*)	P.I.R.E. maximale – bande latérale unique (axe 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 - -17dBm	Conformément à la spécification déclarée et publiée du concepteur de l'équipement
U5	Polarisation	Circulaire anti-horaire	(conforme à EN 12253)
U5a	Polarisation croisée	XPD: Dans l'axe de visée: (REDCR) RSU r □□15 dB (DSRC-VU) OBU t □□10 dB	(conforme à EN 12253)

Point	*Paramètre*	*Valeur(s)*	*Remarque*
		À -3 dB: (REDCR) RSU r □10 dB	
		(DSRC-VU) OBU t □□6 dB	
U6	Modulation de sous-porteuse	2-PSK	(conforme à EN 12253)
		Données codées synchronisées avec la sous-porteuse: les transitions des données codées coïncident avec les transitions de la sous-porteuse.	
U6b	Cycle de fonctionnement	Cycle de fonctionnement: 50 % ± α, α ≤ 5 %	(conforme à EN 12253)
U6c	Modulation sur porteuse	Multiplication de sous-porteuse modulée par la porteuse.	(conforme à 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)	(conforme à EN 12253)
U8 (*)	Débit binaire	250 kbit/s	(conforme à EN 12253)
U8a	Tolérance de l'horloge bit	□□1000 ppm	(conforme à EN 12253)
U9	Taux d'erreur binaire (B.E.R.) pour la communication	$\leq 10^{-6}$	(conforme à EN 12253)
U11	Zone de communication	La région spatiale dans laquelle se situe la DSRC-VU, telle que ses émissions soient reçues par le REDCR avec un B.E.R. inférieur à celui indiqué par U9a.	(conforme à EN 12253)
U12a(*)	Gain de conversion (limite inférieure)	1 dB pour chaque bande latérale	
		Plage angulaire: circulairement symétrique entre l'axe de visée et ± 35°	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.
		et dans la plage -45° - +45° correspondant au plan parallèle à la surface de la route, lorsque la DSRC-VU est installée ultérieurement dans le véhicule (Azimuth)	

Point	*Paramètre*	*Valeur(s)*	*Remarque*
U12b(*)	Gain de conversion (limite supérieure)	10 dB pour chaque bande latérale	Moins que la plage de valeurs spécifiée pour chaque bande latérale à l'intérieur d'un cône circulaire autour de l'axe de visée, de □ 45° d'angle d'ouverture
U13	Préambule	Préambule obligatoire.	(conforme à EN 12253)
U13a	Préambule Longueur et structure	32 à 36 µs, modulé par sous-porteuse uniquement, puis 8 bits "0" en codage NRZI.	(conforme à EN 12253)
U13b	Bits non significatifs	La DSRC-VU peut émettre au maximum 8 bits après le drapeau de fin. Un RSU (REDCR) n'est pas tenu de tenir compte de ces bits supplémentaires.	(conforme à EN 12253)

(*) - Paramètres de liaison montante soumis à essai de conformité selon l'essai de paramétrage pertinent prévu par la norme EN 300 674-1

5.3.3 Conception de l'antenne

5.3.3.1 Antenne REDCR

DSC_30 La conception de l'antenne *REDCR* dépend de la conception commerciale, dans les limites définies à la section 5.3.2, et adaptée pour optimiser la performance de lecture du *DSRC-REDCR* aux fins spécifiques et pour les circonstances de lecture pour lesquelles le *REDCR* a été conçu pour fonctionner.

5.3.3.2 Antenne VU

DSC_31 La conception de l'antenne *DSRC-VU* dépend de la conception commerciale, dans les limites définies à la section 5.3.2, et adaptée pour optimiser la performance de lecture du *DSRC-REDCR* aux fins spécifiques et pour les circonstances de lecture pour lesquelles le *REDCR* a été conçu pour fonctionner.

DSC_32 L'antenne VU est fixée sur le pare-brise du véhicule ou à proximité de celui-ci, comme spécifié à la section 5.1 ci-dessus.

DSC_33 Dans l'environnement d'essai en atelier (cf. section 6.3), une antenne DSRC-VU, installée selon la section 5.1, doit pouvoir se connecter à l'aide d'une communication d'essai standard et effectuer la transaction RTM telle que définie au présent appendice, à une distance située entre 2 et 10 mètres, plus de 99 % du temps en moyenne, sur plus de 1000 interrogations en lecture.

5.4 Exigences du protocole DSRC pour RTM

5.4.1 Vue d'ensemble

DSC_34 Le protocole de transaction pour télécharger *les données* au moyen de la liaison d'interface DSRC 5,8 GHz respecte les étapes suivantes. La présente section décrit un flux de transaction dans les conditions idéales sans retransmission ou interruption de la communication.

NOTE: l'objectif de l'étape d'initialisation (Étape 1) est d'établir la communication entre le *REDCR* et les DSRC-VU présentes dans la zone de transaction (maître-esclave) DSRC à 5,8 GHz, mais qui n'ont pas encore établi de communication avec le *REDCR*, puis d'en avertir les processus d'application.

- **Étape 1** Initialisation. Le *REDCR* envoie une trame contenant une «table de service de balise» (BST) qui inclut les identificateurs d'application (AID) dans la liste de services pris en charge. Dans l'application RTM, elle correspond simplement au service de valeur AID = 2 (Freight&Fleet). La *DSRC-VU* évalue la BST reçue et répond (cf. ci-dessous) avec la liste des applications prises en charge dans le domaine Freight&Fleet ou ne répond pas si aucune n'est prise en charge. Si le *REDCR* ne propose pas AID = 2, la DSRC-VU ne répond pas au REDCR.
- **Étape 2** La *DSRC-VU* envoie une trame contenant une demande pour une allocation de fenêtre privée.
- **Étape 3** Le *REDCR* envoie une trame contenant une allocation de fenêtre privée.
- **Étape 4** La *DSRC-VU* utilise cette fenêtre privée allouée pour envoyer une trame contenant sa table de service de véhicule (VST). Cette VST comprend la liste de toutes les instanciations d'applications différentes prises en charge par cette *DSRC-VU* dans le cadre d'une valeur AID = 2. Les différentes instanciations sont identifiées au moyen d'EID générés de manière exclusive. Chacun est associé à une valeur de paramètres «marque de contexte d'application» indiquant la norme et l'application prises en charge.
- **Étape 5** Ensuite le *REDCR* analyse la VST proposée et décide soit de mettre fin à la connexion (RELEASE) car rien ne l'intéresse dans l'offre de la VST (c'est-à-dire qu'il reçoit une VST d'une *DSRC-VU* qui ne prend pas en charge la transaction RTM), soit de lancer une instanciation d'application, s'il reçoit une VST appropriée.
- **Étape 6** À cette fin, le REDCR envoie une trame contenant une commande pour extraire les données RTM en identifiant l'instanciation de l'application RTM par la spécification de son identificateur (tel qu'indiqué par la DSRC-VU dans la VST) avant d'allouer une fenêtre privée.
- **Étape 7** La *DSRC-VU* utilise la fenêtre privée qui vient d'être allouée pour envoyer une trame qui contient l'identificateur adressé correspondant à l'instanciation de l'application RTM tel que fourni dans la 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 se répète.
- **Étape 9** Le *REDCR* confirme la réception des données en envoyant une trame contenant une commande RELEASE à la *DSRC-VU* pour mettre fin à la session OU en cas d'échec de la validation d'un accusé de réception du LDPU, elle revient à l'étape 6.

Cf. figure 14.6 pour une illustration du protocole de transaction.

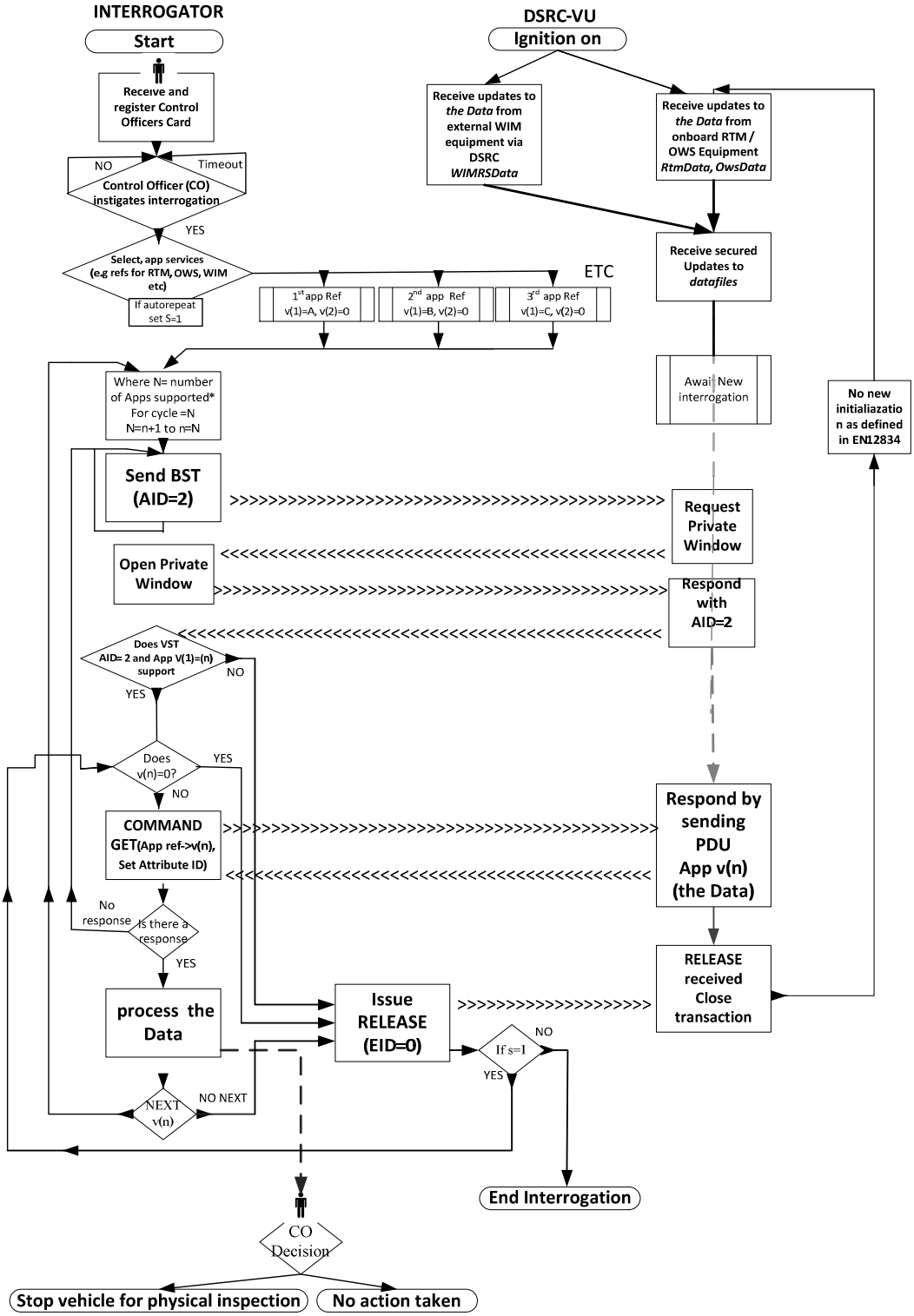


Figure 14.6 — Déroulement d'une procédure RTM via DSRC à 5,8 GHz

5.4.2 Commandes

DSC_35 Les commandes suivantes sont les seules fonctions utilisées dans une phase de transaction RTM

- **INITIALISATION.request:** commande émanant du REDCR sous la forme d'une diffusion avec la définition des applications prises en charge par le REDCR.
- **INITIALISATION.response**: réponse émanant de la DSRC-VU confirmant la connexion et contenant la liste des instances d'application prises en charge, avec les caractéristiques et les informations relatives à la façon de les adresser (EID).
- **GET.request:** commande émanant du *REDCR* et envoyée à la *DSRC-VU* spécifiant l'instanciation de l'application à adresser au moyen d'un EID défini, tel que reçu dans la VST, donnant instructions à la *DSRC-VU* d'envoyer l'attribut ou les attributs sélectionnés avec *les données*. L'objectif de la commande GET est que le *REDCR* obtienne *les données* de la *DSRC-VU*.
- **GET.response:** réponse de la *DSRC-VU* contenant *les données* demandées.
- **ACTION.request ECHO:** commande donnant instruction à la *DSRC-VU* de renvoyer les données de la *DSRC-VU* au *REDCR*. L'objectif de la commande ECHO est de permettre aux ateliers ou aux infrastructures d'essai d'homologation de vérifier que la liaison DSRC fonctionne sans devoir accéder aux éléments d'authentification de sécurité.
- **ACTION**.response ECHO: réponse de la DSRC-VU à la commande ECHO.
- **EVENT_REPORT.request** RELEASE: commande informant la *DSRC-VU*que la transaction est terminée. L'objectif de la commande RELEASE est de mettre fin à la session avec la *DSRC-VU*. Dès réception de RELEASE, la *DSRC-VU* ne répond plus à aucune interrogation dans le cadre de la connexion en cours. Remarque: la norme EN 12834 prévoit qu'une DSRC-VU ne se connecte pas deux fois au même interrogateur sauf si elle a quitté la zone de communication pendant 255 secondes ou si l'ID de balise de l'interrogateur a changé.

5.4.3 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	Ac
1	REDCR	>	DSRC-VU	Initialisation de la liaison de communication – Demande	Le REDCR diffuse la BST
2	*DSRC-VU*	>	*REDCR*	*Initialisation de la liaison de communication – Réponse*	*Si la BST prend en charge AID=2 alors la DSRC-VU demande l'allocation d'une fenêtre privée*
3	REDCR	>	DSRC-VU	Alloue une fenêtre privée	Envoie une trame contenant une allocation de fenêtre privée
4	*DSRC-VU*	>	*REDCR*	*Envoie une VST*	*Envoie une trame contenant une VST*
5	REDCR	>	DSRC-VU	Envoie GET.request concernant les données figurant dans l'attribut pour l'EID spécifique	
6	*DSRC-VU*	>	*REDCR*	*Envoie GET.response avec l'attribut demandé pour l'EID spécifique*	*Envoie l'attribut (RTMData, OWSData….) avec les données pour l'EID spécifique*
7	REDCR	>	DSRC-VU	Envoie GET.request concernant les données d'un autre attribut (si nécessaire)	
8	*DSRC-VU*	>	*REDCR*	*Envoie GET.response avec l'attribut demandé*	*Envoie l'attribut avec les données pour l'EID spécifique*

9	REDCR	>	DSRC-VU	Accuse réception des données	Envoie la commande RELEASE qui met fin à la transaction
10	*DSRC-VU*			*Met fin à la transaction*	

Un exemple de la séquence de transaction et du contenu des trames échangées figure aux sections 5.4.7 et 5.4.8.

5.4.4 Structures de données

DSC_37 La structure sémantique des *données* ayant emprunté l'interface DSRC 5,8 GHz doit être cohérente avec la description faite au présent appendice. La présente section spécifie la manière dont ces données sont structurées.

DSC_38 Les données utiles (données RTM) correspondent à la concaténation des:

1. données EncryptedTachographPayload, qui résultent du cryptage de TachographPayload tel que défini dans ASN.1 à la section 5.4.5. La méthode de cryptage fait l'objet d'une description à l'appendice 11.
2. DSRCSecurityData, qui font l'objet d'une description à l'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 normalisée prise en charge dans 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
-- Imports data attributes and elements from EFC which are used for RTM
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition
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)};


-- Definitions of the RTM functions:
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})

-- Definitions of the RTM attributes:
RtmData ::= SEQUENCE {
  encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting
TachographPayload as per Appendix 11 --}),
  DSRCSecurityData OCTET STRING
  }
TachographPayload ::= SEQUENCE {
            tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
            tp15638SpeedingEvent            BOOLEAN, -- 1= Irregularities in speed (see Annex 1C)
            tp15638DrivingWithoutValidCard  BOOLEAN,    -- 1= Invalid card usage (see Annex 1C)
            tp15638DriverCard               BOOLEAN,-- 0= Indicates a valid driver card  (see Annex
1C)
            tp15638CardInsertion            BOOLEAN, -- 1= Card insertion while driving (see Annex
1C)
            tp15638MotionDataError          BOOLEAN, -- 1= Motion data error (see Annex 1C)
            tp15638VehicleMotionConflict    BOOLEAN, -- 1= Motion conflict (see Annex 1C)
            tp156382ndDriverCard            BOOLEAN, -- 1= Second driver card inserted (see Annex
1C)
            tp15638CurrentActivityDriving   BOOLEAN, -- 1= other activity selected;
                                                                    -- 0= driving selected
            tp15638LastSessionClosed        BOOLEAN, -- 1= improperly, 0= properly, closed
            tp15638PowerSupplyInterruption  INTEGER (0..127), -- Supply interrupts in the last 10
days
            tp15638SensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
-- All subsequent time related types as defined in Annex 1C.
            tp15638TimeAdjustment           INTEGER(0..4294967295), -- Time of the last time
adjustment
            tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
            tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
            tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration
data
```

```
tp15638DateTachoConnected  INTEGER(0..4294967295), -- Date tachograph connected

                tp15638CurrentSpeed             INTEGER (0..255), -- Last current recorded speed
                tp15638Timestamp                INTEGER(0..4294967295) -- Timestamp of current record[2]
                }
 Rtm-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its 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,
 -- values from 16 to 255 reserved for ISO/CEN usage
      }}

 END
```

5.4.5 Éléments de RtmData, actions effectuées et définitions

DSC_41 Les valeurs de données à calculer par la VU et utilisées pour actualiser les données sécurisées dans la DSRC-VU sont calculées selon les règles prévues au tableau 14.3:

Tableau 14.3 - Éléments de RtmData, actions effectuées et définitions

(1) *Élément de données RTM*	*(2)* *Action effectuée par la VU*		*(3)* *Définition des données ASN.1*
RTM1 **Plaque**	La VU définit la valeur de l'élément de données RTM1	Plaque d'immatriculation du véhicule	tp15638VehicleRegstrati onPlate LPN,

(1) *Élément de données RTM*	*(2)* *Action effectuée par la VU*		*(3)* *Définition des données ASN.1*
d'immatriculation du véhicule	*tp15638VehicleRegistrationPlate* provenant de la valeur enregistrée du type de données *VehicleRegistrationIdentification* tel que défini à l'appendice 1 *VehicleRegistrationIdentification*	exprimée par une chaîne de caractères	--Plaque d'immatriculation du véhicule importée de la norme ISO 14906 avec les limitations spécifiées dans EN 15509; il s'agit d'une SEQUENCE comprenant un code pays suivi d'un indicateur alphabétique suivi du numéro d'immatriculation propre; ce dernier contient toujours 14 octets (avec des zéros de remplissage). Ainsi, la longueur de type LPN conformément à la norme EN 15509 est toujours de 17 octets, dont 14 correspondent à la plaque d'immatriculation réelle.
RTM2 **Événement «Excès de vitesse»**	La VU génère une valeur booléenne pour l'élément de données RTM2 tp15638SpeedingEvent. La valeur tp15638SpeedingEvent est calculée par la VU d'après le nombre d'événements «excès de vitesse» (tel que défini à l'annexe 1C) enregistrés dans la VU 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	1 (TRUE) – Indique des irrégularités de vitesse au cours des 10 derniers jours d'occurrence	tp15638speedingEvent BOOLEAN,

(1) *Élément de données RTM*	*(2)* *Action effectuée par la VU*		*(3)* *Définition des données ASN.1*
	(vrai). AUTREMENT, si aucun événement n'est survenu au cours des 10 derniers jours d'occurrence, tp15638SpeedingEvent prend la valeur FALSE (faux).		
RTM3 **Conduite sans carte valide**	La VU génère une valeur booléenne pour l'élément de données RTM3 tp15638DrivingWithoutValidCard. La VU attribue la valeur TRUE à la variable tp15638DrivingWithoutValidCard si les données de la VU ont enregistré au moins un événement de type «Conduite sans carte valable» (tel que défini à l'annexe 1C) 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) = Indique l'utilisation d'une carte invalide	tp15638DrivingWithoutValidCard BOOLEAN,
RTM4 **Carte de conducteur valide**	La VU génère une valeur booléenne pour l'élément de données RTM4 tp15638DriverCard basée sur les données enregistrées dans la VU et conformément à l'appendice 1. Si aucune carte de conducteur valide n'est	0 (FALSE) = Indique une carte de conducteur valide	tp15638DriverCard BOOLEAN,

(1) *Élément de données RTM*	*(2)* *Action effectuée par la VU*		*(3)* *Définition des données ASN.1*
	présente, la VU attribue la valeur TRUE à la variable. AUTREMENT, si une carte de conducteur valide est présente, la VU attribue la valeur FALSE à la variable.		
RTM5 **Insertion d'une carte pendant la conduite**	La VU génère une valeur booléenne pour l'élément de données RTM5. La VU attribue la valeur TRUE à la variable tp15638CardInsertion si les données de la VU ont enregistré au moins un événement de type «Insertion d'une carte pendant la conduite» (tel que défini à l'annexe 1C) 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'insertion d'une carte pendant la conduite au cours des 10 derniers jours d'occurrence	tp15638CardInsertion BOOLEAN,
RTM6 **Erreur de données de mouvement**	La VU génère une valeur booléenne pour l'élément de données RTM6. La VU attribue la valeur TRUE à la variable tp15638MotionDataError si les données de la VU ont enregistré au moins un événement de type «erreur de données de mouvement» (tel que défini à l'annexe 1C) au cours des 10 derniers jours d'occurrence.	1 (TRUE) = Indique une erreur de données de mouvement au cours des 10 derniers jours d'occurrence	tp15638motionDataError BOOLEAN,

(1) *Élément de données RTM*	*(2)* *Action effectuée par la VU*		*(3)* *Définition des données ASN.1*
	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.		
RTM7 **Conflit concernant le mouvement du véhicule**	La VU génère une valeur booléenne pour l'élément de données RTM7. La VU assigne la valeur TRUE à la variable tp15638vehicleMotionConflict si les données de la VU ont enregistré au moins un événement de type «conflit concernant le mouvement du véhicule» (valeur '0A'H) au cours des 10 derniers jours d'occurrence.	1 (TRUE) = Indique un conflit concernant le mouvement du véhicule au cours des 10 derniers jours d'occurrence	tp15638vehicleMotionConflict BOOLEAN,
	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.		
RTM8 **Deuxième carte de conducteur**	La VU génère une valeur booléenne pour l'élément de données RTM8 sur la base de l'annexe 1C («Données relatives à l'activité du conducteur» ÉQUIPAGE et CONVOYEUR). Si une deuxième carte de conducteur valide est présente, la VU attribue la valeur TRUE à la variable. AUTREMENT, en	1 (TRUE) = Indique qu'une deuxième carte de conducteur a été insérée	tp156382ndDriverCard BOOLEAN,

(1) *Élément de données RTM*	*(2)* *Action effectuée par la VU*		*(3)* *Définition des données ASN.1*
	l'absence d'une deuxième carte de conducteur valide, la VU attribue la valeur FALSE à la variable.		
RTM9 **Activité en cours**	La VU génère une valeur booléenne pour l'élément de données RTM9. Si l'activité en cours est enregistrée dans la VU en tant qu'activité autre que «CONDUITE» (telle que définie à l'annexe 1C), la VU attribue la valeur TRUE à la variable. AUTREMENT, si l'activité en cours est enregistrée dans la VU comme «CONDUITE», la VU attribue la valeur FALSE à la variable.	1 (TRUE) = autre activité sélectionnée; 0 (FALSE) = conduite sélectionnée	tp15638currentActivityDriving BOOLEAN
RTM10 **Clôture de la dernière session**	La VU 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 1C, la VU attribue la valeur TRUE à la variable. AUTREMENT, si la dernière session d'une carte a été correctement clôturée, la VU attribue la valeur FALSE à la variable.	1 (TRUE) = la clôture de session a échoué 0 (FALSE) = la clôture de session a abouti	tp15638lastSessionClosed BOOLEAN
RTM11 **Coupure de l'alimentation électrique**	La VU génère une valeur exprimée par un nombre entier pour l'élément de données RTM11.	-- Nombre de coupures de l'alimentation électrique au cours des 10 derniers jours d'occurrence	tp15638powerSupplyInterruption INTEGER (0..127),

(1) *Élément de données RTM*	*(2)* *Action effectuée par la VU*		*(3)* *Définition des données ASN.1*
	La VU affecte une valeur à la variable tp15638PowerSupplyInterruption égale à la coupure d'électricité la plus longue (conformément aux dispositions de l'article 9 du règlement (UE) n° 165/2014), de type «interruption de l'alimentation électrique» (tel que défini à l'annexe 1C). 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.		
RTM12 **Anomalie du capteur**	La VU génère une valeur indiquée par un nombre entier pour l'élément de données RTM12. La VU attribue à la variable sensorFault une valeur de: - 1 si un événement de type anomalie de capteur '35'H a été enregistré au cours des 10 derniers jours, - 2 si un événement de type anomalie du récepteur GNSS (interne ou externe, avec les valeurs enum '51'H ou '52'H) a été enregistré au	--erreur de capteur un octet conformément au dictionnaire des données	tp15638SensorFault INTEGER (0..255),

(1) *Élément de données RTM*	*(2)* *Action effectuée par la VU*	*(3)* *Définition des données ASN.1*
	cours des 10 derniers jours. - 3 si un événement de type anomalie de communication du dispositif GNSS externe '53'H a été enregistré au cours des 10 derniers jours d'occurrence. - 4 si des anomalies de capteur et des anomalies de récepteur GNSS ont été enregistrées au cours des 10 derniers jours d'occurrence - 5 si des anomalies de capteur et des anomalies de communication du dispositif GNSS externe ont été enregistrées au cours des 10 derniers jours d'occurrence - 6 si des anomalies de récepteur GNSS et des anomalies de communication du dispositif GNSS externe ont été enregistrées au cours des 10 derniers jours d'occurrence - 7 si des anomalies des trois types ont été enregistrées au cours des 10 derniers jours d'occurrence. AUTREMENT, une valeur de 0 est attribuée si aucun événement n'a été enregistré au cours des 10 derniers jours	

(1) *Élément de données RTM*	*(2)* *Action effectuée par la VU*		*(3)* *Définition des données ASN.1*
	d'occurrence.		
RTM13 **Remise à l'heure**	La VU génère une valeur indiquée par un nombre entier (timeReal de l'appendice 1) pour l'élément de données RTM13, en fonction de la présence de la présence de données concernant la remise à l'heure (telles que définies à l'annexe 1C). La VU doit attribuer la valeur horaire correspondant au dernier événement de remise à l'heure. AUTREMENT, si aucun événement «remise à l'heure» (tel que défini à l'annexe 1C) n'est présent dans la VU, la valeur attribuée est 0.	Heure de la dernière remise à l'heure	tp15638TimeAdjustment INTEGER(0..4294967295),
RTM14 **Tentative d'infraction à la sécurité**	La VU génère une valeur indiquée par un nombre entier (timeReal de l'appendice 1) pour l'élément de données RTM14, en fonction de la présence d'une tentative d'infraction à la sécurité (telle que définie à l'annexe 1C). La VU doit attribuer la valeur horaire correspondant au dernier événement de tentative d'infraction à la sécurité enregistrée par la VU. AUTREMENT, si aucune «tentative d'infraction à la sécurité» (telle que définie à l'annexe 1C) n'est présente dans les	Heure de la dernière tentative d'infraction -- Valeur par défaut = 0x00FF	tp15638LatestBreachAttempt INTEGER(0..4294967295),

(1) *Élément de données RTM*	*(2)* *Action effectuée par la VU*		*(3)* *Définition des données ASN.1*
	données de la VU, la valeur 0x00FF est attribuée.		
RTM15 **Dernier étalonnage**	La VU génère une valeur indiquée par un nombre entier (timeReal de l'appendice 1) pour l'élément de données RTM15, en fonction de la présence de données de dernier étalonnage (tel que défini à l'annexe 1C). La VU doit attribuer la valeur temporelle des deux derniers étalonnages (RTM15 et RTM16), fixée dans VuCalibrationData comme le précise l'appendice 1. La VU attribue la valeur pour RTM15 au timeReal du dernier enregistrement d'étalonnage.	Heure des données de dernier étalonnage	tp15638LastCalibrationData INTEGER(0..4294967295),
RTM16 **Étalonnage précédent**	La VU génère une valeur indiquée par un nombre entier (timeReal de l'appendice 1) pour l'élément de données RTM16 de l'enregistrement d'étalonnage précédant celui du dernier étalonnage. AUTREMENT, si aucun étalonnage n'a été effectué précédemment, la VU attribue la valeur 0 à RTM16.	Heure des données de l'étalonnage précédent	tp15638PrevCalibrationData INTEGER(0..4294967295),
RTM17 **Date de connexion du tachygraphe**	Pour l'élément de données RTM17, la VU attribue une valeur indiquée par un nombre entier (timeReal de	Date de connexion du tachygraphe	tp15638DateTachoConnected INTEGER(0..4294967295),

(1) *Élément de données RTM*	*(2)* *Action effectuée par la VU*		*(3)* *Définition des données ASN.1*
	l'appendice 1). La VU attribue la valeur temporelle de l'installation initiale de la VU. La VU extrait ces données des VuCalibrationData (appendice 1) des vuCalibrationRecords, où CalibrationPurpose est égal à: '03'H		
RTM18 **Vitesse actuelle**	La VU génère une valeur exprimée par un nombre entier pour l'élément de données RTM18. La VU attribue comme valeur pour l'élément RTM18 la dernière vitesse actuelle enregistrée au moment de la dernière mise à jour des RtmData.	Dernière vitesse actuelle enregistrée	tp15638CurrentSpeed INTEGER (0..255),
RTM19 **Horodatage**	Pour l'élément de données RTM19, la VU attribue une valeur indiquée par un nombre entier (timeReal de l'appendice 1). La VU attribue comme valeur pour l'élément RTM19 le moment de la dernière mise à jour des RtmData.	Horodatage de l'enregistrement TachographPayload actuel	tp15638Timestamp INTEGER(0..4294967295),

5.4.6 Mécanisme de transfert de données

DSC_42 Les données utiles définies précédemment sont réclamées par le REDCR après la phase d'initialisation puis sont transmises par la *DSRC-VU* dans la fenêtre allouée. Le REDCR utilise la commande GET pour extraire les données.

DSC_43 Pour tous les échanges DSRC, les données sont codées à l'aide des règles PER (Packed Encoding Rules).

5.4.7 Description détaillée de la transaction DSRC

DSC_44 L'initialisation est conforme aux dispositions DSC_44 à DSC_48 et des tableaux 14.4 à 14.9. Durant la phase d'initialisation, le REDCR commence à envoyer une trame contenant une BST (table de service de balise) selon les normes EN 12834 et EN 13372, 6.2, 6.3, 6.4, et 7.1 avec le paramétrage défini au tableau 14.4 ci-après.

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 ou 1
MandApplications	Pas d'extension, EID non présent, paramètre non présent, AID= 2
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 suivant, 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		
	BeaconID SEQUENCE {		Applications NonMand non
	ManufacturerId INTEGER (0..65535)	0	présentes
		xxx	Identificateur du fabricant
7		xxxx xxxx	

Octet #		*Attribut/Champ*	*Bits dans l'octet*	*Description*
8			xxxx x	
	IndividualID	INTEGER (0..134217727)		
			xxx	ID 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				Pas d'extension.
	Profile	INTEGER (0..127,...)	0000 0000	Profil d'exemple 0
17	MandApplications	SEQUENCE (SIZE(0..127,...)) OF {	0000 0001	Pas d'extension, Nombre mandApplications = 1
18				
			0	EID non présent
			0	
		SEQUENCE {		
		OPTION indicator		Paramètre non présent
	AID	OPTION indicator DSRCApplicationEntityID } }	00 0010	Pas d'extension. AID= 2 Freight&Fleet
19	ProfileList	SEQUENCE (0..127,...) OF Profile }	0000 0000	Pas d'extension, nombre de profils dans la liste = 0
20			xxxx xxxx	Séquence de contrôle de trame
21		FCS	xxxx xxxx	
22		Flag	0111 1110	Drapeau de fin

DSC_45 Lorsqu'une *DSRC-VU* reçoit une BST, elle demande l'allocation d'une fenêtre privée, telle que définie dans les normes EN 12795 et EN 13372, 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 de la DSRC-VU
3			xxxx xxxx	
4			xxxx xxxx	

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
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 REDCR répond en allouant une fenêtre privée, comme le définissent les normes EN 12795 et EN 13372, 7.1.1 sans paramétrage RTM particulier.
Le tableau 14.7 fournit 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 de la DSRC-VU
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 la *DSRC-VU* reçoit l'allocation de fenêtre privée, elle envoie sa VST (table de service de véhicule) telle que définie dans les normes EN 12834 et EN 13372, 6.2., 6,3, 6.4. et 7.1. avec le paramétrage spécifié au tableau 14.8, en utilisant la fenêtre de transmission 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 REDCR
Fragmentation header	Pas de fragmentation
Layer 2 settings	PDU de commande, Commande UI

DSC_48 La *DSRC-VU* prend en charge l'application «Freight&Fleet», identifiée par l'identificateur d'application '2'. D'autres identificateurs d'application peuvent être pris en charge, mais ne doivent pas être présents dans cette

VST, car la BST exige uniquement AID = 2. Le champ «Applications» contient une liste des instances d'application prises en charge dans la *DSRC-VU*. Pour chaque instanciation 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 représente la norme associée, sa partie (9 pour RTM) et éventuellement sa version, ainsi qu'un EID généré par la DSRC-VU 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	
3		xxxx xxxx	
4		xxxx xxxx	Adresse de liaison de la DSRC-VU
5		xxxx xxxx	spécifique
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	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 DSRCApplicationEntityID	00 0010	Pas d'extension. AID= 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Défini dans le cadre de l'OBU et identifie 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 {		
	StandardIdentifier	0000 0110	Identificateur d'objet de la norme, partie et version prise en charge.
17	standardIdentifier	0000 0110	Exemple: ISO (1) Standard (0) TARV
18		0010 1000	(15638) part9(9) Version1 (1).
19		1000 0000	Le premier octet est 06H, qui est
20		1111 1010	l'identificateur d'objet. Le deuxième octet est 06H, qui est sa longueur. Les

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
21		0001 0110	6 octets suivants codent l'identificateur d'objet de l'exemple.
22		0000 1001	
23		0000 0001	Remarque: un seul élément de la séquence est présent (l'élément optionnel RtmCommProfile est omis).
24	ObeConfiguration Sequence {		
	OPTION indicator	0	ObeStatus non présent
	EquipmentClass INTEGER	xxx xxxx	
25	(0..32767)	xxxx xxxx	
26		xxxx xxxx	Identificateur du fabricant pour la DSRC-VU tel qu'il figure au registre ISO 14816
	ManufacturerId INTEGER		
27	(0..65535)	xxxx xxxx	
28		xxxx xxxx	
29	FCS	xxxx xxxx	Séquence de contrôle de trame
30	Flag	0111 1110	Drapeau de fin

DCS_49 Le REDCR lit ensuite les données en émettant une commande GET, conforme à la commande GET définie dans les normes EN 13372 6.2, 6.3, 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 de la DSRC-VU spécifique
Chaining	Non
Element Identifier (EID)	Comme spécifié dans la 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 sollicitée

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 de la DSRC-VU spécifique
3		xxxx xxxx	

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	PDU de commande
7	LLC Control field	n111 0111	Commande ACn sollicitée, bit n
8	Fragmentation header	1xxx x001	Pas de fragmentation
9	Get.request	0110	Demande Get
	SEQUENCE {	0	Éléments d'authentification d'accès non présents
	OPTION indicator		
	OPTION indicator	0	IID non présent
	OPTION indicator	1	AttributeIdList présent
	Fill BIT STRING(SIZE(1))	0	Mis à 0.
10	EID INTEGER(0..127,…)	xxxx xxxx	L'EID de l'instance d'application RTM, tel que spécifié dans la VST. Pas d'extension
11	AttributeIdList SEQUENCE OF {	0000 0001	Pas d'extension, nombre d'attributs = 1
	AttributeId		
	}}		
12		0000 0001	AttributeId=1, RtmData. Pas d'extension
13	FCS	xxxx xxxx	Séquence de contrôle de trame
14		xxxx xxxx	
15	Flag	0111 1110	Drapeau de fin

DSC_50 Lorsque la *DSRC-VU* reçoit la demande GET, elle envoie une réponse GET avec les données demandées conformes à la réponse GET définie par la norme EN 13372, 6.2, 6.3, 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	Comme indiqué dans la VST.
Access Credentials	Non
Fragmentation	Non
Layer2 settings	PDU de réponse, réponse disponible et commande acceptée, commande ACn

Le tableau 14.13 montre un exemple de lecture des 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 de la DSRC-VU
3		xxxx xxxx	spécifique
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	PDU de réponse
7	LLC Control field	n111 0111	Réponse disponible, commande
8	LLC Status field	0000 0000	Réponse disponible et commande
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
	OPTION indicator	0	Statut de retour non présent
		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 { AttributeId	0000 0001	Pas d'extension, AttributeId=1 (RtmData)
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	

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
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 REDCR met alors fin à la connexion en émettant une commande EVENT_REPORT RELEASE conforme aux normes EN 13372, 6.2, 6.3, 6.4 et EN 12834 ,7.3.8, sans paramétrage RTM spécifique. Le tableau 14.14 montre 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 de la DSRC-VU 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
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

Octet #	*Attribut/Champ*	*Bits dans l'octet*	*Description*
13		xxxx xxxx	
14	Flag	0111 1110	Drapeau de fin

DSC_52 La *DSRC-VU* n'est pas censée répondre à la commande RELEASE. Il est alors mis fin à la communication.

5.4.8 Description de la transaction d'essai DSRC

DSC_53 Les essais exhaustifs, comprenant la sécurisation des données, doivent être menés conformément aux dispositions de l'appendice 11 Mécanismes communs de sécurité, par les 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 régulière demandant le décryptage et la compréhension du contenu des données décryptées sont menés conformément aux dispositions de l'appendice 11 Mécanismes communs de sécurité et de l'appendice 9 Homologation – Liste des essais minimaux requis.

Cependant, il est possible de procéder à un essai de la communication DSRC de base avec la commande ECHO. De tels essais peuvent se révéler nécessaires lors de la mise en service, lors des inspections régulières ou sur demande des autorités de contrôle compétentes ou conformément aux dispositions du règlement (UE) n° 165/2014 (cf. 6 ci-dessous).

DSC_55 Pour procéder à cet essai de communication de base, la commande ECHO est émise par le REDCR 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 REDCR* envoie une «table de service de balise» (BST) contenant les identificateurs d'application (AID) dans la liste de services pris en charge. Dans les applications RTM, cela correspond simplement au service de valeur AID = 2.
- La *DSRC-VU* évalue la BST reçue et répond lorsqu'elle détecte que la BST demande Freight&Fleet (AID = 2). Si *le REDCR* ne propose pas AID = 2, la *DSRC-VU* met fin à la transaction avec *le REDCR*.
- Étape 2 *La DSRC-VU* envoie une demande d'allocation de fenêtre privée.
- Étape 3 Le REDCR envoie une allocation de fenêtre privée.
- Étape 4 La *DSRC-VU* utilise cette fenêtre privée allouée pour envoyer sa table de service de véhicule (VST). Cette VST comprend la liste de toutes les instanciations d'application différentes prises en charge par cette *DSRC-VU* dans le cadre d'une valeur AID = 2. Les différentes instanciations sont identifiées au moyen d'EID générés de manière exclusive. Chacun est associé à une valeur de paramètres indiquant l'instance de l'application prise en charge.

- Étape 5 Ensuite *le REDCR* analyse la VST proposée et décide soit de mettre fin à la connexion (RELEASE) car rien ne l'intéresse dans l'offre de la VST (c'est-à-dire qu'il reçoit une VST d'une *DSRC-VU* qui n'est pas une RTM VU), soit, s'il reçoit une VST appropriée, de lancer une instanciation d'application.
- Étape 6 Le *REDCR* émet une commande (ECHO) vers la *DSRC-VU* spécifique et alloue une fenêtre privée.

- Étape 7 La *DSRC-VU* utilise la fenêtre privée qui vient d'être allouée pour envoyer une trame de réponse.

Les tableaux suivants donnent un exemple pratique de session d'échange ECHO.

DSC_56 L'initialisation est effectuée conformément aux dispositions de la section 5.4.7 (DSC_44 – DSC_48) et des tableaux 14.4 – 14.9.

DSC_57 Le REDCR émet alors une commande ACTION, ECHO conforme à la norme ISO 14906, contenant 100 octets de données, sans paramétrage particulier pour RTM. Le tableau 14.15 indique le contenu de la trame envoyée par le REDCR.

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 de la DSRC-VU 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 sollicitée, 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	
11 46 14	FCS	xxxx xxxx	Séquence de contrôle de trame
11 57 15		xxxx xxxx	
11 68 16	Flag	0111 1110	Drapeau de fin

DSC_58 Lorsque la *DSRC-VU* reçoit la demande ECHO, elle envoie une réponse ECHO sur 100 octets de données en reflétant la commande reçue, conformément aux dispositions de la norme ISO 14906, sans paramétrage RTM spécifique. Le tableau 14.16 montre 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 la VU 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	Non utilisé
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
115		xxxx xxxx	
116	Flag	0111 1110	Drapeau de fin

5.5 Conformité à la directive 2015/71/CE

5.5.1 Vue d'ensemble

DSC_59 Pour respecter la directive (UE) 2015/719 sur les poids et les dimensions maximaux des poids lourds, le protocole de transaction de téléchargement des données OWS utilisant la liaison d'interface DSRC 5,8 GHz est le même que celui servant aux données RTM (cf. 5.4.1). La seule différence réside dans le fait

que l'identificateur d'objet associé à la norme TARV respecte la norme ISO 15638 (TARV) partie 20 concernant les WOB/OWS.

5.5.2 Commandes

DSC_60 Les commandes servant à une transaction OWS sont identiques à celles utilisées pour une transaction RTM.

5.5.3 Séquence de commande d'interrogation

DSC_61 La séquence de commande d'interrogation concernant les données OWS est identique à celle concernant les données RTM.

5.5.4 Structures de données

DSC_62 Les données utiles (données OWS) correspondent à la concaténation des données:

1. EncryptedOwsPayload, qui correspondent au cryptage de OwsPayload tel que défini en ASN.1 à la section 5.5.5. La méthode de cryptage est identique à celle adoptée pour RtmData, spécifiée à l'appendice 11;
2. DSRCSecurityData, calculées avec les mêmes algorithmes que pour RtmData, dont les spécifications se trouvent à l'appendice 11.

5.5.5 Module ASN.1 de la transaction DSRC OWS

DSC_63. Le module ASN.1 concernant les données DSRC dans l'application RTM est défini comme suit:

```
TarvOws {iso(1) standard(0) 15638
part20(20) version1(1)} DEFINITIONS
AUTOMATIC TAGS
::= BEGIN
IMPORTS
-- Imports data attributes and elements from EFC which are used for OWS
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition
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)};

-- Definitions of the OWS functions:
OWS-InitialiseComm-Request ::= BST
OWS-InitialiseComm-Response::= VST
OWS-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid,
accessCredentials ABSENT, iid ABSENT, attrIdList})
```

```
   OWS-DataRetrieval-Response::= Get-Response {OwsContainer} (WITH COMPONENTS {..., eid,
   iid ABSENT})
   OWS-TerminateComm::= Event-Report-Request {OwsContainer}(WITH COMPONENTS {mode (FALSE),
   eid (0),
   eventType (0)})
   OWS-TestComm-Request::= Action-Request {OwsContainer} (WITH COMPONENTS {..., eid (0),
   actionType
   (15), accessCredentials ABSENT, iid ABSENT})
   OWS-TestComm-Response::= Action-Response {OwsContainer} (WITH COMPONENTS {..., fill
   (SIZE(1)), eid
   (0), iid ABSENT})

   -- Definitions of the OWS attributes:
   OwsData :: = SEQUENCE {
    encryptedOwsPayload OCTET STRING (SIZE(51)) (CONSTRAINED BY { -- calculated
   encrypting OwsPayload as per Appendix 11 --}),
    DSRCSecurityData OCTET STRING
    }
   OwsPayload :: = SEQUENCE {
             tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN
   15509.
             recordedWeight INTEGER (0..65535),         -- 0= Total measured weight of
   the  heavy goods vehicle
             -- with 10 Kg resolution.
             axlesConfiguration OCTET STRING SIZE (3),  -- 0= 20 bits allowed for the
   number                                                                          -
   - of axles for 10 axles.
             axlesRecordedWeight OCTET STRING SIZE (20), -- 0= Recorded Weight for each
   axle
                                                          -- with 10 Kg resolution.
             tp15638Timestamp            INTEGER(0..4294967295)-- Timestamp of current
   record
    }

Ows-ContextMark ::= SEQUENCE {
 standardIdentifier      StandardIdentifier, -- identifier of the TARV part and its
 version
         }

StandardIdentifier ::= OBJECT IDENTIFIER
 OwsContainer ::= 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},
    reserved10                  [10]   NULL,
```

```
    OwsContextmark              [11]   Ows-ContextMark,
    OwsData                     [12]   OwsData,
    reserved13                  [13]   NULL,
    reserved14                  [14]   NULL,
    time                        [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
    }}

END
```

5.5.6 Éléments OwsData, actions effectuées et définitions

Les éléments OwsData sont définis de manière à satisfaire aux dispositions de la directive (UE) 2015/719 relative aux poids et aux dimensions maximaux des poids lourds. Leur signification est la suivante:

- recordedWeight représente le poids total mesuré du poids lourd avec une résolution de 10 kg, tel que défini par la norme EN ISO 14906. Par exemple, une valeur de 2500 représente un poids total de 25 tonnes.
- axlesConfiguration représente la configuration du poids lourd en termes de nombre d'essieux. La configuration est définie par le masque de bit de 20 bits (étendu à partir de la norme EN ISO 14906). Un masque de deux bits représente la configuration d'un essieu, selon la structure suivante:
    - La valeur 00B signifie que la valeur est «indisponible» parce que le véhicule ne possède pas l'équipement permettant de mesurer le poids à l'essieu.
    - La valeur 01B signifie que l'essieu est absent.
    - La valeur 10B signifie que l'essieu est présent et que le poids a été calculé et collecté et qu'il est communiqué dans le champ axlesRecordedWeight
    - La valeur 11B est réservée à de futures utilisations.

  Les quatre derniers bits sont réservés à des utilisations ultérieures.

Nombre d'essieux										
Nombre d'essieux dont est pourvu le tracteur			Nombre d'essieux dont est pourvue la remorque							
00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	
										RFU (4 bits)

- axlesRecordedWeight représente le poids spécifique enregistré pour chaque essieu avec une résolution de 10 kg. Deux octets servent à chaque essieu. Par exemple, une valeur de 150 représente un poids total de 1 500 kg.

Les autres types de données sont définis en 5.4.5.

5.5.7 Mécanismes de transfert de données

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 (cf. 5.4.6).

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 5.6.

5.6 Transfert de données entre la DSRC-VU et la VU

5.6.1 Connexion physique et interfaces

DSC_66 La connexion entre la *VU* et la *DSRC-VU* peut être établie soit par un câble physique, soit par le biais d'une communication sans fil de courte portée reposant sur le protocole Bluetooth v4.0 BLE.

DSC_67 Indépendamment du choix de la connexion physique et de l'interface, les exigences suivantes doivent être satisfaites:

DSC_68 a) Pour que la fourniture de la VU et de la DSRC-VU, voire de différents lots de la DSRC-VU, puisse être sous-traitées à plusieurs fournisseurs, la connexion reliant la VU et la DSRC-VU doit être une connexion ouverte normalisée. La VU doit être connectée à la DSRC-VU:

i) via un câble fixe de 2 mètres au minimum avec un connecteur mâle homologué à 11 broches Straight DIN 41612 H11 sur la DSRC-VU, s'emboîtant dans un connecteur femelle homologué DIN/ISO correspondant sur la VU;

ii) via Bluetooth Low Energy (BLE); ou

iii) via une connexion normalisée ISO 11898 ou SAE J1939.

DSC_69 b) la définition des interfaces et de la connexion entre la VU et la DSRC-VU doit être compatible avec les commandes du protocole d'application définies à la section 5.6.2 et

DSC_70 c) la VU et la DSRC-VU doivent permettre l'opération de transfert de données par la connexion en termes de performance et d'alimentation électrique.

5.6.2 Protocole d'application

DSC_71 Le protocole d'application entre le dispositif de communication à distance de la VU et la DSRC-VU est responsable du transfert régulier des données de communication à distance de la VU vers le DSRC.

DSC_72 Les principales commandes suivantes sont identifiées:

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 les données RTM
4. Accusé de réception de 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. Les commandes sont adressées par la VU à la DSRC-VU. Le LinkIdentifier est défini par la VU et communiqué à la DSRC-VU pour suivre une liaison de communication spécifique.
  (Note: cela permet d'assurer la prise en charge de liaisons ultérieures et d'autres applications ou d'autres modules comme la pesée à bord).
- `RCDT-Communication Link Initialization – Response` sert à la DSRC-VU pour fournir la réponse à la demande d'initialiser la liaison de communication. La commande est adressée par la DSRC-VU à la VU. La commande fournit le résultat de l'initialisation à titre de réponse = 1 (Réussite) ou =0 (Échec).

DSC_75 L'initialisation de la liaison de communication a lieu après l'installation, l'étalonnage et le démarrage du moteur ou de la VU

.

- `RCDT - Send Data` sert à la VU pour envoyer les RCDTData signées (c'est-à-dire, les *données de communication à distance*) à la DSRC-VU. Les données sont envoyées toutes les 60 secondes. Le paramètre DataTransactionId identifie la transmission spécifique de données. Le LinkIdentifier sert également à faire en sorte que la liaison appropriée soit correcte.
- `RCDT - Data Acknowledgment` est envoyé par la DSRC-VU pour apporter un retour à la VU quant à la réception des données à partir d'une commande `RCDT - Send Data` identifiée par le paramètre DataTransactionId. Le paramètre de réponse est 1 (Réussite) ou 0 (Échec). Si une VU reçoit plus de trois réponses égales à 0 ou si la VU ne reçoit pas de RCDT Data Acknowledgment pour un RCDT - Send Data antérieur avec un DataTransactionId spécifique, la VU génère et mémorise un événement.
- `RCDT-Communication Link Termination request` est envoyé par la VU à la DSRC-VU pour mettre fin à une liaison avec un LinkIdentifier spécifique.

DSC_76 Au redémarrage de la DSRC-VU ou d'une VU, il est nécessaire de supprimer toutes les liaisons de communication existantes, car il pourrait demeurer des liaisons «fantômes» du fait de la coupure brutale d'une VU.

- `RCDT-Communication Link Termination – Response` est envoyé par la DSRC-VU à la VU pour confirmer la demande de fin de la liaison de la VU pour le LinkIdentifier spécifique.

5.7 Traitement des erreurs

5.7.1 Enregistrement et communication des données dans la DSRC-VU

DSC_77 *Les données* sont fournies déjà sécurisées par la fonction *VUSM* à la *DSRC-VU*. La *VUSM* vérifie que les données enregistrées dans la *DSRC-VU* le sont de manière satisfaisante. L'enregistrement et le

signalement de toutes les erreurs survenues pendant le transfert de données depuis la *VU* vers la mémoire de la *DSRC-VU* doivent être consignés avec le type EventFaultType et la valeur enum d'erreur de communication '62'H Dispositif de communication à distance, accompagnées de l'horodatage.

DSC_78 La *VU* tient à jour un fichier identifié par un intitulé unique aisément identifiable par les inspecteurs aux fins de l'enregistrement des «Anomalies de communication internes à la VU».

DSC_79 Si la VUPM tente d'obtenir les données VU du module de sécurité (pour les transférer à la DSRC-VU), mais échoue, elle doit mémoriser cet échec avec le type EventFaultType et la valeur enum d'erreur de communication *'62'H Dispositif de communication à distance*, ainsi que l'horodatage. L'anomalie de communication est détectée lorsque, plus de trois fois consécutives, un message `RCDT Data Acknowledgment` n'est pas reçu pour le `RCDT Send Data` correspondant (c'est-à-dire muni du même DataTransactionId `dans les messages Send Data et Acknowledgment`).

5.7.2 Anomalies de communication sans fil

DSC_80 La gestion des anomalies de communication est cohérente avec les dispositions des normes DSRC, à savoir EN 300 674-1, EN 12253, EN 12795, EN 12834 et les paramètres appropriés de la norme EN 13372.

5.7.2.1 Anomalies de cryptage et de signature

DSC_81 Les anomalies de cryptage et de signature sont gérées conformément aux dispositions de l'appendice 11 Mécanismes communs de sécurité et ne figurent pas dans les messages d'erreur associés au transfert de données DSRC.

5.7.2.2 Relevé des anomalies

Le support DSRC désigne une communication sans fil dynamique dans un environnement marqué par des conditions atmosphériques et d'interférences incertaines, en particulier dans les cas où sont combinés le REDCR portable et le véhicule en circulation impliqués dans cette application. Il est donc nécessaire de distinguer une «anomalie de lecture» d'une condition d'«erreur». Dans une transaction avec une interface sans fil, l'anomalie de lecture est courante et entraîne habituellement une nouvelle tentative, c'est-à-dire la rediffusion de la BST et une nouvelle tentative de séquence, qui dans la plupart des cas mènent à une connexion de communication réussie et au transfert des données, sauf si le véhicule ciblé devient hors portée pendant le temps nécessaire à la retransmission. (Une instance «réussie» de «lecture» peut requérir plusieurs tentatives).

L'anomalie de lecture peut provenir du fait que les antennes ne sont pas appairées correctement (anomalie de «visée»); du fait que l'une des antennes est blindée – de manière délibérée ou à cause de la présence physique d'un autre véhicule; d'interférences radio, en particulier à proximité de communications WIFI autour de 5,8 GHz ou d'autres types de communication sans fil d'accès public; ou de l'interférence avec des radars ou encore du fait des conditions atmosphériques (p. ex. pendant un orage); ou simplement en raison d'un déplacement hors de la portée de la communication DSRC. Les cas individuels d'anomalies de lecture, par essence, ne peuvent pas faire l'objet d'un relevé. En effet, la communication n'a pas eu lieu.

Cependant, si l'agent des autorités de contrôle compétentes cible un véhicule et tente d'interroger sa *DSRC-VU*, mais qu'aucun transfert de données n'aboutit, cette anomalie peut s'expliquer par une falsification délibérée. Par conséquent, l'agent des autorités de contrôle compétentes a besoin d'un moyen de consigner l'anomalie et d'alerter ses collègues en aval d'un risque d'infraction. Les collègues peuvent intercepter le véhicule et procéder à une inspection physique. Toutefois, aucune communication n'ayant abouti, la DSRC-VU ne peut fournir aucune donnée concernant cette anomalie. Ce type de rapport doit donc être une fonction intégrée à la conception de l'équipement du REDCR.

L'«anomalie de lecture» est techniquement différente d'une «erreur». Dans ce contexte, une «erreur» désigne l'acquisition d'une valeur fausse.

Les données transférées à la *DSRC-VU* sont fournies déjà sécurisées et doivent donc faire l'objet d'une vérification par le fournisseur de données (cf. 5.4).

Les données transférées ultérieurement par l'interface aérienne sont soumises à des contrôles de redondance cyclique au niveau de la communication. Si le CRC les valide, les données sont exactes. Si le CRC ne les valide pas, les données sont transmises à nouveau. La probabilité que des données erronées passent à travers un contrôle CRC est tellement faible qu'elle peut être ignorée.

Si le CRC ne valide pas les données et que le temps manque pour procéder à une retransmission et à une réception des données exactes, la situation n'entraîne pas une erreur, mais une instanciation d'une catégorie spécifique d'anomalie de lecture.

Les seules données d'«anomalie» significatives qui peuvent être enregistrées sont le nombre d'initiations de transactions réussies qui ne se concluent pas par un transfert des données au REDCR.

DSC_82 Le *REDCR* doit donc mémoriser et horodater 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 REDCR. Ces données sont disponibles pour l'agent des autorités de contrôle compétentes et sont enregistrées dans la mémoire de l'équipement REDCR. Les moyens d'y parvenir relèvent de la conception du produit ou de la spécification des autorités de contrôle compétentes.

Les seules données d'«erreur» significatives qui peuvent être enregistrées sont le nombre de fois où le REDCR échoue à décrypter *les données* reçues. Cependant, il est à noter que cela ne concerne que l'efficience du logiciel REDCR. Les données peuvent être décryptées techniquement, mais pas interprétées du point de vue sémantique.

DSC_83 Le *REDCR* enregistre et horodate par conséquent le nombre de tentatives infructueuses de décryptage des données reçues par l'interface DSRC.

6 Mise en service et essais d'inspection périodiques relatifs à la fonction de communication à distance

6.1 Généralités

DSC_84 Deux catégories d'essais sont prévues pour la fonction de communication à distance:

1) Un essai ECHO pour valider le canal de communication sans fil *DSRC-REDCR* >>-:-< *DSRC-VU*.
2) Un essai de sécurité de bout en bout pour s'assurer qu'une carte d'atelier est en mesure d'accéder au contenu de données signées et cryptées créé par la VU et transmis à l'aide du canal de communication sans fil.

6.2 ECHO

La présente section contient des dispositions spécifiques pour vérifier uniquement l'activité fonctionnelle de la liaison *DSRC-REDCR* >>-:-<*DSRC-VU*.

L'objectif de la commande ECHO est de permettre aux ateliers ou aux infrastructures d'essai d'homologation de vérifier que la liaison DSRC fonctionne sans devoir accéder aux éléments d'authentification de sécurité. L'équipement d'essai doit donc uniquement être en mesure d'initialiser une communication DSRC (envoi d'une BST avec AID = 2), d'envoyer la commande ECHO et, dans l'hypothèse où la communication DSRC fonctionne, de recevoir la réponse ECHO. Cf. 5.4.8 pour davantage de détails. Dans l'hypothèse où cette réponse est reçue correctement, le fonctionnement de la liaison DSRC (*DSRC-REDCR* >>-:-< *DSRC-VU*) peut être validé comme satisfaisant.

6.3 Essais de validation du contenu des données sécurisées

DSC_85 Cet essai sert à valider le flux de données de bout en bout sur le plan de la sécurité. Il est nécessaire de disposer d'un lecteur d'essai DSRC pour procéder à cet essai. Le lecteur d'essai DSRC assure les mêmes fonctionnalités et est mis en œuvre selon les mêmes spécifications que le lecteur utilisé par les agents de la force publique, avec une seule différence, à savoir qu'une carte d'atelier est utilisée pour authentifier l'utilisateur du lecteur, plutôt qu'une carte de contrôle. Il est possible de procéder à cet essai 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 à la DSRC-VU les données sécurisées de détection précoce.

DSC_86 Le personnel d'atelier doit placer le lecteur d'essai DSRC à une distance située entre 2 et 10 mètres devant le véhicule.

DSC_87 Le personnel d'atelier doit ensuite insérer une carte d'atelier dans le lecteur d'essai DSRC pour adresser une interrogation portant sur les données de détection précoce à l'unité embarquée sur le véhicule. Après une interrogation réussie, le personnel d'atelier accède aux données reçues pour vérifier que leur intégrité et leur décryptage sont validés.

FR

APPENDICE 15

MIGRATION: GERER LA COEXISTENCE DE PLUSIEURS GENERATIONS D'EQUIPEMENTS

TABLE DES MATIERES

1. Définitions

Aux fins du présent appendice, les définitions suivantes sont applicables:

tachygraphe intelligent: tel que défini à la présente annexe (chapitre 1: définition bbb);

tachygraphe de première génération: tel que défini par le présent règlement (article 2: définition 1);

tachygraphe de deuxième génération: tel que défini par le présent règlement (article 2: définition 7);

date d'introduction: telle que définie dans la présente annexe (chapitre 1: définition ccc);

équipement spécialisé intelligent (IDE): équipement servant à télécharger des données, comme défini à l'appendice 7 de la présente annexe.

2. Dispositions générales

2.1. Présentation de la transition

Le préambule de la présente annexe présente la transition de la première à la deuxième génération de tachygraphes.

Outre les dispositions de ce préambule:

- La première génération de capteurs de mouvement ne sera pas interopérable avec la deuxième génération d'unités embarquées sur les véhicules.
- L'installation de la deuxième génération des capteurs de mouvement sur les véhicules commencera en même temps que celle de la deuxième génération d'unités embarquées sur les véhicules.
- le téléchargement de données et l'équipement d'étalonnage devront évoluer pour être compatibles avec les deux générations d'équipement d'enregistrement et de cartes tachygraphiques.

2.2. Interopérabilité entre les unités embarquées sur les véhicules et les cartes

Il est entendu que la première génération de cartes tachygraphiques est interopérable avec la première génération d'unités embarquées sur les véhicules (conformément à l'annexe 1B de la présente directive), alors que la deuxième génération de cartes tachygraphiques est interopérable avec la deuxième génération d'unités embarquées sur les véhicules (conformément à l'annexe 1C de la présente directive). De plus, les exigences ci-dessous s'appliquent.

MIG_001 Hormis les dispositions prévues aux exigences MIG_004 et MIG_005, les cartes tachygraphiques de première génération peuvent continuer à être utilisée dans les unités embarquées sur les véhicules de deuxième génération jusqu'à expiration de leur validité. Leurs détenteurs peuvent toutefois demander leur replacement par des cartes tachygraphiques de deuxième génération dès que ces dernières sont disponibles.

MIG_002 Les unités embarquées sur des véhicules de deuxième génération pourront utiliser toute carte de conducteur, de contrôleur et d'entreprise valides de première génération qui auront été insérés.

MIG_003 Les ateliers pourraient supprimer définitivement cette possibilité dans lesdites unités embarquées sur les véhicules, de sorte que la première génération de cartes tachygraphiques ne serait plus acceptée. Cela ne pourrait avoir lieu qu'après que la Commission européenne ait lancé une procédure visant à demander aux ateliers de procéder ainsi, par exemple, lors de chaque inspection périodique du tachygraphe.

MIG_004 La deuxième génération d'unités embarquées sur des véhicules ne pourra utiliser que des cartes d'ateliers de deuxième génération.

MIG_005 Pour déterminer le mode de fonctionnement de la deuxième génération d'unités embarquées sur les véhicules, il suffira de consulter les types de cartes valides insérées, indépendamment de leur génération.

MIG_006 Toute carte tachygraphique de deuxième génération valide pourra être utilisée sur des unités embarquées de première génération exactement de la même manière qu'une carte tachygraphique de première génération de type identique.

2.3. Interopérabilité entre les unités embarquées sur les véhicules 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 sur les véhicules, et que la deuxième génération de capteurs de mouvement est interopérable avec la deuxième génération d'unités embarquées sur les véhicules. De plus, les exigences ci-dessous s'appliquent.

MIG_007 Les unités embarquées sur les véhicules de deuxième génération ne pourront pas être couplées et utilisées les capteurs de mouvement de première génération.

MIG_008 Les capteurs de mouvement de deuxième génération pourront être couplés et utilisés soit uniquement avec des unités embarquées sur les véhicules de deuxième génération, soit avec les deux générations d'unités embarquées sur les véhicules.

2.4. Interopérabilité entre les unités embarquées sur les véhicules, les cartes tachygraphiques et l'équipement de téléchargement de données

MIG_009 L'équipement de téléchargement de données peut être utilisé avec une seule génération d'unités embarquées sur des véhicules et de cartes tachygraphiques ou avec les deux.

2.4.1 Téléchargement direct de carte par IDE

MIG_010 Les données sont téléchargées par IDE depuis les cartes tachygraphiques d'une génération qui ont été insérées dans les lecteurs de cartes, selon les mécanismes de sécurité et les protocoles de téléchargement des données de cette génération, et les données téléchargées sont au format défini pour ladite génération.

MIG_011 Pour permettre le contrôle des conducteurs par des autorités de contrôles autres que celles de l'UE, il sera également possible de télécharger des cartes de conducteurs (et d'ateliers) de deuxième génération de la même manière que les cartes de conducteurs (et d'ateliers) de première génération. Ce type de téléchargement inclura:

- des EF (fichiers élémentaires) `IC` et `ICC` non signés,
- des EF (de première génération) `Card_Certificate` et `CA_Certificate` non signés,
- d'autres EF de données d'application (au sein du DF (fichier spécialisé) `TACHO`) nécessaires au protocole de téléchargement des cartes de première génération. Ces informations seront protégées par une signature numérique conformément aux mécanismes de sécurité de première génération.

Ce type de téléchargement n'inclura pas d'EF de données d'application uniquement présents sur les cartes de lecteurs (et d'ateliers) de deuxième génération (EF de données d'application au sein du DF `TACHO_G2`).

2.4.2 Téléchargement de carte via une unité embarquée sur un véhicule

MIG_012 Les données sont téléchargées depuis une carte de deuxième génération insérée dans une unité embarquée sur un véhicule de première génération selon le protocole de téléchargement de données de la première génération. La carte réagira aux commandes de l'unité embarquée sur le véhicule exactement de la même manière qu'une carte de première génération. Les données téléchargées auront le même format que les données téléchargées depuis une carte de première génération.

MIG_013 Les données sont téléchargées depuis une carte de première génération insérée dans une unité embarquée sur un véhicule de deuxième génération selon le protocole de téléchargement de données défini à l'appendice 7 de la présente annexe. L'unité embarquée sur le véhicule adressera des commandes à la carte exactement de la même manière qu'une unité embarquée sur un véhicule de première génération. Les données téléchargées auront le format défini pour les cartes de première génération.

2.4.3 Téléchargement d'unité embarquée sur un véhicule

MIG_014 Les données sont téléchargées depuis une unité embarquée sur un véhicule de deuxième génération selon les mécanismes de sécurité de deuxième génération et le protocole de téléchargement de données défini à l'appendice 7 de la présente annexe.

MIG_015 Pour permettre le contrôle des conducteurs par des autorités de contrôles autres que celles de l'UE et le téléchargement de données des unités embarquées sur les véhicules par des ateliers autres que ceux de l'UE, il peut également être rendu possible de télécharger des données depuis des unités embarquées sur des véhicules de deuxième génération selon les mécanismes de sécurité de première génération et le protocole de téléchargement de données de première génération. Les données téléchargées auront le même format que les données téléchargées depuis une unité embarquée sur un véhicule de première génération. Cette fonctionnalité peut être sélectionnée grâce aux commandes du menu.

2.5. Interopérabilité entre les unités embarquées sur les véhicules et l'équipement d'étalonnage

MIG_016 L'équipement d'étalonnage pourra procéder à l'étalonnage de chaque génération de tachygraphe selon le protocole d'étalonnage de cette génération. L'équipement d'étalonnage peut être utilisé avec une seule génération 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 la date d'introduction.

MIG_018 Les essais d'interopérabilité seront prêts à commencer sur demande des fabricants au plus tard **15 mois** avant la date d'introduction.

MIG_019 Les clés et les certificats officiels seront à la disposition des fabricants au moins **12 mois** avant la date d'introduction.

MIG_020 Les États membres pourront émettre des cartes d'ateliers de deuxième génération au plus tard **3 mois** avant la date d'introduction.

MIG_021 Les États membres pourront émettre tous les types de cartes tachygraphiques de deuxième génération au plus tard **1 mois avant le lancement**.

4. Dispositions relatives à la période qui suit le lancement

MIG_022 Après la date d'introduction, les États membres n'émettront que des cartes tachygraphiques de deuxième génération.

MIG_023 Les fabricants d'unités embarquées sur un véhicule ou de capteurs de mouvement seront autorisés à produire des unités embarquées sur un véhicule ou des capteurs de mouvement de première génération tant qu'ils resteront utilisés sur le terrain, de façon à pouvoir remplacer les composants qui dysfonctionneraient.

MIG_024 Les fabricants d'unités embarquées sur un véhicule ou de capteurs de mouvement seront autorisés à demander et à obtenir le maintien de l'homologation pour des unités embarquées sur un véhicule ou des capteurs de mouvement de première génération dont le type est déjà homologué.

FR

APPENDICE 16 ADAPTATEUR POUR LES VÉHICULES DES TYPES M 1 ET N1

Table des matières

1. Abréviations et documents de référence

1.1. Abréviations

À déf. À définir

VU Unité embarquée sur le véhicule (*Vehicle Unit*)

1.2. Normes de référence

ISO 16844-3 Véhicules routiers — Systèmes tachygraphiques — Partie 3: Interface des capteurs de mouvement

2. Caractéristiques générales et fonctions de l'adaptateur

2.1. Description générale de l'adaptateur

ADA_001 L'adaptateur fournit une VU connectée avec 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 munis d'un appareil de contrôle conformément au présent règlement.

Il est installé et utilisé uniquement dans les types de véhicule définis au point yy) «adaptateur», lorsqu'il n'est pas mécaniquement possible d'installer un autre type de capteur de mouvement existant conforme par ailleurs aux dispositions de la présente annexe et de ses appendices 1 à 16.

L'adaptateur n'est pas mécaniquement connecté à un élément mobile du véhicule mais 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 IC, section 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 générant des impulsions entrantes dirigées vers le capteur de mouvement intégré. Le capteur de mouvement intégré lui-même est connecté à la VU, si bien que l'interface entre la VU 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 la VU.

2.3. Sécurité

ADA_004 La sécurité de l'adaptateur n'est pas certifiée conforme aux objectifs de sécurité générique du capteur de mouvement définis à l'appendice 10 de la présente annexe, mais conforme aux exigences de sécurité spécifiées au point 4.4 du présent appendice.

3. Exigences relatives à l'appareil de contrôle lorsqu'un adaptateur est installé

Les exigences figurant dans le présent chapitre et dans les chapitres suivants indiquent comment les exigences énoncées dans la présente annexe doivent être comprises lorsqu'un adaptateur est utilisé. Les numéros des exigences 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, sauf indications contraires dans le présent appendice.

ADA_006 Lorsqu'un adaptateur est installé, l'appareil de contrôle comporte des câbles, l'adaptateur (comprenant un capteur de mouvement) et une VU (01).

ADA_007 La fonction de détection d'événements et/ou d'anomalies de l'appareil de contrôle est modifiée comme suit:

- l'événement «coupure d'alimentation» est déclenché par la VU, lorsqu'elle n'est pas en mode étalonnage, en cas d'interruption de l'alimentation électrique du capteur de mouvement intégré (79) dépassant 200 millisecondes (ms);
- l'événement «erreur sur les données de mouvement» est déclenché par la VU en cas d'interruption du flux de données normal entre le capteur de mouvement intégré et la VU et/ou en cas d'anomalie d'intégrité ou d'authentification de données au cours de l'échange de données entre le capteur de mouvement intégré et la VU (83);
- l'événement «tentative d'atteinte à la sécurité» est déclenché par la VU pour tout autre événement affectant la sécurité du capteur de mouvement intégré, lorsqu'il n'est pas en mode étalonnage (85),
- l'anomalie «appareil de contrôle» est déclenchée par la VU, lorsqu'elle n'est pas en mode 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 la VU permet de coupler automatiquement le capteur de mouvement intégré à la VU (202, 204).

4. Exigences de construction et de fonctionnement de l'adaptateur

4.1. Connexion et adaptation des impulsions de vitesse entrantes

ADA_011 L'interface d'entrée de l'adaptateur accepte des impulsions de fréquences représentatives de la vitesse du véhicule et de la distance parcourue. Les caractéristiques électriques des impulsions entrantes sont: *à déf. 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 la fourchette de valeurs du facteur k définie dans la présente annexe (4 000 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 manière 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 la VU 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 doit être inviolable. Il est scellé de manière à ce que toute tentative de manipulation soit aisément décelable (par exemple, lors d'une inspection visuelle, voir ADA_035). Les scellements répondent 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 ni sans rompre 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 extraites qu'à partir de l'entrée de l'adaptateur.

4.5. Caractéristiques de performance

ADA_020 L'adaptateur fonctionne correctement dans la fourchette de températures définie par le fabricant.

ADA_021 L'adaptateur fonctionne correctement dans une fourchette de taux d'humidité allant de 10 % à 90 % (214).

ADA_022 L'adaptateur est protégé contre les surtensions, l'inversion de polarités 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 ces circonstances, l'unité embarquée enregistrera et stockera une anomalie du capteur (88),

soit posséder un élément de détection qui soit protégé des champs magnétiques ou insensible à ceux-ci (217).

ADA_024 L'adaptateur est conforme à la réglementation internationale R10 de la CEE-ONU, relative à la compatibilité électromagnétique, et est protégé contre les décharges électrostatiques et les transitoires (218).

4.6. Matériaux

ADA_025 L'adaptateur satisfait au niveau de protection (*à déf. par le fabricant, en fonction de la position de l'installation*) (220, 221).

ADA_026 Le boîtier de l'adaptateur est jaune.

4.7. Inscriptions

ADA_027 Une plaque signalétique est fixée sur l'adaptateur et comporte 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 de l'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 comporte aussi 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 sur les véhicules le sont uniquement par des fabricants de véhicules ou par des ateliers agréés autorisés à installer, activer et calibrer les tachygraphes numériques et intelligents.

ADA_030 L'atelier agréé qui installe l'adaptateur ajuste 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 est 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 est scellé (voir ADA_017);
- le boîtier du capteur intégré est 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 est scellé au véhicule;
- la connexion entre l'adaptateur et l'équipement qui lui fournit ses impulsions d'entrée est 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 1C) de l'appareil de contrôle comporte 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 indiqué 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 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 est soumis pour homologation tout entier, muni de l'adaptateur (425).

ADA_038 Tout adaptateur peut être soumis pour homologation en tant que tel ou en tant que composant d'un appareil de contrôle.

ADA_039 Cette homologation doit inclure des essais fonctionnels portant sur l'adaptateur. Les résultats positifs de chacun de ces essais sont établis par un certificat approprié (426).

7.2. Certificat fonctionnel

ADA_040 Le certificat fonctionnel de l'adaptateur ou de l'appareil de contrôle comportant un adaptateur n'est délivré au fabricant de l'adaptateur que si les essais fonctionnels minimaux suivants ont été passés avec succès.

N°	*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 avec la documentation	
2.2.		Identification / marquages 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 menés par le fabricant	Résultats des essais environnementaux du fabricant	ADA_020, ADA_021, ADA_022, ADA_024
5.			**Essais de compatibilité électromagnétique**

N°	*Essai*	*Description*	*Exigences connexes*
5.1	Émissions rayonnées et susceptibilité	S’assurer de la conformité avec la directive 2006/28/CE	ADA_024
5.2	Résultats des essais menés par le fabricant	Résultats des essais environnementaux du fabricant	ADA_024