II

(Actes non législatifs)

RÈGLEMENTS

RÈGLEMENT D'EXÉCUTION (UE) 2018/502 DE LA COMMISSION

du 28 février 2018

modifiant le règlement d'exécution (UE) 2016/799 fixant les exigences applicables à la construction, aux essais, à l'installation, à l'utilisation et à la réparation des tachygraphes et de leurs composants

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) n° 165/2014 du Parlement européen et du Conseil du 4 février 2014 relatif aux tachygraphes dans les transports routiers ([1]), et notamment son article 11 et son article 12, paragraphe 7,

considérant ce qui suit:

(1) Le règlement (UE) n° 165/2014 a instauré le tachygraphe intelligent, tachygraphe numérique de deuxième génération connecté au système mondial de navigation par satellite (ci-après «GNSS») et comprenant un dispositif de communication à distance à des fins de détection précoce et une interface facultative avec les systèmes de transport intelligents.

(2) Les exigences techniques applicables à la construction, aux essais, à l'installation, à l'utilisation et à la réparation des tachygraphes et de leurs composants sont définies dans le règlement d'exécution (UE) 2016/799 de la Commission ([2]).

(3) Conformément aux articles 8, 9 et 10 du règlement (UE) n° 165/2014, les tachygraphes installés dans les véhicules immatriculés pour la première fois le 15 juin 2019 ou après cette date doivent être des tachygraphes intelligents. Il convient, dès lors, de modifier le règlement d'exécution (UE) 2016/799 afin que les dispositions techniques qu'il arrête s'appliquent à partir de cette date.

(4) Pour assurer la conformité avec l'article 8 du règlement (UE) n° 165/2014, qui prévoit que la position du véhicule doit être enregistrée toutes les trois heures de temps de conduite accumulé, le règlement d'exécution (UE) 2016/799 devrait être modifié de manière à permettre le stockage d'informations sur la position du véhicule à intervalles de trois heures, au moyen d'une métrique qui ne peut pas être réinitialisée, et à éviter toute confusion avec le «temps de conduite sans interruption», qui est une métrique remplissant une autre fonction.

(5) L'unité embarquée sur le véhicule peut se présenter sous la forme d'un seul élément ou de plusieurs composants répartis dans le véhicule. Par conséquent, le GNSS et la communication spécialisée à courte portée (DSRC) pourraient être pris en charge par des dispositifs internes ou externes à l'élément principal de l'unité embarquée. Lorsque ces deux dispositifs sont externes, il devrait être possible de les homologuer, ainsi que l'élément principal de l'unité embarquée sur le véhicule, en tant que composants afin d'adapter le processus d'homologation du tachygraphe intelligent aux besoins du marché.

(6) Il convient de modifier les règles relatives au stockage des événements «Conflit temporel» et les remises à l'heure afin d'établir une distinction entre, d'une part, les remises à l'heure automatiques déclenchées par d'éventuelles tentatives de manipulation ou un dysfonctionnement du tachygraphe et, d'autre part, les remises à l'heure provoquées par d'autres interventions, comme un entretien.

(7) Les identificateurs de données devraient pouvoir opérer une distinction entre les données téléchargées depuis un tachygraphe intelligent et les données téléchargées depuis un tachygraphe d'une génération antérieure.

([1]) JO L 60 du 28.2.2014, p. 1.

([2]) Règlement d'exécution (UE) 2016/799 de la Commission du 18 mars 2016 mettant en œuvre le règlement (UE) n° 165/2014 du Parlement européen et du Conseil en ce qui concerne les exigences applicables à la construction, aux essais, à l'installation, à l'utilisation et à la réparation des tachygraphes et de leurs composants (JO L 139 du 26.5.2016, p. 1).

(8) La période de validité d'une carte d'entreprise doit être portée à cinq ans, au lieu de deux, pour qu'elle corresponde à celle de la carte de conducteur.

(9) La description de certaines anomalies et événements, la validation de la saisie du lieu de début et/ou de fin de la période de travail journalière, l'utilisation du consentement du conducteur pour l'interface ITS (système de transport intelligent) en ce qui concerne les données transmises par l'unité embarquée sur le véhicule par l'intermédiaire du réseau du véhicule, ainsi que d'autres aspects techniques, devraient être mieux circonscrits.

(10) Pour garantir que la certification des scellements du tachygraphe est à jour, il y a lieu de les adapter à la nouvelle norme de sécurité des scellements mécaniques apposés sur les tachygraphes.

(11) Le présent règlement s'applique à la construction, aux essais, à l'installation et à l'utilisation de systèmes comprenant également des équipements radioélectriques relevant de la directive 2014/53/UE du Parlement européen et du Conseil ([1]). Cette dernière régit de manière horizontale la mise sur le marché et la mise en service d'équipements électriques et électroniques utilisant des ondes radioélectriques à des fins de communication et/ou de radiorepérage, notamment en ce qui concerne la sécurité électrique, la compatibilité avec les autres systèmes, l'accès au spectre radioélectrique, l'accès aux services d'urgence et/ou d'autres dispositions de délégation. Pour garantir l'utilisation efficiente du spectre radioélectrique, prévenir les perturbations radioélectriques, assurer la sécurité et la compatibilité électromagnétique des équipements radioélectriques et satisfaire à toute autre exigence spécifique faisant l'objet d'une délégation, le présent règlement devrait être sans préjudice de ladite directive.

(12) Il y a lieu, dès lors, de modifier le règlement d'exécution (UE) 2016/799.

(13) Les mesures prévues par le présent règlement sont conformes à l'avis du comité visé à l'article 42, paragraphe 3, du règlement (UE) n° 165/2014,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Le règlement d'exécution (UE) 2016/799 est modifié comme suit:

1) l'article 1er est modifié comme suit:

a) les paragraphes 2 et 3 sont remplacés par le texte suivant:

«2. La construction, les essais, l'installation, l'inspection, l'utilisation et la réparation des tachygraphes intelligents et de leurs composants sont conformes aux exigences techniques énoncées à l'annexe IC du présent règlement.

3. Les tachygraphes autres que les tachygraphes intelligents continuent, en matière de construction, d'essais, d'installation, d'inspection, d'utilisation et de réparation, de satisfaire aux exigences de l'annexe I du règlement (UE) n° 165/2014 ou de l'annexe IB du règlement (CEE) n° 3821/85 du Conseil (*), selon le cas.

(*) Règlement (CEE) n° 3821/85 du Conseil du 20 décembre 1985 concernant l'appareil de contrôle dans le domaine des transports par route (JO L 370 du 31.12.1985, p. 8).»;

b) le paragraphe 5 suivant est ajouté:

«5. Le présent règlement est sans préjudice de l'application de la directive 2014/53/UE du Parlement européen et du Conseil (*).

(*) Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE (JO L 153 du 22.5.2014, p. 62).»;

2) l'article 2 est modifié comme suit:

a) la définition 3 est remplacée par le texte suivant:

«3. "dossier fabricant", le dossier complet, sous forme électronique ou imprimée, contenant toutes les informations fournies par le fabricant ou son mandataire à l'autorité d'homologation aux fins de l'homologation d'un tachygraphe ou d'un composant de tachygraphe, y compris les certificats visés à l'article 12, paragraphe 3, du règlement (UE) n° 165/2014, l'exécution des essais définis à l'annexe IC du présent règlement, ainsi que les dessins, photographies et autres documents pertinents;»;

([1]) Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE (JO L 153 du 22.5.2014, p. 62).

b) la définition 7 est remplacée par le texte suivant:

«7. "tachygraphe intelligent" ou "tachygraphe de deuxième génération", un tachygraphe numérique conforme aux articles 8, 9 et 10 du règlement (UE) n° 165/2014 ainsi qu'à l'annexe IC du présent règlement;»;

c) la définition 8 est remplacée par le texte suivant:

«8. "composant de tachygraphe", l'un des éléments suivants: l'unité embarquée sur le véhicule, le capteur de mouvement, la feuille d'enregistrement, le dispositif GNSS externe et le dispositif externe de détection précoce à distance;»;

d) la définition suivante est ajoutée:

«10. "unité embarquée sur le véhicule", le tachygraphe à l'exclusion du capteur de mouvement et des câbles de connexion de ce capteur.

Elle peut se présenter sous la forme d'un seul élément ou de plusieurs composants répartis dans le véhicule et comprend une unité de traitement, une mémoire électronique, une fonction de mesure du temps, deux interfaces pour cartes à mémoire pour le conducteur et le convoyeur, une imprimante, un écran, des connecteurs ainsi que des dispositifs permettant la saisie de données par l'utilisateur, un récepteur GNSS et un dispositif de communication à distance.

L'unité embarquée sur le véhicule peut se composer des éléments suivants soumis à homologation:

— une unité composée d'un seul élément (intégrant un récepteur GNSS et un dispositif de communication à distance),

— un élément principal (intégrant un dispositif de communication à distance) et un récepteur GNSS externe,

— un élément principal (intégrant un récepteur GNSS) et un dispositif de communication à distance externe,

— un élément principal, un récepteur GNSS externe et un dispositif de communication à distance externe.

Si l'unité embarquée sur le véhicule se présente sous la forme de plusieurs éléments répartis dans le véhicule, son élément principal est celui qui comprend l'unité de traitement, la mémoire électronique et la fonction de mesure du temps.

Le terme "unité embarquée sur le véhicule (VU)" désigne l'"unité embarquée sur le véhicule" ou l'"élément principal de l'unité embarquée sur le véhicule"»;

3) à l'article 6, le troisième alinéa est remplacé par le texte suivant:

«Toutefois, l'annexe IC s'applique à compter du 15 juin 2019, à l'exception de l'appendice 16, qui s'applique à compter du 2 mars 2016.»;

4) l'annexe IC est modifiée conformément à l'annexe I du présent règlement;

5) l'annexe II est modifiée conformément à l'annexe II du présent règlement.

Article 2

Entrée en vigueur

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 28 février 2018.

Par la Commission

Le président

Jean-Claude JUNCKER

ANNEXE I

L'annexe I C du règlement (UE) 2016/799 est modifiée comme suit:

1) la table des matières est modifiée comme suit:

a) le point 3.12.5 est remplacé par le point suivant:

«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 accumulé sont atteintes»;

b) le point 4.5.3.2.16 est remplacé par le texte suivant:

«4.5.3.2.16 Données relatives aux lieux où les trois heures de temps de conduite accumulé ont été atteintes»;

c) le point 4.5.4.2.14 est remplacé par le texte suivant:

«4.5.4.2.14 Données relatives aux lieux où les trois heures de temps de conduite accumulé ont été atteintes»;

d) le point 6.2 est remplacé par le texte suivant:

«6.2 Vérification de composants neufs ou réparés»;

2) le point 1 est modifié comme suit:

a) La définition ll) est remplacée par la définition suivante:

«ll) "dispositif de communication à distance" ou "dispositif de détection précoce à distance":

l'équipement de l'unité embarquée sur le véhicule utilisé pour les contrôles routiers ciblés;»;

b) la définition tt) est remplacée par la définition suivante:

«tt) "remise à l'heure":

un réglage de l'heure actuelle; ce réglage peut être exécuté de manière automatique à intervalles réguliers, sur la base de l'heure fournie par le récepteur GNSS, ou être effectué en mode "étalonnage";»;

c) le premier tiret de la définition yy) est remplacé par le texte suivant:

«— 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 Parlement européen et du Conseil (*), telle que modifiée en dernier lieu),»;

d) une nouvelle définition fff) est ajoutée:

«fff) "temps de conduite accumulé":

valeur représentant le nombre total de minutes de temps de conduite accumulé d'un véhicule donné.

La valeur du temps de conduite accumulé est un comptage libre de l'ensemble des minutes comptabilisées comme de la CONDUITE par la fonction de suivi des activités de conduite de l'appareil de contrôle. Elle n'est utilisée que pour déclencher l'enregistrement de la position du véhicule à chaque fois qu'un multiple de trois heures de conduite accumulé est atteint. L'accumulation débute au moment de l'activation de l'appareil de contrôle. Elle n'est affectée par aucune autre condition (p. ex. "hors champ" ou "trajet en ferry/train").

La valeur du temps de conduite accumulé n'est pas destinée à être affichée, imprimée ou téléchargée;»;

3) au point 2.3, le paragraphe 13, dernier tiret, est remplacé par le texte suivant:

«— les unités embarquées ont une période de validité opérationnelle normale de 15 ans à partir de la date effective de leurs certificats mais peuvent être utilisées pendant 3 mois supplémentaires, uniquement aux fins du téléchargement de données.»;

4) au point 2.4, le premier paragraphe est remplacé par le texte suivant:

«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'unité embarquée sur véhicule et le dispositif GNSS externe, le cas échéant, 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.»;

5) au point 3.2, le paragraphe 27, deuxième tiret, est remplacé par le texte suivant:

«— des positions correspondant aux lieux où le temps de conduite accumulé atteint un multiple de trois heures,»;

6) au point 3.4, le paragraphe 49 est remplacé par le texte suivant:

«49) Le premier changement d'activité vers PAUSE/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).»;

7) au point 3.6.1, le paragraphe 59 est remplacé par le texte suivant:

«59) Le conducteur indique alors l'emplacement actuel du véhicule, ce qui est considéré comme une saisie temporaire.

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

— saisie d'un lieu où débute la période de travail journalière actuelle lors de la saisie manuelle en application de l'exigence 61,

— saisie suivante d'un lieu où débute la période de travail journalière actuelle si le détenteur de la carte n'indique aucun emplacement de début ou de fin de la période de travail lors de la saisie manuelle en application de l'exigence 61.

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

— saisie suivante d'un lieu où s'achève la période de travail journalière actuelle si le détenteur de la carte n'indique aucun emplacement de début ou de fin de la période de travail lors de la saisie manuelle en application de l'exigence 61.»;

8) au point 3.6.2, les sixième et septième tirets sont remplacés par le texte suivant:

«— un lieu où s'est achevée une période de travail journalière précédente, associé à l'heure correspondante (qui écrase et valide 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 (qui valide une saisie temporaire effectuée lors du dernier retrait de la carte).»;

9) le point 3.9.15 est remplacé par le texte suivant:

«3.9.15 Événement "Conflit temporel"

86) 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 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 depuis au moins 30 jours.»;

10) au point 3.9.17, le tiret suivant est ajouté:

«— anomalie sur l'interface ITS (le cas échéant)»;

11) le point 3.10 est modifié comme suit:

i) le texte précédant le tableau figurant au paragraphe 89 est remplacé par ce qui suit:

«L'appareil de contrôle détecte les anomalies par des autotests et des tests intégrés, selon le tableau suivant:»;

ii) la ligne suivante est ajoutée au tableau:

«Interface ITS (facultatif)	Fonctionnement correct»	

12) au point 3.12, le deuxième tiret est remplacé par le texte suivant:

«— 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 accumulé 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 6570 positions sont comprises dans ces "365 jours",»;

13) le point 3.12.5 est modifié comme suit:

a) le titre et le paragraphe 108 sont remplacés par le texte suivant:

«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 accumulé sont atteintes

108) 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 accumulé 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.»;

b) le paragraphe 110, quatrième tiret, est remplacé par le texte suivant:

«— le type de saisie (début, fin ou 3 heures de temps de conduite accumulé),»;

c) le paragraphe 111 est remplacé par le texte suivant:

«111) 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 accumulé sont atteintes.»;

14) au point 3.12.7, le paragraphe 116 est remplacé par le texte suivant:

«116) L'appareil de contrôle enregistre et stocke dans sa mémoire la vitesse instantanée du véhicule et la date et l'heure correspondante à chaque seconde d'au moins les 24 dernières heures au cours desquelles le véhicule était en mouvement.»;

15) le tableau figurant au point 3.12.8 est modifié comme suit:

a) l'élément suivant est inséré entre les éléments «Absence d'informations de positionnement en provenance du récepteur GNSS» et «Erreur sur les données de mouvement»:

«Erreur de communication avec le dispositif GNSS externe	— 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.»

b) l'élément «Conflit temporel» est remplacé par le texte suivant:

«Conflit temporel	— l'événement le plus grave (c'est-à-dire celui présentant l'écart le plus important entre la date et l'heure de l'appareil de contrôle et la date et l'heure du GNSS) des 10 derniers jours d'occurrence, — les 5 événements les plus graves 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.»

16) au point 3.20, le paragraphe 200 est remplacé par le texte suivant:

«200) 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 d'unité embarquée sur le véhicule 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.

Le consentement du conducteur ne s'applique pas aux données transmises par l'appareil de contrôle au réseau du véhicule. En cas de traitement ultérieur, hors du réseau du véhicule, des données à caractère personnel introduites dans le réseau du véhicule, il relève de la responsabilité du constructeur du véhicule de s'assurer que ce traitement de données à caractère personnel est conforme au règlement (UE) 2016/679 (le "règlement général sur la protection des données").

Le consentement du conducteur ne s'applique pas non plus aux données tachygraphiques téléchargées vers une entreprise à distance (exigence 193), ce cas de figure étant contrôlé par le droit d'accès de la carte d'entreprise.

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

— ces données constituent un ensemble de données existantes sélectionnées qui proviennent du dictionnaire de données du tachygraphe (appendice 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 permet de communiquer le statut du consentement du conducteur aux autres plateformes du réseau du véhicule.

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

17) au point 3.23, le paragraphe 211 est remplacé par le texte suivant:

«211) Le réglage de l'heure de l'horloge interne de la VU est automatiquement réajusté toutes les 12 heures. Lorsque ce réajustement est impossible en raison de l'indisponibilité du signal GNSS, 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.»;

18) au point 3.26, les paragraphes 225 et 226 sont remplacés par le texte suivant:

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

— nom et adresse du fabricant,

— numéro de pièce du fabricant et année de fabrication,

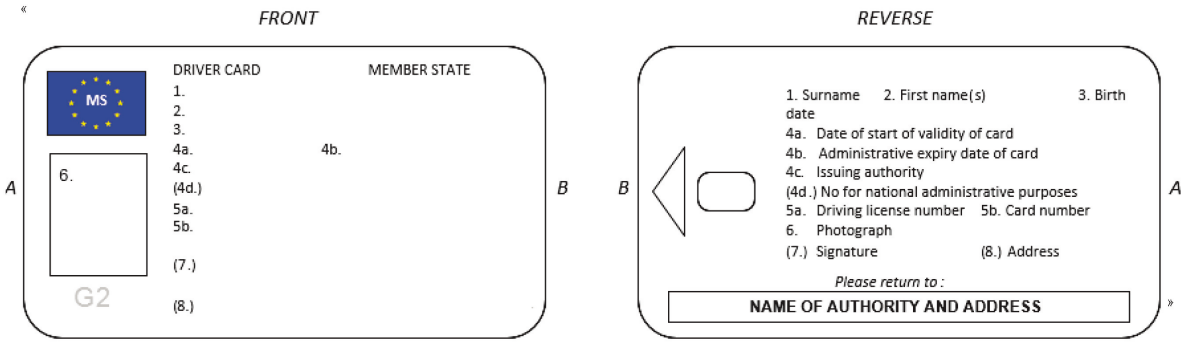
— numéro de série,

— marque d'homologation.

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

19) au point 4.1, le dessin correspondant au recto et au verso de la carte de conducteur est remplacé par le dessin suivant:

«



»

20) au point 4.5.3.1.8, le paragraphe 263, premier tiret, est remplacé par le texte suivant:

«— anomalie de la carte (lorsque la carte est à l'origine de l'anomalie),»;

21) au point 4.5.3.2.8, le paragraphe 288, premier tiret, est remplacé par le texte suivant:

«— anomalie de la carte (lorsque la carte est à l'origine de l'anomalie),»;

22) le point 4.5.3.2.16 est remplacé par le texte suivant:

«4.5.3.2.16 Données relatives aux lieux où les trois heures de temps de conduite accumulé ont été atteintes

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

— la date et l'heure où le temps de conduite accumulé atteint un multiple de trois heures,

— la position du véhicule,

— la précision GNSS, la date et l'heure de détermination de la position,

— le kilométrage du véhicule.

306) La carte de conducteur doit pouvoir stocker au moins 252 enregistrements de ce type.»;

23) le point 4.5.4.2.14 est remplacé par le texte suivant:

«4.5.4.2.14 Données relatives aux lieux où les trois heures de temps de conduite accumulé ont été atteintes

353) La carte d'atelier doit permettre le stockage des données suivantes relatives à la position du véhicule lorsque le temps de conduite accumulé atteint un multiple de trois heures:

— la date et l'heure où le temps de conduite accumulé atteint un multiple de trois heures,

— la position du véhicule,

— la précision GNSS, la date et l'heure de détermination de la position,

— le kilométrage du véhicule.

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

24) au point 5.2, le paragraphe 396 est remplacé par le texte suivant:

«396) 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 cas échéant,

— le numéro de série de l'appareil de communication à distance, le cas échéant,

— 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.»;

25) le point 5.3 est modifié comme suit:

a) un nouveau paragraphe 398 *bis*) est ajouté après le paragraphe 398)

«398 *bis*) Les scellements susmentionnés sont certifiés sur la base de la norme EN 16882:2016.»;

b) au paragraphe 401, le deuxième alinéa est remplacé par le texte suivant:

«Ce numéro d'identification unique est défini comme suit: MMNNNNNNNN, 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 NNNNNNNN est le numéro alphanumérique du scellement, unique dans le domaine du fabricant.»;

c) le paragraphe 403 est remplacé par le texte suivant:

«403) Les fabricants de scellements doivent être enregistrés dans une base de données dédiée lorsqu'ils obtiennent la certification d'un modèle de scellement selon la norme EN 16882:2016 et rendre publics leurs numéros d'identification de scellements par une procédure établie par la Commission européenne.»;

d) le paragraphe 404 est remplacé par le texte suivant:

«404) Les ateliers et constructeurs de véhicules agréés doivent, dans le cadre du règlement (UE) n° 165/2014, n'utiliser que des scellements certifiés selon la norme EN 16882:2016 issus des fabricants de scellements répertoriés dans la base de données mentionnée ci-dessus.»;

26) le point 6.2 est remplacé par le texte suivant:

«6.2. Vérification de composants neufs ou réparés

407) 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.»;

27) au point 6.3, le paragraphe 408 est remplacé par le texte suivant:

«408) 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. L'ensemble de l'installation doit être scellé conformément au chapitre 5.3 et comprendre un étalonnage.»;

28) le point 8.1) est modifié comme suit

a) au point 8.1, le texte introductif précédant le paragraphe 425 est remplacé par le texte suivant:

«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 externe 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 son ou ses composants d'appareil de contrôle avec tout autre composant d'appareil de contrôle, pour autant que chaque composant soit conforme aux exigences contenues dans la présente annexe. Les fabricants peuvent également demander l'homologation de l'appareil de contrôle.

Comme décrit dans la définition 10 de l'article 2 du présent règlement, les unités embarquées ont des variantes en ce qui concerne l'assemblage des composants. Quel que soit l'assemblage des composants de l'unité embarquée sur véhicule, l'antenne externe et (le cas échéant) du coupleur d'antenne connecté au récepteur GNSS ou au dispositif de communication à distance ne sont pas couverts par l'homologation de l'unité embarquée sur véhicule.

Les fabricants ayant obtenu l'homologation de leur appareil de contrôle doivent néanmoins tenir une liste publique des antennes et coupleurs compatibles avec chaque unité embarquée sur véhicule, dispositif GNSS externe et équipement externe de communication à distance homologués.»;

b) le paragraphe 427 est remplacé par le texte suivant:

«427) 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 (s'il est requis au titre de la présente annexe),

— d'un certificat de fonctionnement,

— et d'un certificat d'interopérabilité (s'il est requis au titre de la présente annexe)

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

29) l'appendice 1 est modifié comme suit:

a) la table des matières est modifiée comme suit:

i) le point 2.63 est remplacé par le texte suivant:

«2.63 Réservé pour une utilisation future»;

ii) le point 2.78 est remplacé par le texte suivant:

«2.78 GNSSAccumulatedDriving»;

iii) le point 2.79 est remplacé par le texte suivant:

«2.79 GNSSAccumulatedDrivingRecord»;

iv) le point 2.111 est remplacé par le texte suivant:

«2.111 NoOfGNSSADRecords»;

v) le point 2.160 est remplacé par le texte suivant:

«2.160 Réservé pour une utilisation future»;

vi) le point 2.203 est remplacé par le texte suivant:

«2.203 VuGNSSADRecord»;

vii) le point 2.204 est remplacé par le texte suivant:

«2.204 VuGNSSADRecordArray»;

viii) le point 2.230 est remplacé par le texte suivant:

«2.230 Réservé pour une utilisation future»;

ix) le point 2.231 est remplacé par le texte suivant:

«2.231 Réservé pour une utilisation future»;

b) au point 2, le texte suivant est ajouté avant le point 2.1:

«Pour les types de données de carte utilisés pour les applications de génération 1 et 2, la taille indiquée dans le présent appendice est celle relative à l'application de génération 2. La taille relative à l'application de génération 1 est censée être déjà connue du lecteur. Les numéros des exigences de l'annexe IC relatives à ces types de données couvrent à la fois les applications de génération 1 et de génération 2.»;

c) le point 2.19 est remplacé par le texte suivant:

«2.19. **CardEventData**

Génération 1:

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

```
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'événements correspondant à un type d'événement donné (ou à cette catégorie d'événements dans laquelle se rangent les tentatives d'atteinte à la sécurité).

Génération 2:

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

```
CardEventData ::= SEQUENCE SIZE(11) 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'événements correspondant à un type d'événement donné (ou à cette catégorie d'événements dans laquelle se rangent les tentatives d'atteinte à la sécurité).»;

d) le point 2.30 est remplacé par le texte suivant:

«2.30. **CardRenewalIndex**

Indice de renouvellement d'une carte [définition i)].

```
CardRenewalIndex::= IA5String(SIZE(1))
```

Attribution de valeur: (cf. chapitre 7 de la présente annexe).

"0" Première édition.

Ordre croissant: "0, …, 9, A, …, Z" »;

e) au point 2.61, le texte suivant le titre «Génération 2» est remplacé par le texte suivant:

```
«DriverCardApplicationIdentification ::= SEQUENCE {
typeOfTachographCardId          EquipmentType,
cardStructureVersion            CardStructureVersion,
noOfEventsPerType               NoOfEventsPerType,
noOfFaultsPerType               NoOfFaultsPerType,
activityStructureLength         CardActivityLengthRange,
noOfCardVehicleRecords          NoOfCardVehicleRecords,
noOfCardPlaceRecords            NoOfCardPlaceRecords,
noOfGNSSADRecords               NoOfGNSSADRecords,
noOfSpecificConditionRecords    NoOfSpecificConditionRecords
noOfCardVehicleUnitRecords      NoOfCardVehicleUnitRecords
}
```

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

noOfGNSSADRecords indique le nombre de relevés de temps de conduite accumulé GNSS que la carte est susceptible de sauvegarder.

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

noOfCardVehicleUnitRecords indique le nombre de relevés utilisés par les unités embarquées sur le véhicule que la carte est susceptible de mémoriser.»;

f) le point 2.63 est remplacé par le texte suivant:

«2.63. **Réservé pour une utilisation future**»;

g) au point 2.67, le texte suivant le titre «Génération 2» est remplacé par le texte suivant:

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

```
--GNSS Facility                 (8),
--Remote Communication Module   (9),
--ITS interface module          (10),
--Plaque                        (11),--may be used in SealRecord
--M1/N1 Adapter                 (12),--may be used in SealRecord
--European Root CA (ERCA)       (13),
--Member State CA (MSCA)        (14),
--External GNSS connection      (15),--may be used in SealRecord
--Unused                        (16),--used in SealDataVu
--Driver Card (Sign)            (17),--only to be used in the CHA
                                field of a signing certificate
--Workshop Card (Sign)          (18), --only to be used in the CHA
                                field of a signing certificate
--Vehicle Unit (Sign)           (19), --only to be used in the CHA
                                field of a signing certificate
--RFU                           (20..255)
```

Note 1: 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.

Note 2: Dans le champ CardHolderAuthorisation (CHA) d'un certificat de génération 2, les valeurs (1), (2) et (6) doivent être interprétées comme indiquant un certificat d'authentification mutuelle du type d'équipement concerné. Pour indiquer le certificat à utiliser pour la création d'une signature numérique, les valeurs (17), (18) ou (19) doivent être utilisées.»;

h) au point 2.70, le texte suivant le titre «Génération 2» est remplacé par le texte suivant:

«Génération 2:

'0x'H	événements généraux,
'00'H	absence d'informations complémentaires,
'01'H	insertion d'une carte non valable,
'02'H	conflit de carte,
'03'H	chevauchement temporel,
'04'H	conduite sans carte appropriée,
'05'H	insertion de carte en cours de conduite,
'06'H	dernière session incorrectement clôturée,
'07'H	excès de vitesse,
'08'H	Coupure d'alimentation électrique,
'09'H	erreur sur les données de mouvement,
'0A'H	conflit concernant le mouvement du véhicule,
'0B'H	conflit temporel (GNSS contre l'horloge interne de la VU),
'0C'H	erreur de communication avec l'équipement de communication à distance,
'0D'H	absence d'informations de positionnement en provenance du récepteur GNSS,
'0E'H	erreur de communication avec le dispositif GNSS externe,
'0F'H	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	détection de violation du dispositif GNSS,
'1A'H	défaut d'authentification du dispositif GNSS externe,
'1B'H	expiration du certificat du dispositif GNSS externe,
'1C'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	récepteur du dispositif GNSS interne,
'37'H	dispositif GNSS externe,
'38'H	dispositif de communication à distance,
'39'H	interface ITS,
'3A'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.»;

i) le point 2.71 est remplacé par le texte suivant:

«2.71. **ExtendedSealIdentifier**

Génération 2:

L'identifiant de scellement étendu identifie un scellement de manière unique (exigence 401, annexe IC).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                OCTET STRING (SIZE(2)),
   sealIdentifier                  OCTET STRING (SIZE(8))
}
```

manufacturerCode correspond au code du fabricant du scellement.

sealIdentifier désigne l'identifiant du scellement, unique pour le fabricant.»;

j) les points 2.78 et 2.79 sont remplacés par le texte suivant:

«2.78 **GNSSAccumulatedDriving**

Génération 2:

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

```
GNSSAccumulatedDriving := SEQUENCE {
   gnssADPointerNewestRecord       INTEGER(0..NoOfGNSSADRecords -1),
   gnssAccumulatedDrivingRecords   SET SIZE(NoOfGNSSADRecords) OF
                                   GNSSAccumulatedDrivingRecord
}
```

gnssADPointerNewestRecord désigne l'indice du dernier relevé de temps de conduite accumulé GNSS actualisé par le système.

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

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

2.79. **GNSSAccumulatedDrivingRecord**

Génération 2:

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

```
GNSSAccumulatedDrivingRecord ::= SEQUENCE {
  timeStamp                    TimeReal,
  gnssPlaceRecord              GNSSPlaceRecord,
  vehicleOdometerValue         OdometerShort
}
```

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

gnssPlaceRecord contient les informations relatives à la position du véhicule.

vehicleOdometerValue est la valeur affichée par le compteur kilométrique pour laquelle le temps de conduite accumulé atteint un multiple de trois heures.»;

k) le point 2.86 est remplacé par le texte suivant:

«2.86. **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, d'une carte tachygraphique ou d'un dispositif GNSS externe.

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.»;

l) le point 2.92 est remplacé par le texte suivant:

«2.92. **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(16)),
}
```

»;

m) le point 2.111 est remplacé par le texte suivant:

«2.111. **NoOfGNSSADRecords**

Génération 2:

Nombre de relevés de temps de conduite accumulé GNSS que la carte est susceptible de sauvegarder.

$$\text{NoOfGNSSADRecords ::= INTEGER (0..2}^{16}\text{-1)}$$

Assignation de valeur: cf. appendice 2.»;

n) au point 2.120, l'assignation de valeur «16H» est remplacée par le texte suivant:

«'16'H VuGNSSADRecord »;

o) le point 2.160 est remplacé par le texte suivant:

«2.160. **Réservé pour une utilisation future**»;

p) le point 2.162 est remplacé par le texte suivant:

«2.162. **TimeReal**

Code associé à un champ combinant date et heure exprimées en secondes à compter de 00h00m00s TUC le 1er janvier 1970 (UTC).

```
TimeReal {INTEGER: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.»;

q) le point 2.179 est remplacé par le texte suivant:

«2.179 **VuCardRecord**

Génération 2:

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à la carte tachygraphique utilisée (exigence 132, annexe IC).

```
VuCardRecord ::= SEQUENCE {
cardNumberAndGenerationInformation      FullCardNumberAndGeneration,
cardExtendedSerialNumber                ExtendedSerialNumber,
cardStructureVersion                    CardStructureVersion,
cardNumber                              CardNumber
}
```

cardNumberAndGenerationInformation est le numéro complet et la génération de la carte utilisée (type de données 2.74).

cardExtendedSerialNumber tel qu'extrait du fichier EF_ICC sous le FM de la carte.

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.»;

r) les points 2.203 et 2.204 sont remplacés par le texte suivant:

«2.203 **VuGNSSADRecord**

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 accumulé atteint un multiple de trois heures (exigences 108 et 110, annexe IC).

```
VuGNSSADRecord ::= SEQUENCE {
   timeStamp                        TimeReal,
   cardNumberAndGenDriverSlot       FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot     FullCardNumberAndGeneration,
   gnssPlaceRecord                  GNSSPlaceRecord,
   vehicleOdometerValue             OdometerShort
}
```

timeStamp désigne la date et l'heure où le temps de conduite accumulé 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.

vehicleOdometerValue est la valeur affichée par le compteur kilométrique pour laquelle le temps de conduite accumulé atteint un multiple de trois heures.

2.204. **VuGNSSADRecordArray**

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 accumulé atteint un multiple de trois heures (exigences 108 et 110, annexe IC).

```
VuGNSSADRecordArray ::= SEQUENCE {
   recordType                    RecordType,
   recordSize                    INTEGER(1..65535),
   noOfRecords                   INTEGER(0..65535),
   records                       SET SIZE(noOfRecords) OF VuGNSSADRecord
}
```

recordType indique le type de relevé (VuGNSSADRecord).

Assignation de valeur: Cf. RecordType

recordSize indique la taille des VuGNSSADRecord exprimée en octets.

noOfRecords désigne le nombre de relevés dans les relevés définis.

records désigne un jeu de relevés de temps de conduite accumulé GNSS.»;

s) les points 2.230 et 2.231 sont remplacés par le texte suivant:

«2.230. Réservé pour une utilisation future.

2.231. Réservé pour une utilisation future»;

t) au point 2.234, le texte qui suit le titre «Génération 2» est remplacé par le texte suivant:

```
«WorkshopCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId              EquipmentType,
    cardStructureVersion                CardStructureVersion,
    noOfEventsPerType                   NoOfEventsPerType,
    noOfFaultsPerType                   NoOfFaultsPerType,
    activityStructureLength             CardActivityLengthRange,
    noOfCardVehicleRecords              NoOfCardVehicleRecords,
    noOfCardPlaceRecords                NoOfCardPlaceRecords,
    noOfCalibrationRecords              NoOfCalibrationRecords,
    noOfGNSSADRecords                   NoOfGNSSADRecords,
    noOfSpecificConditionRecords        NoOfSpecificConditionRecords,
    noOfCardVehicleUnitRecords          NoOfCardVehicleUnitRecords
}
```

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

noOfGNSSADRecords indique le nombre de relevés de temps de conduite accumulé GNSS que la carte est susceptible de sauvegarder.

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

noOfCardVehicleUnitRecords indique le nombre de relevés utilisés par les unités embarquées sur le véhicule que la carte est susceptible de mémoriser»;

30) l'appendice 2 est modifié comme suit:

a) au point 1.1, les abréviations suivantes sont ajoutées:

«CHA Autorisation d'un titulaire de certificat

DO Objet de données»;

b) le point 3.3 est modifié comme suit:

i) le paragraphe TCS_24 est remplacé par le texte suivant:

«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 et UPDATE BINARY sont spécifiées au chapitre 4. Les conditions d'accès des autres commandes sont spécifiées dans les tableaux suivants. Le terme "non applicable" est utilisé s'il n'est pas exigé de prendre en charge cette commande. Dans ce cas, la commande est ou n'est pas prise en charge, mais la condition d'accès est hors champ.»;

ii) au paragraphe TCS_25, le tableau est remplacé par le tableau suivant:

«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

Commande	Carte du conducteur	Carte atelier	Carte de contrôle	Carte d'entreprise
PERFORM 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»

iii) au paragraphe TCS_26, le tableau est remplacé par le tableau suivant:

«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
PERFORM 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»

iv) au paragraphe TCS_27, le tableau est remplacé par le tableau suivant:

«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
PERFORM HASH of FILE	Sans objet	Sans objet	Sans objet	Sans objet
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Sans objet	Sans objet	Sans objet	Sans objet
Verify	Sans objet	ALW	Sans objet	Sans objet»

c) au point 3.4, le paragraphe TCS_29 est remplacé par le texte suivant:

«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"

SW1	SW2	Signification
64	00	Erreur d'exécution - État de la mémoire rémanente inchangé. Erreur d'intégrité
65	00	Erreur d'exécution - État de la mémoire rémanente modifié.
65	81	Erreur d'exécution - État de la mémoire rémanente modifié - Défaillance de la mémoire.
66	88	Erreur de sécurité: Total de contrôle cryptographique erroné (en cours 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	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

Les mots d'état supplémentaires au sens de la norme ISO/IEC 7816-4 peuvent être renvoyés si leur comportement n'est pas explicitement mentionné dans le présent appendice.

Par exemple, les mots d'état suivants peuvent éventuellement être renvoyés:

6881: Canal logique non pris en charge

6882: Messagerie sécurisée non prise en charge»;

d) au point 3.5.1.1, le paragraphe TCS_38, dernier tiret, est remplacé par le texte suivant:

«— 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 "**6500**".»;

e) au point 3.5.1.2, le paragraphe TCS_41, dernier tiret, est remplacé par le texte suivant:

«— 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 "**6500**".»;

f) au point 3.5.2.1, le paragraphe TCS_43, sixième tiret, est remplacé par le texte suivant:

«— 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**".»;

g) le point 3.5.2.1.1 est modifié comme suit:

i) au paragraphe TCS_45, le tableau est remplacé par le tableau suivant:

«Octet	Longueur	Valeur	Description
#1	1	"81h"	T_{PV}: balise indiquant la valeur des données ordinaires
#2	L	"NNh" ou "81 NNh"	L_{PV}: longueur des données renvoyées (=Le original). L équivaut à 2 octets si L_{PV}> 127 octets.
#(2+L) - #(1+L+NN)	NN	"XX..XXh"	Valeur des données ordinaires
#(2+L+NN)	1	"99h"	Balise d'état de traitement (SW1-SW2) - facultatif pour la messagerie sécurisée de génération 1
#(3+L+NN)	1	"02h"	Longueur de l'état de traitement – facultatif pour la messagerie sécurisée de génération 1
#(4+L+NN) - #(5+L+NN)	2	"XX XXh"	État de traitement de l'APDU de réponse non protégée - facultatif pour la messagerie sécurisée de génération 1
#(6+L+NN)	1	"8Eh"	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)

Octet	Longueur	Valeur	Description
#(8+L+NN)-#(7+M+L+NN)	M	"XX..XXh"	Total de contrôle cryptographique
SW	2	"XXXXh"	Mots d'état (SW1, SW2)»

ii) au paragraphe TCS_46, le tableau est remplacé par le tableau suivant:

«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 LPI 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 - facultatif pour la messagerie sécurisée de génération 1
#(4+L+MM) - #(5+L+MM)	2	"XX XXh"	État de traitement de l'APDU de réponse non protégée – facultatif pour la messagerie sécurisée de génération 1
#(6+L+MM)	1	"8Eh"	TCC: balise indiquant le total de contrôle cryptographique
#(7+L+MM)	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+MM)-#(7+N+L+MM)	N	"XX..XXh"	Total de contrôle cryptographique
SW	2	"XXXXh"	Mots d'état (SW1, SW2)»

h) au point 3.5.2.2, le paragraphe TCS_50, sixième tiret, est remplacé par le texte suivant:

«— 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**".»;

i) le point 3.5.2.3, paragraphe TCS_52, est modifié comme suit:

i) la dernière ligne du tableau est remplacée par la suivante:

«Le	1	"XXh"	Conformément à la norme ISO/IEC 7816-4»

ii) la phrase suivante est ajoutée:

«Si T=0, la carte suppose la valeur Le = "00h" si aucune messagerie sécurisée n'est appliquée.

Si T=1, l'état de traitement renvoyé est "6700" si Le="01h".»;

j) au point 3.5.2.3, le paragraphe TCS_53, sixième tiret, est remplacé par le texte suivant:

«— 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**".»;

k) au point 3.5.3.2, le paragraphe TCS_63, sixième tiret, est remplacé par le texte suivant:

«— 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**".»;

l) au point 3.5.5, le paragraphe TCS_72 est remplacé par le texte suivant:

«TCS_72 Le PIN indiqué 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.»;

m) au point 3.5.8, le paragraphe TCS_95 est remplacé par le texte suivant:

«TCS_95 Si la commande INTERNAL AUTHENTICATE aboutit, la clé de session active de génération 1, pour autant qu'elle existe, est effacée et cesse d'être disponible. Pour disposer d'une nouvelle clé de session de génération 1, il convient d'exécuter avec succès la commande EXTERNAL AUTHENTICATE pour le mécanisme d'authentification de génération 1.

Remarque: Pour les clés de session de génération 2, voir l'appendice 11, paragraphes CSM_193 et CSM_195. Si les clés de session de génération 2 sont établies et que la carte tachygraphique reçoit la commande INTERNAL AUTHENTICATE en clair APDU, elle abandonne la session de messagerie sécurisée de génération 2 et détruit les clés de session de génération 2.»;

n) au point 3.5.9, le paragraphe TCS_97 est remplacé par le texte suivant:

«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. également TCS_34. Si cette commande EXTERNAL AUTHENTICATE de génération 2 aboutit, la clé de session active de génération 1, pour autant qu'elle existe, est effacée et cesse d'être disponible.

Remarque: Pour les clés de session de génération 2, voir l'appendice 11, paragraphes CSM_193 et CSM_195. Si les clés de session de génération 2 sont établies et que la carte tachygraphique reçoit la commande EXTERNAL AUTHENTICATE en clair APDU, elle abandonne la session de messagerie sécurisée de génération 2 et détruit les clés de session de génération 2.»;

o) au point 3.5.10, la ligne suivante est ajoutée au tableau du paragraphe TCS_101:

«5 + L + 1	1	"00h"	Conformément à la norme ISO/IEC 7816-4»

p) au point 3.5.11.2.3, les paragraphes suivants sont ajoutés au paragraphe TCS_114:

«— Si le currentAuthenticatedTime de la carte est ultérieur à la date d'expiration de la clé publique sélectionnée, le logiciel renvoie l'état de traitement "**6A88**".

Remarque: En cas de MSE: SET AT pour authentification de VU, la clé mentionnée est une clé publique VU_MA. La carte définit la clé publique VU_MA pour utilisation, si elle est disponible dans sa mémoire, correspondant à la référence du titulaire du certificat (CHR) indiquée dans la zone de données de la commande (la carte peut identifier les clés publiques VU_MA au moyen du champ CHA du certificat). Une carte ne renvoie "6A 88" à cette commande que lorsque seule la clé publique VU_Sign est disponible ou lorsqu'aucune clé publique de l'unité embarquée sur véhicule n'est disponible. Voir la définition du champ CHA à l'appendice 11 et la définition du type de données EquipmentType à l'appendice 1.

De même, en cas de commande MSE: SET DST indiquant un EQT (une VU ou une carte) est envoyée à une carte de contrôle, aux termes du paragraphe CSM_234, la clé mentionnée est toujours une clé EQT_Sign à utiliser lors de la vérification d'une signature numérique. Selon la figure 13 de l'appendice 11, la carte de contrôle enregistre toujours la clé publique EQT_Sign pertinente. Dans certains cas, la carte de contrôle peut avoir enregistré la clé publique EQT_MA correspondante. La carte de contrôle définit toujours la clé publique EQT_Sign pour utilisation lorsqu'elle reçoit une commande MSE: SET DST.»;

q) le point 3.5.13 est modifié comme suit:

(i) le paragraphe TCS_121 est remplacé par le texte suivant:

«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 PERFORM HASH of FILE, si un DF est sélectionné et si la carte tachygraphique est réinitialisée.»;

ii) le paragraphe TCS_123 est remplacé par le texte suivant:

«TCS_123 L'application tachygraphique de génération 2 doit prendre en charge l'algorithme SHA-2 (SHA-256, SHA-384 ou SHA-512), spécifié par la méthode de cryptage à l'appendice 11, partie B, pour la clé de signature de carte Card_Sign.»;

iii) le tableau figurant au paragraphe TCS_124 est remplacé par le tableau suivant:

«Octet	Longueur	Valeur	Description
CLA	1	"80h"	CLA
INS	1	"2Ah"	Exécution d'une opération de sécurité
P1	1	"90h"	Balise: Hash
P2	1	"00h"	Algorithme implicitement connu Pour l'application tachygraphique de génération 1: SHA-1 Pour l'application tachygraphique de génération 2: l'algorithme SHA-2 (SHA-256, SHA-384 ou SHA-512), défini par la méthode de cryptage à l'appendice 11, partie B, pour la clé de signature de carte Card_Sign»

r) le point 3.5.14 est modifié comme suit:

le texte suivant l'intitulé, jusqu'au paragraphe TCS_126, est remplacé par le texte suivant:

«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 exécuter cette commande. Pour l'application tachygraphique de génération 2, seule la carte du conducteur et la carte d'atelier possèdent une clé de signature de génération 2; les autres 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. Si la commande n'est pas accessible dans le MF, le logiciel doit interrompre la commande avec un code d'erreur adapté.

Cette commande est conforme à la norme ISO/IEC 7816-8. Son usage est restreint relativement à la norme en question.»;

s) le point 3.5.15 est modifié comme suit:

i) le tableau figurant au paragraphe TCS_133 est remplacé par le tableau suivant:

«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	"XXh"	Longueur Lc de la zone de données suivante
#6	1	"9Eh"	Balise indiquant une signature numérique
#7 ou #7-#8	L	"NNh" ou "81 NNh"	Longueur de la signature numérique (L équivaut à 2 octets si la signature numérique est plus longue que 127 octets): 128 octets codés conformément à l'appendice 11 partie A pour l'application tachygraphique de génération 1. Selon la courbe retenue pour l'application tachygraphique de génération 2 (cf. appendice 11 partie B).
#(7+L)-#(6+L+NN)	NN	"XX..XXh"	Contenu de la signature numérique»

ii) au paragraphe TCS_134, le tiret suivant est ajouté:

«— Si la clé publique sélectionnée (utilisée pour vérifier la signature numérique) possède un CHA.LSB (CertificateHolderAuthorisation.equipmentType) inadapté à la vérification de la signature numérique telle que prévue par l'appendice 11, le logiciel renvoie l'état de traitement "**6985**".»;

t) le point 3.5.16 est modifié comme suit:

i) au paragraphe TCS_138, la ligne suivante est ajoutée au tableau:

«5 + L + 1	1	"00h"	Conformément à la norme ISO/IEC 7816-4»

ii) l'alinéa suivant est ajouté au paragraphe TCS_139:

«— "**6985**" indique que le timbre horodateur sur 4 octets indiqué dans la zone de données de la commande est antérieur à cardValidityBegin ou postérieur à cardExpiryDate.»;

u) le point 4.2.2 est modifié comme suit:

i) dans la structure de données du paragraphe TCS_154, les lignes allant de DF Tachograph G2 à EF CardMA_Certificate et de EF GNSS_Places à la fin du paragraphe sont remplacées par le texte suivant:

«

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
DF Tachograph_G2		*20268*	*40316*	
EF Application_Identification		*17*	*17*	
DriverCardApplicationIdentification		*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 00}
noOfGNSSADRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00 00}
noOfCardVehicleUnitRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	

...

EF GNSS_Places		*4538*	*6050*	
GNSSContinuousDriving		*4538*	*6050*	
gnssADPointerNewestRecord		2	2	{00 00}
gnssAccumulatedDrivingRecords		4536	6048	
GNSSContinuousDrivingRecord	n_8	*18*	*18*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		14	14	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}

»;

ii) au paragraphe TCS_155, l'élément NoOfGNSSCDRecords du tableau est remplacé par l'élément suivant:

«n_8	NoOfGNSSADRecords	252	336»

v) au point 4.3.1, le texte correspondant à l'abréviation SC4 au paragraphe TCS_156 est remplacé par le texte suivant:

«**SC4** Concernant la commande READ BINARY avec des octets pairs INS:

(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»;

w) le point 4.3.2 est modifié comme suit:

i) dans la structure de données du paragraphe TCS_162, les lignes allant de DF Tachograph G2 à EF CardMA_Certificate, de EF Calibration à extendedSealIdentifier et de EF GNSS_Places à vehicleOdometerValue sont remplacées par le texte suivant:

«

File / Data element	No of Records	Size (bytes) Min	Max	Default Values
DF Tachograph_G2	*1878*		*49787*	
EF Application_Identification	*19*		*19*	
WorkshopCardApplicationIdentificatio	*19*		*19*	
typeOfTachographCardId	1		1	{00}
cardStructureVersion	2		2	{00 00}
noOfEventsPerType	1		1	{00}
noOfFaultsPerType	1		1	{00}
activityStructureLength	2		2	{00 00}
noOfCardVehicleRecords	2		2	{00 00}
noOfCardPlaceRecords	2		2	{00 00}
noOfCalibrationRecords	2		2	{00 00}
noOfGNSSADRecords	2		2	{00 00}
noOfSpecificConditionRecords	2		2	{00 00}
noOfCardVehicleUnitRecords	2		2	{00 00}
EF CardMA_Certificate	*204*		*341*	
...				
EF Calibration		*15668*	*45394*	
WorkshopCardCalibrationData		*15668*	*45394*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*15664*	*45390*	
WorkshopCardCalibrationRecord	n_5	*178*	*178*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
sensorGNSSSerialNumber		8	8	{00..00}
rcmSerialNumber		8	8	{00..00}
vuAbility		1	1	{00}
sealDataCard		56	56	
noOfSealRecords		1	1	{00}
SealRecords		55	55	
SealRecord	5	11	11	
equipmentType		1	1	{00}
extendedSealIdentifier		10	10	{00..00}

...

EF GNSS_Places		*326*	*434*	
└GNSSContinuousDriving		*326*	*434*	
├gnssADPointerNewestRecord		2	2	{00 00}
└gnssAccumulatedDrivingRecords		324	432	
└GNSSContinuousDrivingRecord	n_8	*18*	*18*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		14	14	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
├geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}

»

ii) l'élément NoOfGNSSCDRecords du tableau inclus au paragraphe TCS_163 est remplacé par l'élément suivant:

«n_8	NoOfGNSSADRecords	18	24»

31) dans l'appendice 3, le point 2 est modifié comme suit:

a) la ligne suivante est insérée après la ligne incluant les pictogrammes «Site de début de la période de travail journalière» et «Site de fin de la période de travail journalière»:

«  Position après trois heures de temps de conduite accumulé»;

b) la combinaison de pictogrammes «Réglage de l'heure (en atelier)» est remplacée par la combinaison suivante:

«  Conflit temporel ou réglage de l'heure (en atelier)»;

c) les combinaisons de pictogrammes suivantes sont ajoutées à la liste des événements:

«  Absence d'informations de positionnement en provenance du récepteur GNSS ou Erreur de communication avec le dispositif GNSS externe;

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

32) l'appendice 4 est modifié comme suit:

a) le point 2 est modifié comme suit:

i) le numéro de bloc 11.4 est remplacé par le numéro suivant:

«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	pihh:mm Cou Reg
longitude de la position enregistrée	lon ±DDD°MM.M'
latitude de la position enregistrée	lat ± DD°MM.M'
horodatage de la détermination de la position	hh:mm
Compteur kilométrique	x xxx xxx **km**»

ii) le numéro de bloc 11.5 est remplacé par le numéro suivant:

«11.5 *Positions après trois heures de temps de conduite accumulé*
pi=position après trois heures de temps de conduite accumulé

heure	pihh:mm
longitude de la position enregistrée	lon ± DDD°MM.M'
latitude de la position enregistrée	lat ± DD°MM.M '
horodatage de la détermination de la position	hh:mm
Compteur kilométrique	x xxx xxx **km**»

b) au point 3.1, la position 11.5 du format du tirage quotidien est remplacée par ce qui suit:

«11.5	Positions après trois heures de temps de conduite accumulé par ordre chronologique»

c) au point 3.2, le format du tirage quotidien est remplacé comme suit:

«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	Positions après trois heures de temps de conduite accumulé par ordre chronologique
11.7	Totaux par activité
11.2	Synthèse des périodes sans carte dans le lecteur du convoyeur
11.4	Lieux saisis par ordre chronologique
11.5	Positions après trois heures de temps de conduite accumulé par ordre chronologique

11.8	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	Positions après trois heures de temps de conduite accumulé par ordre chronologique
11.9	Totaux par activité pour ce conducteur
13.1	Délimiteur d'événements et d'anomalies
13.4	Enregistrements d'événements/anomalies (5 derniers événements ou anomalies enregistrés ou en cours dans la VU)
22.1	Lieu du contrôle
22.2	Signature du contrôleur
22.3	De (heure)
22.4	À (heure) (espace disponible pour un conducteur dépourvu de carte lui permettant d'indiquer les périodes qui correspondent à ses prestations)
22.5	Signature du conducteur»

d) au point 3.7, le paragraphe PRT_014 est remplacé par le texte suivant:

«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»

33) l'appendice 7 est modifié comme suit:

a) le point 1.1 est remplacé par le texte suivant:

«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.

Les données téléchargées à partir d'une VU sont signées conformément aux dispositions de l'appendice 11, Mécanismes de sécurité communs, partie B (tachygraphe de deuxième génération), excepté lorsque le contrôle des conducteurs est effectué par des autorités de contrôle autres que celles de l'UE, au moyen d'une carte de contrôle de première génération, auquel cas les données sont signées conformément aux dispositions de l'appendice 11, Mécanismes de sécurité communs, partie A (tachygraphe de première génération), conformément à l'appendice 15 Migration, exigence MIG_015.

Cet appendice spécifie dès lors deux types de téléchargements de données à partir de la VU:

— téléchargement de données de la VU de génération 2, fournissant la structure de données de génération 2 et signées conformément aux dispositions de l'appendice 11, Mécanismes de sécurité communs, partie B,

— téléchargement de données de la VU de génération 1, fournissant la structure de données de génération 1 et signées conformément aux dispositions de l'appendice 11, Mécanismes de sécurité communs, partie A,

De même, on distingue deux types de téléchargements de données à partir de cartes de conducteur de deuxième génération insérées dans une VU, comme indiqué aux paragraphes 3 et 4 du présent appendice.»;

b) le point 2.2.2 est modifié comme suit:

i) le tableau est remplacé par le tableau suivant:

«Structure du message	4 octets max. En-tête				255 octets max. Données			1 octet Total de contrôle
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 ou 21		97
Activités	80	EE	F0	06	36	02 ou 22	Date	CS
Événements et anomalies	80	EE	F0	02	36	03 ou 23		99
Vitesse instantanée	80	EE	F0	02	36	04 ou 24		9A
Données techniques	80	EE	F0	02	36	05 ou 25		9B
Téléchargement (download) d'une carte	80	EE	F0	02	36	06	Lecteur	CS

Structure du message	4 octets max. En-tête				255 octets max. Données			1 octet Total de contrôle
IDE -> **<- VU**	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	DONNÉES	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»

ii) les tirets suivants sont ajoutés aux remarques suivant le tableau:

«— Les TRTP 21 à 25 sont utilisés pour les demandes de téléchargement de données de la VU de génération 2, les TRTP 01 à 05 sont utilisés pour les demandes de téléchargement de données de la VU de génération 1, qui ne peuvent être acceptées par la VU que dans le cadre des contrôles des conducteurs effectués par des autorités de contrôle autres que celles de l'UE, au moyen d'une carte de contrôle de première génération.

— Les TRTP 11 à 19 et 31 à 39 sont réservés aux demandes de téléchargement propres au fabricant.»;

c) le point 2.2.2.9 est modifié comme suit:

i) le paragraphe DDP_011 est remplacé par le texte suivant:

«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. Pour les téléchargements de données de la VU, deux différentes valeurs TRTP peuvent être utilisées pour chaque type de transfert:

Type de transfert de données	Valeur de TRTP pour les téléchargements de données de la VU de génération 1	Valeur de TRTP pour les téléchargements de données de la VU de génération 2
Récapitulatif	01	21
Activités associées à une date précise	02	22
Événements et anomalies	03	23
Vitesse instantanée	04	24
Données techniques	05	25

Type de transfert de données	Valeur de TRTP
Téléchargement de carte	06»

ii) le paragraphe DDP_054 est remplacé par le texte suivant:

«DDP_054 Il est obligatoire pour l'IDE de demander un transfert de données du type "récapitulatif" (TRTP 01 ou 21) 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 ou 22), le message de demande de transfert de données comporte l'indication du jour civil (format `TimeReal`) auquel le téléchargement est associé.»;

d) au point 2.2.2.10, le paragraphe DDP_055 est remplacé par le texte suivant:

«DDP_055 Dans le premier cas (TREP 01 ou 21), 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.»;

e) au point 2.2.2.16, le paragraphe DDP_018, dernier tiret, est remplacé par le texte suivant:

«— 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, téléchargement de données de la VU de génération 1 demandé en dehors du cadre du contrôle d'un conducteur par une autorité de contrôle autre qu'une autorité de contrôle de l'UE, etc.).»;

f) le point 2.2.6.1 est modifié comme suit:

i) le premier alinéa du paragraphe DDP_029 est remplacé par le texte suivant:

«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 ou 21 Hex et critères appropriés de séparation et de comptage des sous-messages:»;

ii) l'intitulé «Structure de données de génération 1» est remplacé par le texte suivant:

«Structure de données de génération 1 (TREP 01 Hex)»;

iii) l'intitulé «Structure de données de génération 2» est remplacé par le texte suivant:

«Structure de données de génération 2 (TREP 21 Hex)»;

g) le point 2.2.6.2 est modifié comme suit:

i) le premier alinéa du paragraphe DDP_030 est remplacé par le texte suivant:

«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 ou 22 Hex et critères appropriés de séparation et de comptage des sous-messages:»;

ii) l'intitulé «Structure de données de génération 1» est remplacé par le texte suivant:

«Structure de données de génération 1 (TREP 02 Hex)»;

iii) l'intitulé «Structure de données de génération 2» est remplacé par le texte suivant:

«Structure de données de génération 2 (TREP 22 Hex)»;

iv) l'élément VuGNSSCDRecordArray sous l'intitulé «Structure de données de génération 2 (TREP 22 Hex)» est remplacé comme suit:

«VuGNSSADRecordArray	Positions GNSS du véhicule lorsque le temps de conduite accumulé du véhicule atteint un multiple de trois heures. Si cette section est vide, un en-tête de tableau avec l'expression noOfRecords = 0 est envoyé.»

h) le point 2.2.6.3 est modifié comme suit:

i) le premier alinéa du paragraphe DDP_031 est remplacé par le texte suivant:

«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 ou 23 Hex et critères appropriés de séparation et de comptage des sous-messages:»;

ii) l'intitulé «Structure de données de génération 1» est remplacé par le texte suivant:

«Structure de données de génération 1 (TREP 03 Hex)»;

iii) l'intitulé «Structure de données de génération 2» est remplacé par le texte suivant:

«Structure de données de génération 2 (TREP 23 Hex)»;

iv) l'élément VuTimeAdjustmentGNSSRecordArray sous le titre «Structure de données de génération 2 (TREP 23 Hex)» est supprimé;

i) le point 2.2.6.4 est modifié comme suit:

i) le premier alinéa du paragraphe DDP_032 est remplacé par le texte suivant:

«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 ou 24 Hex et critères appropriés de séparation et de comptage des sous-messages:»;

ii) l'intitulé «Structure de données de génération 1» est remplacé par le texte suivant:

«Structure de données de génération 1 (TREP 04)»;

iii) l'intitulé «Structure de données de génération 2» est remplacé par le texte suivant:

«Structure de données de génération 2 (TREP 24)»;

j) le point 2.2.6.5 est modifié comme suit:

i) le premier alinéa du paragraphe DDP_033 est remplacé par le texte suivant:

«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 ou 25 Hex et critères appropriés de séparation et de comptage des sous-messages:»;

ii) l'intitulé «Structure de données de génération 1» est remplacé par le texte suivant:

«Structure de données de génération 1 (TREP 05)»;

iii) l'intitulé «Structure de données de génération 2» est remplacé par le texte suivant:

«Structure de données de génération 2 (TREP 25)»;

k) au point 3.3, le paragraphe DDP_035 est remplacé par le texte suivant:

«DDP_035 Le téléchargement d'une carte tachygraphique comporte les opérations suivantes:

— Téléchargement des informations communes que contient la carte dans les EF (fichiers élémentaires) ICC et IC. Ces informations à caractère facultatif ne sont protégées par aucune signature numérique.

— (pour les cartes tachygraphiques de première et deuxième générations) Téléchargement des EF dans le fichier spécialisé Tachograph DF:

— Téléchargement des EF Card_Certificate 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 Tachograph DF) sauf l'EF Card_Download. Ces informations sont protégées par une signature numérique, conformément aux dispositions de l'appendice 11, Mécanismes de sécurité communs, partie A.

— Il y a lieu de télécharger au moins les Application_Identification et Identification 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,

— Control_Activity_Data,

— Specific_Conditions,

— (pour les cartes tachygraphiques de deuxième génération uniquement) Excepté lorsque le téléchargement d'une carte de conducteur insérée dans une VU est effectué durant le contrôle des conducteurs par une autorité de contrôle autre qu'une autorité de contrôle de l'UE, au moyen d'une carte de contrôle de première génération, télécharger les EF dans le Tachograph_G2 DF:

— Télécharger les EF CardSignCertificate, CA_Certificate et Link_Certificate (le cas échéant). 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 Tachograph_G2 DF) sauf l'EF Card_Download. Ces informations sont protégées par une signature numérique, conformément aux dispositions de l'appendice 11, Mécanismes de sécurité communs, partie B.

— Il y a lieu de télécharger au moins les Application_Identification et Identification 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,

— Control_Activity_Data,

— Specific_Conditions,

— VehicleUnits_Used,

— GNSS Places.

— Lors du téléchargement d'une carte de conducteur, il convient de mettre à jour la date LastCardDownload dans l'EF Card_Download, dans les DF Tachograph et, le cas échéant, Tachograph_G2 .

— Lors du téléchargement d'une carte d'atelier, il convient de réinitialiser le compteur d'étalonnage enregistré dans l'EF Card_Download dans les DF Tachograph et, le cas échéant, Tachograph_G2 .

— Lors du téléchargement d'une carte d'atelier, l'EF `Sensor_Installation_Data` dans les DF `Tachograph` et, le cas échéant, `Tachograph_G2` n'est pas téléchargé.»;

l) au point 3.3.2, le premier alinéa du paragraphe DDP_037 est remplacé par le texte suivant:

«La séquence du téléchargement des EF ICC, IC, Card_Certificate (ou CardSignCertificate pour le DF Tachograph_G2), CA_Certificate et Link_Certificate (pour le DF Tachograph_G2 uniquement) est la suivante:»;

m) au point 3.3.3, le tableau est remplacé comme suit:

«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, partie A ou B. Cette commande n'est pas une commande ISO.
Calculer le hachage du fichier et enregistrer temporairement la valeur de hachage retenue			
OK	⇨		
	⇦	**Read Binary**	Si le fichier contient plus de données que 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	conformément à **3.4** Data storage format
	⇦	**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	conformément à **3.4** Data storage format»

n) au point 3.4.2, le paragraphe DDP_046 est remplacé par le texte suivant:

«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) dans le Tachograph ou pour les informations communes que contient la carte	3 octets
FDI (2 octets) || "01"	Balise pour signature d'EF (FDI) dans le DF Tachograph	3 octets
FDI (2 octets) || "02"	Balise pour EF (FDI) dans le DF Tachograph_G2	3 octets
FDI (2 octets) || "03"	Balise pour signature d'EF (FDI) dans le DF Tachograph_G2	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 de l'EF ICC
C1 00 00	00 C2	— Données de l'EF Card_Certificate
		— ...
05 05 00	0A 2E	Données de l'EF Vehicles_Used (dans le DF Tachograph)
05 05 01	00 80	Signature de l'EF Vehicles_Used (dans le DF Tachograph)
05 05 02	0A 2E	Données de l'EF Vehicles_Used (dans le DF Tachograph_G2)
05 05 03	xx xx	Signature de l'EF Vehicles_Used (dans le DF Tachograph_G2)»

o) au point 4, le paragraphe DDP_049 est remplacé par le texte suivant:

«DDP_049 Cartes de conducteur de première génération: Les données doivent être téléchargées selon 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.

Cartes de conducteur de deuxième génération: 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 3 ainsi qu'à l'envoi à l'IDE de toutes les données extraites de la carte dans le format de fichier TLV approprié (cf. 3.4.2) et encapsulées dans un message "Réponse positive à une demande de transfert de données".»;

34) au point 2 de l'appendice 8, le paragraphe suivant l'intitulé «Références» est remplacé par le texte suivant:

«ISO 14230-2: Véhicules routiers — Systèmes de diagnostic — Protocole à mots clés 2000 — Partie 2: Couche de liaison de données.

Première édition: 1999.»;

35) l'appendice 9 est modifié comme suit:

a) dans la table des matières, le point 6 est remplacé par le texte suivant:

«6. ESSAIS DES ÉQUIPEMENTS EXTERNES DE COMMUNICATION À DISTANCE»;

b) au point 1.1, le premier tiret est remplacé par le texte suivant:

«— 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,»;

c) au point 2, le tableau des essais fonctionnels de l'unité embarquée sur le véhicule est remplacé par ce qui suit:

«N°	Essai	Description	Exigences connexes
1	**Examen administratif**		
1.1	Documentation	Exactitude de la documentation	
1.2	Résultats des essais menés par le fabricant	Résultats des essais menés par le fabricant pendant la phase d'intégration. Démonstrations sur papier.	88, 89,91
2	**Inspection visuelle**		
2.1	Conformité 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		02, 03, 04, 05, 07, 382
3.2	Modes d'exploitation		09 à 11*, 134, 135
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*, 134
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, 134
3.8	Surveillance de l'état de conduite		54, 55, 134
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, 134

N°	Essai	Description	Exigences connexes
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		136, 137, 138*, 139*, 141*, 142, 143 144, 145, 146*, 147*, 148*, 149, 150
3.28	Affichage		90, 134, 151 à 168, PIC_001, DIS_001
3.29	Impression		90, 134, 169 à 181, PIC_001, PRT_001 à PRT_014
3.30	Avertissement		134, 182 à 191, PIC_001
3.31	Téléchargement de données à destination de supports externes		90, 134, 192 à 196
3.32	Communication à distance pour les contrôles routiers ciblés		197 à 199
3.33	Données de sortie à destination de dispositifs externes supplémentaires		200, 201
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

N°	Essai	Description	Exigences connexes
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 à – 20 °C) Cet essai satisfait à la norme CEI 60068-2-1: Essais d'environnement — Partie 2-1: essais - essai A: froid Essai conforme à la norme ISO 16750-4: Chapitre 5.1.2.2: Essai 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 2 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.	219

N°	Essai	Description	Exigences connexes
		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/s^2, RMS longitudinal 11,8 m/s^2, RMS latéral 13,1 m/s^2, 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.	
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

N°	Essai	Description	Exigences connexes
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 = +37V Ri = 2 ohms impulsion 2b: Vs = +20V Ri = 0,05 ohms impulsion 3a: Vs = – 150V Ri = 50 ohms impulsion 3b: Vs = +150V Ri = 50 ohms impulsion 4: Vs = – 16 V Va = – 12 V t6 = 100 ms impulsion 5: Vs = + 120 V, Ri = 2,2 ohms, td = 250 ms Pour les versions 12V: conformité avec la norme ISO 7637-1 + Règlement CEE n° 10 Rév. 3: impulsion 1: Vs = –+75V Ri = 10 ohms impulsion 2a: Vs = +37V Ri = 2 ohms impulsion 2b: Vs = +10V Ri = 0,05 ohms impulsion 3a: Vs = – 112V Ri = 50 ohms impulsion 3b: Vs = +75V 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»

d) le point 6 est remplacé par le texte suivant:

«6. ESSAI DES ÉQUIPEMENTS EXTERNES 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
3.	**Essais de fonctionnement**		
3.1	Communication à distance pour les contrôles routiers ciblés		4, 197 à 199

N°	Essai	Description	Exigences connexes
3.2	Enregistrement et stockage de données sur la mémoire		91
3.3	Communication avec l'unité embarquée sur le véhicule		Appendice 14, paragraphes DSC_66 à DSC_70, DSC_71 à DSC_76
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 à -20 °C) Cet essai satisfait à la norme CEI 60068-2-1: Essais d'environnement — Partie 2-1: essais - essai A: froid Essai conforme à la norme ISO 16750-4: Chapitre 5.1.2.2: Essai 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 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	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 IP 40)	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

N°	Essai	Description	Exigences connexes
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 = +37V Ri = 2 ohms impulsion 2b: Vs = +20V Ri = 0,05 ohms impulsion 3a: Vs = -150V Ri = 50 ohms impulsion 3b: Vs = +150V Ri = 50 ohms impulsion 4: Vs = -16 V Va = -12 V t6 = 100 ms impulsion 5: Vs = + 120 V, Ri = 2,2 ohms, td = 250 ms Pour les versions 12V: conformité avec la norme ISO 7637-1 + Règlement CEE n° 10 Rév. 3: impulsion 1: Vs = -75V Ri = 10 ohms impulsion 2a: Vs = +37V Ri = 2 ohms impulsion 2b: Vs = +10V Ri = 0,05 ohms impulsion 3a: Vs = -112V Ri = 50 ohms impulsion 3b: Vs = +75V 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»

e) le tableau du point 8 relatif aux essais d'interopérabilité est remplacé par ce qui suit:

«N°	Essai	Description
	8.1 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.

N°	Essai	Description
	8.2 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.
	8.3 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.»

36) l'appendice 11 est modifié comme suit:

a) au point 8.2.3, le paragraphe CSM_49 est remplacé par le texte suivant:

«CSM_49 Les unités embarquées sur véhicule, les cartes tachygraphiques et les dispositifs GNSS externes devront être compatibles avec les algorithmes SHA-256, SHA-384 et SHA-512 définis dans [SHS].»;

b) au point 9.1.2, le premier alinéa du paragraphe CSM_58 est remplacé par le texte suivant:

«CSM_58 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 d'un certificat de lien est de 17 ans plus trois mois. La figure 1 de la section 9.1.7 l'illustre également.»;

c) au point 9.1.4, le paragraphe CSM_72 est remplacé par le texte suivant:

«CSM_72 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 sa MSCA afin d'obtenir un certificat VU correspondant, signé par la MSCA. La clé privée sert uniquement à une unité embarquée sur véhicule.»

d) le point 9.1.5 est modifié comme suit:

i) le paragraphe CSM_83 est remplacé par le texte suivant:

«CSM_83 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 qui la génère doit adresser la clé publique à sa MSCA afin d'obtenir un certificat pour carte correspondant, signé par la MSCA. La clé privée sert uniquement à la carte tachygraphique.»;

ii) le paragraphe CSM_88 est remplacé par le texte suivant:

«CSM_88 La durée de validité d'un certificat Card_MA est la suivante:

— Pour les cartes de conducteur: 5 ans

— Pour les cartes d'entreprise: 5 ans

— Pour les cartes de contrôle: 2 ans

— Pour les cartes d'atelier: 1 an»;

iii) au paragraphe CSM_91, le texte suivant est ajouté:

«— En outre, uniquement pour les cartes de contrôle, les cartes d'entreprise et les cartes d'atelier et seulement si ces cartes sont émises dans les trois premiers mois de la période de validité d'un nouveau certificat EUR: le certificat EUR plus ancien de deux générations, le cas échéant.

Remarque pour le dernier point: par exemple, au cours des trois premiers mois du certificat ERCA(3) (voir la figure 1), les cartes mentionnées incluent le certificat ERCA(1). L'inclusion du certificat ERCA est nécessaire pour permettre à ces cartes d'effectuer des téléchargements de données à partir des VU d'ERCA(1), dont la durée de vie normale de 15 ans, à laquelle s'ajoute la période de téléchargement des données de trois mois, expire au cours de ces mois; voir le dernier point de l'exigence 13 de l'annexe IC.»;

e) le point 9.1.6 est modifié comme suit:

i) le paragraphe CSM_93 est remplacé par le texte suivant:

«CSM_93 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 partie qui la génère doit adresser la clé publique à sa MSCA afin d'obtenir un certificat EGF_MA correspondant, signé par la MSCA. La clé privée sert uniquement au dispositif GNSS externe.»;

ii) le paragraphe CSM_95 est remplacé par le texte suivant:

«CSM_95 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 prévoit la section 11.4 du présent appendice.»;

f) le point 9.1.7 est modifié comme suit:

i) la figure 1 est remplacée par ce qui suit:

«*Figure 1*

Émission et utilisation de différentes générations de certificats racine ERCA, de certificats de lien ERCA, de certificats MSCA et d'équipement

»;

ii) dans les notes relatives à la figure 1, le paragraphe 6 est remplacé par le texte suivant:

«6. Pour gagner de l'espace, la différence entre les durées de validité des certificats Card_MA et des certificats Card_Sign n'est précisée que pour la première génération.»;

g) le point 9.2.1.1 est modifié comme suit:

i) au paragraphe CSM_106, le premier tiret est remplacé par le texte suivant:

«— 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 5D 83" »;

ii) au paragraphe CSM_107, le premier alinéa est remplacé par le texte suivant:

«Chaque fabricant de capteurs de mouvement génère une clé de couplage aléatoire unique K_P pour chaque capteur de mouvement et communique chaque clé de couplage à l'organisme de certification de son 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.»;

iii) le paragraphe CSM_108 est remplacé par le texte suivant:

«CSM_108 Chaque fabricant de capteurs de mouvement génère un numéro de série unique pour chaque capteur de mouvement et communique tous les numéros de série à l'organisme de certification de son 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.»;

h) le point 9.2.2.1 est modifié comme suit:

i) le paragraphe CSM_123 est remplacé par le texte suivant:

«CSM_123 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`.

Remarque:

— Ce numéro de série VU est identique à l'élément vuSerialNumber de VuIdentification (voir l'appendice 1) et à la référence du titulaire de certificat figurant dans les certificats de la VU.

— Le numéro de série de la VU peut ne pas être connu au moment où un fabricant d'unité embarquée sur véhicule demande les clés de DSRC propres à la VU. Dans ce cas, le fabricant de VU envoie l'ID unique de demande de certificat qu'il a utilisé au moment de sa demande de certificats de la VU; cf. CSM_153. Cet ID de demande de certificat est donc identique à la référence des organismes de certification indiquée dans les certificats de la VU.»;

ii) au paragraphe CSM_124, l'exigence en matière d'information à l'étape 2 est remplacée comme suit:

«info = numéro de série VU ou ID de la demande de certificat, comme indiqué au CSM_123»;

iii) le paragraphe CSM_128 est remplacé par le texte suivant:

«CSM_128 La MSCA archive toutes les clés DSRC propres aux VU qu'elle a générées, ainsi que leur numéro de version et le numéro de série VU ou l'ID de la demande de certificat utilisé pour les obtenir.»;

i) au point 9.3.1, le premier alinéa du paragraphe CSM_135 est remplacé par le texte suivant:

«Les règles de codage distinctes (DER) conformes à la norme [ISO 8825-1] servent à encoder les objets de données au sein des certificats. Le tableau 4 présente le codage intégral du certificat, y compris toutes les balises et les longueurs en octets.»;

j) au point 9.3.2.3, le paragraphe CSM_141 est remplacé par le texte suivant:

«CSM_141 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, qui indique le type d'équipement auquel est destiné le certificat. Concernant les certificats VU, les certificats de carte de conducteur et les certificats de carte d'atelier, le type d'équipement est également utilisé pour distinguer les certificats pour l'authentification mutuelle des certificats à utiliser pour la création d'une signature numérique (voir la section 9.1 et l'appendice 1, type de données EquipmentType).»;

k) au point 9.3.2.5, l'alinéa suivant est ajouté au paragraphe CSM_146:

«*Remarque:* pour un certificat de carte, la valeur du CHR est égale à la valeur de l'élément cardExtendedSerialNumber du fichier EF_ICC; voir appendice 2. Pour un certificat EGF, la valeur du CHR est égale à la valeur de l'élément sensorGNSSSerialNumber du fichier EF_ICC; voir appendice 14. Pour un certificat VU, la valeur du CHR est égale à l'élément vuSerialNumber de VuIdentification (voir l'appendice 1), à moins que le fabricant ne connaisse pas le numéro de série propre au fabricant au moment où le certificat est demandé.»;

l) au point 9.3.2.6, le paragraphe CSM_148 est remplacé par le texte suivant:

«CSM_148 La date d'entrée en vigueur du certificat indique la date et l'heure de début de la durée de validité du certificat.»;

m) le point 9.3.3 est modifié comme suit:

i) au paragraphe CSM_151, le premier alinéa est remplacé par le texte suivant:

«Lors de la demande d'un certificat, la MSCA adresse les données suivantes à l'ERCA:»;

ii) le paragraphe CSM_153 est remplacé par le texte suivant:

«CSM_153 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:

— S'il est connu (cf. CSM_154), 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.»;

n) le point 10.2.1 est modifié comme suit:

i) au paragraphe CSM_157, le texte précédant les notes relatives à la figure 4 est remplacé par le texte suivant:

«Les VU adoptent le protocole prévu à la figure 4 pour vérifier la chaîne de certificat d'une carte tachygraphique. Pour chaque certificat lu à partir de la carte, la VU vérifie que le champ "Autorisation du titulaire de certificat" (CHA) est correct:

— Le champ CHA du certificat Card indique un certificat Card pour l'authentification mutuelle (voir l'appendice 1, type de données EquipmentType).

— Le champ CHA du certificat Card.CA indique une MSCA.

— Le champ CHA du certificat Card.Link indique une ERCA.»;

ii) au paragraphe CSM_159, la phrase suivante est ajoutée:

«Si l'enregistrement de tous les autres types de certificats est facultatif, la VU a l'obligation d'enregistrer les nouveaux certificats de lien présentés par une carte.»;

o) le point 10.2.2 est modifié comme suit:

i) au paragraphe CSM_161, le texte précédant la figure 5 est remplacé par le texte suivant:

«Les cartes tachygraphiques adoptent le protocole prévu à la figure 5 pour vérifier la chaîne de certificat d'une VU. Pour chaque certificat présenté par la VU, la carte vérifie que le champ de l'autorisation du titulaire de certificat (CHA) est correct:

— Le champ CHA du certificat VU.Link indique l'ERCA.

— Le champ CHA du certificat VU.CA indique une MSCA.

— Le champ CHA du certificat VU indique un certificat VU pour l'authentification mutuelle (voir l'appendice 1, type de données EquipmentType).»;

ii) le paragraphe CSM_165 est remplacé par le texte suivant:

«CSM_165 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.PKeph). 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.PKeph) reçu. La carte réinitialise Comp(VU.PKeph) après une commande GENERAL AUTHENTICATE réussie.»;

p) le point 10.3 est modifié comme suit:

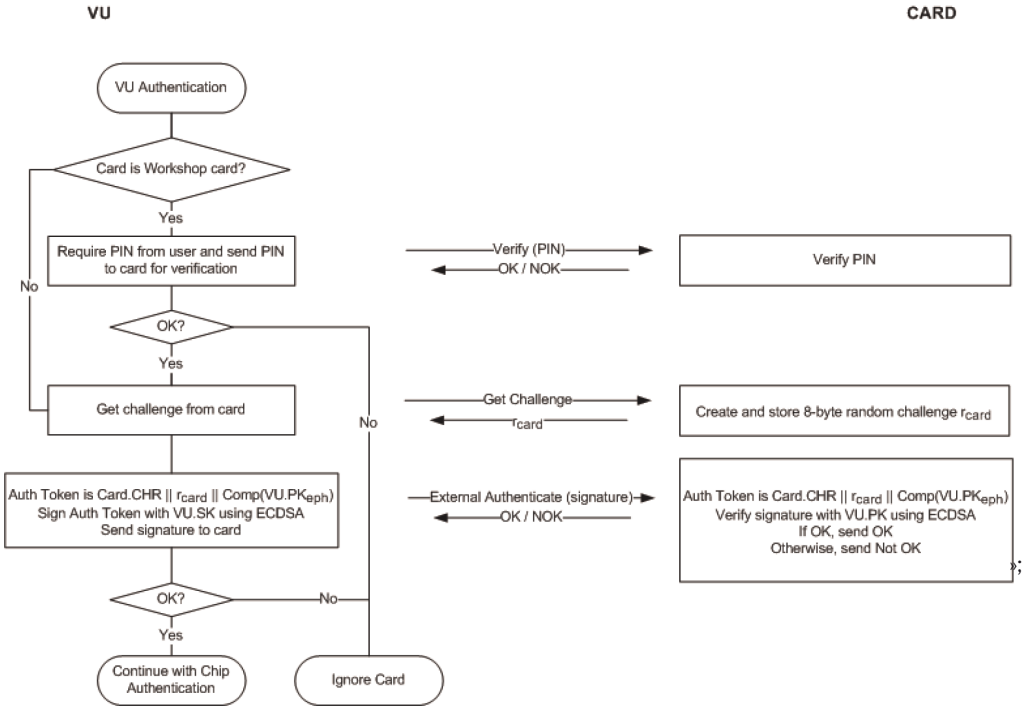
i) le premier alinéa du paragraphe CSM_170 est remplacé par le texte suivant:

«La VU inclut à proximité du défi de la carte, la signature de la référence du titulaire du certificat extraite du certificat de la carte.»;

ii) au paragraphe CSM_171, la figure 6 est remplacée comme suit:

«*Figure 6*

Protocole d'authentification de la VU



»;

iii) le paragraphe CSM_174 est remplacé par le texte suivant:

«CSM_174 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 rcard et l'identificateur de la clé publique éphémère de la VU Comp(VU.PKeph);

— vérifie la signature de la VU à l'aide de l'algorithme ECDSA, en utilisant l'algorithme de hachage associé à la taille de clé de la paire de clés VU_MA de la VU, conformément au CSM_50, combiné à la VU.PK et au jeton d'authentification calculé.»;

q) au point 10.4, le paragraphe CSM_176 est modifié comme suit:

i) le deuxième alinéa est remplacé par le texte suivant:

«2. La VU adresse le point public $VU.PK_{eph}$ de sa paire de clés éphémères à la carte. Le point public est converti en chaîne d'octets comme le précise le [TR-03111]. On utilise la structure cryptée non compressée. Conformément au CSM_164, 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.»;

ii) le sixième alinéa est remplacé par le texte suivant:

«6. En utilisant K_{MAC}, la carte calcule un jeton d'authentification en fonction du point public éphémère de la VU: $T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})$. Le point public prend le format utilisé par la VU (voir le point 2 ci-dessus). La carte envoie N_{PICC} et T_{PICC} à l'unité embarquée sur véhicule.»;

r) au point 10.5.2, le paragraphe CSM_191 est remplacé par le texte suivant:

«CSM_191 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, les objets de données de l'APDU sont complétés 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 2: CLA INS P1 P2 || Lc' || DO '97' || DO'8E' || Le

Cas 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 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 2 ou 4 (octet INS pair) sans cryptage: DO '81' || DO '99' || DO '8E' || SW1SW2

Cas 2 ou no 4 (octet INS pair) avec 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 1 ou 3 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

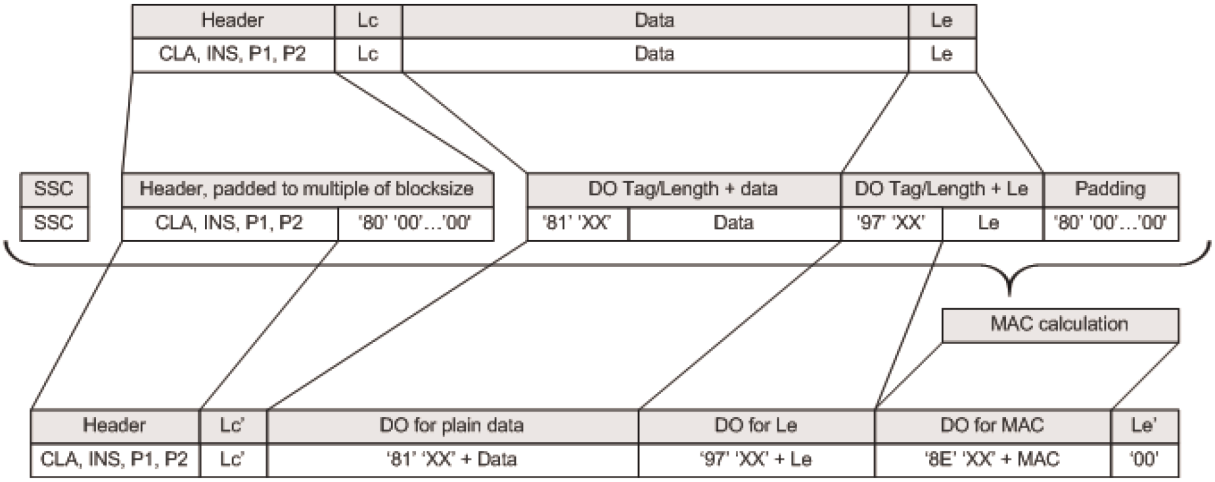


Figure 9

Transformation d'une réponse APDU authentifiée relevant des cas 1 ou 3

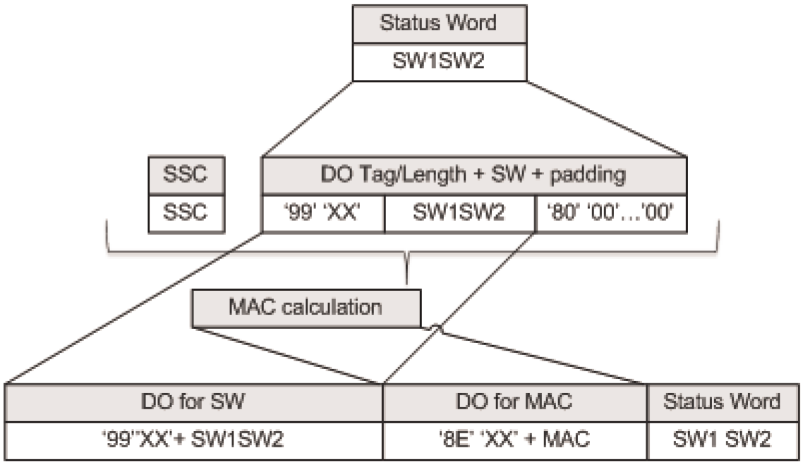
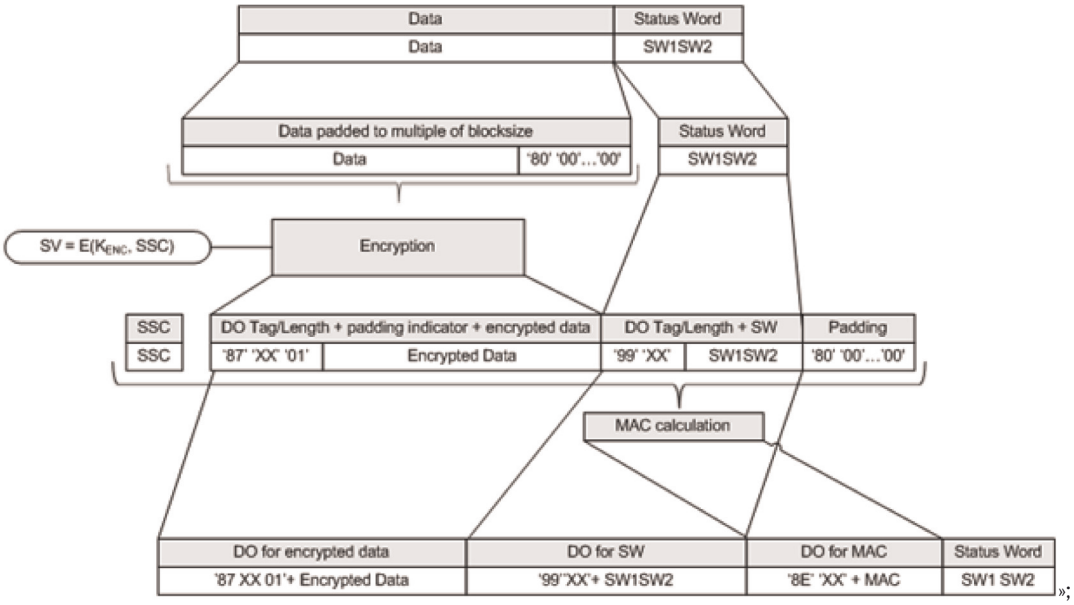


Figure 10

Transformation d'une réponse APDU cryptée et authentifiée relevant des cas 2 ou 4



»;

s) au point 10.5.3, le paragraphe CSM_193 est remplacé par le texte suivant:

«CSM_193 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 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.»;

t) le point 11.3.2 est modifié comme suit:

i) le premier alinéa du paragraphe CSM_208 est remplacé par le texte suivant:

"Pendant le couplage à une VU, un dispositif GNSS externe utilise le protocole décrit à la figure 5 (section 10.2.2) pour vérifier la chaîne de certification de la VU.";

ii) le paragraphe CSM_210 est remplacé par le texte suivant:

«CSM_210 Une fois le certificat VU_MA vérifié, le dispositif GNSS externe mémorise ce certificat pour l'utiliser en fonctionnement normal; cf. section 11.3.3.»;

u) au point 11.3.3, le premier alinéa du paragraphe CSM_211 est remplacé par le texte suivant:

«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 du certificat EGF_MA mémorisé 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.»;

v) au point 12.3, le tableau 6 est remplacé par le tableau suivant:

«*Tableau 6*

Nombre d'octets de données cryptées et en clair par instruction comme le prévoit la norme [ISO 16844-3]

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 (en bits) 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	32 / 48	32 / 48	32 / 48
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
70	demande	Données d'authentification	8	8	16	16	16
80	réponse	Valeur du compteur MoS + données d'authen.	8	8	16	16	16»

w) au point 13.1, l'exigence relative au numéro de série de la VU au paragraphe CSM_224 est remplacée par le texte suivant:

«**Numéro de série de la VU** le numéro de série de la VU ou l'ID de la demande de certificat (type de données VuSerialNumber ou CertificateRequestID) - voir le paragraphe CSM_123»;

x) au point 13.3, le paragraphe CSM_228, deuxième tiret, est remplacé par le texte suivant:

«2. La carte de contrôle utilise la clé maîtresse DSRC indiquée en combinaison avec le numéro de série de la VU ou l'ID de la demande de certificat 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 CSM_124.»;

y) le point 14.3 est modifié comme suit:

i) au paragraphe CSM_234, le texte précédant les notes relatives à la figure 13 est remplacé par le texte suivant:

«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. Pour vérifier la validité temporelle d'un certificat présenté par l'IDE, la carte de contrôle utilise son heure interne actuelle, comme indiqué au CSM_167. La carte de contrôle actualise son heure actuelle si la Date effective d'un certificat authentique représentant une "source d'heure valide" est plus récente que l'heure actuelle de la carte. 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 VU_Sign ou Card_Sign de deuxième génération émis par le même pays que le certificat de carte de ladite carte de contrôle.

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]. Dans les deux cas, pour chaque certificat lu depuis le fichier de données, il est nécessaire de vérifier que le champ "Autorisation du titulaire de certificat" (CHA) est correct:

— Le champ CHA du certificat EQT indique un certificat de la VU ou de la carte (le cas échéant) à signer (voir l'appendice 1, type de données EquipmentType).

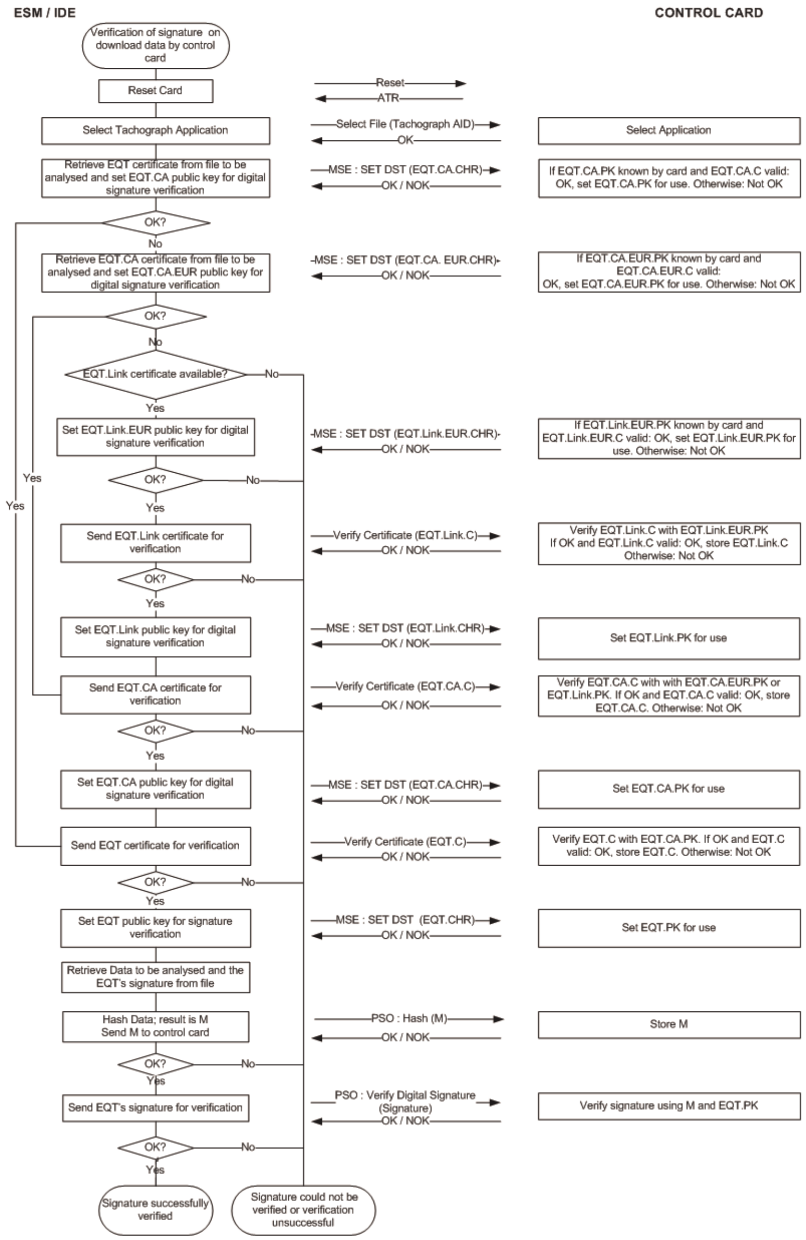
— Le champ CHA du certificat EQT.CA indique une MSCA.

— Le champ CHA du certificat EQT.Link indique une ERCA.»;

ii) la figure 13 est remplacée par ce qui suit:

«*Figure 13*

Protocole de vérification de la signature associée à un fichier de données téléchargé



»;

37) l'appendice 12 est modifié comme suit:

a) le point 3 est modifié comme suit:

i) au paragraphe GNS_4, le deuxième alinéa suivant la figure 2 est remplacé par le texte suivant:

«La résolution de la position repose sur la structure de la phrase RMC décrite ci-dessus. La première partie des champs 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).»;

ii) le paragraphe GNS_5 est remplacé par le texte suivant:

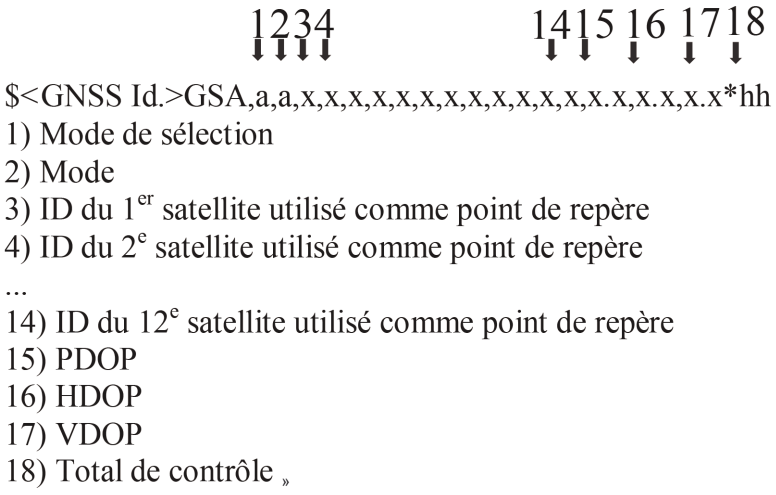
«GNS_5 L'unité embarquée sur le véhicule mémorise dans la base de données de la VU les informations relatives au positionnement en termes de latitude et de longitude selon une résolution d'1/10 minute ou 1/600 degré, comme le décrit l'appendice 1 pour les coordonnées géographiques type.

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 l'identifiant NMEA correspondant pour chaque constellation GNSS et pour le SBAS (Satellite-Based Augmentation System).

Figure 3

Structure de la phrase GSA



iii) le paragraphe GNS_6 est remplacé par le texte suivant:

«GNS_6 La phrase GSA est mémorisée avec le numéro d'enregistrement "02" à "06"»;

b) le point 4.2.1 est modifié comme suit:

i) le paragraphe GNS_16 est remplacé par le texte suivant:

«GNS_16 Le protocole de communication ne doit pas prendre en charge les zones de longueur étendue.»;

ii) le paragraphe GNS_18 est remplacé par le texte suivant:

«GNS_18 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 1.»;

iii) le paragraphe GNS_20 est remplacé par le texte suivant:

«GNS_20 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 1 fournit la modélisation des numéros d'enregistrement et des données. Remarque: il existe cinq phrases GSA correspondant aux constellations GNSS et au SBAS (Satellite-Based Augmentation System).»;

c) au point 4.2.2, le cinquième alinéa du paragraphe GNS_23 est remplacé par le texte suivant:

«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 minimale d'après les systèmes de satellites disponibles (p. ex., lorsque les points de repère sont disponibles).»;

d) au point 4.4.1, le paragraphe GNS_28 est remplacé par le texte suivant:

«GNS_28 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 "0E"H Communication error with the external GNSS facility assorti d'un horodatage indiquant l'heure actuelle. L'événement n'est généré que si les deux conditions suivantes sont satisfaites: a) le tachygraphe intelligent n'est pas en mode étalonnage et b) le véhicule 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.»;

e) au point 4.4.2, le paragraphe GNS_29 est remplacé par le texte suivant:

«GNS_29 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 événement de type EventFaultType enum "19"H Tamper detection of GNSS. Le dispositif GNSS externe peut également arrêter de répondre aux demandes externes.»;

f) au point 4.4.3, le paragraphe GNS_30 est remplacé par le texte suivant:

«GNS_30 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 "0D"H Absence of position information from GNSS receiver 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.»;

g) au point 4.4.4, le texte du paragraphe GNS_31, jusqu'à la figure 4, est remplacé par le texte suivant:

«Si la VU détecte que le certificat EGF utilisé pour l'authentification mutuelle n'est plus valide, la VU génère et enregistre un événement de l'équipement d'enregistrement de type EventFaultType enum *"1B"H External GNSS facility certificate expired* assorti d'un horodatage indiquant l'heure actuelle. La VU utilise encore les données de positionnement GNSS reçues.»;

h) au point 5.2.1, le paragraphe GNS_34 est remplacé par le texte suivant:

«GNS_34 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 "0D"H Absence of position information from GNSS receiver 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.»;

i) le point 6 est remplacé par le texte suivant:

«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)*. 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.»;

38) l'appendice 13 est modifié comme suit:

a) au point 2, le quatrième paragraphe est remplacé par le texte suivant:

«Pour plus de précision, le présent appendice ne spécifie 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 11 — Mécanismes de sécurité communs]).

— Les protocoles Bluetooth® qu'utilise l'interface ITS.»;

b) au point 4.2, le troisième alinéa est remplacé par le texte suivant:

"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. également 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 11 Mécanismes de sécurité communs.";

c) le point 4.3 est modifié comme suit:

i) le premier alinéa est remplacé par le texte suivant:

«Pour des raisons de sécurité, la VU nécessite 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.»;

ii) le troisième paragraphe suivant le tableau 1 est remplacé par le texte suivant:

«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 d'indiquer le code PIN directement sur la VU.»;

d) au point 4.4, le deuxième paragraphe suivant l'intitulé «zone de données» est remplacé par le texte suivant:

«Si les données à manipuler 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.»;

e) l'annexe 1 est modifiée comme suit:

i) le titre est remplacé par le texte suivant:

«1) LISTE DES DONNÉES DISPONIBLES GRÂCE À L'INTERFACE ITS»;

ii) l'élément suivant est inséré dans le tableau au point 3, après l'élément «Absence d'informations de position en provenance du récepteur GNSS»:

«Erreur de communication avec le dispositif GNSS externe	— 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.»

iii) au point 5, le tiret suivant est ajouté:

«— anomalie sur l'interface ITS (le cas échéant)»;

f) les spécifications ASN.1 à l'annexe 3 sont modifiées comme suit:

i) les lignes 206a à 206e ci-après sont insérées après la ligne 206:

```
»206a
206b       DriverID ::= SEQUENCE{
206c       issuingMemberState OCTET STRING (SIZE(3)),
206d       cardNumber OCTET STRING (SIZE(16))
206e }»;
```

ii) les lignes 262 à 264 sont remplacés comme suit:

```
«262    driveRecognize BIT STRING ('00'B UNION '01'B),
263     driverCardDriver1 BIT STRING ('00'B UNION '01'B),
264     driverCardDriver2 BIT STRING ('00'B UNION '01'B), »;
```

iii) la ligne 275 est remplacée comme suit:

```
«275    outOfScopeCondition BIT STRING ('00'B UNION '01'B),«;
```

iv) les lignes 288 à 310 sont remplacés comme suit:

```
«288    driver1WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNION
289     '011'B UNION '100'B UNION '101'B …),
290     driver2WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNION
291     '011'B UNION '100'B UNION '101'B …),
292
293     driver1TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
294     UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
295     '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
296     UNION '1011'B UNION '1100'B UNION '1101'B …),
297
298
299     driver2TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
300     UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
301     '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
302     UNION '1011'B UNION '1100'B UNION '1101'B …),
303
304
305
306     overSpeed BIT STRING ('00 'B UNION '01 'B),
307     driver1Identification DriverID,
308     driver2Identification DriverID,
309
310»
```

v) les lignes 362 et 363 sont remplacées comme suit:

```
«362    driver1MaximumDailyDrivingTime BIT STRING (SIZE(4)),
363     driver2MaximumDailyDrivingTime BIT STRING (SIZE(4)),»;
```

vi) les lignes 410a et 410b suivantes sont insérées après la ligne 410:

```
«410a   comErrorWithExternalGNSSFacility
410b    CommunicationErrorWithTheExternalGNSSFacility,»;
```

vii) les lignes 539a à 539j ci-après sont insérées après la ligne 539:

```
«539a     CommunicationErrorWithTheExternalGNSSFacility ::= SEQUENCE{
539b      beginDate GeneralizedTime,
539c      endDate GeneralizedTime,
539d      cardsType SEQUENCE OF UTF8String,
539e      cardsNumber SEQUENCE OF INTEGER,
539f      issuingMemberState SEQUENCE OF NationAlpha,
539g      cardsGeneration SEQUENCE OF INTEGER,
539h      numberOfSimilarEvent INTEGER
539i            }
539j»;
```

39) l'appendice 14 est modifié comme suit:

a) l'élément 5.5 de la table des matières est remplacé comme suit:

«5.5 Conformité à la directive (UE) 2015/719 ..... 490»;

b) au point 2, le troisième alinéa est remplacé par le texte suivant:

«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.»;

c) le point 5.1 est modifié comme suit:

i) au paragraphe DSC_19, le douzième tiret est remplacé par le texte suivant:

«— L'antenne DSRC-VU est placée de manière à optimiser la communication DSRC entre le véhicule et l'antenne de lecture en bord de route, lorsque le lecteur se trouve à une distance de 15 mètres devant le véhicule et à 2 mètres de hauteur, en ciblant le centre horizontal et vertical du pare-brise. Pour les véhicules légers, une installation sur la partie supérieure du pare-brise convient. Pour tous les autres véhicules, l'antenne DSRC est placée près de la partie inférieure ou de la partie supérieure du pare-brise.»;

ii) au paragraphe DSC_22, le premier alinéa est remplacé par le texte suivant:

«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 elle prend efficacement en charge les cas d'usage décrits en 4.1.2 et en 4.1.3.»;

d) au point 5.4.3, la séquence 7 est remplacée par ce qui suit:

«7	REDCR	>	DSRC-VU	Envoie GET.request concernant les données d'un autre attribut (si nécessaire)»

e) au point 5.4.4, le module ASN.1 au paragraphe DCS_40 est modifié comme suit:

i) la première ligne de la séquence relative au `TachographPayload` est remplacée par ce qui suit:

```
«tp15638VehicleRegistrationPlate LPN – Vehicle Registration Plate as per EN 15509[1]»
```

ii) la note de bas de page 1 suivante est ajoutée:

«1. Si un LPN contient un AlphabetIndicator LatinAlphabetNo2 ou latinCyrillicAlphabet, les caractères spéciaux sont retranscrits par l'unité d'interrogation routière en utilisant les règles spéciales prévues par l'annexe E de la norme ISO/DIS 14 906,2»;

iii) l'exposant 2 est supprimé de la ligne où l'horodatage de l'enregistrement actuel est défini;

iv) le module ASN.1 pour `RtmTransferAck` est remplacé par ce qui suit:

```
«RtmTransferAck ::= INTEGER {
                    Ok (1),
                    NoK (2)
                    } (1..255)»;
```

f) au point 5.4.5, l'élément RTM12 du tableau 14.3 est remplacé par le texte suivant:

«**RTM12** **Anomalie du capteur**	La VU génère une valeur exprimée 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 "36"H ou "37"H) a été enregistré au cours des 10 derniers jours. — 3 si un événement de type erreur de communication avec le dispositif GNSS externe "0E"H a été enregistré au cours des 10 derniers jours — 4 si à la fois des anomalies de capteur et des anomalies de récepteur GNSS ont été enregistrées au cours des 10 derniers jours — 5 si à la fois des anomalies de capteur et des erreurs de communication avec le dispositif GNSS externe ont été enregistrées au cours des 10 derniers jours — 6 si à la fois des anomalies de récepteur GNSS et des erreurs de communication avec le dispositif GNSS externe ont été enregistrées au cours des 10 derniers jours — 7 si des anomalies des trois types ont été enregistrées au cours des 10 derniers jours AUTREMENT, une valeur de 0 est attribuée si aucun événement n'a été enregistré au cours des 10 derniers jours.	– erreur de capteur un octet conformément au dictionnaire des données	`sensorFault INTEGER (0..255),;` »

g) au point 5.4.6, le paragraphe DSC_43 est remplacé par le texte suivant:

«DSC_43
Pour tous les échanges DSRC, les données sont codées à l'aide des règles PER (Packed Encoding Rules) NON ALIGNÉES, à l'exception de `TachographPayload` et `OwsPayload`;, qui sont encodées à l'aide des règles OER (Octet Encoding Rules) définies par la norme ISO/IEC 8825-7, Rec. ITU-T X.696.»;

h) au point 5.4.7, dans la quatrième colonne du tableau 14.9, le texte de la cellule décrivant `Rtm-ContextMark`; est remplacé par ce qui suit:

«Identificateur d'objet de la norme, partie et version prise en charge. Exemple: ISO (1) Standard (0) TARV (15638) part9 (9) Version1 (1).

Le premier octet est 06H, qui est l'identificateur d'objet. Le deuxième octet est 06H, qui est sa longueur. Les 6 octets suivants codent l'identificateur d'objet de l'exemple.»;

i) les points 5.5 et 5.5.1 sont remplacés par le texte suivant:

«5.5. **Conformité à la directive (UE) 2015/719**

5.5.1. *Récapitulatif*

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.»;

j) au point 5.6.1, l'alinéa a) du paragraphe DSC_68 est remplacé par le texte suivant:

«a) Pour que la fourniture de la VU et de la DSRC-VU, voire de différents lots de la DSRC-VU, puisse être sous-traitée à plusieurs fournisseurs, la connexion reliant la VU et la DSRC-VU non interne à la VU doit être une connexion ouverte normalisée. La VU doit être connectée à la DSRC-VU»;

k) au point 5.7.1, le paragraphe DSC_77 est remplacé par le texte suivant:

«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 '0C'H Communication error with the remote communication facility, ainsi que l'horodatage.»;

40) l'appendice 15 est modifié comme suit:

a) au point 2.2, le premier alinéa est remplacé par le texte suivant:

«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 du règlement (CEE) n° 3821/85), alors que la deuxième génération de cartes tachygraphiques est interopérable avec la deuxième génération d'unités embarquées sur les véhicules (conformément à l'annexe IC de la présente directive). De plus, les exigences ci-dessous s'appliquent.»;

b) le point 2.4.1, paragraphe MIG_11, est modifié comme suit:

i) le premier tiret est remplacé par le texte suivant:

«— EF ICC, IC non signés (facultatif), »;

ii) le troisième tiret est remplacé par le texte suivant:

«— d'autres EF de données d'application (au sein du DF Tachograph) 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 conducteur (et d'atelier) de deuxième génération (EF de données d'application au sein du DF Tachograph_G2).»;

c) au point 2.4.3, les points MIG_014 et MIG_015 sont remplacés par le texte suivant:

«MIG_014 En dehors du cadre du contrôle d'un conducteur par des autorités de contrôle autre que celles de l'UE, les données sont téléchargées depuis une unité embarquée sur 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 contrôle autres que celles de l'UE, il peut également être rendu possible de télécharger des données depuis des unités embarquées sur véhicule de deuxième génération selon les mécanismes de sécurité de première génération. Les données téléchargées auront alors 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.»

ANNEXE II

L'annexe II du règlement (UE) 2016/799 est modifiée comme suit:

1) au chapitre I, le point 1, paragraphe b), est remplacé par le texte suivant:

«b) d'un numéro d'homologation correspondant au numéro du certificat d'homologation établi pour le prototype de l'appareil de contrôle, de la feuille d'enregistrement ou de la carte tachygraphique, placé dans une position quelconque à proximité immédiate du rectangle.»;

2) au chapitre III, le point 5 est remplacé par le texte suivant:

«5. Présenté à l'homologation le .....»;

3) au chapitre IV, le point 5 est remplacé par le texte suivant:

«5. Présenté à l'homologation le .....»;