►**B**

RÈGLEMENT (CE) N° 2135/98 DU CONSEIL

du 24 septembre 1998

modifiant le règlement (CEE) n° 3821/85 concernant l'appareil de contrôle dans le domaine des transports par route et la directive 88/599/CEE concernant l'application des règlements (CEE) n° 3820/85 et (CEE) n° 3821/85

(JO L 274 du 9.10.1998, p. 1)

Modifié par:

		Journal officiel		
		n°	page	date
►**M1**	Règlement (CE) n° 1360/2002 de la Commission du 13 juin 2002	L 207	1	5.8.2002

▼B

RÈGLEMENT (CE) Nº 2135/98 DU CONSEIL

du 24 septembre 1998

modifiant le règlement (CEE) nº 3821/85 concernant l'appareil de contrôle dans le domaine des transports par route et la directive 88/599/CEE concernant l'application des règlements (CEE) nº 3820/85 et (CEE) nº 3821/85

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité instituant la Communauté européenne, et notamment son article 75, paragraphe 1, points c) et d),

vu la proposition de la Commission ([1]),

vu l'avis du Comité économique et social ([2]),

statuant conformément à la procédure visée à l'article 189 C du traité ([3]),

(1) considérant que le règlement (CEE) nº 3821/85 du Conseil du 20 décembre 1985 concernant l'appareil de contrôle dans le domaine des transports par route ([4]) fixe un certain nombre de dispositions relatives à la construction, l'installation, l'utilisation et l'essai des appareils de contrôle utilisés dans le transport par route;

(2) considérant que l'expérience a montré que les pressions économiques et concurrentielles dans le domaine des transports par route ont amené certains conducteurs employés par les entreprises de transport à ne pas respecter certaines règles, notamment celles relatives aux temps de conduite et de repos, définies par le règlement (CEE) nº 3820/85 du Conseil du 20 décembre 1985 relatif àl'harmonisation de certaines dispositions en matière sociale dans le domaine des transports par route ([5]);

(3) considérant que les infractions et les fraudes caractérisées mettent en péril la sécurité routière et sont inacceptables, pour des raisons de concurrence, pour le conducteur respectueux de la réglementation;

(4) considérant que l'enregistrement automatique et le contrôle régulier, tant par l'entreprise que par les autorités compétentes, de données relatives aux prestations et au comportement du conducteur, ainsi que celles concernant le mouvement des véhicules, telles que la vitesse et la distance parcourue, sont de nature à améliorer la sécurité routière;

(5) considérant que les dispositions sociales communautaires imposent un certain nombre de contraintes en ce qui concerne les temps de conduite et de repos quotidiens et les temps de conduite et de repos observés sur une période de deux semaines; qu'il est difficile de contrôler le respect de ces dispositions, étant donné que les données sont actuellement enregistrées sur plusieurs feuilles journalières, constituant elles-mêmes le stock de feuilles, couvrant la semaine en cours et le dernier jour de la semaine précédente, à conserver dans la cabine du conducteur;

(6) considérant par conséquent que, pour mettre fin aux abus les plus fréquents auxquels le système actuel donne lieu, il est nécessaire d'introduire de nouveaux équipements de pointe, tels qu'un appareil de contrôle muni d'une unité de stockage électro-

([1]) JO C 243 du 31.8.1994, p. 8 et JO C 370 du 31.12.1985, p. 1.
([2]) JO C 110 du 21.4.1995, p. 19.
([3]) Avis du Parlement européen du 13 juillet 1995 (JO C 249 du 25.9.1995, p. 128), position commune du 11 décembre 1997 (JO C 43 du 9.2.1998, p. 6) et décision du Parlement européen du 31 mars 1998 (JO C 138 du 4.5.1998, p. 26).
([4]) JO L 370 du 31.12.1985, p. 8. Règlement modifié en dernier lieu par le règlement (CE) nº 1056/97 de la Commission (JO L 154 du 12.6.1997, p. 21).
([5]) JO L 370 du 31.12.1985, p. 1.

▼B

nique des informations pertinentes et une carte de conducteur personnelle, ces équipements visant à assurer la disponibilité, la clarté, la facilité de lecture, l'impression et la fiabilité des données enregistrées et permettant d'établir un bilan incontestablede l'activité déployée, d'une part, par le conducteur au cours des derniers jours et, d'autre part, par le véhicule sur une durée de plusieurs mois;

(7) considérant que la sécurité globale du système et de ses composants est un élément essentiel de l'efficacité d'un appareil de contrôle;

(8) considérant qu'il y a lieu de prévoir des dispositions concernant les conditions de délivrance et d'utilisation des cartes à mémoire prévues par l'annexe I B;

(9) considérant que les données relatives à l'activité des conducteurs doivent pouvoir être vérifiées par les conducteurs, par les entreprises qui les emploient et par les autorités compétentes des États membres; qu'il convient toutefois que le conducteur et l'entreprise puissent accéder uniquement aux données pertinentes pour l'exercice de leurs activités respectives;

(10) considérant que l'appareil de contrôle prévu par le présent règlement doit être installé sur les véhicules mis en circulation pour la première fois après la publication au *Journal officiel des Communautés européennes* des spécifications techniques, dont certaines sont définies par la Commission selon la procédure de comité visée à l'article 18 du règlement (CEE) nº 3821/85; qu'une période transitoire est nécessaire aux fins d'assurer que les nouveaux appareils de contrôle soient fabriqués conformément à ces spécifications techniques et obtiennent l'homologation CE;

(11) considérant qu'il est souhaitable que les appareils de contrôle conformes à l'annexe I B offrent également la possibilité d'élargir, pour un coût raisonnable, les fonctions de gestion du matériel roulant;

(12) considérant que, conformément au principe de subsidiarité, une action communautaire est nécessaire pour modifier le règlement (CEE) nº 3821/85 afin de garantir, d'une part, la compatibilité des appareils de contrôle conformes à l'annexe I B avec les cartes à mémoire et, d'autre part, la cohérence des données fournies par les appareils de contrôle conformes aux annexes I et I B;

(13) considérant que les progrès de la technique nécessitent une adaptation rapide des prescriptions techniques définies par les annexes du présent règlement; qu'il convient, pour faciliter la mise en œuvre des mesures nécessaires à cet effet, de prévoir que les adaptations techniques de ces annexes seront approuvées par la Commission, agissant selon la procédure de comité, conformément à la décision 87/373/CEE du Conseil du 13 juillet 1987 fixant les modalités de l'exercice des compétences d'exécution conférées à la Commission ([1]);

(14) considérant que l'introduction d'un nouvel appareil de contrôle implique la modification de certaines dispositions de la directive 88/599/CEE ([2]) concernant l'application des règlements (CEE) nº 3820/85 et (CEE) nº 3821/85,

([1]) JO L 197 du 18.7.1987, p. 33.
([2]) JO L 325 du 29.11.1988, p. 55.

▼B

A ARRÊTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Le règlement (CEE) nº 3821/85 est modifié comme suit

1) À l'article 1er, l'élément de phrase «y compris les annexes I et II» est remplacé par «y compris les annexes I ou I B et II».

2) Aux articles 4, 5, 6, 7, 8 et 11, la référence aux feuilles d'enregistrement est chaque fois suivie des termes «ou (de) (la) carte à mémoire».

3) À l'article 4, est inséré, avant le premier alinéa, le nouvel alinéa suivant:

«Aux fins du présent chapitre, les termes “appareil de contrôle” s'entendent comme “appareil de contrôle ou ses composants”.»

4) À l'article 5, le premier alinéa est remplacé par les alinéas suivants:

«Chaque État membre accorde l'homologation CE à tout modèle d'appareil de contrôle, à tout modèle de feuille d'enregistrement ou (de) carte à mémoire si ceux-ci sont conformes aux prescriptions des annexes I ou I B et si l'État membre est à même de surveiller la conformité de la production au modèle homologué.

La sécurité du système doit être conforme aux prescriptions techniques prévues à l'annexe I B. La Commission, agissant selon la procédure prévue à l'article 18, veille à ce que cette annexe prévoie que l'homologation CE ne puisse être accordée à l'appareil de contrôle que lorsque l'ensemble du système (appareil de contrôle lui-même, carte à mémoire et connexions électriques à la boîte de vitesses) a démontré sa capacité à résister aux tentatives de manipulation ou d'altération des données relatives aux heures de conduite. Les essais nécessaires à cet égard sont effectués par des experts au fait des techniques les plus récentes en matière de manipulation.»

5) À l'article 12:

a) Au paragraphe 1 sont ajoutés les alinéas suivants:

«La durée de validité administrative des cartes d'ateliers et d'installateurs agréés ne peut dépasser un an.

En cas de renouvellement, d'endommagement, de mauvais fonctionnement, de perte ou de vol de la carte délivrée aux ateliers et installateurs agréés, l'autorité fournit une carte de remplacement dans un délai de cinq jours ouvrables suivant la réception d'une demande circonstanciée à cet effet.

Lorsqu'une nouvelle carte est délivrée en remplacement de l'ancienne, la nouvelle carte porte le même numéro d'information “atelier”, mais l'indice est majoré d'une unité. L'autorité délivrant la carte tient un registre des cartes perdues, volées ou défaillantes.

Les États membres prennent toutes les mesures nécessaires pour éviter tout risque de falsification des cartes distribuées aux installateurs et ateliers agréés.»

b) Le paragraphe 2 est remplacé par le texte suivant:

«2. L'installateur ou atelier agréé appose une marque particulière sur les scellements qu'il effectue et, en outre, pour les appareils de contrôle conformes à l'annexe I B, introduit les données électroniques de sécurité permettant, notamment, les contrôles d'authentification. Les autorités compétentes de chaque État membre tiennent un registre des marques et des données électroniques de sécurité utilisées ainsi que des cartes d'ateliers et d'installateurs agréés délivrées.»

c) Le paragraphe 3 est remplacé par le texte suivant:

«3. Les autorités compétentes des États membres transmettent à la Commission la liste des installateurs et ateliers agréés

▼B

ainsi que des cartes qui leur sont délivrées et elles lui communiquent copie des marques et des informations nécessaires relatives aux données électroniques de sécurité utilisées.»

d) Au paragraphe 4, les termes «à l'annexe I» sont remplacés par «aux annexes I et I B».

e) Au paragraphe 5, après les termes «paragraphe 4», sont insérés les termes «ou à l'annexe I B, chapitre VI, point c)».

6) L'article 13 est remplacé par le texte suivant:

«Article 13

L'employeur et les conducteurs veillent au bon fonctionnement et à la bonne utilisation, d'une part, de l'appareil de contrôle et, d'autre part, de la carte de conducteur au cas où le conducteur est appelé à conduire un véhicule équipé d'un appareil de contrôle conforme à l'annexe I B.»

7) À l'article 14:

a) Le paragraphe 1 est remplacé par le texte suivant:

«1. L'employeur délivre aux conducteurs de véhicules équipés d'un appareil de contrôle conforme à l'annexe I un nombre suffisant de feuilles d'enregistrement, compte tenu du caractère individuel de ces feuilles, de la durée du service et de l'obligation de remplacer éventuellement les feuilles endommagées ou celles saisies par un agent chargé du contrôle. L'employeur ne remet aux conducteurs que des feuilles d'un modèle homologué aptes à être utilisées dans l'appareil installé à bord du véhicule.

Au cas où le véhicule est équipé d'un appareil de contrôle conforme à l'annexe I B, l'employeur et le conducteur veillent à ce que, compte tenu de la durée du service, l'impression sur demande visée à l'annexe I B puisse s'effectuer correctement en cas de contrôle.»

b) Les paragraphes 3, 4 et 5 suivants sont ajoutés:

«3. La carte de conducteur visée à l'annexe I B est délivrée, à la demande du conducteur, par l'autorité compétente de l'État membre dans lequel il a sa résidence normale.

Un État membre peut exiger que tout conducteur soumis aux dispositions du règlement (CEE) n° 3820/85 ayant sa résidence normale sur son territoire soit détenteur de la carte de conducteur.

a) Aux fins du présent règlement, on entend par “résidence normale” le lieu où une personne demeure habituellement, c'est-à-dire pendant au moins cent quatre-vingt-cinq jours par année civile, en raison d'attaches personnelles et professionnelles ou, dans le cas d'une personne sans attaches professionnelles, en raison d'attaches personnelles, révélant des liens étroits entre celle-ci et l'endroit où elle habite.

Toutefois, la résidence normale d'une personne dont les attaches professionnelles sont situées dans un lieu différent de celui de ses attaches personnelles, et qui, de ce fait, est amenée à séjourner alternativement dans leslieux différents situés dans deux ou plusieurs États membres, est censée se trouver au lieu de ses attaches personnelles, à condition qu'elle y retourne régulièrement. Cette dernière condition n'est pas requise lorsque la personne effectue un séjour dans un État membre pour l'exécution d'une mission d'une durée déterminée.

b) Les conducteurs apportent la preuve du lieu de leur résidence normale, par tous moyens, notamment par leur carte d'identité, ou par tout autre document valable.

c) Dans le cas où les autorités compétentes de l'État membre de délivrance de la carte de conducteur ont des doutes sur la validité de la déclaration de la résidence normale effectuée

▼B

conformément au point b), ou aux fins de certains contrôles spécifiques, elles peuvent demander des éléments d'information ou des preuves supplémentaires.

d) Les autorités compétentes de l'État membre de délivrance s'assurent, autant que faire se peut, que le demandeur n'est pas déjà titulaire d'une carte de conducteur en cours de validité.

4. a) L'autorité compétente de l'État membre personnalise la carte de conducteur conformément aux dispositions de l'annexe I B.

La durée de validité administrative de la carte de conducteur ne peut dépasser cinq ans.

Le conducteur ne peut être titulaire que d'une seule carte en cours de validité. Il n'est autorisé à utiliser que sa propre carte personnalisée. Il ne doit pas utiliser de carte défectueuse ou dont la validité a expiré.

Lorsqu'une nouvelle carte est délivrée au conducteur en remplacement de l'ancienne, la nouvelle carte porte le même numéro de série de carte de conducteur, mais l'indice est majoré d'une unité. L'autorité délivrant la carte tient un registre des cartes délivrées, volées, perdues ou défectueuses durant une période correspondant au moins à la durée de validité.

En cas d'endommagement, de mauvais fonctionnement, de perte ou de vol de la carte de conducteur, l'autorité fournit une carte de remplacement dans un délai de cinq jours ouvrables suivant la réception d'une demande circonstanciée à cet effet.

En cas de demande de renouvellement d'une carte dont la date de validité arrive à expiration, l'autorité fournit une nouvelle carte avant la date d'échéance pour autant que cette demande lui ait été adressée dans les délais prévus à l'article 15, paragraphe 1, deuxième alinéa.

b) Les cartes de conducteur ne sont délivrées qu'aux demandeurs qui sont soumis aux dispositions du règlement (CEE) nº 3820/85.

c) La carte de conducteur est personnelle. Elle ne peut faire l'objet, pendant la durée de sa validité administrative, d'un retrait ou d'une suspension pour quelque motif que ce soit, sauf si l'autorité compétente d'un État membre constate que la carte a été falsifiée, que le conducteur utilise une carte dont il n'est pas titulaire ou que la carte détenue a été obtenue sur la base de fausses déclarations et/ou de documents falsifiés. Si les mesures de suspension ou de retrait susmentionnées sont prises par un État membre autre que celui qui a délivré la carte, cet État membre renvoie la carte aux autorités de l'État membre qui l'ont délivrée en indiquant les raisons de cette restitution.

d) Les cartes de conducteur délivrées par les États membres sont mutuellement reconnues.

Lorsque le titulaire d'une carte de conducteur en cours de validité délivrée par un État membre a fixé sa résidence normale dans un autre État membre, il peut demander l'échange de sa carte contre une carte de conducteur équivalente; il appartient à l'État membre qui effectue l'échange de vérifier, au besoin, si la carte présentée est effectivement encore en cours de validité.

Les États membres qui effectuent un échange renvoient l'ancienne carte aux autorités de l'État membre qui l'ont délivrée et indiquent les raisons de cette restitution.

e) Lorsqu'un État membre remplace ou échange une carte de conducteur, ce remplacement ou cet échange, ainsi que tout remplacement ou renouvellement ultérieur, est enregistré dans cet État membre.

▼B

f) Les États membres prennent toutes les mesures nécessaires pour éviter tout risque de falsification des cartes de conducteur.

5. Les États membres veillent à ce que les données nécessaires au contrôle du respect du règlement (CEE) nº 3820/85 et de la directive 92/6/CEE du Conseil du 10 février 1992 relative à l'installation et à l'utilisation, dans la Communauté, de limiteurs de vitesse sur certaines catégories de véhicules à moteur (*), enregistrées et gardées en mémoire par les appareils de contrôle conformément à l'annexe I B du présent règlement, soient gardées en mémoire pendant aumoins trois cent soixante-cinq jours après la date de leur enregistrement et puissent être rendues disponibles dans des conditions qui garantissent la sécurité et l'exactitude de ces données.

Les États membres prennent toutes les mesures nécessaires pour s'assurer que les opérations de revente ou de mise hors service des appareils de contrôle ne puissent pas nuire notamment à la bonne application du présent paragraphe.

(*) JO L 57 du 2.3.1992, p. 27.»

8) À l'article 15:

a) Au paragraphe 1, et au paragraphe 2, premier alinéa, la référence aux feuilles d'enregistrement est chaque fois suivie des termes «ou (de) (la) carte de conducteur».

b) Au paragraphe 1:

— l'alinéa suivant est inséré après le premier alinéa:

«Lorsque les conducteurs souhaitent renouveler leur carte de conducteur, ils doivent en faire la demande auprès des autorités compétentes de l'État membre dans lequel ils ont leur résidence normale, au plus tard quinze jours ouvrables avant la date d'expiration de la carte.»;

— l'alinéa suivant est ajouté après le troisième alinéa:

«En cas d'endommagement, de mauvais fonctionnement, de perte ou de vol de la carte de conducteur, les conducteurs doivent en demander, dans les sept jours de calendrier, le remplacement auprès des autorités compétentes de l'État membre dans lequel ils ont leur résidence normale.»

c) Après le paragraphe 5, le paragraphe suivant est inséré:

«5 *bis*. Le conducteur introduit dans l'appareil de contrôle conforme à l'annexe I B le symbole du pays où il commence et celui du pays où il finit sa période de travail journalière. Un État membre peut toutefois imposer aux conducteurs de véhicules effectuant un transport intérieur sur son territoire d'ajouter au symbole du pays des spécifications géographiques plus détaillées, pour autant que cet État membre les ait notifiées à la Commission avant le 1er avril 1998 et que leur nombre n'excède pas vingt.

Les entrées des données susvisées sont activées par le conducteur, elles peuvent être soit entièrement manuelles, soit automatiques lorsque l'appareil de contrôle est relié à un système de positionnement par satellite.»

d) Au paragraphe 6, premier alinéa, sont ajoutés, en début de phrase, après le mot «appareil», les termes «de contrôle défini à l'annexe I».

e) Le paragraphe 7 est remplacé par le texte suivant:

«7. Lorsque le conducteur conduit un véhicule équipé d'un appareil de contrôle conforme à l'annexe I, il doit être en mesure de présenter, à toute demande des agents de contrôle:

— les feuilles d'enregistrement de la semaine en cours et, en tout cas, la feuille du dernier jour de la semaine précédente au cours duquel il a conduit,

— la carte de conducteur s'il est titulaire d'une telle carte

▼B

et

— les documents d'impression issus de l'appareil de contrôle défini à l'annexe I B et relatifs aux groupes de temps indiqués au paragraphe 3, deuxième tiret, points a), b), c) et d), dans le cas où le conducteur aurait conduit un véhicule équipé d'un tel appareil de contrôle durant la période visée au premier tiret du présent paragraphe.

Lorsque le conducteur conduit un véhicule équipé d'un appareil de contrôle conforme à l'annexe I B, il doit être en mesure de présenter, à toute demande des agents de contrôle:

— la carte de conducteur dont il est titulaire

et

— les feuilles d'enregistrement correspondant à la même période que celle visée au premier alinéa, premier tiret, dans le cas où il aurait conduit, pendant cette période, un véhicule équipé d'un appareil de contrôle conforme à l'annexe I.

Un agent habilité peut contrôler le respect du règlement (CEE) nº 3820/85 par l'analyse des feuilles d'enregistrement, des données affichées ou imprimées qui ont été enregistrées par l'appareil de contrôle ou par la carte de conducteur et, à défaut, par l'analyse de tout autre document probant permettant de justifier le non-respect d'une disposition telle que celles prévues à l'article 16, paragraphes 2 et 3.»

f) Le paragraphe suivant est ajouté:

«8. Il est interdit de falsifier, d'effacer ou de détruire les enregistrements faits sur la feuille d'enregistrement, les données stockées dans l'appareil de contrôle ou la carte de conducteur, ainsi que les documents d'impression issus de l'appareil de contrôle défini à l'annexe I B. Il est également interdit de manipuler l'appareil de contrôle, la feuille d'enregistrement ou la carte deconducteur de manière à falsifier les enregistrements et/ou les documents d'impression, à les rendre inaccessibles ou à les détruire. Le véhicule ne peut être équipé d'aucun dispositif permettant d'effectuer les manipulations mentionnées ci-dessus.»

9) À l'article 16:

a) Le paragraphe 2 est remplacé par le texte suivant:

«2. Durant la période de panne ou de mauvais fonctionnement de l'appareil de contrôle, le conducteur reporte les indications relatives aux groupes de temps, dans la mesure où ceux-ci ne sont plus enregistrés ou imprimés par l'appareil de contrôle de façon correcte, sur la ou les feuilles d'enregistrement ou sur une feuille *ad hoc* à joindre soit à la feuille d'enregistrement, soit à la carte de conducteur et sur laquelle il reporte les éléments permettant de l'identifier (nom et numéro de son permis de conduire ou nom et numéro de sa carte de conducteur), y compris sa signature.

En cas de perte, de vol, de détérioration ou de mauvais fonctionnement de sa carte, le conducteur imprime, à la fin de son voyage, les indications relatives aux groupes de temps enregistrés par l'appareil de contrôle et reporte sur le document d'impression les éléments permettant de l'identifier (nom et numéro de son permis de conduire ou nom et numéro de sa carte de conducteur) et y appose sa signature.»

b) Le paragraphe suivant est ajouté:

«3. En cas de détérioration ou de mauvais fonctionnement de sa carte, le conducteur la retourne à l'autorité compétente de l'État membre dans lequel il a sa résidence normale. Le vol de la carte de conducteur doit faire l'objet d'une déclaration en bonne et due forme auprès des autorités compétentes de l'État où le vol s'est produit.

▼B

La perte de la carte de conducteur doit faire l'objet d'une déclaration en bonne et due forme auprès des autorités compétentes de l'État qui l'a délivrée et auprès de celles de l'État membre de résidence normale dans le cas où celles-ci seraient différentes.

Le conducteur peut continuer à conduire son véhicule sans carte personnelle durant une période maximale de quinze jours de calendrier, ou pendant une période plus longue s'il le faut pour permettre au véhicule de regagner le siège de l'entreprise, à condition qu'il puisse justifier de l'impossibilité de présenter ou d'utiliser sa carte durant cette période.

Lorsque les autorités de l'État membre dans lequel le conducteur a sa résidence normale sont différentes de celles qui ont délivré sa carte et qu'elles sont appelées à procéder au renouvellement, au remplacement ou à l'échange de la carte de conducteur, elles informent les autorités qui ont délivré l'ancienne carte des motifs exacts de son renouvellement, de son remplacement ou de son échange.»

10) L'article 17 est remplacé par le texte suivant:

«Article 17

1. Les modifications qui sont nécessaires pour l'adaptation des annexes aux progrès techniques sont arrêtées selon la procédure prévue à l'article 18.

2. Les spécifications techniques relatives aux points suivants de l'annexe I B sont arrêtées, dans les meilleurs délais, et si possible avant le 1er juillet 1998, selon la même procédure:

a) chapitre II:

— point d), 17:

affichage et impression des défaillances de l'appareil de contrôle,

— point d), 18:

affichage et impression des défaillances de la carte de conducteur,

— point d), 21:

affichage et impression de rapports de synthèse;

b) chapitre III:

— point a), 6.3:

normes applicables pour la protection de l'électronique embarquée contre les parasites électriques et les charges magnétiques,

— point a), 6.5:

protection (sécurité) de la totalité du système,

— point c), 1:

signaux d'avertissement pour dysfonctionnements internes de l'appareil de contrôle,

— point c), 5:

format des signaux d'avertissement,

— point f):

erreurs maximales tolérées;

c) chapitre IV, point A:

— point 4:

normes,

— point 5:

sécurité, y compris la protection des données,

— point 6:

températures,

▼B

— point 8:

caractéristiques électriques,

— point 9:

structure logique de la carte de conducteur,

— point 10:

fonctions et commandes,

— point 11:

fichiers élémentaires;

et chapitre IV, point B;

d) chapitre V:

imprimante et impression standard.»

11) L'article 18 est remplacé par le texte suivant:

«Article 18

1. Lorsqu'il est fait référence à la procédure définie au présent article, la Commission est assistée par un comité composé des représentants des États membres et présidé par le représentant de la Commission.

2. Le représentant de la Commission soumet au comité un projet des mesures à prendre. Le comité émet son avis sur ce projet, dans un délai que le président peut fixer en fonction de l'urgence de la question en cause. L'avis est émis à la majorité prévue à l'article 148, paragraphe 2, du traité pour l'adoption des décisions que le Conseil est appelé à prendre sur proposition de la Commission. Lors des votes au sein du comité, les voix des représentants des États membres sont affectées de la pondération définie à l'article précité. Le président ne prend pas part au vote.

3. a) La Commission arrête les mesures envisagées lorsqu'elles sont conformes à l'avis du comité.

b) Lorsque les mesures envisagées ne sont pas conformes à l'avis du comité, ou en l'absence d'avis, la Commission soumet sans tarder au Conseil une proposition relative aux mesures à prendre. Le Conseil statue à la majorité qualifiée.

Si à l'expiration d'un délai de trois mois à compter de la saisine du Conseil, celui-ci n'a pas statué, les mesures proposées sont arrêtées par la Commission.»

12) L'annexe I B, figurant à l'annexe du présent règlement, est ajoutée.

Article 2

1. a) Les véhicules mis en circulation pour la première fois plus de vingt-quatre mois après la date de publication, au *Journal officiel des Communautés européennes*, de l'acte à arrêter en vertu de l'article 17, paragraphe 2, du règlement (CEE) n° 3821/85, tel que modifié par le présent règlement, devront être équipés d'un appareil de contrôle conforme aux prescriptions de l'annexe I B du règlement (CEE) n° 3821/85.

b) À compter de la date d'entrée en vigueur des dispositions du point a), les véhicules affectés au transport de personnes qui comportent, outre le siège du conducteur, plus de huit places assises et ont un poids maximal excédant 10 tonnes, de même que les véhicules affectés au transport de marchandises qui ont un poids maximal excédant 12 tonnes, immatriculés pour la première fois à partir du 1er janvier 1996, sont soumis, dans la mesure où la transmission des signaux s'effectue entièrement électriquement vers l'appareil de contrôle dont ils sont équipés, aux dispositions de l'annexe I B du règlement (CEE) n° 3821/85 lorsqu'il est procédé au remplacement dudit appareil.

2. Les États membres prennent les mesures nécessaires pour pouvoir délivrer les cartes de conducteur au plus tard vingt et un mois après la date de publication de l'acte visé au paragraphe 1, point a).

▼B

3. Au cas où, douze mois après la date de la publication de l'acte visé au paragraphe 1, aucune homologation CE n'aurait été accordée pour un appareil de contrôle conforme aux prescriptions de l'annexe I B du règlement (CEE) nº 3821/85, la Commission présentera au Conseil une proposition visant à proroger les délais prévus aux paragraphes 1 et 2.

4. Les conducteurs qui, avant la date prévue au paragraphe 2, conduisent un véhicule équipé d'un appareil de contrôle conforme aux prescriptions de l'annexe I B du règlement (CEE) nº 3821/85 et auxquels les autorités compétentes n'ont pas encore pu délivrer de carte de conducteur impriment, à la fin de leur période de travail journalière, les indications relatives aux groupes de temps enregistrés par l'appareil de contrôle, reportent sur le document d'impression les éléments permettant de les identifier (nom et numéro de permis de conduire) et y apposent leur signature.

Article 3

La directive 88/599/CEE est modifiée comme suit:

1) À l'article 3, le paragraphe 2 est remplacé par le texte suivant:

«2. Les contrôles sur route portent sur les éléments suivants:

— les périodes de conduite quotidiennes, les interruptions et les périodes de repos quotidiennes. S'il y a manifestement eu des irrégularités, ils portent également sur les feuilles d'enregistrement des jours précédents, qui doivent se trouver à bord du véhicule conformément à l'article 15, paragraphe 7, du règlement (CEE) nº 3821/85 tel que modifié par le règlement (CE) nº 2135/98 (*), et/ou sur les données mémorisées pour la même période dans la carte de conducteur et/ou dans la mémoire de l'appareil de contrôle conforme(s) à l'annexe I B,

— le cas échéant, pour la période visée à l'article 15, paragraphe 7, du règlement (CEE) nº 3821/85, les éventuels dépassements de la vitesse autorisée du véhicule, définis comme étant toutes périodes de plus d'une minute pendant lesquelles la vitesse du véhicule excède 90 km/h pour les véhicules de la catégorie N_3 ou 105 km/h pour les véhicules de la catégorie M_3, les catégories N_3 et M_3 s'entendant comme celles définies à l'annexe I de la directive 70/156/CEE (**),

— le cas échéant, les vitesses instantanées du véhicule telles qu'enregistrées par l'appareil de contrôle pendant, au plus, les vingt-quatre dernières heures d'utilisation du véhicule,

— le cas échéant, la dernière période de repos hebdomadaire,

— le fonctionnement correct de l'appareil de contrôle (constatation d'une éventuelle manipulation de l'appareil et/ou de la carte de conducteur et/ou des feuilles d'enregistrement) ou, le cas échéant, la présence de documents visés à l'article 14, paragraphe 5, du règlement (CEE) nº 3820/85.

(*) Règlement (CE) nº 2135/98 du Conseil du 24 septembre 1998 modifiant le règlement (CEE) nº 3821/85 concernant l'appareil de contrôle dans le domaine des transports par route et la directive 88/599/CEE concernant l'application des règlements (CEE) nº 3820/85 et (CEE) nº 3821/85 (JO L 274 du 9.10.1998, p. 1).

(**) Directive 70/156/CEE du Conseil du 6 février 1970 concernant le rapprochement des législations des États membres relatives à la réception des véhicules à moteur et de leurs remorques (JO L 42 du 23.2.1970, p. 1). Directive modifiée en dernier lieu par la directive 97/27/CE (JO L 233 du 25.8.1997, p. 1).»

2) À l'article 4, le paragraphe 3 est remplacé par le texte suivant:

«3. Aux fins du présent article, les contrôles effectués par les autorités compétentes dans leurs propres locaux, sur la base des documents et/ou données pertinents qui leur sont remis, sur leur demande, par les entreprises, ont la même valeur que les contrôles effectués dans les locaux des entreprises.»

▼B

Article 4

Le présent règlement entre en vigueur le jour suivant celui de sa publication au *Journal officiel des Communautés européennes*.

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

▼**M1**

ANNEXE

«*ANNEXE I B*

EXIGENCES APPLICABLES À LA CONSTRUCTION, AUX ESSAIS, À L'INSTALLATION ET À L'INSPECTION

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

TABLE DES MATIÈRES

▼**M1**

▼**M1**

▼**M1**

▼**M1**

I. DÉFINITIONS

Aux fins de la présente annexe, on entend par:

a) **«activation»:**

la phase au cours de laquelle l'appareil de contrôle devient pleinement opérationnel et met en service toutes les fonctions, y compris les fonctions de sécurité;

L'activation d'un appareil de contrôle nécessite l'utilisation d'une carte d'atelier et l'introduction de son code d'identification.

b) **«authentification»:**

une fonction destinée à établir et vérifier une identité;

c) **«authenticité»:**

le fait qu'une information provient d'une partie dont l'identité peut être vérifiée;

d) **«test intégré»:**

des essais exécutables sur demande, par une action de l'opérateur ou d'un appareil externe;

e) **«jour civil»:**

une journée comprise entre 00.00 heure et 24.00 heures; tous les jours civils sont liés à l'heure universelle coordonnée (HUC);

f) **«étalonnage»:**

la mise à jour ou la confirmation des paramètres du véhicule à conserver en mémoire; les paramètres du véhicule comprennent l'identification du véhicule (numéro d'identification, numéro d'immatriculation et État membre d'immatriculation) et les caractéristiques du véhicule [w, k, l, taille des pneumatiques, réglage du limiteur de vitesse (le cas échéant), heure TUC, kilométrage];

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

g) **«numéro de carte»:**

un code alphanumérique à 16 positions constituant un numéro d'identification unique d'une carte tachygraphique dans un État membre; ce numéro comporte un indice séquentiel (le cas échéant), un indice de remplacement et un indice de renouvellement;

Chaque carte est ainsi identifiable par le code de l'État membre qui l'a délivrée et par le numéro de carte.

h) **«indice séquentiel de la carte»:**

le 14e caractère alphanumérique du numéro de carte, utilisé pour différencier les cartes délivrées à une société ou un organisme habilité à recevoir plusieurs cartes tachygraphiques; la société ou l'organisme est identifié par les 13 premières positions du numéro de carte;

i) **«indice de renouvellement de la carte»:**

le 16e caractère alphanumérique du numéro de carte, incrémenté à chaque renouvellement de la carte du tachygraphe;

j) **«indice de remplacement de la carte»:**

le 15e caractère du numéro de carte, incrémenté à chaque remplacement de la carte tachygraphique;

k) **«coefficient caractéristique du véhicule»:**

la caractéristique numérique donnant la valeur du signal de sortie émis par la partie du véhicule qui relie celui-ci à l'appareil de contrôle (arbre de sortie de boîte de vitesses ou essieu) pendant que le véhicule se déplace sur une distance d'un kilomètre dans les conditions d'essai standard (voir chapitre VI.5). Le coefficient caractéristique est exprimé en impulsions par kilomètre (w: … imp/km);

l) **«carte d'entreprise»:**

une carte tachygraphique délivrée par les autorités d'un État membre au propriétaire ou au détenteur de véhicules équipés d'un appareil de contrôle;

La carte d'entreprise identifie l'entreprise et permet l'affichage, le téléchargement et l'impression de données stockées dans l'appareil de contrôle verrouillé par cette entreprise.

▼M1

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

la caractéristique numérique donnant la valeur du signal d'entrée nécessaire pour indiquer et enregistrer une distance parcourue d'un kilomètre; cette constante est exprimée en impulsions par kilomètre (w#= … imp/km);

n) **le «temps de conduite continue» est calculé par l'appareil de contrôle comme** ([1])**:**

la somme des temps de conduite accumulés par un conducteur donné depuis la fin de sa dernière période de DISPONIBILITÉ ou de PAUSE/REPOS ou INCONNUE ([2]) de 45 minutes ou plus (cette période peut avoir été divisée en plusieurs périodes de 15 minutes ou plus). Les calculs tiennent compte, au besoin, des activités antérieures stockées sur la carte de conducteur. Lorsque le conducteur n'a pas inséré sa carte, les calculs sont fondés sur les données enregistrées sur la mémoire pendant la période en cours où aucune carte n'a été insérée, et se rapportant au lecteur pertinent;

o) **«carte de contrôleur»:**

une carte tachygraphique délivrée par les autorités d'un État membre à une autorité de contrôle compétente;

La carte de contrôleur identifie l'organisme de contrôle et éventuellement le responsable du contrôle, et permet l'accès aux données stockées dans la mémoire ou sur les cartes de conducteur, pour lecture, impression et/ou téléchargement.

p) **«temps de pause cumulé» la durée calculée dans l'appareil de contrôle comme** ([1])**:**

le temps de pause cumulé est la somme des périodes de DISPONIBILITÉ ou de PAUSE/REPOS ou INCONNUES ([2]) de 15 minutes ou plus par un conducteur donné, depuis la fin de sa dernière période de DISPONIBILITÉ ou PAUSE/REPOS ou INCONNUE ([2]) de 45 minutes ou plus (cette période peut avoir été divisée en plusieurs périodes de 15 minutes ou plus).

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

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

q) **«mémoire»:**

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

r) **«signature numérique»:**

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

s) **«téléchargement»:**

la copie, avec signature numérique, d'une partie ou de la totalité d'un ensemble de données stockées sur la mémoire de l'unité embarquée sur le véhicule ou sur la mémoire d'une carte tachygraphique;

Le téléchargement ne peut en aucun cas modifier ou effacer les données.

t) **«carte de conducteur»:**

une carte tachygraphique délivrée par les autorités d'un État membre à un conducteur donné;

La carte de conducteur donne l'identité du conducteur et permet le stockage des données relatives à l'activité du conducteur.

([1]) Ce mode de calcul du temps de travail continu et du temps de pause cumulé permet à l'appareil de contrôle de lancer en temps voulu l'avertissement relatif au temps de travail continu. Il ne préjuge pas l'interprétation légale de ces temps.

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

▼M1

u) **«circonférence effective des pneumatiques»:**

la moyenne des distances parcourues par chacune des roues entraînant le véhicule (roues motrices) lors d'une rotation complète. La mesure de ces distances est effectuée dans des conditions standard (voir chapitre VI.5) et est exprimée sous la forme l = … mm. Les constructeurs de véhicules peuvent remplacer la mesure de ces distances par un calcul théorique tenant compte de la répartition du poids du véhicule sur les essieux, à vide et en ordre de marche ([1]). Les méthodes de ce calcul théorique seront approuvées par une autorité compétente nationale.

v) **«événement»:**

opération anormale détectée par l'appareil de contrôle et pouvant provenir d'une tentative de fraude;

w) **«anomalie»:**

opération anormale détectée par l'appareil de contrôle et pouvant provenir d'un dysfonctionnement ou d'une panne de l'appareil;

x) **«installation»:**

le montage de l'appareil de contrôle dans un véhicule;

y) **«capteur de mouvement»:**

élément de l'appareil de contrôle émettant un signal représentatif de la vitesse et/ou de la distance parcourue par le véhicule;

z) **«carte non valable»:**

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

aa) **«hors champ»:**

tous les cas où l'utilisation de l'appareil n'est pas requise, conformément au règlement (CEE) nº 3820/85 du Conseil;

bb) **«excès de vitesse»:**

le dépassement de la vitesse autorisée pour le véhicule, pendant toute période de plus de 60 secondes au cours de laquelle la vitesse mesurée du véhicule dépasse la limite fixée pour le réglage du dispositif de limitation de vitesse dans la directive 92/6/CEE du 10 février 1992 relative à l'installation et à l'utilisation, dans la Communauté, de limiteurs de vitesse sur certaines catégories de véhicules à moteur ([2]);

cc) **«inspection périodique»:**

une série d'opérations de contrôle destinées à s'assurer que l'appareil de contrôle fonctionne correctement et que ses réglages correspondent aux paramètres du véhicule;

dd) **«imprimante»:**

un composant de l'appareil de contrôle qui permet d'imprimer les données stockées;

ee) **«appareil de contrôle»:**

l'ensemble des équipements destinés à être installés sur des véhicules routiers pour indiquer, enregistrer et stocker automatiquement ou semi-automatiquement des données concernant le mouvement de ces véhicules et certaines périodes de travail des conducteurs;

ff) **«renouvellement»:**

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

gg) **«réparation»:**

toute réparation d'un capteur de mouvement ou d'une unité embarquée sur un véhicule qui impose de le ou de la déconnecter de son alimentation électrique ou d'autres composants de l'appareil de contrôle, ou de l'ouvrir;

([1]) Directive 97/27/CE du Parlement européen et du Conseil, du 22 juillet 1997, concernant les masses et dimensions de certaines catégories de véhicules à moteur et de leurs remorques, et modifiant la directive 70/156/CEE (JO L 233 du 25.8.1997, p. 1).

([2]) JO L 57 du 2.3.1992, p. 27.

▼M1

hh) **«remplacement»:**

délivrance d'une carte tachygraphique en remplacement d'une carte existante qui a été déclarée perdue, volée ou ne fonctionnant pas correctement, et a été retournée à l'autorité qui l'a délivrée; le remplacement comporte toujours le risque que deux cartes en cours de validité coexistent;

ii) **«certification de sécurité»:**

le processus consistant à certifier, par un organisme de certification ITSEC ([1]), que l'appareil de contrôle (ou le composant de cet appareil) ou la carte tachygraphique satisfait aux exigences de sécurité définies à l'appendice 10 concernant les objectifs généraux de sécurité;

jj) **«autotest»:**

les tests automatiques effectués périodiquement par l'appareil de contrôle afin de déceler les anomalies;

kk) **«carte tachygraphique»:**

une carte à mémoire destinée à être utilisée sur l'appareil de contrôle; les cartes tachygraphiques permettent l'identification, par l'appareil de contrôle, du détenteur de la carte (ou du groupe auquel il appartient), ainsi que le téléchargement et le stockage de données; une carte tachygraphique peut appartenir à l'un des types suivants:

— carte de conducteur,

— carte de contrôleur,

— carte d'atelier,

— carte d'entreprise;

ll) **«homologation»:**

processus mené par un État membre et visant à certifier que l'appareil de contrôle (ou un composant) ou la carte tachygraphique satisfait aux exigences du présent règlement;

mm) **«dimension des pneumatiques»:**

la désignation des dimensions des pneumatiques (roues motrices externes) conformément à la directive 92/23/CEE ([2]);

nn) **«identification du véhicule»:**

les numéros permettant d'identifier le véhicule: numéro d'immatriculation avec indication de l'État membre d'immatriculation, et numéro d'identification du véhicule ([3]);

oo) **«unité embarquée sur le véhicule (UEV)»:**

l'appareil de contrôle, à l'exclusion du capteur de mouvement et des câbles de connexion de ce capteur; l'unité embarquée sur le véhicule peut se présenter sous forme d'un seul élément ou de plusieurs composants répartis dans le véhicule, dans la mesure où elle est conforme aux exigences de sécurité du présent règlement;

pp) **«semaine», aux fins du calcul dans l'appareil de contrôle:**

une période comprise entre 00.00 heure TUC le lundi et 24.00 heures le dimanche;

qq) **«carte d'atelier»:**

une carte tachygraphique délivrée par les autorités d'un État membre à un constructeur d'appareil de contrôle, un installateur, un constructeur de véhicules ou un atelier, homologué par cet État membre;

la carte d'atelier indique l'identité du détenteur et permet l'essai et l'étalonnage de l'appareil de contrôle et/ou le téléchargement à partir de cet appareil.

II. CARACTÉRISTIQUES GÉNÉRALES ET FONCTIONS DE L'APPAREIL DE CONTRÔLE

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

([1]) Recommandation 95/144/CE du Conseil, du 7 avril 1995, concernant des critères communs d'évaluation de la sécurité des technologies de l'information (JO L 93 du 26.4.1995, p. 27).
([2]) JO L 129 du 14.5.1992, p. 95.
([3]) Directive 76/114/CEE du 18.12.1975 (JO L 24 du 30.1.1976, p. 1).

▼M1

1. **Caractéristiques générales**

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

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

L'unité embarquée sur le véhicule comprend une unité de traitement, une mémoire électronique, une horloge temps réel, deux interfaces pour cartes à mémoire (conducteur et convoyeur), une imprimante, un écran, un dispositif visuel d'avertissement, un connecteur d'étalonnage/de téléchargement, ainsi que des dispositifs permettant la saisie de données par l'utilisateur.

L'appareil de contrôle peut être relié à d'autres dispositifs par des connecteurs additionnels.

Toute insertion ou connexion de toute fonction ou dispositif(s), homologué(s) ou non, dans ou à l'appareil de contrôle, ne doit pas interférer ou être susceptible d'interférer avec le fonctionnement correct et sûr de l'appareil de contrôle, ni avec les dispositions du règlement.

Les utilisateurs de l'appareil de contrôle indiquent leur identité par l'intermédiaire de cartes tachygraphiques.

L'appareil de contrôle ouvre des droits d'accès sélectifs aux données et fonctions, selon le type et/ou l'identité de l'utilisateur.

L'appareil de contrôle enregistre et stocke des données dans sa mémoire et sur les cartes tachygraphiques.

Ces fonctions sont assurées dans le respect de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ([1]).

2. **Fonctions**

L'appareil de contrôle doit assurer les fonctions suivantes:

— surveillance des insertions et retraits de carte,
— mesure de la vitesse et de la distance parcourue,
— mesure du temps,
— suivi des activités du conducteur,
— suivi de la situation de conduite,
— saisie manuelle de données par le conducteur:
  — lieu de début et/ou de fin des périodes journalières de travail,
  — saisie manuelle des activités du conducteur,
  — saisie des conditions particulières,
— gestion des verrouillages d'entreprise,
— suivi des activités de contrôle,
— détection des événements et/ou des anomalies,
— autotests intégrés,
— lecture de données stockées sur la mémoire,
— enregistrement et stockage de données sur la mémoire,
— lecture des cartes tachygraphiques,
— enregistrement et stockage de données sur les cartes tachygraphiques,
— affichage,
— impression,
— avertissement,
— téléchargement de données vers des médias externes,
— sortie de données vers des dispositifs externes additionnels,
— étalonnage,
— mise à l'heure.

3. **Modes de fonctionnement**

L'appareil de contrôle doit permettre quatre modes de fonctionnement:

— mode «opérationnel»,
— mode «contrôle»,
— mode «étalonnage»,
— mode «entreprise».

([1]) JO L 281 du 23.11.1995, p. 31.

▼**M1**

L'appareil de contrôle doit passer dans les modes suivants de fonctionnement selon la carte tachygraphique valable insérée dans l'interface de carte:

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

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

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

Toutes les fonctions énumérées au point II.2 doivent être disponibles dans tous les modes de fonctionnement, à l'exception de:

— la fonction d'étalonnage, accessible uniquement en mode étalonnage,

— la fonction de mise à l'heure, limitée dans les modes autres que le mode étalonnage,

— la saisie manuelle par le conducteur, accessible uniquement en mode opérationnel et en mode étalonnage,

— la fonction de gestion des verrouillages d'entreprise, accessible uniquement en mode entreprise,

— le suivi des activités de contrôle, accessible uniquement en mode contrôle,

— la fonction de téléchargement, non accessible en mode opérationnel (sauf dans les cas prévus à l'exigence 150).

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

— en mode opérationnel, toute identification personnelle [nom et prénom(s)] ne correspondant pas à la carte tachygraphique insérée sera masquée, et tout numéro de carte ne correspondant à la carte tachygraphique insérée sera partiellement masqué (un caractère sur deux, de gauche à droite),

— en mode entreprise, les données relatives au conducteur (exigences 081, 084 et 087) peuvent être extraites seulement pour les périodes non verrouillées par une autre entreprise (telle qu'identifiée par les 13 premiers chiffres du numéro de la carte d'entreprise),

— lorsqu'aucune carte n'est insérée dans l'appareil de contrôle, seules peuvent être extraites les données relatives au conducteur pour le jour même et les 8 jours civils précédents.

4. **Sécurité**

Le système de sécurité 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, et enfin à vérifier l'intégrité et l'authenticité des données téléchargées.

Afin d'assurer la sécurité du système, l'appareil de contrôle doit satisfaire à des exigences spécifiées dans les objectifs généraux de sécurité pour le capteur de mouvement et l'unité embarquée sur le véhicule (appendice 10).

▼M1

III. EXIGENCES CONSTRUCTIVES ET FONCTIONNELLES APPLICABLES À L'APPAREIL DE CONTRÔLE

1. **Suivi de l'insertion et du retrait des cartes**

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

Lors de l'insertion d'une carte, l'appareil de contrôle vérifie la validité de la carte et identifie son type.

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

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

2. **Mesure de la vitesse et de la distance parcourue**

Cette fonction assure une mesure en continu et permet d'indiquer la valeur kilométrique correspondant à la distance totale parcourue par le véhicule.

Cette fonction assure une mesure en continu et permet d'indiquer la vitesse du véhicule.

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

Les dispositifs indicateurs de vitesse et kilométriques installés sur tout véhicule muni d'un appareil de contrôle conforme au présent règlement doivent satisfaire aux exigences concernant les tolérances maximales fixées dans la présente annexe (chapitre III, points 2.1 et 2.2).

2.1. ***Mesure de la distance parcourue***

La distance parcourue peut être mesurée de manière à:

— soit cumuler les mouvements en marche avant et en marche arrière,

— soit prendre uniquement en compte les mouvements en marche avant.

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

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

— ± 1 % avant installation,

— ± 2 % lors de l'installation et des inspections périodiques,

— ± 4 % en service.

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

2.2. ***Mesure de la vitesse***

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

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

— d'une tolérance de ± 2 km/h pour les variations du signal d'entrée (variations dues aux pneumatiques, etc.),

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

l'appareil de contrôle doit, pour les vitesses comprises entre 20 et 180 km/h, et pour des coefficients caractéristiques du véhicule compris entre 4 000 et 25 000 imp/km, mesurer la vitesse avec une tolérance de ± 1 km/h (à vitesse constante).

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

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

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

3. **Mesure du temps**

La fonction de mesure du temps doit assurer une mesure en continue et un affichage numérique de la date et de l'heure HUC.

▼M1

La date et l'heure HUC doivent être utilisés dans l'ensemble de l'appareil de contrôle (enregistrements, tirages papier, échange de données, affichage …).

Afin de visualiser l'heure locale, il doit être possible de changer le décalage horaire de l'heure affichée, par paliers d'une demi-heure.

La dérive temporelle ne doit pas excéder ± 2 secondes par jour dans les conditions d'homologation.

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

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

4. **Suivi des activités du conducteur**

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

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

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

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

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

Le premier changement d'activité 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 doit par conséquent annuler le passage à l'activité TRAVAIL).

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

Étant donnée une minute civile, toute activité de CONDUITE survenue pendant une partie de cette minute entraînera la comptabilisation de la minute entière comme de la CONDUITE.

Étant donnée une minute civile, toute activité de CONDUITE survenue au cours de la minute qui précède et de la minute qui suit immédiatement entraînera la comptabilisation de la minute entière comme de la CONDUITE.

Étant donnée une minute civile non considérée comme activité de CONDUITE en application des exigences précédentes, la minute entière sera considérée comme relevant de la même activité que l'activité continue la plus longue survenue dans la minute (ou de la plus récente en cas de plusieurs activités de même durée).

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

5. **Surveillance de la situation de conduite**

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

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

6. **Saisie manuelle par le conducteur**

6.1. ***Saisie du lieu de début et/ou de fin de la période de travail journalière***

Cette fonction doit permettre la saisie du lieu de début et/ou de fin de la période de travail journalière du conducteur et/ou du convoyeur.

On entend par lieu le pays et, le cas échéant, la région.

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

L'appareil de contrôle doit permettre d'ignorer ce message.

Il doit être possible de saisir le lieu de début et/ou de fin d'une période de travail journalière sans carte ou à un autre moment que lors de l'insertion ou du retrait d'une carte.

▼M1

6.2. ***Saisie manuelle des activités du conducteur***

Lors de l'insertion d'une carte de conducteur (ou d'atelier), et seulement à ce moment, l'appareil de contrôle doit:

— rappeler au détenteur de la carte la date et l'heure du dernier retrait de sa carte,

— demander au détenteur de la carte d'indiquer si l'insertion de la carte représente la poursuite d'une période de travail journalière en cours.

L'appareil de contrôle doit permettre au détenteur de la carte d'ignorer la question, ou d'y répondre par l'affirmative, ou d'y répondre par la négative:

— dans le cas où le détenteur de la carte ignore la question, l'appareil de contrôle invite le détenteur de la carte à indiquer «le lieu où commence la période de travail journalière». L'appareil de contrôle doit donner la possibilité de ne rien indiquer. Si un lieu est indiqué, il est alors enregistré dans la mémoire ainsi que sur la carte tachygraphique, et relié à l'heure de l'insertion de la carte.

— dans le cas où le détenteur de la carte répond par l'affirmative ou la négative, l'appareil de contrôle invite le détenteur de la carte à saisir manuellement ses activités, ainsi que la date et l'heure du début et de la fin de chacune d'elles, uniquement parmi les activités TRAVAIL, DISPONIBILITÉ, PAUSE/REPOS, et uniquement au cours de la période comprise entre le dernier retrait de la carte et l'insertion actuelle, et sans permettre que ces activités se chevauchent. Les procédures applicables sont les suivantes:

  — Dans le cas où le détenteur de la carte répond par l'affirmative à la question, l'appareil de contrôle doit inviter le détenteur de la carte à saisir manuellement les activités, dans l'ordre chronologique, pour la période comprise entre le dernier retrait de la carte et l'insertion actuelle. Le processus se termine lorsque l'heure de fin d'une activité saisie manuellement correspond à l'heure d'insertion de la carte.

  — Dans le cas où le détenteur de la carte répond par la négative, l'appareil de contrôle:

    — invite le détenteur de la carte à saisir manuellement les activités dans l'ordre chronologique depuis l'heure de retrait de la carte jusqu'à la fin de la période de travail journalière correspondante (ou des activités liées au véhicule en cause dans le cas où la période de travail journalière se poursuit sur une feuille d'enregistrement). L'appareil de contrôle doit donc, avant de permettre au détenteur de la carte de saisir manuellement chaque activité, inviter le détenteur de la carte à indiquer si l'heure de fin de la dernière activité enregistrée représente la fin de la dernière période de travail (voir remarque ci-après),

    Remarque: dans le cas où le détenteur de la carte ne déclare pas l'heure d'achèvement de la dernière période de travail, et saisit manuellement une activité dont l'heure d'achèvement correspond à l'heure d'insertion de la carte, l'appareil de contrôle:

      — considère que la période de travail journalière s'est achevée au commencement de la première période de REPOS (ou demeurant INCONNUE) après le retrait de la carte, ou au moment de ce retrait si aucune période de repos n'a été saisie (et si aucune période ne demeure INCONNUE),

      — considère que l'heure de commencement (voir ci-après) correspond à l'heure d'insertion de la carte,

      — exécute les étapes décrites ci-après;

    — ensuite, si l'heure d'achèvement de la période de travail en cause est différente de l'heure de retrait de la carte, ou si le lieu de fin de la période de travail journalière n'a pas été saisi à ce moment-là, invite le détenteur de la carte à «confirmer ou saisir le lieu de fin de la période de travail journalière» (l'appareil de contrôle doit permettre de ne rien indiquer); si un lieu est saisi, il doit être enregistré sur la carte tachygraphique, et uniquement s'il est différent de celui saisi lors du retrait de la carte (le cas échéant), et relié à l'heure d'achèvement de la période de travail;

    — ensuite, invite le détenteur de la carte à "saisir une heure de début" de la période de travail journalière en cours (ou des activités liées au véhicule actuel dans le cas où le détenteur de la carte a auparavant utilisé une feuille d'enregistrement au cours de cette période), et invite le détenteur de la carte à saisir un «lieu où commence la période de travail journalière» (l'appareil de contrôle doit permettre de ne rien indiquer); si un lieu est indiqué, il est enregistré sur la carte tachygraphique et lié à l'heure de commencement précitée; si cette heure correspond à celle de l'insertion de la carte, le lieu est également enregistré dans la mémoire;

▼M1

— ensuite, si cette heure de commencement est différente de celle de l'insertion de la carte, un message invite le détenteur de la carte à saisir manuellement des activités, dans l'ordre chronologique, à partir de cette heure de commencement et jusqu'à l'heure d'insertion de la carte; le processus s'achève lorsque l'heure d'achèvement d'une activité saisie manuellement correspond à l'heure d'insertion de la carte.

— L'appareil de contrôle doit alors permettre au détenteur de la carte de modifier toute activité saisie, jusqu'à la validation par la sélection d'une commande particulière, qui empêche toute modification ultérieure.

— Si une réponse affirmative ou négative n'est pas suivie de la saisie d'activités, l'appareil de contrôle doit considérer que le détenteur a ignoré la question.

Au cours de l'ensemble de ce processus, l'appareil de contrôle doit attendre la saisie de données avec les temporisations suivantes:

— en l'absence d'interaction avec l'interface homme/machine de l'appareil pendant 1 minute (avec avertissement visuel et éventuellement auditif, après 30 secondes) ou,

— lors du retrait de la carte ou de l'insertion d'une autre carte de conducteur (ou d'atelier) ou,

— lors de la mise en mouvement du véhicule,

auquel cas l'appareil de contrôle validera toute donnée déjà saisie.

6.3. ***Saisie de conditions particulières***

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

— «HORS CHAMP» (début, fin)

— «TRAJET EN FERRY/TRAIN»

Un «TRAJET EN FERRY/TRAIN» ne peut survenir lorsque la condition «HORS CHAMP» est ouverte.

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

7. **Gestion des verrouillages d'entreprise**

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

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

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

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

le déverrouillage est automatique lorsqu'une autre société verrouille.

Dans le cas où une société verrouille et où le verrouillage précédent a été effectué pour la même société, on supposera que le verrouillage prédédent n'a pas été déverrouillé et qu'il est toujours en fonction.

8. **Suivi des activités de contrôle**

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

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

9. **Détection des événements et/ou des anomalies**

Cette fonction détecte les événements et/ou anomalies suivantes:

9.1. ***Événement «insertion d'une carte non valable»***

Cet événement est déclenché par l'insertion d'une carte non valable et/ou lorsque la validité d'une carte insérée vient à expiration.

▼M1

9.2. ***Événement «conflit de carte»***

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

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

9.3. ***Événement «chevauchement temporel»***

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

9.4. ***Événement «conduite sans carte appropriée»***

Cet événement est déclenché pour toute combinaison de cartes tachygraphiques marquées d'une croix dans le tableau suivant, lorsque l'activité du conducteur devient «CONDUITE», ou en cas de changement de mode de fonctionnement lorsque l'activité du conducteur est CONDUITE:

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

9.5. ***Événement «insertion d'une carte en cours de conduite»***

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

9.6. ***Événement «dernière session incorrectement clôturée»***

Cet événement est déclenché lorsque l'appareil de contrôle détecte lors de l'insertion de la carte que, malgré les dispositions du chapitre III, paragraphe 1, la session précédente n'a pas été correctement clôturée (la carte a été retirée avant que toutes les données nécessaires aient été enregistrées sur la carte). Cet événement ne peut concerner que les cartes de conducteur et d'atelier.

▼M1

9.7. ***Événement «excès de vitesse»***

Cet événement est déclenché lors de chaque excès de vitesse.

9.8. ***Événement «interruption de l'alimentation électrique»***

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

9.9. ***Événement «erreur sur les données de mouvement»***

Cet événement est déclenché en cas d'interruption du flux normal de données entre le capteur de mouvement et l'unité embarquée sur le véhicule et/ou en cas d'erreur sur l'intégrité des données ou l'authentification des données au cours de l'échange de données entre le capteur de mouvement et l'UEV.

9.10. ***Événement «tentative d'atteinte à la sécurité»***

Cet événement est déclenché en cas de tout autre événement affectant la sécurité du capteur de mouvement et/ou de l'unité embarquée sur le véhicule, telle que spécifiée dans le cadre des objectifs généraux de sécurité pour ces composants, dans les modes autres qu'étalonnage.

9.11. ***Anomalie «carte»***

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

9.12. ***Anomalie «appareil de contrôle»***

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

— anomalie interne de l'UEV
— anomalie de l'imprimante
— anomalie de l'affichage
— anomalie de téléchargement
— anomalie du capteur

10. **Autotests et tests intégrés**

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

Élément à tester	Autotest	Test intégré
Logiciel		Intégrité
Mémoire de données	Accès	Accès, intégrité des données
Dispositifs d'interface carte	Accès	Accès
Clavier		Contrôle manuel
Imprimante	(au choix du constructeur)	Imprimante
Écran		Contrôle visuel
Téléchargement (effectué uniquement lors du téléchargement)	Fonctionnement correct	
Capteur	Fonctionnement correct	Fonctionnement correct

11. **Lecture de la mémoire**

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

▼M1

12. **Enregistrement et stockage dans la mémoire**

Aux fins du présent paragraphe,

— on entend par «365 jours» 365 jours civils d'activité moyenne de conducteurs dans un véhicule. L'activité moyenne par jour dans un véhicule est définie comme au moins 6 conducteurs ou convoyeurs, 6 cycles d'insertion/retrait de cartes et 256 changements d'activités. «365 jours» incluent donc au moins 2 190 conducteurs/convoyeurs et 93 440 changements d'activité.

— les heures sont enregistrées avec une résolution d'une minute, sauf indication contraire,

— les valeurs kilométriques sont enregistrées avec une résolution de 1 kilomètre,

— les vitesses sont enregistrées avec une résolution de 1 km/h.

Les données enregistrées dans la mémoire ne doivent pas être affectées par une coupure de l'alimentation électrique externe d'une durée inférieure à douze mois dans les conditions d'homologation.

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

12.1. ***Données d'identification de l'appareil***

12.1.1. *Données d'identification de l'unité embarquée sur le véhicule*

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

— nom du constructeur,

— adresse du fabricant,

— numéro des pièces,

— numéro de série,

— numéro de la version du logiciel,

— date d'installation de la version du logiciel,

— année de construction de l'appareil,

— numéro d'homologation.

Les données d'identification de l'unité embarquée sur le véhicule sont enregistrées et stockées une fois pour toutes par le fabricant de l'unité embarquée sur le véhicule, sauf les données concernant le logiciel et le numéro d'homologation, qui peuvent être modifiés en cas d'évolution du logiciel.

12.1.2. *Données d'identification du capteur de mouvement*

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

— nom du constructeur,

— numéro des pièces,

— numéro de série,

— numéro d'homologation,

— identificateur du composant de sécurité intégré (par ex numéro de série du microprocesseur interne),

— identificateur du système d'exploitation (par ex numéro de la version du logiciel).

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

L'unité embarquée sur le véhicule doit pouvoir enregistrer et stocker dans sa mémoire les données suivantes d'identification du capteur de mouvement auquel il est couplé:

— numéro de série,

— numéro d'homologation,

— date du premier couplage.

12.2. ***Éléments de sécurité***

L'appareil de contrôle doit pouvoir stocker les éléments de sécurité suivants:

— clé publique européenne,

— certificat de l'État membre,

— certificat de l'appareil,

— clé privée de l'appareil.

▼M1

Les éléments de sécurité de l'appareil de contrôle sont insérés dans l'appareil par le fabricant de l'unité embarquée sur le véhicule.

12.3. ***Données concernant l'insertion et le retrait de la carte de conducteur***

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

— les nom et prénom(s) du détenteur de la carte tels que stockés sur la carte,
— le numéro de la carte, l'État membre qui l'a délivrée et la date d'expiration tels que stockés sur la carte,
— la date et l'heure d'insertion,
— le kilométrage du véhicule au moment de l'insertion de la carte,
— le lecteur dans lequel est insérée la carte,
— la date et l'heure du retrait,
— le kilométrage du véhicule au moment du retrait de la carte,
— les informations suivantes relatives au dernier véhicule utilisé par le conducteur, telles que stockées sur la carte:
  — numéro et État membre d'immatriculation,
  — date et heure du retrait de la carte,
— un code indiquant si le détenteur de la carte a saisi manuellement des activités lors de l'insertion de la carte ou non.

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

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

12.4. ***Données relatives à l'activité du conducteur***

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

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

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

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

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

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

12.5. ***Lieux de début et/ou de fin des périodes journalières de travail***

L'appareil de contrôle enregistre et stocke dans sa mémoire, lorsque le conducteur/convoyeur saisit le lieu de début et/ou de fin d'une période de travail journalière:

— le cas échéant, le numéro de carte de conducteur/convoyeur et l'État membre qui a délivré la carte,
— la date et l'heure de la saisie (ou la date et l'heure liées à la saisie lorsque celle-ci est effectuée lors de la procédure de saisie manuelle),
— le type de donnée saisie (début ou fin d'une période de travail journalière, conditions de la saisie),
— le pays et la région saisis,
— le kilométrage du véhicule.

La mémoire doit pouvoir conserver les données relatives au début et/ou à la fin des périodes journalières de travail pendant au moins 365 jours (en supposant que deux saisies sont effectuées quotidiennement par chaque conducteur).

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

▼M1

12.6. ***Kilométrage***

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

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

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

12.7. ***Relevés détaillés de la vitesse***

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.

12.8. ***Données événementielles***

Aux fins du présent point, le temps est enregistré à la seconde près.

L'appareil de contrôle enregistre et stocke dans sa mémoire les données suivantes pour chaque événement détecté, conformément aux règles de stockages suivantes:

Événement	Règles de stockage	Données à enregistrer pour chaque événement
Conflit de cartes	— les 10 événements les plus récents	— date et heure de début d'événement, — date et heure de fin d'événement, — type, numéro et État membre ayant délivré chacune des deux cartes à l'origine du conflit
Conduite sans carte appropriée	— l'événement le plus long pour chacun des 10 derniers jours d'occurrence, — les 5 événements les plus longs au cours des 365 derniers jours	— date et heure de début d'événement, — date et heure de fin d'événement, — type, numéro et État membre ayant délivré la carte insérée au début et/ou à la fin de l'événement, — nombre d'événements semblables survenus le même jour
Insertion de carte en cours de conduite	— le dernier événement pour chacun des 10 derniers jours d'occurrence	— date et heure de l'événement, — type, numéro et État membre ayant délivré la carte, — nombre d'événements semblables survenus le même jour
Clôture incorrecte de la dernière session	— les 10 événements les plus récents	— date et heure de l'insertion de la carte, — type, numéro et État membre ayant délivré la carte, — données relatives à la dernière session telles qu'elles figurent sur la carte: — date et heure de l'insertion, — numéro et État membre d'immatriculation
Excès de vitesse ([1])	— événement le plus grave (c.-à.-d. celui présentant la vitesse moyenne la plus	— date et heure du début de l'événement, — date et heure de la fin de

▼**M1**

Événement	Règles de stockage	Données à enregistrer pour chaque événement
	élevée) des 10 derniers jours d'occurrence, — les 5 événements les plus graves au cours des 365 derniers jours, — premier événement survenu après le dernier étalonnage	l'événement, — vitesse maximale mesurée au cours de l'événement, — vitesse moyenne arithmétique mesurée au cours de l'événement, — type, numéro et État membre ayant délivré la carte (le cas échéant), — nombre d'événements semblables survenus le même jour
Interruption de l'alimentation électrique ([2])	— événement le plus long pour chacun des 10 derniers jours d'occurrence, — les 5 événements les plus longs pour les 365 derniers jours	— date et heure du début de l'événement, — date et heure de la fin de l'événement, — type, numéro et État membre ayant délivré la carte insérée au début et/ou à la fin de l'événement, — nombre d'événements semblables survenus le même jour
Erreur sur les données de mouvement	— événement le plus long pour chacun des 10 derniers jours d'occurrence, — les 5 événements les plus longs pour les 365 derniers jours	— date et heure du début de l'événement, — date et heure de la fin de l'événement, — type, numéro et État membre ayant délivré la carte insérée au début et/ou à la fin de l'événement, — nombre d'événements semblables survenus le même jour
Tentative d'atteinte à la sécurité	— les 10 événements les plus récents pour chaque type d'événements	— date et heure du début de l'événement (le cas échéant), — date et heure de la fin de l'événement, — type, numéro et État membre ayant délivré la carte insérée au début et/ou à la fin de l'événement, — type d'événement

([1]) L'appareil de contrôle doit également enregistrer et stocker dans sa mémoire:
— la date et l'heure du dernier CONTRÔLE D'EXCÈS DE VITESSE,
— la date et l'heure du premier excès de vitesse après ce CONTRÔLE D'EXCÈS DE VITESSE,
— le nombre d'excès de vitesse survenus depuis le dernier CONTRÔLE D'EXCÈS DE VITESSE.

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

12.9. ***Données relatives aux anomalies***

Aux fins du présent point, le temps est enregistré à la seconde près.

L'appareil de contrôle doit essayer d'enregistrer et de stocker dans sa mémoire les données suivantes pour chaque anomalie détectée, conformément aux règles de stockage suivantes:

Anomalie	Règles de stockage	Données à enregistrer pour chaque anomalie
Anomalie de carte	— les dix dernières anomalies de carte de conducteur	— date et heure de début de l'anomalie, — date et heure de fin de l'ano-

▼M1

Anomalie	Règles de stockage	Données à enregistrer pour chaque anomalie
		malie, — type, numéro et État membre ayant délivré la carte
Anomalies de l'appareil de contrôle	— les 10 anomalies les plus récentes pour chaque type d'anomalie, — la première anomalie après le dernier étalonnage	— date et heure de début de l'anomalie, — date et heure de fin de l'anomalie, — type de l'anomalie, — type, numéro et État membre ayant délivré la carte insérée au début/à la fin de l'anomalie

12.10. ***Données relatives à l'étalonnage***

L'appareil de contrôle enregistre et stocke dans sa mémoire les données ayant trait:

— aux paramètres d'étalonnage connus au moment de l'activation,

— à son tout premier étalonnage après son activation,

— à son premier étalonnage dans le véhicule où il se trouve actuellement (tel qu'identifié par le numéro d'identification du véhicule),

— les 5 étalonnages les plus récents (lorsque plusieurs étalonnages interviennent le même jour civil, seul le dernier est archivé).

Les données suivantes sont enregistrées pour chacun de ces étalonnages:

— objet de l'étalonnage (activation, première installation, installation, contrôle périodique, autre),

— nom et adresse de l'atelier,

— numéro de la carte d'atelier, État membre ayant délivré la carte et date d'expiration de la carte,

— identification du véhicule,

— paramètres mis à jour ou confirmés: w, k, l, taille des pneumatiques, réglage du limiteur de vitesse, compteur kilométrique (ancienne et nouvelle valeurs), date et heure (ancienne et nouvelle valeurs).

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

— première connexion à une UEV (date, heure, numéro d'homologation de l'UEV, numéro de série de l'UEV),

— dernière connexion à une UEV (date, heure, numéro d'homologation de l'UEV, numéro de série de l'UEV).

12.11. ***Données concernant la remise à l'heure***

L'appareil de contrôle enregistre et stocke dans sa mémoire les données ayant trait à:

— la plus récente remise à l'heure,

— les 5 plus grandes corrections depuis le dernier étalonnage,

effectuées en mode étalonnage hors du cadre d'un étalonnage périodique (déf. f).

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

— date et heure, ancienne valeur,

— date et heure, nouvelle valeur,

— nom et adresse de l'atelier,

— numéro de la carte d'atelier, État membre ayant délivré la carte et date d'expiration de la carte.

12.12. ***Données relatives aux activités de contrôle***

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

— date et heure du contrôle,

▼M1

— numéro de la carte de contrôleur et État membre ayant délivré la carte,

— type de contrôle (affichage et/ou tirage papier et/ou téléchargement depuis l'UEV et/ou téléchargement depuis la carte).

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

12.13. ***Données relatives au verrouillage d'entreprise***

L'appareil de contrôle enregistre et stocke dans sa mémoire les données suivantes ayant trait aux 20 plus récents verrouillages d'entreprise:

— date et heure du verrouillage,

— date et heure du déverrouillage,

— numéro de la carte d'entreprise et État membre ayant délivré cette carte,

— nom et adresse de l'entreprise.

12.14. ***Données relatives au téléchargement***

L'appareil de contrôle enregistre et stocke dans sa mémoire les données suivantes ayant trait au dernier téléchargement depuis la mémoire vers des médias extérieurs en mode «société» ou «étalonnage»

— date et heure du téléchargement,

— numéro de la carte d'entreprise ou d'atelier et État membre ayant délivré la carte,

— nom de l'entreprise ou de l'atelier.

12.15. ***Données relatives aux conditions particulières***

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

— date et heure de la saisie,

— type de condition particulière.

La mémoire doit pouvoir conserver les données relatives aux conditions particulières pendant au moins 365 jours (en supposant qu'en moyenne 1 condition est ouverte et fermée par jour). Lorsque la capacité de stockage est épuisée, les données nouvelles remplacent les données les plus anciennes.

13. **Lecture des cartes tachygraphiques**

L'appareil de contrôle doit pouvoir lire sur les cartes tachygraphiques, au besoin, les données nécessaires pour:

— identifier le type de la carte, le détenteur de la carte, le véhicule utilisé précédemment, la date et l'heure du dernier retrait et l'activité sélectionnée à ce moment,

— vérifier que la dernière session a été correctement clôturée,

— calculer le temps de conduite continue du conducteur, le temps de pause cumulé et les temps de conduite cumulés pour la semaine précédente et la semaine en cours,

— imprimer les demandes d'impression de données enregistrées sur une carte de conducteur,

— télécharger une carte de conducteur sur un média externe.

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

14. **Enregistrement et stockage sur cartes tachygraphiques**

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

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

L'appareil de contrôle met à jour les données concernant l'activité du conducteur et le lieu (telles que spécifiées aux points 5.2.5 et 5.2.6 du chapitre IV) stockées sur les cartes de conducteur et/ou d'atelier en cours de validité, avec les données relatives à l'activité et au lieu saisies manuellement par le détenteur de la carte.

La mise à jour des données enregistrées sur les cartes tachygraphiques est réalisée de telle manière que, lorsque cela est nécessaire compte tenu de la capa-

▼M1

cité réelle de stockage de la carte, les données les plus récentes remplacent les données les plus anciennes.

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

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

15. **Affichage**

L'affichage doit comporter au moins 20 caractères.

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

Le dispositif d'affichage doit accepter les caractères latins 1 et les caractères grecs tels que définis dans les parties 1 et 7 de la norme ISO 8859, comme indiqué dans l'appendice 1 du chapitre IV «jeux de caractères». L'affichage peut utiliser des graphies simplifiées (par ex., les caractères accentués peuvent être affichés sans accent, ou les minuscules peuvent être affichées en majuscules).

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

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

L'appareil de contrôle doit pouvoir afficher:

— des données concernant les anomalies,

— des données d'avertissement,

— des données relatives à l'accès aux menus,

— d'autres données demandées par l'utilisateur.

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

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

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

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

Le format d'affichage est indiqué à l'appendice 5.

15.1. ***Affichage par défaut***

Lorsqu'aucune autre information ne doit être affichée, l'appareil de contrôle affiche, par défaut, les indications suivantes:

— heure locale (TUC + correction fixée par le conducteur),

— mode de fonctionnement,

— activité en cours du conducteur et du convoyeur,

— informations sur le conducteur:

  — si son activité en cours est la CONDUITE, son temps de conduite continue et son temps de pause cumulé,

  — si l'activité en cours n'est pas la CONDUITE, la durée de l'activité en cours (depuis sa sélection) et le temps de pause cumulé,

— informations sur le convoyeur:

  — durée de son activité (depuis sa sélection).

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

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

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

▼M1

Lorsqu'une condition «HORS CHAMP» est ouverte, le pictogramme approprié doit apparaître pour indiquer que cette condition est ouverte (l'activité du conducteur en cours peut ne pas être affichée en même temps).

15.2. ***Affichage d'avertissement***

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

15.3. ***Menu d'accès***

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

15.4. ***Autres affichages***

Il doit être possible d'afficher sur demande:

— la date et l'heure TUC,

— le mode de fonctionnement (s'il n'est pas indiqué par défaut),

— le temps de conduite continue et le temps de pause cumulé du conducteur,

— le temps de conduite continue et le temps de pause cumulé du convoyeur,

— le temps de conduite cumulé du conducteur pour la semaine précédente et la semaine en cours,

— le temps de conduite cumulé du convoyeur pour la semaine précédente et pour la semaine en cours,

— le contenu d'un des six tirages papier correspondants, dans le même format que le tirage papier lui-même.

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

16. **Impression**

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

— activités du conducteur stockées sur la carte,

— activités du conducteur stockées sur l'unité embarquée sur le véhicule,

— événements et anomalies stockées sur la carte,

— événements et anomalies stockées sur l'unité embarquée sur le véhicule,

— données techniques,

— excès de vitesse.

Le détail du format et du contenu à respecter pour ces tirages papier est spécifié à l'appendice 4.

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

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

Les tirages papier «activités du conducteur figurant sur la carte» et «événements et anomalies figurant sur la carte» ne peuvent être obtenues que lorsqu'une carte de conducteur ou d'atelier est insérée dans l'appareil de contrôle. L'appareil de contrôle met à jour les données stockées sur la carte en cause avant de lancer l'impression.

Afin d'imprimer les «activités du conducteur figurant sur la carte» ou les «événements et anomalies figurant sur la carte», l'appareil de contrôle doit:

— soit sélectionner automatiquement la carte de conducteur ou la carte d'atelier si une seule de ces cartes est insérée,

— soit comporter une commande permettant de sélectionner la carte source ou de sélectionner la carte insérée dans le lecteur «conducteur» si ces deux cartes sont insérées dans l'appareil de contrôle.

L'imprimante doit pouvoir imprimer 24 caractères par ligne.

La taille minimale des caractères est de 2,1 mm de hauteur et de 1,5 mm de largeur.

▼M1

L'imprimante doit accepter les caractères latin 1 et les caractères grecs définis dans la norme ISO 8859, parties 1 et 7, comme indiqué à l'appendice 1 du chapitre 4, «Jeux de caractères».

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

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

Le papier utilisé par l'appareil de contrôle doit porter la marque d'homologation appropriée et l'indication du (ou des) type(s) d'appareil de contrôle avec le(s)quel(s) il peut être utilisé. Les tirages papier doivent rester facilement lisibles et identifiables dans les conditions normales de stockage, en termes d'intensité lumineuse, d'humidité et de température, pendant au moins un an.

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

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

17. **Avertissements**

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

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

L'appareil de contrôle prévient le conducteur 15 minutes avant et au moment du dépassement d'un temps de conduite continue de 4 h 30 min.

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

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

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

Dans ce dernier cas, ils doivent comporter le symbole «T» et être de couleur orangée.

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

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

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

18. **Téléchargement de données vers des médias externes**

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

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

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

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

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

▼M1

19. **Données transmises à des dispositifs additionnels externes**

Lorsque l'appareil de contrôle ne comporte pas de fonctions d'affichage de la vitesse et/ou du kilométrage, l'appareil doit produire des signaux de sortie permettant l'affichage de la vitesse du véhicule et/ou de la distance totale parcourue par le véhicule.

L'unité embarquée sur le véhicule doit également permettre de transmettre les données suivantes à l'aide d'une liaison série dédiée indépendante appropriée à partir d'un bus de connexion CAN optionnel [ISO 11898 Véhicules routiers — échanges d'information numérique — Gestionnaire de réseau de communication à vitesse élevée (CAN)], afin qu'elles puissent être traitées par d'autres unités électroniques installées dans le véhicule:

— date et heure TUC,

— vitesse du véhicule,

— distance totale parcourue par le véhicule (compteur kilométrique),

— activité en cours pour le conducteur et le convoyeur,

— indication éventuelle qu'une carte tachygraphique est insérée dans le lecteur «conducteur» et dans le lecteur «convoyeur» et (le cas échéant) informations concernant l'identification de ces cartes (numéro et État membre de délivrance).

D'autres données peuvent être transmises en plus de cette liste minimale.

Lorsque le contact du véhicule est en position MARCHE, ces données sont transmises en permanence. Lorsque le contact est en position ARRÊT, la transmission se poursuit au moins pour les données concernant les changements d'activité du conducteur et du convoyeur et/ou l'insertion ou le retrait d'une carte tachygraphique. Si ces données n'ont pu être transmises alors que le contact du véhicule était en position ARRÊT, elles le sont lorsque le contact est à nouveau en position MARCHE.

20. **Étalonnage**

La fonction d'étalonnage permet:

— le couplage automatique du capteur de mouvement avec l'UEV,

— l'adaptation numérique de la constante k de l'appareil de contrôle au coefficient caractéristique w du véhicule (les véhicules comportant deux rapports d'essieux ou plus doivent être munis d'un commutateur permettant d'aligner ces divers rapports sur le rapport pour lequel l'appareil a été adapté au véhicule),

— la mise à l'heure (sans restriction),

— l'ajustement du kilométrage,

— la mise à jour des données d'identification du capteur de mouvement stockées dans la mémoire,

— la mise à jour ou la confirmation d'autres paramètres connus par l'appareil de contrôle: identification du véhicule, w, l, taille des pneumatiques et réglage du limiteur de vitesse le cas échéant.

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

— la mise à jour des données d'installation du capteur de mouvement détenues par le capteur de mouvement (au besoin),

— la copie, dans la mémoire de l'UEV, des données d'identification du capteur de mouvement.

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

21. **Mise à l'heure**

La fonction de mise à l'heure doit permettre de régler l'heure dans la limite d'une minute à intervalles d'au moins 7 jours.

La fonction de mise à l'heure doit permettre de régler l'heure sans restriction en mode étalonnage.

▼M1

22. **Caractéristiques**

L'unité embarquée sur le véhicule doit pouvoir fonctionner correctement dans une gamme de températures allant de − 20 ºC à 70 ºC, et le capteur de mouvement dans une gamme de températures allant de − 40 ºC à 135 ºC. Le contenu de la mémoire doit être conservé jusqu'à des températures de − 40 ºC.

L'appareil de contrôle doit pouvoir fonctionner correctement dans une gamme d'humidité comprise entre 10 % et 90 %.

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

L'appareil de contrôle doit être conforme à la directive 95/54/CE du 31 octobre 1995 ([1]) portant adaptation au progrès technique de la directive 72/245/CEE du Conseil ([2]), concernant la compatibilité électromagnétique, et doit être protégé contre les décharges électrostatiques et les transitoires.

23. **Matériaux**

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

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

L'unité embarquée sur le véhicule doit satisfaire au niveau de protection IP 40, et le capteur de mouvement au niveau de protection IP 64, aux termes de la norme IEC 529.

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

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

24. **Inscriptions**

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

— à côté du chiffre indiquant la distance parcourue, l'unité de mesure de cette distance, indiquée par l'abréviation «km»,

— à côté du chiffre indiquant la vitesse, l'indication «km/h».

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

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

— nom et adresse du fabricant de l'appareil,

— numéro de pièce du fabricant et année de fabrication de l'appareil,

— numéro de série de l'appareil,

— marque d'homologation de l'appareil.

Lorsque l'espace disponible est insuffisant pour faire figurer l'ensemble des indications précitées, la plaque signalétique doit indiquer au moins le nom ou le logo du fabricant, et le numéro du composant.

IV. EXIGENCES CONSTRUCTIVES ET FONCTIONNELLES APPLICABLES AUX CARTES TACHYGRAPHIQUES

1. **Données visibles**

La page de couverture doit comporter:

les mots «carte de conducteur» ou «carte de contrôleur» ou «carte d'atelier» ou «carte d'entreprise» imprimés en gros caractères dans la ou les langue(s) officielle(s) de l'État membre qui a délivré la carte, selon le type de carte.

([1]) JO L 266 du 8.11.1995, p. 1.
([2]) JO L 152 du 6.7.1972, p. 15.

▼**M1**

les mêmes mots dans les autres langues officielles de la Communauté, imprimés au dos de la carte:

ES	TARJETA DEL CONDUCTOR	TARJETA DE CONTROL	TARJETA DEL CENTRO DE ENSAYO	TARJETA DE LA EMPRESA
DA	FØRERKORT	KONTROLKORT	VÆRKSTEDS-KORT	VIRKSOMHEDS-KORT
DE	FAHRERKARTE	KONTROLL-KARTE	WERKSTATT-KARTE	UNTERNEHMENS-KARTE
EL	ΚΑΡΤΑ ΟΔΗΟΥ	ΚΑΡΤΑ ΕΛΕΓΧΟΥ	ΚΑΡΤΑ ΚΕΝΤΡΟΥ ΔΟΚΙΜΩΝ	ΚΑΡΤΑ ΕΠΙΧΕΙΡΗΣΗΣ
EN	DRIVER CARD	CONTROL CARD	WORKSHOP CARD	COMPANY CARD
FR	CARTE DE CONDUCTEUR	CARTE DE CONTRÔLEUR	CARTE D'ATE-LIER	CARTE D'ENTRE-PRISE
GA	CÁRTA TIOMÁNAÍ	CÁRTA STIÚRTHA	CÁRTA CEARD-LAINNE	CÁRTA COMHLACHTA
IT	CARTA DEL CONDUCENTE	CARTA DI CONTROLLO	CARTA DELL'OF-FICINA	CARTA DELL'A-ZIENDA
NL	BESTUURDERS KAART	CONTROLE-KAART	WERKPLAATS-KAART	BEDRIJFSKAART
PT	CARTÃO DE CONDUTOR	CARTÃO DE CONTROLO	CARTÃO DO CENTRO DE ENSAIO	CARTÃO DE EMPRESA
FIN	KULJETTAJA KORTTILLA	VALVONTA KORTILLA	TESTAUSASEMA KORTILLA	YRITYSKORTILLA
SV	FÖRARKORT	KONTROLLKORT	VERKSTADS-KORT	FÖRETAGSKORT

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

le code de l'État membre qui a délivré la carte, imprimé en blanc sur fond bleu dans un rectangle entouré de 12 étoiles jaunes. Les codes sont les suivants:

B Belgique

DK Danemark

D Allemagne

GR Grèce

E Espagne

F France

IRL Irlande

I Italie

L Luxembourg

NL Pays-Bas

A Autriche

P Portugal

FIN Finlande

S Suède

UK Royaume-Uni

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

▼**M1**

	Carte de conducteur	Carte de contrôleur	Carte d'entreprise ou d'atelier
1.	nom du conducteur	nom de l'organisme de contrôle	nom de l'entreprise ou de l'atelier
2.	prénom(s) du conducteur	nom du contrôleur (le cas échéant)	nom du détenteur de la carte (le cas échéant)
3.	date de naissance du conducteur	prénom(s) du contrôleur (le cas échéant)	prénom(s) de détenteur de la carte (le cas échéant)
4.(a)	date de début de validité de la carte		
(b)	date d'expiration de la carte (le cas échéant)		
(c)	nom de l'autorité qui a délivré la carte (peut être imprimé en page 2)		
(d)	numéro différent de celui indiqué au point 5, pour raisons administratives (facultatif)		
5.(a)	Numéro du permis de conduire (à la date de délivrance de la carte de conducteur)		
5.(b)	Numéro de la carte		
6.	Photographie du conducteur	Photographie du contrôleur (facultatif)	—
7.	Signature du conducteur	Signature du détenteur (facultatif)	
8.	Lieu habituel de résidence, ou adresse postale du détenteur (facultatif)	Adresse postale de l'organisme de contrôle	Adresse postale de l'entreprise ou de l'atelier

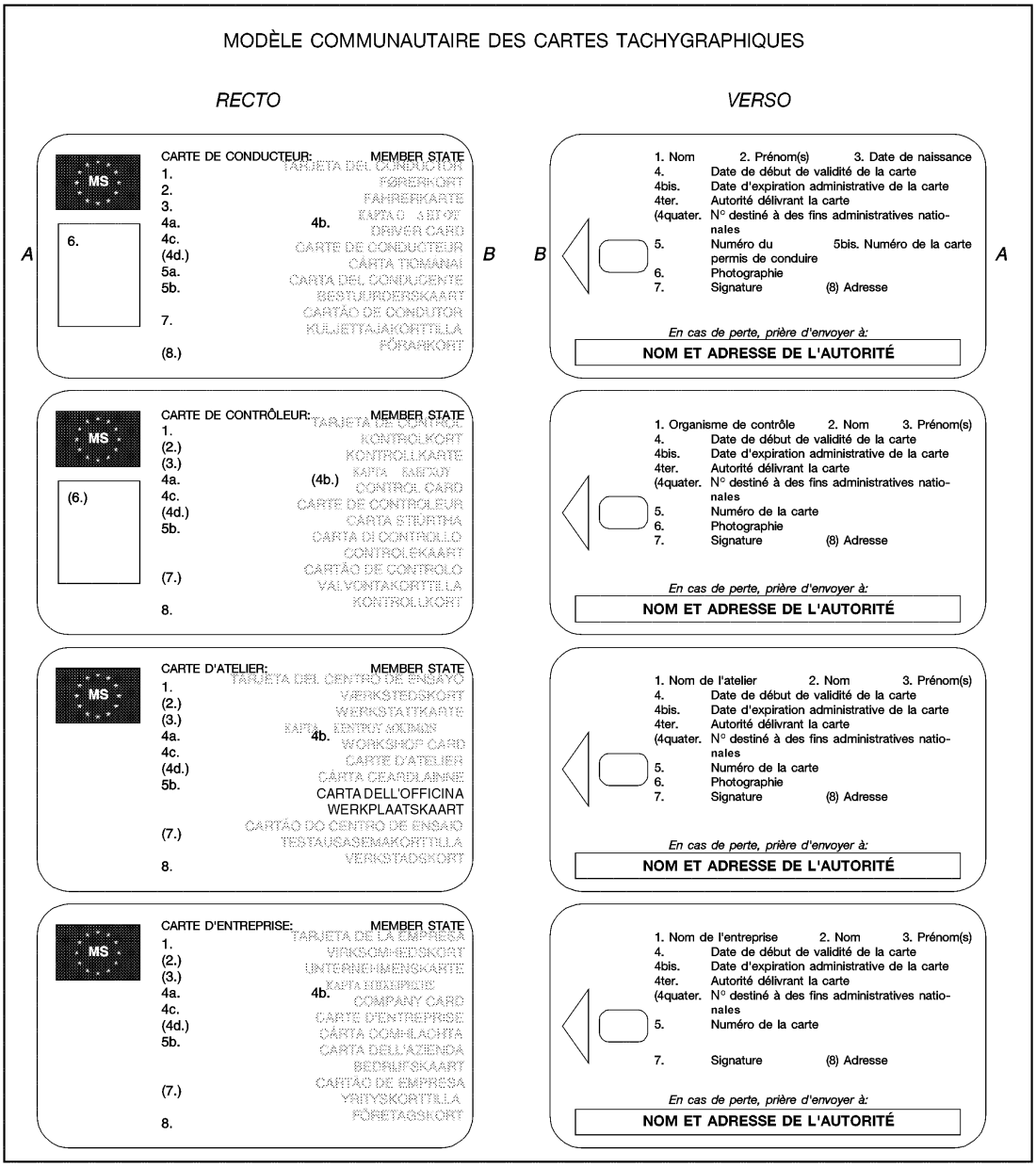
les dates sont indiquées sous la forme «jj/mm/aaaa» ou «jj.mm.aaaa»

le verso doit comporter:

une légende des numéros indiqués au recto;

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

▼**M1**



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

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

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

— impression de fond de sécurité finement guillochée et irisée,
— chevauchement de l'impression de fond de sécurité et de la photographie,
— au moins une ligne bicolore micro-imprimée.

Après consultation de la Commission, les États membres peuvent ajouter des couleurs et des inscriptions, tels que des symboles nationaux et des éléments de sécurité, sans préjudice des autres dispositions de la présente annexe.

2. **Sécurité**

La sécurité du système vise à protéger l'intégrité et l'authenticité des données échangées entre les cartes et l'appareil de contrôle, ainsi que l'intégrité et

▼M1

l'authenticité des données téléchargées à partir des cartes, en autorisant uniquement certaines opérations d'inscription sur les cartes par l'appareil de contrôle, en excluant toute possibilité de falsification des données stockées sur les cartes, en empêchant les manipulations et en détectant toute tentative en ce sens.

Afin d'assurer cette sécurité, les cartes tachygraphiques doivent satisfaire aux exigences de sécurité définies dans l'objectif général de sécurité applicable aux cartes tachygraphiques (appendice 10).

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

3. **Normes**

Les cartes tachygraphiques doivent être conformes aux normes suivantes:

— ISO/CEI 7810 Cartes d'identification — caractéristiques physiques,
— ISO/CEI 7816 Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts:
  — Partie 1: caractéristiques physiques,
  — Partie 2: dimensions et emplacement des contacts,
  — Partie 3: signaux électriques et protocoles de transmission,
  — Partie 4: commandes intersectorielles pour les échanges,
  — Partie 8: commandes intersectorielles de sécurité,
— ISO/CEI 10373 Cartes d'identification — méthodes d'essai,

4. **Spécifications environnementales et électriques**

Les cartes tachygraphiques doivent pouvoir fonctionner correctement dans toutes les conditions climatiques normalement observées sur le territoire communautaire, et au minimum dans une gamme de température comprise entre − 25 ºC et + 70 ºC, avec des pointes occasionnelles à + 85 ºC, «occasionnelles» signifiant d'une durée inférieure à 4 heures et à moins de 100 reprises au cours de la durée de vie de la carte.

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

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

En fonctionnement, les cartes tachygraphiques doivent satisfaire à la directive 95/54/CE de la Commission, du 31 octobre 1995, relative à la compatibilité électromagnétique ([1]), et doivent être protégées contre les décharges électrostatiques.

5. **Stockage des données**

Aux fins du présent paragraphe,

— les heures sont enregistrées à la minute près, sauf indication contraire,
— le kilométrage est enregistré au kilomètre près,
— les vitesses sont enregistrées au kilomètre/heure près.

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

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

Toutes les données additionnelles susceptibles d'être stockées sur une carte tachygraphique en relation avec d'autres applications éventuellement présentes sur la carte, doivent être stockées conformément à la directive 95/46/CE ([2]).

5.1. ***Identification de la carte et données de sécurité***

5.1.1. *Identification des applications*

Les cartes tachygraphiques doivent pouvoir stocker les données suivantes pour l'identification des applications:

— identification de l'application tachygraphique,

([1]) JO L 266 du 8.11.1995, p. 1.
([2]) JO L 281 du 23.11.1995, p. 31.

▼M1

— identification du type de carte tachygraphique.

5.1.2. *Identification du microprocesseur*

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

— numéro de série du circuit intégré,

— références de fabrication du circuit intégré.

5.1.3. *Identification des cartes à circuit intégré*

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

— numéro de série de la carte (y compris les références de fabrication),

— numéro d'homologation de la carte,

— identification personnelle de la carte,

— identification de l'intégrateur,

— identificateur du circuit intégré.

5.1.4. *Éléments de sécurité*

Les cartes tachygraphiques doivent pouvoir stocker les données suivantes pour l'identification de la carte:

— clé publique européenne,

— certificat de l'État membre,

— certificat de la carte,

— clé privée de la carte.

5.2. ***Carte de conducteur***

5.2.1. *Identification de la carte*

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

— numéro de la carte,

— État membre ayant délivré la carte, nom de l'autorité compétente pour la délivrance, date de délivrance,

— date de début de validité de la carte, date d'expiration.

5.2.2. *Identification du détenteur de la carte*

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

— nom du détenteur,

— prénoms du détenteur de la carte,

— date de naissance,

— langue habituelle.

5.2.3. *Renseignements concernant le permis de conduire*

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

— État membre qui a délivré le permis, nom de l'autorité compétente pour la délivrance,

— numéro du permis de conduire (au moment de la délivrance de la carte).

5.2.4. *Données concernant le véhicule utilisé*

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

— date et heure de la première utilisation du véhicule (c'est-à-dire de la première insertion de la carte pour cette période d'utilisation du véhicule, ou 00h00 si la période d'utilisation est en cours à cette heure-là),

— kilométrage du véhicule à ce moment,

▼M1

— date et heure de la dernière utilisation du véhicule (c'est-à-dire le dernier retrait de la carte pour cette période d'utilisation du véhicule, ou 23h59 si la période d'utilisation est en cours à cette heure-là),
— kilométrage du véhicule à ce moment,
— numéro et État membre d'immatriculation du véhicule.

La carte de conducteur doit pouvoir stocker au moins 84 fiches de ce type.

5.2.5. *Données relatives à l'activité du conducteur*

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

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

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

Les données énumérées aux exigences 197 et 199 doivent être stockées d'une manière permettant de retrouver les activités dans l'ordre de leur occurrence, même en cas de chevauchement temporel.

5.2.6. *Lieux de début/de fin des périodes journalières de travail*

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

— date et heure de la saisie (ou date/heure liée à la saisie, si celle-ci est réalisée au cours de la procédure de saisie manuelle),
— type de saisie (début ou fin, condition de saisie),
— pays et région saisis,
— kilométrage du véhicule.

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

5.2.7. *Données relatives aux événements*

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

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

— chevauchement temporel (lorsque la carte est la cause de l'événement),
— insertion d'une carte en cours de conduite (lorsque cet événement concerne la carte),
— clôture incorrecte de la session précédente (lorsque cet événement concerne la carte),
— interruption de l'alimentation électrique,
— erreur sur les données de mouvement,
— tentatives d'atteinte à la sécurité.

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

— code d'événement,
— date et heure de début d'événement (ou de l'insertion de la carte dans le cas où l'événement était en cours à ce moment-là),
— date et heure de la fin de l'événement (ou du retrait de la carte si l'événement était en cours à ce moment-là),
— numéro et État membre d'immatriculation du véhicule dans lequel l'événement est survenu.

▼M1

Remarque: concernant l'événement «chevauchement temporel»:

— la date et l'heure du début de l'événement doivent correspondre à la date et à l'heure du retrait de la carte du véhicule précédent,

— la date et l'heure de la fin de l'événement doivent correspondre à la date et à l'heure de l'insertion de la carte dans le véhicule actuel,

— les données relatives au véhicule doivent correspondre au véhicule actuel où l'événement est apparu.

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

— la date et l'heure du début de l'événement doivent correspondre à la date et à l'heure de l'insertion de la carte correspondant à la session incorrectement clôturée,

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

— les données relatives au véhicule doivent correspondre au véhicule dans lequel la session a été incorrectement clôturée.

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

5.2.8. *Données relatives aux anomalies*

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

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

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

— anomalie de l'appareil de contrôle.

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

— code de l'anomalie,

— date et heure de début de l'anomalie (ou de l'insertion de la carte dans le cas où l'anomalie était en cours à ce moment-là),

— date et heure de la fin de l'anomalie (ou du retrait de la carte si l'anomalie était en cours à ce moment-là),

— numéro et État membre d'immatriculation du véhicule dans lequel l'anomalie est survenue.

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

5.2.9. *Données relatives aux activités de contrôle*

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

— date et heure du contrôle,

— numéro de la carte de contrôleur et État membre qui l'a délivrée,

— type de contrôle [affichage et/ou impression et/ou téléchargement à partir de l'UEV et/ou à partir de la carte (voir remarque)],

— période téléchargée, le cas échéant,

— numéro et État membre d'immatriculation du véhicule dans lequel le contrôle a été effectué.

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

La carte de conducteur doit permettre le stockage de ces données.

5.2.10. *Données concernant les sessions pour chaque carte*

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

— date et heure d'ouverture de la session (c.-à.-d. de l'insertion de la carte), à la seconde près,

— numéro et État membre d'immatriculation du véhicule.

▼M1

5.2.11. *Données relatives aux conditions particulières*

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

— date et heure de la saisie,

— type de condition particulière.

La carte de conducteur doit permettre le stockage de 56 fiches de ce type.

5.3. ***Carte d'atelier***

5.3.1. *Éléments de sécurité*

La carte d'atelier doit permettre le stockage d'un numéro personnel d'identification.

La carte d'atelier doit permettre le stockage des clés cryptographiques nécessaires pour le couplage du capteur de mouvement à l'unité embarquée sur le véhicule.

5.3.2. *Identification de la carte*

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

— numéro de la carte,

— État membre ayant délivré la carte, autorité compétente pour la délivrance, date de délivrance,

— date de début de validité de la carte, et date d'expiration.

5.3.3. *Identification du détenteur de la carte*

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

— nom de l'atelier,

— adresse de l'atelier,

— nom du détenteur,

— prénom(s) du détenteur,

— langue habituelle.

5.3.4. *Données concernant le véhicule utilisé*

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

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

5.3.5. *Données concernant l'activité du conducteur*

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

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

5.3.6. *Données concernant la fin et/ou le début des périodes de travail journalières*

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

La carte d'atelier doit permettre le stockage d'au moins 3 paires de données.

5.3.7. *Données relatives aux événements et aux anomalies*

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

La carte d'atelier doit permettre le stockage des trois derniers événements de chaque type (soit 18 événements) et des six dernières anomalies de chaque type (soit 12 anomalies).

5.3.8. *Données concernant les activités de contrôle*

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

▼M1

5.3.9. *Données concernant l'étalonnage et la mise à l'heure*

La carte d'atelier doit permettre le stockage des données relatives aux étalonnages et/ou aux réglages temporels réalisés alors que la carte est insérée dans l'appareil.

Chaque fiche d'étalonnage doit contenir les données suivantes:

— objet de l'étalonnage (première installation, installation, inspection périodique, autre),

— identification du véhicule,

— paramètres mise à jour ou confirmés [w, k, l, taille des pneumatiques, réglage du limiteur de vitesse, compteur kilométrique (valeurs nouvelle et ancienne), date et heure (valeurs nouvelle et ancienne)],

— identification de l'appareil de contrôle (numéros des pièces et de série de l'UEV, numéro de série du capteur de mouvement).

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

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

La carte d'atelier doit comporter un compteur indiquant le nombre d'étalonnages réalisés depuis le dernier téléchargement.

5.3.10. *Données concernant les conditions particulières*

La carte d'atelier doit permettre le stockage des données relatives aux conditions particulières de la même manière qu'une carte de conducteur. La carte d'atelier doit permettre le stockage de deux fichiers contenant de telles données.

5.4. ***Carte de contrôleur***

5.4.1. *Identification de la carte*

La carte de contrôleur doit permettre le stockage des données suivantes pour l'identification de la carte:

— numéro de la carte,

— État membre ayant délivré la carte, nom de l'autorité compétente pour la délivrance, date de délivrance,

— date de début de validité de la carte, date d'expiration (le cas échéant).

5.4.2. *Identification du détenteur de la carte*

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

— nom de l'organisme de contrôle,

— adresse de l'organisme de contrôle,

— nom du détenteur,

— prénom(s) du détenteur,

— langue habituelle.

5.4.3. *Données relatives aux activités de contrôle*

La carte de contrôleur doit permettre le stockage des données suivantes relatives aux activités de contrôle:

— date et heure du contrôle,

— type du contrôle (affichage et/ou impression et/ou téléchargement à partir de l'UEV et/ou à partir de la carte),

— période téléchargée (le cas échéant),

— numéro et État membre d'immatriculation du véhicule contrôlé,

— numéro de la carte de conducteur contrôlée et État membre qui l'a délivrée.

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

5.5. ***Carte d'entreprise***

5.5.1. *Identification de la carte*

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

— numéro de la carte,

▼M1

— État membre qui a délivré la carte, autorité compétente pour la délivrance, date de délivrance,

— date de début de validité de la carte, date d'expiration (le cas échéant).

5.5.2. *Identification du détenteur de la carte*

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

— nom de l'entreprise,

— adresse de l'entreprise.

5.5.3. *Données concernant l'activité de l'entreprise*

La carte d'entreprise doit permettre le stockage des données suivantes concernant les activités de l'entreprise:

— date et heure de l'activité,

— type de l'activité (verrouillage et/ou déverrouillage de l'UEV, téléchargement à partir de l'UEV et/ou de la carte),

— période téléchargée (le cas échéant),

— numéro et État membre d'immatriculation du véhicule,

— numéro de la carte et État membre qui l'a délivrée (en cas de téléchargement à partir de la carte).

La carte d'entreprise doit permettre le stockage de 230 fiches de ce type.

V. INSTALLATION DE L'APPAREIL DE CONTRÔLE

1. **Installation**

L'appareil de contrôle neuf est livré non activé aux monteurs ou aux constructeurs de véhicules, avec tous les paramètres d'étalonnage figurant sur la liste du chapitre III, paragraphe 20, réglés aux valeurs par défaut appropriées et à jour. Lorsqu'aucune valeur particulière ne convient, on aura recours à des séries de points d'interrogation pour les paramètres alphabétiques et au 0 pour les paramètres numériques.

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

Avant son activation, l'appareil de contrôle ne doit ni enregistrer ni stocker les données visées au chapitre III, points 12.3 à 12.9, et points 12.12 à 12.14.

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

Les constructeurs de véhicules ou les monteurs doivent activer l'appareil de contrôle installé avant que le véhicule ne quitte les locaux où a été effectuée l'installation.

L'activation de l'appareil de contrôle doit être déclenchée automatiquement par la première insertion d'une carte d'atelier dans une quelconque des interfaces destinées aux cartes.

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

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

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

L'installation doit être suivie d'un étalonnage. Le premier étalonnage doit comporter la saisie du numéro d'immatriculation du véhicule et intervenir dans les 2 semaines suivant l'installation ou l'attribution d'un numéro d'immatriculation, si celle-ci intervient en dernier.

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

2. **Plaquette d'installation**

Après la vérification de l'appareil de contrôle une fois installé, une plaquette d'installation bien visible et facilement accessible doit être fixée sur, à l'intérieur, ou à côté de l'appareil de contrôle. Après chaque inspection par un atelier ou un monteur agréé, une nouvelle plaquette est fixée à la place de la précédente.

▼M1

La plaquette doit comporter les indications suivantes:

— nom, adresse ou raison commerciale du monteur ou de l'atelier agréé,
— coefficient caractéristique du véhicule, sous la forme «w = … imp/km»,
— constante de l'appareil de contrôle, sous la forme «k = … imp/km»,
— circonférence effective des pneumatiques, sous la forme «l = … mm»,
— taille des pneumatiques,
— date à laquelle le coefficient caractéristique du véhicule a été déterminé, et la circonférence effective des pneumatiques mesurée,
— numéro d'identification du véhicule.

3. **Scellement**

Les parties suivantes doivent être scellées:

— toute connexion qui, si elle était déconnectée, entraînerait des modifications indécelables ou des pertes de données indécelables,
— la plaquette d'installation, sauf si elle est fixée de telle manière qu'elle ne puisse être enlevée sans détruire les indications qu'elle porte.

Les scellements précités peuvent être retirés:

— en cas d'urgence,
— afin d'installer, d'ajuster ou de réparer un limiteur de vitesse ou tout autre dispositif contribuant à la sécurité routière, pour autant que l'appareil de contrôle continue à fonctionner de manière fiable et correcte, et qu'il soit scellé à nouveau par un monteur ou un atelier agréé (conformément au chapitre VI) immédiatement après l'installation du limiteur de vitesse ou de tout autre dispositif contribuant à la sécurité routière, ou dans les sept jours pour les autres cas.

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

VI. CONTRÔLES, INSPECTIONS ET RÉPARATIONS

Les prescriptions concernant les circonstances dans lesquelles les scellés peuvent être retirés, comme indiqué à l'article 12, paragraphe 5, du règlement (CEE) nº 3821/85 tel que modifié en dernier lieu par le règlement (CE) nº 2135/98, sont définies au chapitre V, partie 3 de la présente annexe.

1. **Agrément des monteurs ou des ateliers**

Les États membres agréent, contrôlent régulièrement et certifient les organismes chargés des tâches suivantes:

— installations,
— contrôles,
— inspections,
— réparations.

Dans le cadre de l'article 12, paragraphe 1, du présent règlement, les cartes d'atelier seront uniquement délivrées aux monteurs et/ou aux ateliers agréés pour l'activation et/ou l'étalonnage d'appareils de contrôle, conformément à la présente annexe et qui, sauf cas dûment motivé:

— ne sont pas éligibles pour une carte d'entreprise, et
— dont les autres activités professionnelles ne sont pas de nature à compromettre la sécurité globale du système telle que définie à l'appendice 10.

2. **Vérification d'instruments neufs ou réparés**

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 III, points 2.1 et 2.2.

3. **Inspection des installations**

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 III, points 2.1. et 2.2.

4. **Inspections périodiques**

Des inspections périodiques des appareils montés sur les véhicules ont lieu après toute réparation, ou après toute modification du coefficient caractéristique du véhicule ou de la circonférence effective des pneumatiques, ou lorsque l'horloge

▼M1

TUC est fausse de plus de 20 minutes, ou lorsque le numéro d'immatriculation a changé, et au moins une fois tous les deux ans (24 mois).

Ces inspections comprennent les vérifications suivantes:

— fonctionnement correct de l'appareil de contrôle, y compris la fonction de stockage de données sur les cartes tachygraphiques,

— conformité aux dispositions du chapitre III, points 2.1 et 2.2 concernant les tolérances maximales à l'installation,

— présence de la marque d'homologation sur l'appareil de contrôle,

— présence de la plaquette d'installation,

— intégrité des scellements sur l'appareil et sur les autres parties de l'installation,

— taille des pneumatiques et circonférence effective des pneumatiques.

Ces inspections comprennent un étalonnage.

5. **Mesure des erreurs**

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

— véhicule à vide en ordre de marche,

— pression des pneumatiques conforme aux instructions du fabricant,

— usure des pneumatiques dans les limites autorisées en droit national,

— mouvement du véhicule:

  — le véhicule doit avancer, sous l'action de son propre moteur, en ligne droite sur sol plat à une vitesse de 50 + 5 km/h. La distance mesurée doit être d'au moins 1 000 m.

— pour autant qu'elles soient d'une précision comparable, d'autres méthodes, comme par exemple l'utilisation d'un banc approprié, peuvent également être mises en œuvre pour l'essai.

6. **Réparations**

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

Les ateliers agréés délivrent aux entreprises de transport un certificat attestant que les données ne peuvent être téléchargées lorsqu'un dysfonctionnement de l'appareil de contrôle empêche de télécharger les données stockées, même après réparation à l'atelier même. Les ateliers conservent une copie de chaque certificat délivré, pendant au moins un an.

VII. DÉLIVRANCE DES CARTES

Les processus mis en place par les États membres pour la délivrance des cartes sont conformes aux prescriptions suivantes:

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

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

Une carte tachygraphique délivrée en remplacement d'une carte tachygraphique existante doit avoir le même numéro que celle qu'elle remplace, sauf l'indice de remplacement, qui doit être augmenté d'une unité (dans une série 0 à 9, A à Z).

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

Une carte tachygraphique délivrée en renouvellement d'une carte existante doit porter le même numéro que cette dernière, sauf pour l'indice de remplacement, qui doit être remis à «0», et pour l'indice de renouvellement, qui doit être augmenté d'une unité (dans une série de 0 à 9, A à Z).

L'échange d'une carte tachygraphique existante, aux fins de la modification de données administratives, doit suivre les règles applicables au renouvellement s'il est effectué à l'intérieur d'un même État membre, ou les règles applicables à une première délivrance s'il est effectué dans un autre État membre.

Dans le cas d'une carte d'atelier ou de contrôleur non nominative, la rubrique «nom du détenteur de la carte» doit être complétée par le nom de l'atelier ou de l'organisme de contrôle.

▼M1

VIII. HOMOLOGATION DE L'APPAREIL DE CONTRÔLE ET DES CARTES TACHYGRAPHIQUES

1. **Généralités**

Aux fins du présent chapitre, on entend par «appareil de contrôle», l'appareil de contrôle ou ses composants. Aucune homologation n'est requise pour le(s) câble(s) reliant le capteur de mouvement à l'UEV. Le papier utilisé pour l'appareil de contrôle est considéré comme un composant de l'appareil.

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

L'homologation d'un appareil de contrôle et de cartes tachygraphiques comporte des essais liés à la sécurité, des essais fonctionnels et des essais d'interopérabilité. Les résultats positifs à chacun de ces essais sont attestés par un certificat approprié.

Les autorités d'homologation des États membres n'accorderont pas de certificat d'homologation conformément à l'article 5 du présent règlement tant qu'elles ne sont pas en possession:

— d'un certificat de sécurité,

— d'un certificat de fonctionnement,

— d'un certificat d'interopérabilité,

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

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

Les procédures pour la mise à niveau in situ du logiciel de l'appareil de contrôle doivent être approuvées par l'autorité qui a accordé l'homologation pour l'appareil de contrôle concerné. La mise à niveau logicielle ne doit ni modifier ni supprimer aucune donnée relative à l'activité du conducteur stockée dans l'appareil de contrôle. Le logiciel ne peut être mis à niveau que sous la responsabilité du fabricant de l'appareil de contrôle.

2. **Certificat de sécurité**

Le certificat de sécurité est délivré conformément aux dispositions de l'appendice 10 de la présente annexe.

3. **Certificat de fonctionnement**

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

Un certificat de fonctionnement est délivré par le fabricant uniquement après que l'appareil a obtenu des résultats positifs à tous les essais fonctionnels spécifiés à l'appendice 9.

L'autorité d'homologation délivre le certificat de fonctionnement. Ce certificat comporte, outre le nom de son bénéficiaire et le nom du modèle, une liste détaillée des essais réalisés et des résultats obtenus.

4. **Certificat d'interopérabilité**

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

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

Les demandes sont officiellement enregistrées lorsque le laboratoire est en possession:

— de l'ensemble du matériel et des documents nécessaires pour les essais d'interopérabilité,

— du certificat de sécurité correspondant,

— du certificat de fonctionnement correspondant.

La date de l'enregistrement de la demande est notifiée au fabricant.

Aucun essai d'interopérabilité ne sera réalisé par le laboratoire sur un appareil de contrôle ou une carte tachygraphique qui n'a pas reçu de certificat de sécurité et de certificat de fonctionnement.

▼M1

Tout fabricant demandant des essais d'interopérabilité s'engage à laisser au laboratoire chargé des essais l'ensemble du matériel et de la documentation fournis aux fins des essais.

Les essais d'interopérabilité sont effectués, conformément au paragraphe 5 de l'appendice 9 de la présente annexe, sur tous les types d'appareil de contrôle ou de cartes tachygraphiques:

— dont l'homologation est en cours de validité,

— dont l'homologation est en instance et pour lesquels existe un certificat d'interopérabilité en cours de validité.

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

En cas de résultat négatif des essais d'interopérabilité sur un ou plusieurs appareil(s) d'enregistrement ou carte(s) tachygraphique(s), comme prévu à l'exigence 283, le certificat d'interopérabilité n'est pas délivré tant que le fabricant concerné n'a pas apporté les modifications nécessaires et que l'appareil ou la carte n'a pas satisfait à tous les essais d'interopérabilité. Le laboratoire détermine l'origine du problème avec l'aide du fabricant concerné, et s'efforce d'assister ce fabricant dans la recherche d'une solution technique. Dans les cas où le fabricant a modifié son produit, il lui incombe de s'assurer auprès des autorités compétentes de la validité du certificat de sécurité et du certificat de fonctionnement.

Le certificat d'interopérabilité est valable six mois. Il expire à la fin de cette période si le fabricant n'a pas reçu un certificat d'homologation correspondant. Il est transmis par le fabricant à l'autorité d'homologation de l'État membre qui a délivré le certificat de fonctionnement.

Tout élément susceptible d'être à l'origine d'une anomalie d'interopérabilité ne doit pas être utilisé pour réaliser des bénéfices ni pour accéder à une position dominante.

5. **Certificat d'homologation**

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

Une copie du certificat d'homologation doit être transmise par l'autorité d'homologation au laboratoire chargé des essais d'interopérabilité lors de la délivrance de ce certificat au fabricant.

Le laboratoire compétent pour les essais d'interopérabilité doit mettre à jour, sur un site Internet public, la liste des modèles d'appareil de contrôle ou de cartes tachygraphiques:

— pour lesquels une demande d'essais d'interopérabilité a été enregistrée,

— qui ont reçu un certificat d'interopérabilité (même provisoire),

— qui ont reçu un certificat d'homologation.

6. **Procédure exceptionnelle: premier certificat d'interopérabilité**

Pendant une période de quatre mois après qu'un premier couple appareil de contrôle/cartes tachygraphiques (cartes de conducteur, d'atelier, de contrôleur et d'entreprise) a été certifié interopérable, tous les certificats d'interopérabilité délivrés (y compris ce tout premier) en relation avec des demandes reçues pendant cette période seront considérés comme provisoires.

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

Si des anomalies d'interopérabilité apparaissent au cours de cette période, le laboratoire chargé des essais d'interopérabilité détermine la cause des problèmes observés, avec l'aide de tous les fabricants concernés, et les invite à apporter les modifications nécessaires.

Si à la fin de cette période, des problèmes d'interopérabilité demeurent, le laboratoire chargé des essais d'interopérabilité détermine, en collaboration avec les fabricants concernés et avec les autorités d'homologation qui ont délivré les certificats fonctionnels correspondants, les causes des anomalies d'interopérabilité, et définissent les modifications que chaque constructeur concerné doit apporter. La recherche de solutions techniques peut se prolonger pendant un maximum de deux mois, après quoi la Commission, en l'absence de solution commune, et après consultation du laboratoire chargé des essais d'interopérabilité, décide du (ou des) appareil(s) et des cartes auxquels est délivré un certificat d'interopérabilité définitif, en précisant les raisons de son choix.

Toute demande d'essais d'interopérabilité enregistrée par le laboratoire entre la fin de la période de quatre mois après le premier certificat d'interopérabilité provisoire et la date de la décision de la Commission visée à l'exigence 294 est

▼**M1**

repoussée jusqu'à la résolution des problèmes d'interopérabilité initiaux. Ces demandes sont ensuite traitées dans l'ordre de leur enregistrement.

▼M1

Appendice 1

DICTIONNAIRE DE DONNÉES

TABLE DES MATIÈRES

▼**M1**

2.39. CompanyCardApplicationIdentification …

2.40. CompanyCardHolderIdentification …

2.41. ControlCardApplicationIdentification …

2.42. ControlCardControlActivityData …

2.43. ControlCardHolderIdentification …

2.44. ControlType …

2.45. CurrentDateTime …

2.46. DailyPresenceCounter …

2.47. Datef …

2.48. Distance …

2.49. DriverCardApplicationIdentification …

2.50. DriverCardHolderIdentification …

2.51. EntryTypeDailyWorkPeriod …

2.52. EquipmentType …

2.53. EuropeanPublicKey …

2.54. EventFaultType …

2.55. EventFaultRecordPurpose …

2.56. ExtendedSerialNumber …

2.57. FullCardNumber …

2.58. HighResOdometer …

2.59. HighResTripDistance …

2.60. HolderName …

2.61. K-ConstantOfRecordingEquipment …

2.62. KeyIdentifier …

2.63. L-TyreCircumference …

2.64. Language …

2.65. LastCardDownload …

2.66. ManualInputFlag …

2.67. ManufacturerCode …

2.68. MemberStateCertificate …

2.69. MemberStatePublicKey …

2.70. Name …

2.71. NationAlpha …

2.72. NationNumeric …

2.73. NoOfCalibrationRecords …

2.74. NoOfCalibrationSinceDonwload …

2.75. NoOfCardPlaceRecords …

2.76. NoOfCardVehicleRecords …

2.77. NoOfCompanyActivityRecords …

2.78. NoOfControlActivityRecords …

2.79. NoOfEventsPerType …

2.80. NoOfFaultsPerType …

2.81. OdometerValueMidnight …

2.82. OdometerShort …

2.83. OverspeedNumber …

2.84. PlaceRecord …

▼**M1**

2.85. PreviousVehicleInfo …

2.86. PublicKey …

2.87. RegionAlpha …

2.88. RegionNumeric …

2.89. RSAKeyModulus …

2.90. RSAKeyPrivateExponent …

2.91. RSAKeyPublicExponent …

2.92. SensorApprovalNumber …

2.93. SensorIdentification …

2.94. SensorInstallation …

2.95. SensorInstallationSecData …

2.96. SensorOSIdentifier …

2.97. SensorPaired …

2.98. SensorPairingDate …

2.99. SensorSerialNumber …

2.100. SensorSCIdentifier …

2.101. Signature …

2.102. SimilarEventsNumber …

2.103. SpecificConditionType …

2.104. SpecificConditionRecord …

2.105. Speed …

2.106. SpeedAuthorised …

2.107. SpeedAverage …

2.108. SpeedMax …

2.109. TDesSessionKey …

2.110. TimeReal …

2.111. TyreSize …

2.112. VehicleIdentificationNumber …

2.113. VehicleRegistrationIdentification …

2.114. VehicleRegistrationNumber …

2.115. VuActivityDailyData …

2.116. VuApprovalNumber …

2.117. VuCalibrationData …

2.118. VuCalibrationRecord …

2.119. VuCardIWData …

2.120. VuCardIWRecord …

2.121. VuCertificate …

2.122. VuCompanyLocksData …

2.123. VuCompanyLocksRecord …

2.124. VuControlActivityData …

2.125. VuControlActivityRecord …

2.126. VuDataBlockCounter …

2.127. VuDetailedSpeedBlock …

2.128. VuDetailedSpeedData …

2.129. VuDownloadablePeriod …

2.130. VuDownloadActivityData …

▼**M1**

▼M1

1. INTRODUCTION

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

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

Le présent appendice a recours à la Notation de syntaxe abstraite numéro un (ASN.1) pour définir les différents types de données. Ce système autorise la définition de données simples et structurées sans nécessiter l'emploi d'une syntaxe de transfert spécifique (règles de codage) qui dépende de l'application et de l'environnement considérés.

Les règles d'affectation des noms du type ASN.1 sont établies en conformité avec la norme ISO/CEI 8824-1. Il en résulte que:

— dans la mesure du possible, la signification d'un type de données est implicitement fournie par le nom qui leur est attribué,

— si un type de données se compose d'autres types de données, le nom de ce type de données se présente encore et toujours sous la forme d'une seule séquence de caractères alphabétiques commençant par une majuscule, quoique ce nom comporte un nombre indéterminé de capitales qui en rappellent la signification,

— de manière générale, les noms de type de données sont en rapport avec le nom des types de données à partir desquels ils sont construits, avec l'équipement au sein duquel les données sont mémorisées et avec la fonction associée aux données considérées.

Si l'emploi d'un type ASN.1 déjà défini dans le cadre d'une autre norme s'impose avec l'appareil de contrôle, ce type ASN.1 sera défini dans le présent appendice.

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

1.2. **Références**

Les abréviations qui suivent apparaissent dans le présent appendice:

ISO 639	Code de représentation des noms de langue. Première édition: 1988.
EN 726-3	Systèmes de cartes d'identification — Cartes et terminaux de télécommunications à circuit(s) intégré(s) — Partie 3: Exigences indépendantes de toute application auxquelles les cartes doivent satisfaire. Décembre 1994.
ISO 3779	Véhicules routiers — Numéro d'identification du véhicule (NIdV) — Contenu et structure. Troisième édition: 1983.
ISO/IEC 7816-5	Technologie de l'information — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 5: Système de numérotation et procédure d'enregistrement des identificateurs d'application. Première édition: 1994 + Révision 1: 1996.
ISO/IEC 8824-1	Technologie de l'information — Notation de syntaxe abstraite numéro un (ASN.1): Spécification de la notation de base. Deuxième édition: 1998.
ISO/IEC 8825-2	Technologie de l'information — Règles de codage en ASN.1: Spécification des règles de codage condensé (RCC). Deuxième édition: 1998.
ISO/IEC 8859-1	Technologie de l'information — Jeux de caractères graphiques codés en octets — Partie 1: Alphabet latin nº 1. Première édition: 1998.
ISO/IEC 8859-7	Technologie de l'information — Jeux de caractères graphiques codés en octets — Partie 7: Alphabet latin/grec. Première édition: 1987.
ISO 16844-3	Véhicules routiers — Systèmes tachygraphiques — Interface des capteurs de mouvement. WD 3-20/05/99.

2. DÉFINITIONS DES TYPES DE DONNÉES

Quel que soit le type de donnée considéré parmi ceux qui suivent, un contenu «inconnu» ou «sans objet» entraînera l'attribution d'une valeur par défaut résultant du remplissage de l'élément de donnée concerné au moyen d'octets 'FF'.

▼M1

2.1. **ActivityChangeInfo**

Ce type de données autorise le codage, en mots de deux octets, d'un état du lecteur à 00h00 et/ou d'un état du conducteur à 00h00 et/ou de changements d'activité, d'état de conduite et/ou d'état de carte se rapportant à un conducteur ou un convoyeur. Il est lié aux exigences 084, 109 *bis*, 199 et 219.

ActivityChangeInfo ::= CHAÎNE D'OCTETS (LONGUEUR(2))

Assignation de valeur — Octet aligné: 'scpaatttttttttttt'B (16 bits)

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

's'B Lecteur:

'0'B: CONDUCTEUR

'1'B: CONVOYEUR

'c'B État de conduite:

'0'B: SEUL

'1'B: ÉQUIPAGE

'p'B État de la carte de conducteur (ou d'atelier) insérée dans le lecteur approprié:

'0'B: INSÉRÉE, la carte est insérée

'1'B: NON INSÉRÉE, aucune carte n'est insérée (ou la carte est retirée)

'aa'B Activité:

'00'B: PAUSE/REPOS

'01'B: DISPONIBILITÉ

'10'B: TRAVAIL

'11'B: CONDUITE

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

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

's'B Lecteur (hors de propos si 'p' = 1 sauf remarque ci-après):

'0'B: CONDUCTEUR

'1'B: CONVOYEUR

'c'B	État de conduite (si 'p' = 0) ou	État de l'activité suivante (si 'p' = 1):
	'0'B: SEUL	'0'B: INCONNU
	'1'B: ÉQUIPAGE	'1'B: CONNU (= saisie manuelle)

'p'B État de la carte:

'0'B: INSÉRÉE, la carte est insérée dans un appareil de contrôle

'1'B: NON INSÉRÉE, aucune carte n'est insérée (ou la carte est retirée)

'aa'B Activité (hors de propos si 'p' = 1 et 'c' = 0 sauf remarque ci-après):

'00'B: PAUSE/REPOS

'01'B: DISPONIBILITÉ

'10'B: TRAVAIL

'11'B: CONDUITE

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

Remarque

en cas de «retrait de la carte»:

— 's' s'applique et indique le lecteur dont la carte a été extraite
— 'c' doit être mis à 0
— 'p' doit être mis à 1
— 'aa' doit coder l'activité en cours sélectionnée au même moment

▼M1

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

2.2. **Address**

Une adresse.

```
Address ::= SÉQUENCE {
    codePage ENTIER (0..255),
    address CHAÎNE D'OCTETS [LONGUEUR(35)]
}
```

codePage (page de codes) spécifie la partie de la norme ISO/CEI 8859 utilisée pour coder l'adresse,

address indique une adresse dont le codage est conforme à la page de codes appropriée de la norme ISO/CEI 8859.

2.3. **BCDString**

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

```
BCDString ::= CHAÎNE DE CARACTÈRES (AVEC COMPOSANTS {
    identification ( AVEC COMPOSANTS {
   fixes PRESENTS }) })
```

BCDString a recours à une notation «hstring». Le chiffre hexadécimal de gauche sera considéré comme le quartet le plus significatif du premier octet. Pour produire un multiple d'octets, il faut insérer le nombre approprié de quartets de droite nuls à partir de la position qu'occupe le quartet le plus significatif du premier octet.

Chiffres admis: 0, 1, … 9.

2.4. **CalibrationPurpose**

Code indiquant la raison de l'enregistrement d'un jeu de paramètres d'étalonnage. Ce type de données est lié aux exigences 097 et 098.

```
CalibrationPurpose ::= CHAÎNE D'OCTETS [LONGUEUR(1)]
```

Assignation de valeur:

′00′H valeur réservée

′01′H activation: enregistrement de paramètres d'étalonnage connus, au moment de l'activation de l'UEV

′02′H première installation: premier étalonnage de l'UEV après son activation

′03′H installation: premier étalonnage de l'unité embarquée sur le véhicule considéré

′04′H inspection périodique

2.5. **CardActivityDailyRecord**

Informations enregistrées sur une carte et se rapportant aux activités auxquelles le conducteur s'est livré pendant un jour civil précis. Ce type de données est lié aux exigences 199 et 219.

```
CardActivityDailyRecord ::= SÉQUENCE {
    activityPreviousRecordLength ENTIER (0..CardActivityLengthRange)
    activityRecordLength ENTIER (0..CardActivityLengthRange)
    activityRecordDate Temps réel
    activityDailyPresenceCounter Compteur de présence journalière
    activityDayDistance Distance,
    activityChangeInfo LONGUEUR DÉFINIE (1..1440) DES ActivityChangeInfo
}
```

▼M1

activityPreviousRecordLength indique la longueur totale du précédent relevé quotidien exprimée en octets. La valeur maximale correspond à la longueur de la CHAÎNE D'OCTETS contenant ces relevés (cf. CardActivityLengthRange paragraphe 3). Lorsque ces données correspondent au relevé quotidien le plus ancien, la valeur de l'activityPreviousRecordLength doit être mise à 0.

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

activityRecordDate indique la date du relevé.

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

activityDayDistance indique la distance totale parcourue le jour considéré.

activityChangeInfo indique le jeu de données ActivityChangeInfo se rapportant au conducteur et au jour considérés. Cette chaîne d'octets ne peut contenir plus de 1 440 valeurs (un changement d'activité par minute). Ce jeu comprend toujours l'ActivityChangeInfo encodant l'état du conducteur à 00h00.

2.6. **CardActivityLengthRange**

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

CardActivityLengthRange ::= ENTIER(0..2^{16}-1)

Assignation de valeur: cf. paragraphe 3.

2.7. **CardApprovalNumber**

Numéro d'homologation de la carte.

CardApprovalNumber ::= Chaîne IA5 [LONGUEUR(8)]

Assignation de valeur: non spécifiée.

2.8. **CardCertificate**

Certificat associé à la clé publique d'une carte.

CardCertificate ::= Certificat

2.9. **CardChipIdentification**

Informations enregistrées sur une carte et se rapportant à l'identification du circuit intégré (CI) de cette carte (exigence 191).

```
CardChipIdentification ::= SÉQUENCE {
    icSerialNumber CHAÎNE D'OCTETS [LONGUEUR(4)],
    icManufacturingReferences CHAÎNE D'OCTETS
    [LONGUEUR(4)]
}
```

icSerialNumber indique le numéro de série du CI défini dans la norme EN 726-3.

icManufacturingReferences indique l'identificateur du fabricant de CI et renvoie aux éléments de fabrication définis dans la norme EN 726-3.

2.10. **CardConsecutiveIndex**

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

CardConsecutiveIndex ::= Chaîne IA5[LONGUEUR(1)]

Assignation de valeur: (cf. Chapitre VII de la présente annexe)

Ordre d'incrémentation: '0, …, 9, A, … , Z, a, … , z'

2.11. **CardControlActivityDataRecord**

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant au dernier contrôle auquel le conducteur considéré a été soumis (exigences 210 et 225).

```
CardControlActivityDataRecord ::= SÉQUENCE {
    controlType Type de contrôle
    controlTime Temps réel
    controlCardNumber Numéro intégral de la carte
```

▼M1

controlVehicleRegistration Identification et immatriculation du véhicule

controlDownloadPeriodBegin Temps réel

controlDownloadPeriodEnd Temps réel

}

controlType indique le type de contrôle exécuté.

controlTime indique la date et l'heure du contrôle exécuté.

controlCardNumber indique le numéro intégral de la carte du contrôleur qui a procédé au contrôle.

controlVehicleRegistration indique le NIV ainsi que l'État membre d'immatriculation du véhicule soumis au contrôle considéré.

controlDownloadPeriodBegin et **controlDownloadPeriodEnd** indiquent la période téléchargée, en cas de téléchargement.

2.12. **CardCurrentUse**

Informations relatives à l'usage effectif de la carte (exigence 212).

CardCurrentUse ::= SÉQUENCE {

sessionOpenTime Temps réel

sessionOpenVehicle Identification et immatriculation du véhicule

}

sessionOpenTime indique l'heure d'insertion de la carte utilisée dans le cadre de l'activité en cours. Cet élément est mis à zéro lors du retrait de la carte.

sessionOpenVehicle correspond à l'identification du véhicule après insertion de la carte. Cet élément est mis à zéro lors du retrait de la carte.

2.13. **CardDriverActivity**

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant aux activités du conducteur (exigences 199 et 219).

CardDriverActivity ::= SÉQUENCE {

activityPointerOldestDayRecord ENTIER (0..CardActivityLengthRange-1),

activityPointerNewestRecord ENTIER (0..CardActivityLengthRange-1),

activityDailyRecords CHAÎNE D'OCTETS [LONGUEUR (CardActivityLengthRange)]

}

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

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

activityDailyRecords indique l'espace affecté à l'enregistrement de données relatives aux activités du conducteur (structure de données: CardActivityDailyRecord) pour chaque jour civil au cours duquel la carte à été utilisée.

Assignation de valeur: cette chaîne d'octets est périodiquement remplie de relevés du type CardActivityDailyRecord. Lors de la première utilisation, le début de l'enregistrement du premier relevé coïncide avec le premier octet de la chaîne. Les relevés suivants sont enregistrés à la fin du précédent. Lorsque la chaîne est saturée, l'enregistrement se poursuit en reprenant au premier octet de la chaîne, sans tenir compte d'aucune interruption susceptible d'affecter un élément d'information quelconque. Avant d'introduire de nouvelles données d'activité dans la chaîne (en étendant l'activityDailyRecord actuel ou en insérant un nouvel activityDailyRecord), lesquelles se substituent aux données d'activité les plus anciennes, il convient d'actualiser l'activityPointerOldestDayRecord pour rendre compte du nouvel emplacement en mémoire qu'occupe désormais le relevé quotidien complet le plus ancien et de mettre à zéro l'activityPreviousRecordLength de ce (nouveau) relevé quotidien complet le plus ancien.

▼M1

2.14. **CardDrivingLicenceInformation**

Informations enregistrées sur une carte de conducteur et se rapportant au permis de conduire du détenteur de la carte (exigence 196).

CardDrivingLicenceInformation ::= SÉQUENCE {

drivingLicenceIssuingAuthority Nom

drivingLicenceIssuingNation Code numérique national

drivingLicenceNumber Chaîne IA5 [LONGUEUR(16)]

}

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

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

drivingLicenceNumber indique le numéro du permis de conduire.

2.15. **CardEventData**

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant aux événements associés au détenteur de la carte (exigences 204 et 223).

CardEventData ::= SÉQUENCE LONGUEUR (6) DES {

cardEventRecords LONGUEUR DÉFINIE(NoOfEventsPerType) DU CardEventRecord

}

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

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

2.16. **CardEventRecord**

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant à un événement associé au détenteur de la carte (exigences 205 et 223).

CardEventRecord ::= SÉQUENCE {

eventType Type d'événement/anomalie

eventBeginTime Temps réel

eventEndTime Temps réel

eventVehicleRegistration Identification et immatriculation du véhicule

}

eventType indique le type d'événement.

eventBeginTime indique la date et l'heure de début d'un événement.

eventEndTime indique la date et l'heure de fin d'un événement.

eventVehicleRegistration indique le NIV ainsi que l'État membre d'immatriculation du véhicule dans lequel l'événement considéré s'est produit.

2.17. **CardFaultData**

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant aux anomalies associées au détenteur de la carte (exigences 207 et 223).

CardFaultData ::= SÉQUENCE LONGUEUR(2) DES {

cardFaultRecords LONGUEUR DÉFINIE(NoOfFaultsPerType) DU CardFaultRecord

}

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

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

▼M1

2.18. **CardFaultRecord**

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant à une anomalie associée au détenteur de la carte (exigences 208 et 223).

```
CardFaultRecord ::= SÉQUENCE {
    faultType Type d'événement/anomalie
    faultBeginTime Temps réel
    faultEndTime Temps réel
    faultVehicleRegistration Identification et immatriculation du véhicule
}
```

faultType indique le type d'anomalie.

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

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

faultVehicleRegistration indique le NIV ainsi que l'État membre d'immatriculation du véhicule dans lequel l'anomalie considérée s'est produite.

2.19. **CardIccIdentification**

Informations enregistrées sur une carte et se rapportant à l'identification de cette carte à circuit intégré (CI) (exigence 192).

```
CardIccIdentification ::= SÉQUENCE {
    clockStopCHAÎNE D'OCTETS [LONGUEUR(1)],
    cardExtendedSerialNumber Numéro de série étendu
    cardApprovalNumber Numéro d'homologation de la carte
    cardPersonaliserID CHAÎNE D'OCTETS [LONGUEUR(1)],
    embedderIcAssemblerId CHAÎNE D'OCTETS [LONGUEUR(5)],
    icIdentifier CHAÎNE D'OCTETS [LONGUEUR(2)]
}
```

clockStop indique le mode Clockstop défini dans la norme EN 726-3.

cardExtendedSerialNumber indique le numéro de série de la carte à circuit intégré ainsi que son numéro de référence industrielle définis dans la norme EN 726-3 et tel qu'ils sont spécifiés par le type de données ExtendedSerialNumber.

cardApprovalNumber indique le numéro d'homologation de la carte.

cardPersonaliserID indique l'ID individuelle de la carte définie dans la norme EN 726-3.

embedderIcAssemblerId indique l'identificateur de l'intégrateur/assembleur de CI défini dans la norme EN 726-3.

icIdentifier indique l'identificateur du CI monté sur la carte et de son fabricant défini dans la norme EN 726-3.

2.20. **CardIdentification**

Informations enregistrées sur une carte et se rapportant à l'identification de celle-ci (exigences 194, 215, 231 et 235).

```
CardIdentification ::= SÉQUENCE
    cardIssuingMemberState Code numérique national
    cardNumber Numéro de la carte
    cardIssuingAuthorityName Nom
    cardIssueDate Temps réel
    cardValidityBegin Temps réel
    cardExpiryDate Temps réel
}
```

cardIssuingMemberState indique le code de l'État membre où est délivrée la carte.

cardNumber indique le numéro de carte de la carte considérée.

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

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

▼M1

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

cardExpiryDate indique la date d'expiration de la carte.

2.21. **CardNumber**

Un numéro de carte conforme à la définition g).

```
CardNumber ::= SÉLECTION {
    SÉQUENCE {
        driverIdentification Chaîne IA5 [LONGUEUR(14)],
        cardReplacementIndex Indice de remplacement de carte
        cardRenewalIndex Indice de renouvellement de carte
    }
    SÉQUENCE {
        ownerIdentification Chaîne IA5 [LONGUEUR(13)],
        cardConsecutiveIndex Indice séquentiel de la carte
        cardReplacementIndex Indice de remplacement de carte
        cardRenewalIndex Indice de renouvellement de carte
    }
}
```

driverIdentification indique l'identification individuelle d'un conducteur recensé dans un État membre.

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

cardConsecutiveIndex indique l'indice séquentiel de la carte considérée.

cardReplacementIndex indique l'indice de remplacement de la carte.

cardRenewalIndex indique l'indice de renouvellement de la carte.

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

2.22. **CardPlaceDailyWorkPeriod**

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant aux lieux de début et/ou de fin des périodes de travail journalières (exigences 202 et 221).

```
CardPlaceDailyWorkPeriod ::= SÉQUENCE {
    placePointerNewestRecord ENTIER(0..NoOfCardPlaceRecords-1),
    placeRecords LONGUEUR DÉFINIE (NoOfCardPlaceRecords) DU PlaceRecord
}
```

placePointerNewestRecord indique l'indice du dernier relevé de site actualisé par le système.

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

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

2.23. **CardPrivateKey**

Clé privée d'une carte.

```
CardPrivateKey ::= Exposant privé de clé RSA
```

2.24. **CardPublicKey**

Clé publique d'une carte.

```
CardPublicKey ::= Clé publique
```

2.25. **CardRenewalIndex**

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

```
CardRenewalIndex ::= Chaîne IA5[LONGUEUR(1)]
```

▼M1

Assignation de valeur: (cf. Chapitre VII de la présente annexe).

′0′ Première édition.

Ordre croissant: ′0, …, 9, A, …, Z′

2.26. **CardReplacementIndex**

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

CardReplacementIndex ::= Chaîne IA5[LONGUEUR(1)]

Assignation de valeur: (cf. Chapitre VII de la présente annexe).

′0′ Carte originale.

Ordre croissant: ′0, …, 9, A, …, Z′

2.27. **CardSlotNumber**

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

CardSlotNumber ::= ENTIER {

driverSlot (0),

co-driverSlot (1)

}

Assignation de valeur: absence d'informations complémentaires.

2.28. **CardSlotsStatus**

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

CardSlotsStatus ::= CHAÎNE D'OCTETS [LONGUEUR(1)]

Assignation de valeur — Octet aligné: ′ccccdddd′B:

′cccc′B Identification du type de carte insérée dans le lecteur réservé au convoyeur

′dddd′B Identification du type de carte insérée dans le lecteur réservé au conducteur

à l'aide des codes d'identification suivants:

′0000′B aucune carte n'est insérée dans un lecteur

′0001′B une carte de conducteur est insérée dans un lecteur

′0010′B une carte d'atelier est insérée dans un lecteur

′0011′B une carte de contrôleur est insérée dans un lecteur

′0100′B une carte d'entreprise est insérée dans un lecteur.

2.29. **CardStructureVersion**

Code indiquant la version de la structure mise en œuvre au sein d'une carte tachygraphique.

CardStructureVersion ::= CHAÎNE D'OCTETS [LONGUEUR(2)]

Assignation de valeur: ′aabb′H:

′aa′H Index des modifications apportées à la structure

′bb′H Index des modifications concernant l'utilisation des éléments d'information définis pour la structure donnée par l'octet de poids fort.

2.30. **CardVehicleRecord**

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant à une période d'utilisation d'un véhicule donné pendant un jour civil déterminé (exigences 197 et 217).

CardVehicleRecord ::= SÉQUENCE {

vehicleOdometerBegin Compteur kilométrique

vehicleOdometerEnd Compteur kilométrique

vehicleFirstUse Temps réel

vehicleLastUse Temps réel

vehicleRegistration Identification et immatriculation du véhicule

▼M1

vuDataBlockCounter Compteur de blocs de données de l'UEV

}

vehicleOdometerBegin indique la valeur affichée par le compteur kilométrique d'un véhicule donné au début de la période d'utilisation considérée.

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

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

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

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

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

2.31. **CardVehiclesUsed**

Informations enregistrées sur une carte de conducteur ou d'atelier et se rapportant aux véhicules utilisés par le détenteur de la carte (exigences 197 et 217).

CardVehiclesUsed := SÉQUENCE {

vehiclePointerNewestRecord ENTIER(0..NoOfCardVehicleRecords-1),

cardVehicleRecords LONGUEUR DÉFINIE(NoOfCardVehicleRecords) DU CardVehicleRecord

}

vehiclePointerNewestRecord indique l'indice du dernier relevé de véhicule actualisé par le système.

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

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

2.32. **Certificate**

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

Certificate ::= CHAÎNE D'OCTETS [LONGUEUR(194)]

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

2.33. **CertificateContent**

Le contenu (accessible) du certificat d'une clé publique aux termes de l'appendice 11 «Mécanismes de sécurité communs».

CertificateContent ::= SÉQUENCE {

certificateProfileIdentifier ENTIER(0..255),

certificationAuthorityReference Identificateur de clé

certificateHolderAuthorisation Autorisation accordée au titulaire du certificat

certificateEndOfValidity Temps réel

certificateHolderReference Identificateur de clé

publicKey Clé publique

}

certificateProfileIdentifier indique la version du certificat correspondant.

Assignation de valeur: ′01h′ pour cette version.

certificationAuthorityReference identifie l'organisme de certification qui a délivré le certificat considéré. Ces données font également référence à la clé publique de cet organisme de certification.

certificateHolderAuthorisation identifie les droits du titulaire du certificat.

certificateEndOfValidity indique la date d'expiration administrative du certificat.

▼M1

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

publicKey indique la clé publique certifiée par ce certificat.

2.34. **CertificateHolderAuthorisation**

Identification des droits d'un titulaire de certificat.

```
CertificateHolderAuthorisation ::= SÉQUENCE {
    tachographApplicationID CHAÎNE D'OCTETS [LONGUEUR(6)]
    equipmentType Type d'équipement
}
```

tachographApplicationID indique l'identificateur de l'application tachygraphique.

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

equipmentType identifie le type d'équipement visé par le certificat.

Assignation de valeur: en conformité avec le type de données EquipmentType. 0 si le certificat émane de l'un des États membres.

2.35. **CertificateRequestID**

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

```
CertificateRequestID ::= SÉQUENCE {
    requestSerialNumber ENTIER(0..2^32-1)
    requestMonthYear Chaîne DCB[LONGUEUR(2)]
    crIdentifier CHAÎNE D'OCTETS [LONGUEUR(1)]
    manufacturerCode Code du fabricant
}
```

requestSerialNumber indique le numéro de série de la demande de certificat, propre au fabricant, ainsi que le mois ci-après.

requestMonthYear identifie le mois et l'année de la demande de certificat.

Assignation de valeur: Codage DCB du mois (deux chiffres) et de l'année (les deux derniers chiffres).

crIdentifier est un identificateur permettant de faire la distinction entre une demande de certificat et un numéro de série étendu.

Assignation de valeur: 'FFh'.

Code du fabricant correspond au code numérique du fabricant qui a émis la demande de certificat.

2.36. **CertificationAuthorityKID**

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

```
CertificationAuthorityKID ::= SÉQUENCE {
    nationNumeric Code numérique national
    nationAlpha Code alphanumérique national
    keySerialNumber ENTIER(0..255)
    additionalInfo CHAÎNE D'OCTETS [LONGUEUR(2)]
    caIdentifier CHAÎNE D'OCTETS [LONGUEUR(1)]
}
```

nationNumeric indique le code numérique national de l'organisme de certification.

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

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

▼M1

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

caIdentifier est un identificateur permettant de faire la distinction entre l'identificateur d'une clé associée à un organisme de certification et d'autres identificateurs de clé.

ssignation de valeur: ′01h′.

2.37. **CompanyActivityData**

Informations enregistrées sur une carte d'entreprise et se rapportant aux activités menées avec cette carte (exigence 237).

```
CompanyActivityData ::= SÉQUENCE {
    companyPointerNewestRecord ENTIER(0..NoOfCompanyActivityRecords-1),
    companyActivityRecords LONGUEUR DÉFINIE(NoOfCompanyActivityRecords) DES
        companyActivityRecord SÉQUENCE {
            companyActivityType Type d'activité de l'entreprise
            companyActivityTime Temps réel
            cardNumberInformation Numéro intégral de la carte
            vehicleRegistrationInformation Identification et immatriculation du véhicule
            downloadPeriodBegin Temps réel
            downloadPeriodEnd Temps réel
        }
}
```

companyPointerNewestRecord indique l'indice du dernier relevé d'activité de l'entreprise actualisé par le système.

Assignation de valeur: nombre correspondant au numérateur du relevé d'activité de l'entreprise, commençant par une série de ′0′ pour la première occurrence d'un relevé d'activité de l'entreprise dans la structure considérée.

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

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

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

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

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

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

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

2.38. **CompanyActivityType**

Code indiquant une activité menée par une entreprise recourant à l'utilisation de sa carte d'entreprise.

```
CompanyActivityType ::= INTEGER {
    Téléchargement de la carte (1),
    Téléchargement de l'UEV (2),
    Verrouillage de l'UEV (3),
    Déverrouillage de l'UEV (4)
}
```

2.39. **CompanyCardApplicationIdentification**

Informations enregistrées sur une carte d'entreprise et se rapportant à l'identification de l'application de la carte (exigence 190).

```
CompanyCardApplicationIdentification ::= SÉQUENCE {
    typeOfTachographCardId Type d'équipement
```

▼M1

```
    cardStructureVersion Version de la structure de la carte
    noOfCompanyActivityRecords Nombre des relevés d'activité
    de l'entreprise
}
```

typeOfTachographCardId spécifie le type de la carte mise en application.

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

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

2.40. **CompanyCardHolderIdentification**

Informations enregistrées sur une carte d'entreprise et se rapportant à l'identification du détenteur de la carte (exigence 236).

```
CompanyCardHolderIdentification ::= SÉQUENCE {
    companyName Nom
    companyAddress Adresse,
    cardHolderPreferredLanguage Langue de travail
}
```

companyName indique le nom de l'entreprise du titulaire.

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

cardHolderPreferredLanguage indique la langue de travail préférentielle du titulaire.

2.41. **ControlCardApplicationIdentification**

Informations enregistrées sur une carte de contrôleur et se rapportant à l'identification de l'application de la carte (exigence 190).

```
ControlCardApplicationIdentification ::= SÉQUENCE {
    typeOfTachographCardId Type d'équipement
    cardStructureVersion Version de la structure de la carte
    noOfControlActivityRecords Nombre des relevés d'activité de
    contrôle
}
```

typeOfTachographCardId spécifie le type de la carte mise en application.

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

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

2.42. **ControlCardControlActivityData**

Informations enregistrées sur une carte de contrôleur et se rapportant aux activités de contrôle exécutées à l'aide de cette carte (exigence 233).

```
ControlCardControlActivityData ::= SÉQUENCE {
    controlPointerNewestRecord ENTIER (0..Nombre de relevés
    d'activité de contrôle-1),
    controlActivityRecords LONGUEUR DÉFINIE (NoOfControl
    ActivityRecords) DES
        controlActivityRecord SÉQUENCE {
            controlType Type de contrôle
            controlTime Temps réel
            controlledCardNumber Numéro intégral de la carte
            controlledVehicleRegistration Identification et immatri-
            culation du véhicule
            controlDownloadPeriodBegin Temps réel
            controlDownloadPeriodEnd Temps réel
        }
}
```

controlPointerNewestRecord indique l'indice du dernier relevé d'activité de contrôle actualisé par le système.

▼M1

Assignation de valeur: nombre correspondant au numérateur du relevé d'activité de contrôle, commençant par une série de '0' pour la première occurrence d'un relevé d'activité de contrôle dans la structure considérée.

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

controlActivityRecord indique la séquence d'informations associée à un contrôle.

controlType indique le type du contrôle.

controlTime indique la date et l'heure du contrôle.

controlledCardNumber indique le numéro de la carte ainsi que l'État membre qui délivre la carte contrôlée.

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

controlDownloadPeriodBegin et **controlDownloadPeriodEnd** indiquent, le cas échéant, la période téléchargée.

2.43. **ControlCardHolderIdentification**

Informations enregistrées sur une carte de contrôleur et se rapportant à l'identification du détenteur de la carte (exigence 232).

ControlCardHolderIdentification ::= SÉQUENCE {

controlBodyName Nom

controlBodyAddress Adresse

cardHolderName Nom du titulaire

cardHolderPreferredLanguage Langue de travail

}

controlBodyName indique le nom de l'organisme de contrôle dont dépend le détenteur de la carte.

controlBodyAddress indique l'adresse de l'organisme de contrôle dont dépend le détenteur de la carte.

cardHolderName indique les nom et prénom(s) du détenteur de la carte de contrôleur.

cardHolderPreferredLanguage indique la langue de travail préférentielle du détenteur de la carte.

2.44. **ControlType**

Code indiquant les activités menées pendant un contrôle. Ce type de données est lié aux exigences 102, 210 et 225.

ControlType ::= CHAÎNE D'OCTETS [LONGUEUR(1)]

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

'c'B téléchargement de la carte:

'0'B: pas de téléchargement de la carte pendant cette activité de contrôle

'1'B: téléchargement de la carte pendant cette activité de contrôle

'v'B téléchargement de l'UEV:

'0'B: pas de téléchargement de l'UEV pendant cette activité de contrôle

'1'B: téléchargement de l'UEV pendant cette activité de contrôle

'p'B impression:

'0'B: pas d'impression pendant cette activité de contrôle

'1'B: exécution d'un tirage pendant cette activité de contrôle

'd'B affichage:

'0'B: pas d'affichage de données pendant cette activité de contrôle

'1'B: affichage de données pendant cette activité de contrôle

'xxxx'B Inutilisé.

2.45. **CurrentDateTime**

Date et heure de l'appareil de contrôle.

CurrentDateTime ::= Temps réel

▼M1

Assignation de valeur: absence d'informations complémentaires.

2.46. **DailyPresenceCounter**

Compteur enregistré sur une carte de conducteur ou d'atelier, incrémenté d'une unité par jour civil d'insertion de cette carte dans le lecteur d'une UEV. Ce type de données est lié aux exigences 199 et 219.

DailyPresenceCounter ::= BCDString[LONGUEUR(2)]

Assignation de valeur: numérotation consécutive dont la valeur maximale est égale à 9 999, la numérotation recommençant par le numéro 0. Lors de la première entrée en vigueur d'une carte, le compteur correspondant est à zéro.

2.47. **Datef**

Date exprimée dans un format numérique immédiatement imprimable.

Datef ::= SÉQUENCE {

année BCDString[LONGUEUR(2)]

mois BCDString[LONGUEUR(1)]

jour BCDString[LONGUEUR(1)]

}

Assignation de valeur:

yyyy Année

mm Mois

dd Jour

'00000000'H dénote explicitement l'absence de date.

2.48. **Distance**

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

Distance ::= ENTIER(0..2^{16}-1)

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

2.49. **DriverCardApplicationIdentification**

Informations enregistrées sur une carte de conducteur et se rapportant à l'identification de l'application de la carte (exigence 190).

DriverCardApplicationIdentification ::= SÉQUENCE {

typeOfTachographCardId Type d'équipement

cardStructureVersion Version de la structure de la carte

noOfEventsPerType Nombre d'événements par type

noOfFaultsPerType Nombre d'anomalies par type

activityStructureLength Nombre d'octets affectés aux relevés d'activité

noOfCardVehicleRecords Nombre des relevés de véhicule enregistrés sur la carte

noOfCardPlaceRecords Nombre des relevés de site enregistrés sur la carte

}

typeOfTachographCardId spécifie le type de la carte mise en application.

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

noOfEventsPerType indique le nombre d'événements que la carte est susceptible de sauvegarder par type d'événement.

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

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

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

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

▼**M1**

2.50. **DriverCardHolderIdentification**

Informations enregistrées sur une carte de conducteur et se rapportant à l'identification du détenteur de la carte (exigence 195).

DriverCardHolderIdentification ::= SÉQUENCE {

cardHolderName Nom du titulaire

cardHolderBirthDate Date de naissance du titulaire

cardHolderPreferredLanguage Langue de travail

}

cardHolderName indique les nom et prénom(s) du détenteur de la carte de conducteur.

cardHolderBirthDate indique la date de naissance du détenteur de la carte de conducteur.

cardHolderPreferredLanguage indique la langue de travail préférentielle du détenteur de la carte.

2.51. **EntryTypeDailyWorkPeriod**

Code permettant de faire la distinction entre le lieu de début et de fin d'une période de travail journalière et les conditions de saisie de ces données.

EntryTypeDailyWorkPeriod ::= ENTIER

Début, temps relatif = heure d'insertion de la carte ou de saisie (0),

Fin, temps relatif = heure de retrait de la carte ou de saisie (1),

Début, entrée manuelle du temps relatif (heure de début) (2),

Fin, entrée manuelle du temps relatif (fin de la période de travail) (3),

Début, temps relatif adopté par l'UEV (4),

Fin, temps relatif adopté par l'UEV (5)

}

Assignation de valeur: conformément à la norme ISO/CEI 8824-1.

2.52. **EquipmentType**

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

EquipmentType ::= ENTIER(0..255)

- - Réservé (0),

- - Carte de conducteur (1),

- - Carte d'atelier (2),

- - Carte de contrôleur (3),

- - Carte d'entreprise (4),

- - Carte de fabrication (5),

- - Unité embarquée sur véhicule (6),

- - Capteur de mouvement (7),

- - RFU (8..255)

Assignation de valeur: conformément à la norme ISO/CEI 8824-1.

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

2.53. **EuropeanPublicKey**

Clé publique européenne.

EuropeanPublicKey ::= Clé publique

2.54. **EventFaultType**

Code caractérisant un événement ou une anomalie.

EventFaultType ::= CHAÎNE D'OCTETS [LONGUEUR(1)]

Assignation de valeur:

′0x′H	Événements à caractère général
′00′H	Absence d'informations complémentaires

▼**M1**

′01′H	Insertion d'une carte non valable
′02′H	Conflit de carte
′03′H	Chevauchement temporel
′04′H	Conduite sans carte appropriée
′05′H	Insertion de carte en cours de conduite
′06′H	Dernière session incorrectement clôturée
′07′H	Excès de vitesse
′08′H	Interruption de l'alimentation électrique
′09′H	Erreur sur les données de mouvement
′0A′H .. ′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 .. ′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 .. ′2F′H	RFU
′3x′H	Anomalies affectant l'appareil de contrôle
′30′H	Absence d'informations complémentaires
′31′H	Anomalie interne affectant l'UEV
′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 .. ′3F′H	RFU
′4x′H	Anomalies affectant une carte
′40′H	Absence d'informations complémentaires
′41′H .. ′4F′H	RFU
′50′H .. ′7F′H	RFU
′80′H .. ′FF′H	Propre au fabricant.

2.55. **EventFaultRecordPurpose**

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

EventFaultRecordPurpose ::= CHAÎNE D'OCTETS [LONGUEUR(1)]

Assignation de valeur:

′00′H	l'un des 10 (derniers) événements ou anomalies les plus récents
′01′H	l'événement le plus long survenu au cours de chacun des 10 derniers jours d'occurrence
′02′H	l'un des 5 événements les plus longs enregistrés au cours des 365 derniers jours

▼M1

′03′H	le dernier événement survenu au cours de chacun des 10 derniers jours d'occurrence
′04′H	l'événement le plus sérieux enregistré au cours de chacun des 10 derniers jours d'occurrence
′05′H	l'un des 5 événements les plus sérieux enregistrés au cours des 365 derniers jours
′06′H	le premier événement ou anomalie survenu après le dernier étalonnage
′07′H	un événement ou une anomalie en cours
′08′H .. ′7F′H	RUU
′80′H .. ′FF′H	spécifique au fabricant

2.56. **ExtendedSerialNumber**

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

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

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

monthYear identifie le mois et l'année de fabrication (ou de l'attribution d'un numéro de série).

Assignation de valeur codage BCD du mois (deux chiffres) et de l'année (les deux derniers chiffres).

type est un identificateur du type d'équipement utilisé.

Assignation de valeur: propre au fabricant, la valeur ′FFh′ étant réservée.

Code du fabricant: correspond au code numérique du fabricant de l'équipement considéré.

2.57. **FullCardNumber**

Code permettant d'identifier avec certitude une carte tachygraphique.

```
FullCardNumber ::= SÉQUENCE {
    cardType Type d'équipement
    cardIssuingMemberState Code numérique national
    cardNumber Numéro de la carte
}
```

cardType indique le type de la carte tachygraphique.

cardIssuingMemberState indique le code de l'État membre qui a délivré la carte considérée.

cardNumber indique le numéro de la carte.

2.58. **HighResOdometer**

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

```
HighResOdometer ::= ENTIER(0..2^32-1)
```

Assignation de valeur: binaire sans signe. Valeur exprimée en 1/200 de km et se situant dans une plage d'exploitation comprise entre 0 et 21 055 406 km.

2.59. **HighResTripDistance**

Distance parcourue pendant tout ou partie d'un trajet.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Assignation de valeur: binaire sans signe. Valeur exprimée en 1/200 de km et se situant dans une plage d'exploitation comprise entre 0 et 21 055 406 km.

▼M1

2.60. **HolderName**

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

HolderName ::= SÉQUENCE {

holderSurname Nom

holderFirstNames Nom

}

holderSurname indique le nom du titulaire. Ce nom ne s'accompagne d'aucun titre.

Assignation de valeur: si la carte considérée n'est pas individuelle, holderSurname contient les même données que companyName, workshopName ou controlBodyName.

holderFirstNames indique le(s) prénom(s) et initiale(s) du titulaire.

2.61. **K-ConstantOfRecordingEquipment**

Constante de l'appareil de contrôle [définition m)].

K-ConstantOfRecordingEquipment ::= ENTIER(0..2^{16}-1)

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

2.62. **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 ::= SÉLECTION {

extendedSerialNumber Numéro de série étendu

certificateRequestID ID de demande de certificat

certificationAuthorityKID ID de la clé de l'organisme de certification

}

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

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

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

2.63. **L-TyreCircumference**

Circonférence effective des pneumatiques [définition u)].

L-TyreCircumference ::= ENTIER(0..2^{16}-1)

Assignation de valeur: binaire sans signe. Valeur exprimée en 1/8 de mm et se situant dans une plage d'exploitation comprise entre 0 et 8 031 mm.

2.64. **Language**

Code identifiant une langue de travail.

Language ::= Chaîne IA5 [LONGUEUR(2)]

Assignation de valeur: code composé de deux lettres minuscules, en conformité avec la norme ISO 639.

2.65. **LastCardDownload**

Date et heure, enregistrées sur une carte de conducteur, du dernier téléchargement d'une carte (à d'autres fins que le contrôle). Cette date peut être mise à jour par une UEV ou tout lecteur de carte.

LastCardDownload ::= TimeReal

Assignation de valeur: absence d'informations complémentaires.

2.66. **ManualInputFlag**

Code permettant d'identifier si un détenteur de carte a procédé ou non à la saisie manuelle d'activités du conducteur lors de l'insertion de cette carte (exigence 081).

ManualInputFlag ::= ENTIER {

▼**M1**

noEntry (0)

manualEntries (1)

}

Assignation de valeur: absence d'informations complémentaires.

2.67. **ManufacturerCode**

Code identifiant un fabricant.

ManufacturerCode ::= ENTIER (0..255)

Assignation de valeur:

′00′H	Aucune information disponible
′01′H	Valeur réservée
′02′H .. ′0F′H	Réservé à une utilisation ultérieure
′10′H	ACTIA
′11′H .. ′17′H	Réservé aux fabricants dont le nom commence par ′A′
′18′H .. ′1F′H	Réservé aux fabricants dont le nom commence par ′B′
′20′H .. ′27′H	Réservé aux fabricants dont le nom commence par ′C′
′28′H .. ′2F′H	Réservé aux fabricants dont le nom commence par ′D′
′30′H .. ′37′H	Réservé aux fabricants dont le nom commence par ′E′
′38′H .. ′3F′H	Réservé aux fabricants dont le nom commence par ′F′
′40′H	Giesecke & Devrient GmbH
′41′H	GEM plus
′42′H .. ′47′H	Réservé aux fabricants dont le nom commence par ′G′
′48′H .. ′4F′H	Réservé aux fabricants dont le nom commence par ′H′
′50′H .. ′57′H	Réservé aux fabricants dont le nom commence par ′I′
′58′H .. ′5F′H	Réservé aux fabricants dont le nom commence par ′J′
′60′H .. ′67′H	Réservé aux fabricants dont le nom commence par ′K′
′68′H .. ′6F′H	Réservé aux fabricants dont le nom commence par ′L′
′70′H .. ′77′H	Réservé aux fabricants dont le nom commence par ′M′
′78′H .. ′7F′H	Réservé aux fabricants dont le nom commence par ′N′
′80′H	OSCARD
′81′H .. ′87′H	Réservé aux fabricants dont le nom commence par ′O′
′88′H .. ′8F′H	Réservé aux fabricants dont le nom commence par ′P′
′90′H .. ′97′H	Réservé aux fabricants dont le nom commence par ′Q′
′98′H .. ′9F′H	Réservé aux fabricants dont le nom commence par ′R′
′A0′H	SETEC
′A1′H	SIEMENS VDO
′A2′H	STONERIDGE
′A3′H .. ′A7′H	Réservé aux fabricants dont le nom commence par ′S′
′AA′H	TACHOCONTROL
′AB′H .. ′AF′H	Réservé aux fabricants dont le nom commence par ′T′
′B0′H .. ′B7′H	Réservé aux fabricants dont le nom commence par ′U′
′B8′H .. ′BF′H	Réservé aux fabricants dont le nom commence par ′V′
′C0′H .. ′C7′H	Réservé aux fabricants dont le nom commence par ′W′
′C8′H .. ′CF′H	Réservé aux fabricants dont le nom commence par ′X′
′D0′H .. ′D7′H	Réservé aux fabricants dont le nom commence par ′Y′
′D8′H .. ′DF′H	Réservé aux fabricants dont le nom commence par ′Z′

2.68. **MemberStateCertificate**

Le certificat de la clé publique d'un État membre délivré par l'organisme de certification européen.

MemberStateCertificate ::= Certificat

2.69. **MemberStatePublicKey**

Clé publique d'un État membre.

▼**M1**

MemberStatePublicKey ::= Clé publique

2.70. **Name**

Nom.

```
Name ::= SÉQUENCE {
    codePage ENTIER (0..255),
    name CHAÎNE D'OCTETS [LONGUEUR(35)]
}
```

codePage spécifie la partie de la norme ISO/CEI 8859 employée pour coder le nom.

name indique un nom dont le codage est conforme à la page de codes appropriée de la norme ISO/CEI 8859.

2.71. **NationAlpha**

Renvoi alphabétique à un pays, en conformité avec le codage classique des nations qui caractérise les étiquettes autocollantes appliquées sur les pare-chocs et/ou les documents harmonisés émis par les compagnies d'assurances (carte verte).

NationAlpha ::= Chaîne IA5 [LONGUEUR(3)]

Assignation de valeur:

′ ′	Aucune information disponible
′A′	Autriche
′AL′	Albanie
′AND′	Andorre
′ARM′	Arménie
′AZ′	Azerbaïdjan
′B′	Belgique
′BG′	Bulgarie
′BIH′	Bosnie-et-Herzégovine
′BY′	Belarus
′CH′	Confédération suisse
′CY′	Chypre
′CZ′	République tchèque
′D′	Allemagne
′DK′	Danemark
′E′	Espagne
′EST′	Estonie
′F′	France
′FIN′	Finlande
′FL′	Liechtenstein
′FR′	Îles Féroé
′UK′	Royaume-Uni, Alderney, Guernesey, Jersey, Île de Man, Gibraltar
′GE′	Géorgie
′GR′	Grèce
′H′	Hongrie
′HR′	Croatie
′I′	Italie
′IRL′	Irlande
′IS′	Islande
′KZ′	Kazakhstan
′L′	Luxembourg
′LT′	Lituanie
′LV′	Lettonie
′M′	Malte
′MC′	Monaco

▼**M1**

′MD′	République de Moldova
′MK′	Macédoine
′N′	Norvège
′NL′	Pays-Bas
′P′	Portugal
′PL′	Pologne
′RO′	Roumanie
′RSM′	Saint-Marin
′RUS′	Fédération de Russie
′S′	Suède
′SK′	Slovaquie
′SLO′	Slovénie
′TM′	Turkménistan
′TR′	Turquie
′UA′	Ukraine
′V′	Cité du Vatican
′YU′	Yougoslavie
′UNK′	Inconnu
′EC′	Communauté européenne
′EUR′	Reste de l'Europe
′WLD′	Reste du monde.

2.72. **NationNumeric**

Code numérique désignant un pays.

NationNumeric ::= ENTIER(0..255)

Assignation de valeur:

- - Aucune information disponible (00)H,
- - Autriche (01)H,
- - Albanie (02)H,
- - Andorre (03)H,
- - Arménie (04)H,
- - Azerbaïdjan (05)H,
- - Belgique (06)H,
- - Bulgarie (07)H,
- - Bosnie-et-Herzégovine (08)H,
- - Bélarus (09)H,
- - Confédération suisse (0A)H,
- - Chypre (0B)H,
- - République tchèque (0C)H,
- - Allemagne (0D)H,
- - Danemark (0E)H,
- - Espagne (0F)H,
- - Estonie (10)H,
- - France (11)H,
- - Finlande (12)H,
- - Liechtenstein (13)H,
- - Îles Féroé (14)H,
- - Royaume-Uni (15)H,
- - Géorgie (16)H,
- - Grèce (17)H,
- - Hongrie (18)H,
- - Croatie (19)H,
- - Italie (1A)H,
- - Irlande (1B)H,

▼**M1**

- - Islande (1C)H,
- - Kazakhstan (1D)H,
- - Luxembourg (1E)H,
- - Lituanie (1F)H,
- - Lettonie (20)H,
- - Malte (21)H,
- - Monaco (22)H,
- - République de Moldova (23)H,
- - Macédoine (24)H,
- - Norvège (25)H,
- - Pays-Bas (26)H,
- - Portugal (27)H,
- - Pologne (28)H,
- - Roumanie (29)H,
- - Saint-Marin (2A)H,
- - Fédération de Russie (2B)H,
- - Suède (2C)H,
- - Slovaquie (2D)H,
- - Slovénie (2E)H,
- - Turkménistan (2F)H,
- - Turquie (30)H,
- - Ukraine (31)H,
- - Cité du Vatican (32)H,
- - Yougoslavie (33)H,
- - RFU (34..FC)H,
- - Communauté européenne (FD)H,
- - Reste de l'Europe (FE)H,
- - Reste du monde (FF)H

2.73. **NoOfCalibrationRecords**

Nombre des relevés d'étalonnage qu'une carte d'atelier est susceptible de mémoriser.

NoOfCalibrationRecords ::= ENTIER(0..255)

Assignation de valeur: cf. paragraphe 3.

2.74. **NoOfCalibrationsSinceDownload**

Compteur indiquant le nombre d'étalonnages exécutés avec une carte d'atelier depuis son dernier téléchargement (exigence 230).

NoOfCalibrationsSinceDownload ::= ENTIER(0..2^{16}-1),

Assignation de valeur: absence d'informations complémentaires.

2.75. **NoOfCardPlaceRecords**

Nombre des relevés de site qu'une carte de conducteur ou d'atelier est susceptible de mémoriser.

NoOfCardPlaceRecords ::= ENTIER(0..255)

Assignation de valeur: cf. paragraphe 3.

2.76. **NoOfCardVehicleRecords**

Nombre des relevés de véhicule qu'une carte de conducteur ou d'atelier est susceptible de mémoriser.

NoOfCardVehicleRecords ::= ENTIER(0..2^{16}-1)

Assignation de valeur: cf. paragraphe 3.

2.77. **NoOfCompanyActivityRecords**

Nombre des relevés d'activité d'entreprise qu'une carte d'entreprise est susceptible de mémoriser.

▼M1

NoOfCompanyActivityRecords ::= ENTIER(0..2^{16}-1)

Assignation de valeur: cf. paragraphe 3.

2.78. **NoOfControlActivityRecords**

Nombre des relevés d'activité de contrôle qu'une carte de contrôleur est susceptible de mémoriser.

NoOfControlActivityRecords ::= ENTIER(0..2^{16}-1)

Assignation de valeur: cf. paragraphe 3.

2.79. **NoOfEventsPerType**

Nombre d'événements qu'une carte est susceptible de mémoriser par type d'événement.

NoOfEventsPerType ::= ENTIER(0..255)

Assignation de valeur: cf. paragraphe 3.

2.80. **NoOfFaultsPerType**

Nombre d'anomalies qu'une carte est susceptible de mémoriser par type d'anomalie.

NoOfFaultsPerType ::= ENTIER(0..255)

Assignation de valeur: cf. paragraphe 3.

2.81. **OdometerValueMidnight**

Valeur affichée par le compteur kilométrique du véhicule à minuit pile un jour donné (exigence 090).

OdometerValueMidnight ::= Kilométrage

Assignation de valeur: absence d'informations complémentaires.

2.82. **OdometerShort**

Valeur affichée par le compteur kilométrique du véhicule sous une forme abrégée.

OdometerShort ::= ENTIER(0..2^{24}-1)

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

2.83. **OverspeedNumber**

Nombre d'événements du type excès de vitesse survenus depuis le dernier contrôle d'excès de vitesse.

OverspeedNumber ::= ENTIER(0..255)

Assignation de valeur: 0 signifie qu'aucun événement du type excès de vitesse n'est survenu depuis le dernier contrôle d'excès de vitesse, 1 signifie qu'un événement du type excès de vitesse est survenu depuis le dernier contrôle d'excès de vitesse … 255 signifie que le nombre des événements du type excès de vitesse enregistrés depuis le dernier contrôle d'excès de vitesse est égal ou supérieur à 255.

2.84. **PlaceRecord**

Informations relatives à un lieu de début ou de fin d'une période de travail journalière (exigences 087, 202 et 221).

PlaceRecord ::= SÉQUENCE {

entryTime Temps réel

entryTypeDailyWorkPeriod Entrée du type de période de travail journalière

dailyWorkPeriodCountry Code numérique national

dailyWorkPeriodRegion Code numérique régional

vehicleOdometerValue Kilométrage

}

entryTime indique la date et l'heure de la saisie des données.

entryTypeDailyWorkPeriod indique le type d'entrée.

dailyWorkPeriodCountry indique le pays entré.

▼M1

dailyWorkPeriodRegion indique la région entrée.

vehicleOdometerValue indique la valeur affichée par le compteur kilométrique à l'heure de la saisie du lieu entré.

2.85. **PreviousVehicleInfo**

Informations relatives au véhicule précédemment utilisé par un conducteur lors de l'insertion de sa carte dans le lecteur d'une unité embarquée sur véhicule (exigence 081).

PreviousVehicleInfo ::= SÉQUENCE {

vehicleRegistrationIdentification Identification et immatriculation du véhicule

cardWithdrawalTime Temps réel

}

vehicleRegistrationIdentification indique le NIV ainsi que l'État membre d'immatriculation du véhicule.

cardWithdrawalTime indique la date et l'heure de retrait de la carte.

2.86. **PublicKey**

Clé publique RSA.

PublicKey ::= SÉQUENCE {

rsaKeyModulus Module de clé RSA

rsaKeyPublicExponent Exposant public de clé RSA

}

rsaKeyModulus indique le module de la paire de clés.

rsaKeyPublicExponent indique l'exposant public de la paire de clés.

2.87. **RegionAlpha**

Référence alphabétique aux différentes régions d'un pays déterminé.

RegionAlpha ::= CHAÎNE IA5[LONGUEUR(3)]

Assignation de valeur:

' ' Aucune information disponible

Espagne:

'AN' Andalousie

'AR' Aragon

'AST' Asturies

'C' Cantabrique

'CAT' Catalogne

'CL' Castille-León

'CM' Castille-La Manche

'CV' Valence

'EXT' Estrémadure

'G' Galice

'IB' Baléares

'IC' Canaries

'LR' La Rioja

'M' Madrid

'MU' Murcie

'NA' Navarre

'PV' Pays basque

2.88. **RegionNumeric**

Référence alphabétique aux différentes régions d'un pays déterminé.

RegionNumeric ::= CHAÎNE D'OCTETS[LONGUEUR(1)]

▼**M1**

Assignation de valeur:

′00′H Aucune information disponible

Espagne:

′01′H Andalousie

′02′H Aragon

′03′H Asturies

′04′H Cantabrique

′05′H Catalogne

′06′H Castille-León

′07′H Castille-La Manche

′08′H Valence

′09′H Estrémadure

′0A′H Galice

′0B′H Baléares

′0C′H Canaries

′0D′H La Rioja

′0E′H Madrid

′0F′H Murcie

′10′H Navarre

′11′H Pays basque

2.89. **RSAKeyModulus**

Module d'une paire de clés RSA.

RSAKeyModulus ::= CHAÎNE D'OCTETS[LONGUEUR(128)]

Assignation de valeur: non spécifiée.

2.90. **RSAKeyPrivateExponent**

Exposant privé d'une paire de clés RSA.

RSAKeyPrivateExponent ::= CHAÎNE D'OCTETS[LONGUEUR(128)]

Assignation de valeur: non spécifiée.

2.91. **RSAKeyPublicExponent**

Exposant public d'une paire de clés RSA.

RSAKeyPublicExponent ::= CHAÎNE D'OCTETS[LONGUEUR(20)]

Assignation de valeur: non spécifiée.

2.92. **SensorApprovalNumber**

Numéro d'homologation du capteur.

SensorApprovalNumber ::= Chaîne IA5 [LONGUEUR(8)]

Assignation de valeur: non spécifiée.

2.93. **SensorIdentification**

Informations enregistrées dans la mémoire d'un capteur de mouvement et se rapportant à l'identification de cet élément (exigence 077).

SensorIdentification ::= SÉQUENCE {

sensorSerialNumber Numéro de série du capteur

sensorApprovalNumber Numéro d'homologation du capteur

sensorSCIdentifier Identificateur CS du capteur

sensorOSIdentifier Identificateur SE du capteur

}

sensorSerialNumber indique le numéro de série étendu du capteur de mouvement (numéro de pièce et code du fabricant inclus).

sensorApprovalNumber indique le numéro d'homologation du capteur de mouvement.

▼M1

sensorSCIdentifier indique l'identificateur du composant de sécurité du capteur de mouvement.

sensorOSIdentifier indique l'identificateur du système d'exploitation du capteur de mouvement.

2.94. **SensorInstallation**

Informations enregistrées dans la mémoire d'un capteur de mouvement et se rapportant à l'installation de cet élément (exigence 099).

SensorInstallation ::= SÉQUENCE {

sensorPairingDateFirst Date de couplage du capteur

firstVuApprovalNumber Numéro d'homologation de l'UEV

firstVuSerialNumber Numéro de série de l'UEV

sensorPairingDateCurrent Date de couplage du capteur

currentVuApprovalNumber Numéro d'homologation de l'UEV

currentVUSerialNumber Numéro de série de l'UEV

}

sensorPairingDateFirst indique la date du premier couplage du capteur de mouvement avec une unité embarquée sur véhicule.

firstVuApprovalNumber indique le numéro d'homologation de la première unité embarquée sur véhicule couplée avec le capteur de mouvement.

firstVuSerialNumber indique le numéro de série de la première unité embarquée sur véhicule couplée avec le capteur de mouvement.

sensorPairingDateCurrent indique la date du couplage actuel du capteur de mouvement avec l'unité embarquée sur véhicule.

currentVuApprovalNumber indique le numéro d'homologation de l'unité sur véhicule actuellement couplée avec le capteur de mouvement.

currentVUSerialNumber indique le numéro de série de l'unité sur véhicule actuellement couplée avec le capteur de mouvement.

2.95. **SensorInstallationSecData**

Informations enregistrées sur une carte d'atelier et se rapportant aux données de sécurité nécessaires au couplage de capteurs de mouvement avec des unités embarquées sur véhicule (exigence 214).

SensorInstallationSecData ::= TDesSessionKey

Assignation de valeur: en conformité avec la norme ISO 16844-3.

2.96. **SensorOSIdentifier**

Identificateur du système d'exploitation du capteur de mouvement.

SensorOSIdentifier ::= Chaîne IA5 [LONGUEUR(2)]

Assignation de valeur: propre au fabricant.

2.97. **SensorPaired**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à l'identification du capteur de mouvement couplé avec cette unité embarquée (exigence 079).

SensorPaired ::= SÉQUENCE {

sensorSerialNumber Numéro de série du capteur

sensorApprovalNumber Numéro d'homologation du capteur

sensorPairingDateFirst Date de couplage du capteur

}

sensorSerialNumber indique le numéro de série du capteur de mouvement actuellement couplé avec l'unité embarquée sur véhicule.

sensorApprovalNumber indique le numéro d'homologation du capteur de mouvement actuellement couplé avec l'unité embarquée sur véhicule.

sensorPairingDateFirst indique la date du premier couplage entre une unité sur véhicule et le capteur de mouvement actuellement couplé avec l'unité embarquée sur le véhicule considéré.

▼**M1**

2.98. **SensorPairingDate**

Date d'un couplage du capteur de mouvement avec une unité embarquée sur véhicule.

SensorPairingDate ::= Temps réel

Assignation de valeur: non spécifiée.

2.99. **SensorSerialNumber**

Numéro de série du capteur de mouvement.

SensorSerialNumber ::= ExtendedSerialNumber

2.100. **SensorSCIdentifier**

Identificateur du composant de sécurité du capteur de mouvement.

SensorSCIdentifier ::= Chaîne IA5 [LONGUEUR(8)]

Assignation de valeur: propre au fabricant du composant.

2.101. **Signature**

Signature numérique.

Signature ::= CHAÎNE D'OCTETS[LONGUEUR(128)]

Assignation de valeur: en conformité avec l'appendice 11 (Mécanismes de sécurité communs).

2.102. **SimilarEventsNumber**

Nombre d'événements similaires survenus un jour donné (exigence 094).

SimilarEventsNumber ::= ENTIER(0..255)

Assignation de valeur: 0 n'est pas utilisé, 1 signifie qu'un seul événement de ce type s'est produit et a été enregistré le jour considéré, 2 signifie que deux événements de ce type se sont produits le jour considéré (et un seul d'entre eux a été enregistré), … 255 signifie que le jour considéré a vu la manifestation d'un nombre d'événements de ce type égal ou supérieur à 255.

2.103. **SpecificConditionType**

Code identifiant une condition particulière (exigences 050 *ter*, 105 *bis*, 212 *bis* et 230 *bis*).

SpecificConditionType ::= ENTIER(0..255)

Assignation de valeur:

′00′H	RFU
′01′H	Hors champ — Début
′02′H	Hors champ — Fin
′03′H	Trajet en ferry/train
′04′H .. ′FF′H	RFU

2.104. **SpecificConditionRecord**

Informations enregistrées sur une carte de conducteur, une carte d'atelier ou une unité embarquée sur véhicule et se rapportant à une condition particulière (exigences 105 *bis*, 212 *bis* et 230 *bis*).

SpecificConditionRecord ::= SÉQUENCE {

entryTime Temps réel

specificConditionType Type de condition particulière

}

entryTime indique la date et l'heure d'entrée de ces données.

specificConditionType indique le code identifiant la condition particulière concernée.

2.105. **Speed**

Vitesse du véhicule (km/h).

Speed ::= ENTIER(0..255)

Assignation de valeur: Valeur exprimée en km/h et se situant dans une plage d'exploitation comprise entre 0 et 220 km/h.

▼M1

2.106. **SpeedAuthorised**

Vitesse maximale autorisée du véhicule [définition bb)].

SpeedAuthorised ::= Vitesse

2.107. **SpeedAverage**

Vitesse moyenne mesurée par rapport à une durée préalablement définie (km/h).

SpeedAverage ::= Vitesse

2.108. **SpeedMax**

Vitesse maximale mesurée pendant une durée préalablement définie.

SpeedMax ::= Vitesse

2.109. **TDesSessionKey**

Clé de session Triple DES.

TDesSessionKey ::= SÉQUENCE {

tDesKeyA CHAÎNE D'OCTETS[LONGUEUR(8)]

tDesKeyB CHAÎNE D'OCTETS[LONGUEUR(8)]

}

Assignation de valeur: absence d'informations complémentaires.

2.110. **TimeReal**

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

TimeRealINTEGER:TimeRealRange ::= ENTIER(0..TimeRealRange)

Assignation de valeur — Octet aligné: nombre de secondes écoulées depuis minuit TUC, le 1er janvier 1970.

La date/heure future la plus avancée se situe en l'an 2106.

2.111. **TyreSize**

Désignation des dimensions des pneumatiques.

TyreSize ::= Chaîne IA5 [LONGUEUR(15)]

Assignation de valeur: en conformité avec la directive 92/23/CEE du 31.3.1992 (JO L 129 du 14.5.1992, p. 95).

2.112. **VehicleIdentificationNumber**

Numéro d'identification du véhicule (NIdV) faisant référence au véhicule dans son entier; il s'agit habituellement du numéro de série du châssis ou du numéro de cadre.

VehicleIdentificationNumber ::= Chaîne IA5 [LONGUEUR(17)]

Assignation de valeur: conformément à la norme ISO 3779.

2.113. **VehicleRegistrationIdentification**

Identification d'un véhicule, unique à l'échelle de l'Europe (VIN et État membre).

VehicleRegistrationIdentification ::= SÉQUENCE {

vehicleRegistrationNation Code numérique national

vehicleRegistrationNumber Numéro d'immatriculation du véhicule

}

vehicleRegistrationNation indique le pays d'immatriculation du véhicule.

vehicleRegistrationNumber indique le numéro d'immatriculation du véhicule (VIN).

2.114. **VehicleRegistrationNumber**

Numéro d'immatriculation du véhicule (VIN). Le numéro d'immatriculation est attribué par l'autorité compétente en matière d'immatriculation des véhicules.

VehicleRegistrationNumber ::= SÉQUENCE {

▼M1

codePage ENTIER (0..255),

vehicleRegNumber CHAÎNE D'OCTETS[LONGUEUR(13)]

}

codePage (page de codes) spécifie la partie de la norme ISO/CEI 8859 utilisée pour coder le numéro d'immatriculation du véhicule

vehicleRegNumber indique un VIN dont le codage est conforme à la page de codes appropriée de la norme ISO/CEI 8859.

Assignation de valeur: propre à chaque pays.

2.115. **VuActivityDailyData**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux changements d'activité ainsi qu'aux changements d'état de conduite et/ou d'état de carte pour un jour civil donné (exigence 084) et à l'état des lecteurs à 00h00 ce même jour.

VuActivityDailyData ::= SÉQUENCE {

noOfActivityChanges ENTIER(0..1 440),

activityChangeInfos LONGUEUR DÉFINIE(noOfActivity-Changes) DES ActivityChangeInfo

}

noOfActivityChanges indique le nombre de mots que comporte le jeu Activity-ChangeInfos.

activityChangeInfos indique le jeu de mots ActivityChangeInfo enregistrés dans l'UEV pour le jour considéré. Il comprend toujours deux mots Activity-ChangeInfo donnant l'état des deux lecteurs à 00h00 ce même jour.

2.116. **VuApprovalNumber**

Numéro d'homologation de l'unité embarquée sur véhicule.

VuApprovalNumber ::= Chaîne IA5 [LONGUEUR(8)]

Assignation de valeur: non spécifiée.

2.117. **VuCalibrationData**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux étalonnages successifs de l'appareil de contrôle (exigence 098).

VuCalibrationData ::= SÉQUENCE {

noOfVuCalibrationRecords ENTIER(0..255),

vuCalibrationRecords (noOfVuCalibrationRecords) DU VuCa-librationRecord

}

noOfVuCalibrationRecords indique le nombre des relevés que contient le jeu vuCalibrationRecords.

vuCalibrationRecords indique le jeu de relevés d'étalonnage.

2.118. **VuCalibrationRecord**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à un étalonnage de l'appareil de contrôle (exigence 098).

VuCalibrationRecord ::= SÉQUENCE {

calibrationPurpose Raison de l'étalonnage

workshopName Nom

workshopAddress Adresse

workshopCardNumber Numéro intégral de la carte

workshopCardExpiryDate Temps réel

vehicleIdentificationNumber Numéro d'identification du véhi-cule

vehicleRegistrationIdentification Numéro d'immatriculation du véhicule

wVehicleCharacteristicConstant Coefficient W caractéristique du véhicule

kConstantOfRecordingEquipment Constante K de l'appareil de contrôle

▼M1

lTyreCircumference Circonférence des pneumatiques L

tyreSize Dimensions des pneumatiques

authorisedSpeed Vitesse autorisée

oldOdometerValue Kilométrage

newOdometerValue Kilométrage

oldTimeValue Temps réel

newTimeValue Temps réel

nextCalibrationDate Temps réel

}

calibrationPurpose indique la raison de l'étalonnage.

workshopName, workshopAddress indiquent les nom et adresse de l'atelier.

workshopCardNumber identifie la carte d'atelier utilisée lors de l'étalonnage.

workshopCardExpiryDate indique la carte d'expiration de la carte.

vehicleIdentificationNumber indique le NIdV.

vehicleRegistrationIdentification contient le NIV et l'État membre d'immatriculation.

wVehicleCharacteristicConstant indique le coefficient caractéristique du véhicule.

kConstantOfRecordingEquipment indique la constante de l'appareil de contrôle.

lTyreCircumference indique la circonférence effective des pneumatiques.

tyreSize indique la désignation de la dimension des pneumatiques montés sur le véhicule.

authorisedSpeed indique la vitesse autorisée du véhicule.

oldOdometerValue, newOdometerValue indiquent les ancienne et nouvelle valeurs affichées par le compteur kilométrique.

oldTimeValue, newTimeValue indiquent les anciennes et nouvelles valeurs accordées à la date et à l'heure.

nextCalibrationDate indique la date du prochain étalonnage correspondant au type spécifié dans le champ CalibrationPurpose et auquel l'organisme d'inspection agréé doit procéder.

2.119. **VuCardIWData**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux cycles d'insertion et de retrait des cartes de conducteur ou d'atelier dans le lecteur approprié de cette unité embarquée (exigence 081).

VuCardIWData ::= SÉQUENCE {

noOfIWRecords ENTIER(0..2^{16}-1),

vuCardIWRecords LONGUEURDÉFINIE(noOfIWRecords)DU VuCardIWRecord

}

noOfIWRecords indique le nombre des relevés que contient le jeu vuCardIWRecords

vuCardIWRecords indique un jeu de relevés portant sur les cycles d'insertion et de retrait des cartes.

2.120. **VuCardIWRecord**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant au cycle d'insertion et de retrait d'une carte de conducteur ou d'atelier dans le lecteur approprié de cette unité embarquée (exigence 081).

VuCardIWRecord ::= SÉQUENCE {

cardHolderName Nom du titulaire

fullCardNumber Numéro intégral de la carte

cardExpiryDate Temps réel

cardInsertionTime Temps réel

vehicleOdometerValueAtInsertion Kilométrage

cardSlotNumber Numéro du lecteur de carte

cardWithdrawalTime Temps réel

▼M1

vehicleOdometerValueAtWithdrawal Kilométrage

previousVehicleInfo Informations relatives au véhicule précédent

manualInputFlag Drapeau de saisie manuelle

}

cardHolderName indique les nom et prénom(s) du conducteur ou du détenteur de la carte d'atelier, tels qu'ils sont enregistrés sur celle-ci.

fullCardNumber indique le type, l'État membre où est délivrée la carte et le numéro de celle-ci, tels qu'ils sont enregistrés sur la carte.

cardExpiryDate indique la date d'expiration de la carte telle qu'elle est enregistrée sur celle-ci.

cardInsertionTime indique la date et l'heure d'insertion de la carte.

vehicleOdometerValueAtInsertion indique la valeur affichée par le compteur kilométrique lors de l'insertion de la carte.

cardSlotNumber indique le lecteur dans la fente duquel la carte est insérée.

cardWithdrawalTime indique la date et l'heure de retrait de la carte.

vehicleOdometerValueAtWithdrawal indique la valeur affichée par le compteur kilométrique lors du retrait de la carte.

previousVehicleInfo contient des informations relatives au précédent véhicule utilisé par le conducteur, telles qu'elles sont enregistrées sur la carte.

manualInputFlag correspond à un drapeau permettant d'identifier si le détenteur de la carte a procédé ou non à la saisie manuelle d'activités du conducteur lors de l'insertion de cette carte.

2.121. **VuCertificate**

Certificat associé à la clé publique d'une unité embarquée sur véhicule.

VuCertificate ::= Certificat

2.122. **VuCompanyLocksData**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux verrouillages d'entreprise (exigence 104).

VuCompanyLocksData ::= SÉQUENCE {

noOfLocks ENTIER(0..20),

vuCompanyLocksRecords LONGUEUR DÉFINIE(noOfLocks) DU VuCompanyLocksRecord

}

noOfLocks indique le nombre de verrouillages répertoriés dans les vuCompanyLocksRecords.

vuCompanyLocksRecords correspond au jeu de relevés des verrouillages d'entreprise.

2.123. **VuCompanyLocksRecord**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à un verrouillage d'entreprise déterminé (exigence 104).

VuCompanyLocksRecord ::= SÉQUENCE {

lockInTime Temps réel

lockOutTime Temps réel

companyName Nom

companyAddress Adresse

companyCardNumber Numéro intégral de la carte

}

lockInTime, lockOutTime indiquent les dates et heures de verrouillage et de déverrouillage.

companyName, companyAddress indiquent les nom et adresse de l'entreprise en rapport avec le verrouillage.

companyCardNumber identifie la carte utilisée lors du verrouillage.

▼M1

2.124. **VuControlActivityData**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux contrôles exécutés à l'aide de cette UEV (exigence 102).

```
VuControlActivityData ::= SÉQUENCE {
    noOfControls ENTIER(0..20),
    vuControlActivityRecords LONGUEURDÉFINIE(noOfControls)DU VuControlActivityRecord
}
```

noOfControls indique le nombre des contrôles répertoriés dans les vuControlActivityRecords.

vuControlActivityRecords indique le jeu des relevés d'activité de contrôle.

2.125. **VuControlActivityRecord**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à un contrôle précis exécuté à l'aide de cette UEV (exigence 102).

```
VuControlActivityRecord ::= SÉQUENCE {
    controlType Type de contrôle
    controlTime Temps réel
    controlCardNumber Numéro intégral de la carte
    downloadPeriodBeginTime Temps réel
    downloadPeriodEndTime Temps réel
}
```

controlType indique le type de contrôle.

controlTime indique la date et l'heure du contrôle.

ControlCardNumber identifie la carte de contrôleur utilisée lors du contrôle.

downloadPeriodBeginTime indique l'heure de début de la période téléchargée, en cas de téléchargement.

downloadPeriodEndTime indique l'heure de fin de la période téléchargée, en cas de téléchargement.

2.126. **VuDataBlockCounter**

Compteur enregistré sur une carte et identifiant séquentiellement les cycles d'insertion et de retrait de la carte sur le lecteur approprié d'unités embarquées sur véhicules.

```
VuDataBlockCounter ::= BCDString[LONGUEUR(2)]
```

Assignation de valeur: numérotation consécutive dont la valeur maximale est égale à 9 999, la numérotation recommençant par le numéro 0.

2.127. **VuDetailedSpeedBlock**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à l'évolution de la vitesse du véhicule pendant une minute au cours de laquelle le véhicule était en mouvement (exigence 093).

```
VuDetailedSpeedBlock ::= SÉQUENCE {
    speedBlockBeginDate Temps réel
    speedsPerSecond DUREE DE LA SÉQUENCE(60) D'ÉVALUATION DE LA vitesse
}
```

speedBlockBeginDate indique la date et l'heure de la première vitesse instantanée que comporte le bloc de données.

speedsPerSecond indique la séquence chronologique des vitesses mesurées toutes les secondes pendant la minute qui a commencé à la speedBlockBeginDate (incluse).

2.128. **VuDetailedSpeedData**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à l'évolution de la vitesse du véhicule.

```
VuDetailedSpeedData ::= SEQUENCE
    noOfSpeedBlocks ENTIER(0.2^16-1),
```

▼M1

vuDetailedSpeedBlocks LONGUEUR DÉFINIE (noOfSpeedBlocks) DU VuDetailedSpeedBlock

}

noOfSpeedBlocks indique le nombre des blocs de vitesse que comporte le jeu de vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks indique le jeu de blocs de mesure de la vitesse instantanée.

2.129. **VuDownloadablePeriod**

Dates les plus ancienne et récente pour lesquelles une unité embarquée sur véhicule détient des données relatives aux activités des conducteurs (exigences 081, 084 ou 087).

VuDownloadablePeriod ::= SÉQUENCE {

minDownloadableTime Temps réel

maxDownloadableTime Temps réel

}

minDownloadableTime indique les date et heure de l'insertion de carte, de l'entrée de site ou du changement d'activité le plus ancien enregistrées dans la mémoire de l'unité embarquée sur véhicule.

maxDownloadableTime indique les date et heure du retrait de carte, de l'entrée de site ou du changement d'activité le plus récent enregistrées dans la mémoire de l'unité embarquée sur véhicule.

2.130. **VuDownloadActivityData**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à son dernier téléchargement (exigence 105).

VuDownloadActivityData ::= SÉQUENCE {

downloadingTime Temps réel

fullCardNumber Numéro intégral de la carte

companyOrWorkshopName Nom

}

downloadingTime indique la date et l'heure du téléchargement.

fullCardNumber identifie la carte utilisée pour autoriser le téléchargement.

companyOrWorkshopName indique le nom de l'entreprise ou de l'atelier.

2.131. **VuEventData**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à divers événements (exigence 094 à l'exception des événements du type excès de vitesse).

VuEventData ::= SÉQUENCE {

noOfVuEvents ENTIER(0..255),

vuEventRecords LONGUEURDÉFINIE(noOfVuEvents)DU VuEventRecord

}

noOfVuEvents indique le nombre des événements répertoriés dans le jeu des vuEventRecords.

vuEventRecords indique un jeu de relevés d'événements.

2.132. **VuEventRecord**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à un événement (exigence 094 à l'exception de tout événement du type excès de vitesse).

VuEventRecord ::= SÉQUENCE {

eventType Type d'événement/anomalie

eventRecordPurpose Raison d'un relevé d'événement/anomalie

eventBeginTime Temps réel

eventEndTime Temps réel

cardNumberDriverSlotBegin Numéro intégral de la carte

cardNumberCodriverSlotBegin Numéro intégral de la carte

▼M1

```
    cardNumberDriverSlotEnd Numéro intégral de la carte
    cardNumberCodriverSlotEnd Numéro intégral de la carte
    similarEventsNumber Nombre d'événements similaires
}
```

eventType indique le type d'événement.

eventRecordPurposeindique la raison de l'enregistrement de l'événement considéré.

eventBeginTime indique la date et l'heure de début de l'événement.

eventEndTime indique la date et l'heure de fin de l'événement.

cardNumberDriverSlotBegin identifie la carte insérée dans le lecteur réservé au conducteur, au début de l'événement.

cardNumberCodriverSlotBegin identifie la carte insérée dans le lecteur réservé au convoyeur, au début de l'événement.

cardNumberDriverSlotEnd identifie la carte insérée dans le lecteur réservé au conducteur, à la fin de l'événement.

cardNumberCodriverSlotEnd identifie la carte insérée dans le lecteur réservé au convoyeur, à la fin de l'événement.

similarEventsNumber indique le nombre d'événements similaires survenus le même jour.

Cette séquence s'utilise pour tous les événements, sauf ceux du type excès de vitesse.

2.133. **VuFaultData**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à diverses anomalies (exigence 096).

```
VuFaultData ::= SÉQUENCE {
    noOfVuFaults ENTIER(0..255),
    vuFaultRecords LONGUEURDÉFINIE(noOfVuFaults)DU
    VuFaultRecord
}
```

noOfVuFaults indique le nombre des anomalies répertoriées dans le jeu des vuFaultRecords.

vuFaultRecords indique un jeu de relevés d'anomalies.

2.134. **VuFaultRecord**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à une anomalie (exigence 096).

```
VuFaultRecord ::= SÉQUENCE {
    faultType Type d'événement/anomalie
    faultRecordPurpose Raison d'un relevé d'événement/anomalie
    faultBeginTime Temps réel
    faultEndTime Temps réel
    cardNumberDriverSlotBegin Numéro intégral de la carte
    cardNumberCodriverSlotBegin Numéro intégral de la carte
    cardNumberDriverSlotEnd Numéro intégral de la carte
    cardNumberCodriverSlotEnd Numéro intégral de la carte
}
```

faultType indique le type d'anomalie affectant l'appareil de contrôle.

faultRecordPurpose indique la raison de l'enregistrement de l'anomalie considérée.

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

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

cardNumberDriverSlotBegin identifie la carte insérée dans le lecteur réservé au conducteur, au début de l'anomalie.

cardNumberCodriverSlotBegin identifie la carte insérée dans le lecteur réservé au convoyeur, au début de l'anomalie.

cardNumberDriverSlotEnd identifie la carte insérée dans le lecteur réservé au conducteur, à la fin de l'anomalie.

▼M1

cardNumberCodriverSlotEnd dentifie la carte insérée dans le lecteur réservé au convoyeur, à la fin de l'anomalie.

2.135. **VuIdentification**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à l'identification de l'unité embarquée sur le véhicule (exigence 075).

VuIdentification ::= SÉQUENCE {

vuManufacturerName Nom du fabricant de l'UEV

vuManufacturerAddress Adresse du fabricant de l'UEV

vuPartNumber Numéro de pièce de l'UEV

vuSerialNumber Numéro de série de l'UEV

vuSoftwareIdentification Identification du logiciel de l'UEV

vuManufacturingDate Date de fabrication de l'UEV

vuApprovalNumber Numéro d'homologation de l'UEV

}

vuManufacturerName indique le nom du fabricant de l'unité embarquée sur véhicule.

vuManufacturerAddress indique l'adresse du fabricant de l'unité embarquée sur véhicule.

vuPartNumber indique le numéro de pièce de l'unité embarquée sur véhicule.

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

vuSoftwareIdentification identifie le logiciel mis en œuvre au sein de l'unité embarquée sur véhicule.

vuManufacturingDate indique la date de fabrication de l'unité embarquée sur véhicule.

vuApprovalNumber indique le numéro d'homologation de l'unité embarquée sur véhicule.

2.136. **VuManufacturerAddress**

Adresse du fabricant de l'unité embarquée sur véhicule.

VuManufacturerAddress ::= Address

Assignation de valeur: non spécifiée.

2.137. **VuManufacturerName**

Nom du fabricant de l'unité embarquée sur véhicule.

VuManufacturerName ::= Nom

Assignation de valeur: non spécifiée.

2.138. **VuManufacturingDate**

Date de fabrication de l'unité embarquée sur véhicule.

VuManufacturingDate ::= Temps réel

Assignation de valeur: non spécifiée.

2.139. **VuOverSpeedingControlData**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux événements du type excès de vitesse survenus depuis le dernier contrôle d'excès de vitesse (exigence 095).

VuOverSpeedingControlData ::= SÉQUENCE {

lastOverspeedControlTime Temps réel

firstOverspeedSince Temps réel

numberOfOverspeedSince Nombre d'excès de vitesse

}

lastOverspeedControlTime indique la date et l'heure du dernier contrôle d'excès de vitesse.

firstOverspeedSince indique la date et l'heure du premier excès de vitesse constaté depuis ce contrôle d'excès de vitesse.

▼M1

numberOfOverspeedSince indique le nombre d'événements du type excès de vitesse survenus depuis le dernier contrôle d'excès de vitesse.

2.140. **VuOverSpeedingEventData**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux événements du type excès de vitesse (exigence 094).

```
VuOverSpeedingEventData ::= SÉQUENCE {
    noOfVuOverSpeedingEvents ENTIER(0..255),
    vuOverSpeedingEventRecords LONGUEUR DÉFINIE (noOf-
    VuOverSpeedingEvents) DU VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents indique le nombre d'événements répertoriés dans le jeu vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords indique un jeu de relevés d'événements du type excès de vitesse.

2.141. **VuOverSpeedingEventRecord**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux événements du type excès de vitesse (exigence 094).

```
VuOverSpeedingEventRecord ::= SÉQUENCE {
    eventType Type d'événement/anomalie
    eventRecordPurpose Raison d'un relevé d'événement/anomalie
    eventBeginTime Temps réel
    eventEndTime Temps réel
    maxSpeedValue Vitesse max.
    averageSpeedValue Vitesse moyenne
    cardNumberDriverSlotBegin Numéro intégral de la carte
    similarEventsNumber Nombre d'événements similaires
}
```

eventType indique le type d'événement.

eventRecordPurpose indique la raison de l'enregistrement de l'événement considéré.

eventBeginTime indique la date et l'heure du début de l'événement.

eventEndTime indique la date et l'heure de la fin de l'événement.

maxSpeedValue indique la vitesse maximale mesurée au cours de l'événement.

averageSpeedValue indique la vitesse moyenne arithmétique mesurée au cours de l'événement.

cardNumberDriverSlotBegin identifie la carte insérée dans le lecteur réservé au conducteur, au début de l'événement.

similarEventsNumber indique le nombre d'événements similaires survenus le même jour.

2.142. **VuPartNumber**

Numéro de pièce de l'unité embarquée sur véhicule.

```
VuPartNumber ::= Chaîne IA5 [LONGUEUR(16)]
```

Assignation de valeur: propre au fabricant de l'UEV.

2.143. **VuPlaceDailyWorkPeriodData**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux sites et lieux de début ou de fin des périodes de travail journalières (exigence 087).

```
VuPlaceDailyWorkPeriodData ::= SÉQUENCE {
    noOfPlaceRecords ENTIER(0..255),
    vuPlaceDailyWorkPeriodRecords LONGUEUR DÉFINIE
    (noOfPlaceRecords) DU VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords indique le nombre des relevés répertoriés dans le jeu vuPlaceDailyWorkPeriodRecords.

▼M1

vuPlaceDailyWorkPeriodRecords indique un jeu de relevés de site.

2.144. **VuPlaceDailyWorkPeriodRecord**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant au site ou lieu de début ou de fin d'une période de travail journalière (exigence 087).

VuPlaceDailyWorkPeriodRecord ::= SÉQUENCE {

fullCardNumber Numéro intégral de la carte

placeRecord Relevé de site

}

fullCardNumber indique le type, l'État membre où est délivrée la carte et le numéro de celle-ci.

placeRecord contient des données relatives au site entré.

2.145. **VuPrivateKey**

Clé privée d'une unité embarquée sur véhicule.

VuPrivateKey ::= Exposant privé de clé RSA

2.146. **VuPublicKey**

Clé publique d'une unité embarquée sur véhicule.

VuPublicKey ::= Clé publique

2.147. **VuSerialNumber**

Numéro de série de l'unité embarquée sur véhicule (exigence 075).

VuSerialNumber ::= Numéro de série étendu

2.148. **VuSoftInstallationDate**

Date d'installation de la version du logiciel d'exploitation de l'unité embarquée sur véhicule.

VuSoftInstallationDate ::= Temps réel

Assignation de valeur: non spécifiée.

2.149. **VuSoftwareIdentification**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant au logiciel installé.

VuSoftwareIdentification ::= SÉQUENCE {

vuSoftwareVersion Version du logiciel de l'UEV

vuSoftInstallationDate Date d'installation du logiciel de l'UEV

}

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

vuSoftInstallationDate indique la date d'installation de cette version du logiciel.

2.150. **VuSoftwareVersion**

Numéro de la version du logiciel de l'unité embarquée sur véhicule.

VuSoftwareVersion ::= Chaîne IA5 [LONGUEUR(4)]

Assignation de valeur: non spécifiée.

2.151. **VuSpecificConditionData**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux conditions particulières.

VuSpecificConditionData ::= SÉQUENCE {

noOfSpecificConditionRecords ENTIER(0..2^{16}-1)

specificConditionRecords LONGUEUR DÉFINIE (noOfSpecificConditionRecords) DU SpecificConditionRecord

}

noOfSpecificConditionRecords indique le nombre des relevés répertoriés dans le jeu specificConditionRecords.

▼M1

specificConditionRecords indique un jeu de relevés relatifs à des conditions particulières.

2.152. **VuTimeAdjustmentData**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant aux remises à l'heure exécutées hors du cadre d'un étalonnage complet (exigence 101).

VuTimeAdjustmentData ::= SÉQUENCE {

noOfVuTimeAdjRecords ENTIER(0..6),

vuTimeAdjustmentRecords LONGUEUR DÉFINIE (noOfVuTimeAdjRecords) DU VuTimeAdjustmentRecord

}

noOfVuTimeAdjRecords indique le nombre des relevés répertoriés dans le jeu vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords indique un jeu de relevés de remises à l'heure.

2.153. **VuTimeAdjustmentRecord**

Informations enregistrées dans la mémoire d'une unité embarquée sur véhicule et se rapportant à une remise à l'heure exécutée hors du cadre d'un étalonnage complet (exigence 101).

VuTimeAdjustmentRecord ::= SÉQUENCE {

oldTimeValue Temps réel

newTimeValue Temps réel

workshopName Nom

workshopAddress Adresse

workshopCardNumber Numéro intégral de la carte

}

oldTimeValue, newTimeValue indiquent les anciennes et nouvelles valeurs conférées à la date et à l'heure.

workshopName, workshopAddress indiquent les nom et adresse de l'atelier.

workshopCardNumber identifie la carte d'atelier utilisée pour exécuter la remise à l'heure.

2.154. **Coefficient W caractéristique du véhicule**

Coefficient caractéristique du véhicule [définition k)].

W-VehicleCharacteristicConstant ::= ENTIER(0..2^{16}-1))

Assignation de valeur: Impulsions par kilomètre dans la plage d'exploitation 0 à 64 255 imp/km.

2.155. **WorkshopCardApplicationIdentification**

Informations enregistrées sur une carte d'atelier et se rapportant à l'identification de l'application de la carte (exigence 190).

WorkshopCardApplicationIdentification ::= SÉQUENCE {

typeOfTachographCardId Type d'équipement

cardStructureVersion Version de la structure de la carte

noOfEventsPerType Nombre d'événements par type

noOfFaultsPerType Nombre d'anomalies par type

activityStructureLength Nombre d'octets affectés aux relevés d'activité

noOfCardVehicleRecords Nombre des relevés de véhicule enregistrés sur la carte

noOfCardPlaceRecords Nombre des relevés de site enregistrés sur la carte

noOfCalibrationRecords Nombre des relevés d'étalonnage

}

typeOfTachographCardId spécifie le type de la carte mise en application.

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

▼M1

noOfEventsPerType indique le nombre d'événements que la carte est susceptible de sauvegarder par type d'événement.

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

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

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

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

noOfCalibrationRecords indique le nombre des relevés d'étalonnage que la carte est susceptible de mémoriser.

2.156. **WorkshopCardCalibrationData**

Informations enregistrées sur une carte d'atelier et se rapportant à une activité d'atelier exécutée avec la carte (exigences 227 et 229).

```
WorkshopCardCalibrationData ::= SÉQUENCE {
    calibrationTotalNumber ENTIER(0..2^16-1),
    calibrationPointerNewestRecord ENTIER(0..NoOfCalibration-
    Records-1),
    calibrationRecords LONGUEUR DÉFINIE(NoOfCalibration-
    Records) DU WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber indique le nombre total d'étalonnages exécutés avec la carte.

calibrationPointerNewestRecord indique l'indice du dernier relevé d'étalonnage mis à jour.

Assignation de valeur: nombre correspondant au numérateur du relevé d'étalonnage, commençant par une série de '0' pour la première occurrence d'un relevé d'étalonnage dans la structure considérée.

calibrationRecords indique le jeu de relevés contenant des données d'étalonnage et/ou de réglage temporel.

2.157. **WorkshopCardCalibrationRecord**

Informations enregistrées sur une carte d'atelier et se rapportant à un étalonnage exécuté avec la carte (exigence 227).

```
WorkshopCardCalibrationRecord ::= SÉQUENCE {
    calibrationPurpose Raison de l'étalonnage
    vehicleIdentificationNumber Numéro d'identification du véhi-
    cule
    vehicleRegistration Identification et immatriculation du véhi-
    cule
    wVehicleCharacteristicConstant Coefficient W caractéristique
    du véhicule
    kConstantOfRecordingEquipment Constante K de l'appareil de
    contrôle
    lTyreCircumference Circonférence des pneumatiques L
    tyreSize Dimensions des pneumatiques
    authorisedSpeed Vitesse autorisée
    oldOdometerValue Kilométrage
    newOdometerValue Kilométrage
    oldTimeValue Temps réel
    newTimeValue Temps réel
    nextCalibrationDate Temps réel
    vuPartNumber Numéro de pièce de l'UEV
    vuSerialNumber Numéro de série de l'UEV
    sensorSerialNumber Numéro de série du capteur
}
```

calibrationPurpose indique la raison de l'étalonnage.

vehicleIdentificationNumber indique le NIdV.

▼M1

vehicleRegistration contient le NIV et l'État membre d'immatriculation.

wVehicleCharacteristicConstant indique le coefficient caractéristique du véhicule.

kConstantOfRecordingEquipment indique la constante de l'appareil de contrôle.

lTyreCircumference indique la circonférence effective des pneumatiques.

tyreSize indique la désignation de la dimension des pneumatiques montés sur le véhicule.

authorisedSpeed indique la vitesse maximale autorisée du véhicule.

oldOdometerValue, newOdometerValue indiquent les ancienne et nouvelle valeurs affichées par le compteur kilométrique.

oldTimeValue, newTimeValue indiquent les anciennes et nouvelles valeurs accordées à la date et à l'heure.

nextCalibrationDate indique la date du prochain étalonnage correspondant au type spécifié dans le champ CalibrationPurpose et auquel l'organisme d'inspection agréé doit procéder.

vuPartNumber, vuSerialNumber et **sensorSerialNumber** constituent les éléments d'information nécessaires à l'identification de l'appareil de contrôle.

2.158. **WorkshopCardHolderIdentification**

Informations enregistrées sur une carte d'atelier et se rapportant à l'identification du détenteur de la carte (exigence 216).

WorkshopCardHolderIdentification ::= SÉQUENCE {

workshopName Nom

workshopAddress Adresse

cardHolderName Nom du titulaire

cardHolderPreferredLanguage Langue de travail

}

workshopName indique le nom de l'atelier ou du détenteur de la carte.

workshopAddress indique l'adresse de l'atelier ou du détenteur de la carte.

cardHolderName indique les nom et prénom(s) du détenteur (p.ex. le nom du mécanicien).

cardHolderPreferredLanguage indique la langue de travail préférentielle du détenteur de la carte.

2.159. **WorkshopCardPIN**

Numéro d'identification individuel de la carte d'atelier (exigence 213).

WorkshopCardPIN ::= Chaîne IA5 [LONGUEUR(8)]

Assignation de valeur: le numéro d'identification individuel connu du détenteur de la carte, complété à droite d'une série d'octets 'FF' susceptible de compter 8 octets.

3. DÉFINITIONS DES PLAGES DE VALEURS ET DE DIMENSIONS

Définition des variables employées dans les définitions du paragraphe 2.

Plage de temps réelle ::= 2^{32}-1

3.1. **Définitions se rapportant aux cartes de conducteur:**

Nom de la variable	Minimum	Maximum
CardActivityLengthRange	5 544 octets (28 jours 93 changements d'activité par jour)	13 776 octets (28 jours 240 changements d'activité par jour)
NoOfCardPlaceRecords	84	112
NoOfCardVehicleRecords	84	200
NoOfEventsPerType	6	12

▼**M1**

Nom de la variable	Minimum	Maximum
NoOfFaultsPerType	12	24

3.2. **Définitions se rapportant aux cartes d'atelier:**

Nom de la variable	Minimum	Maximum
CardActivityLengthRange	198 octets (1 jour 93 changements d'activité)	492 octets (1 jour 240 changements d'activité)
NoOfCardPlaceRecords	6	8
NoOfCardVehicleRecords	4	8
NoOfEventsPerType	3	3
NoOfFaultsPerType	6	6
NoOfCalibrationRecords	88	255

3.3. **Définitions se rapportant aux cartes de contrôleur:**

Nom de la variable	Minimum	Maximum
NoOfControlActivityRecords	230	520

3.4. **Définitions se rapportant aux cartes d'entreprise:**

Nom de la variable	Minimum	Maximum
NoOfCompanyActivityRecords	230	520

4. JEUX DE CARACTÈRES

Les chaînes IA5 se composent par définition de caractères ASCII aux termes de la norme ISO/CEI 8824-1. Pour plus de lisibilité et pour faciliter la désignation des caractères, leur assignation de valeur est indiquée ci-après. En cas de divergence, la norme ISO/CEI 8824-1 l'emporte sur cette note d'information.

! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?

@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _

' a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~

D'autres chaînes de caractères (adresse, nom, numéro d'immatriculation du véhicule) utilisent en outre les caractères définis par les codes 192 à 255 définis aux termes de la norme ISO/CEI 8859-1 (jeu de caractères latins 1) ou ISO/CEI 8859-7 (jeu de caractères grecs).

5. CODAGE

Si les règles de codage ASN.1 s'appliquent aux différents types de données définis, leur codage doit être conforme à la norme ISO/CEI 8825-2, variante alignée.

▼**M1**

Appendice 2

CARACTÉRISTIQUES DES CARTES TACHYGRAPHIQUES

TABLE DES MATIÈRES

▼**M1**

▼**M1**

1. INTRODUCTION

1.1. **Abréviations**

Aux fins du présent appendice, les abréviations suivantes sont utilisées.

AUT	Authentifié
CA	Conditions d'accès
CLA	Octet de classe d'une commande UDPA
CCI	Carte à circuit intégré
ch	cycles d'horloge
CI	Circuit intégré
C6, C7	Contacts n^{os} 6 et 7 conformément aux dispositions de la norme ISO/CEI 7816-2
FE	Fichier élémentaire
FM	Fichier maître (FS racine)
FS	Fichier spécialisé
ID	Identificateur
INS	Octet d'instruction d'une commande UDPA
IVT	Informations de vérification de l'identité des titulaires
Lc	Longueur des données d'entrée relatives à une commande UDPA
Le	Longueur des données prévisibles (données de sortie relatives à une commande)
LZI	Longueur de la zone d'information
LZIC	Longueur de la zone d'information réservée à la carte
ME1-ME2	Mots d'état
MS	Messagerie sécurisée
NIP	Numéro d'identification personnel
P1-P2	Octets de paramétrage
PRO-MS	Protégé par messagerie sécurisée
RAR	Réponse à une réinitialisation
RINIT	Réinitialisation (de la carte)
RUU	Réservé à un usage ultérieur
STP	Sélection de transmission de protocole
TJR	Toujours
TS	Caractère RAR initial
UPDA	Unité de données du protocole d'application
ute	Unité de temps élémentaire
Vpp	Tension de programmation
XXh	Valeur XX en notation hexadécimale
||	Symbole de concaténation 03||04=0304

Les abréviations originales en langue anglaise sont les suivantes:

AC	Access conditions
AID	Application Identifier
ALW	Always
APDU	Application Protocol Data Unit (structure of a command)
ATR	Answer To Reset
AUT	Authenticated.
C6, C7	Contacts No 6 and 7 of the card as described in ISO/IEC 7816-2
cc	clock cycles
CHV	Card holder Verification Information
CLA	Class Octet of an ADPU command
DF	Dedicated File. A DF can contain other files (EF or DF)
EF	Elementary File
ENC	Encrypted: Access is possible only by encoding data.
etu	elementary time unit

▼**M1**

IC	Integrated Circuit
ICC	Integrated Circuit Card
ID	Identifier
IFD	Interface Device
IFS	Information Field Size
IFSC	Information Field Size for the card
IFSD	Information Field Size Device (for the Terminal)
INS	Instruction Octet of an ADPU command
Lc	Length of the input data for a APDU command
Le	Length of the expected data (output data for a command)
MF	Master File (root DF)
P1-P2	Parameter bytes
NAD	Node Address used in T=1 protocol
NEV	Never
PIN	Personal Identification Number
PRO SM	Protected with secure messaging
PTS	Protocol Transmission Selection
RFU	Reserved for Future Use
RST	Reset (of the card)
SM	Secure Messaging
SW1-SW2	Status bytes
TS	Initial ATR character
VPP	Programming Voltage
XXh	Value XX in hexadecimal notation
||	Concatenation symbol 03||04=0304

1.2. **Références**

Les références qui suivent apparaissent dans le présent appendice:

EN 726-3	Systèmes de cartes d'identification — Cartes et terminaux de télécommunications à circuit(s) intégré(s) — Partie 3: Exigences indépendantes de toute application auxquelles les cartes doivent satisfaire. Décembre 1994.
ISO/CEI 7816-2	Technologie de l'information — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 2: Dimensions et emplacement des contacts. Première édition: 1999.
ISO/CEI 7816-3	Technologie de l'information — Cartes d'identification — Cartes à circuit(s) intégré(s) pourvues de contacts — Partie 3: Signaux électroniques et protocole de transmission. Édition 2: 1997.
ISO/CEI 7816-4	Technologie de l'information — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 4: Commandes interindustrielles d'intercommunication. Première édition: 1995 + Modification 1: 1997.
ISO/CEI 7816-6	Technologie de l'information — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 6: Éléments de donnée interindustriels. Première édition: 1996 + Cor 1: 1998.
ISO/CEI 7816-8	Technologie de l'information — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 8: Commandes interindustrielles liées à la sécurité. Première édition: 1999.
ISO/CEI 9797	Technologie de l'information — Techniques de sécurisation — Mécanisme de préservation de l'intégrité des données reposant sur l'application d'une fonction de contrôle cryptographique employant un algorithme de chiffrage par bloc. Édition 2: 1994.

2. CARACTÉRISTIQUES ÉLECTRIQUES ET PHYSIQUES

Tous les signaux électroniques doivent être en conformité avec la norme ISO/CEI 7816-3, sauf indication contraire.

L'emplacement et les dimensions des contacts de la carte considérée doivent être conformes à la norme ISO/CEI 7816-2.

▼M1

2.1. **Tension d'alimentation et consommation de courant**

Le fonctionnement de la carte considérée doit être conforme aux spécifications et se situer dans les limites de consommation arrêtées dans la norme ISO/CEI 7816-3.

Le fonctionnement de la carte doit être assuré par une tension d'alimentation V_{cc} = 3 V (± 0,3 V) ou V_{cc} = 5 V (± 0,5 V).

La sélection de la tension appropriée doit s'opérer en conformité avec la norme ISO/CEI 7816-3.

2.2. **Tension de programmation V_{pp}**

La carte ne doit nécessiter l'application d'aucune tension de programmation au niveau de la broche C6. Il est prévu que la broche C6 d'un PIF quelconque ne sera pas connectée. Si le contact C6 est susceptible d'être connecté à la tension d'alimentation V_{cc} de la carte, il ne peut être raccordé à la masse. Cette tension ne doit donner lieu à aucune interprétation.

2.3. **Génération et fréquence d'horloge**

La carte doit fonctionner dans une plage de fréquences comprise entre 1 et 5 MHz. Au cours d'une même session de carte, la fréquence d'horloge est susceptible de subir des fluctuations de l'ordre de ± 2 %. La fréquence d'horloge est générée par l'unité embarquée sur véhicule et non par la carte considérée. Le coefficient d'utilisation peut varier entre 40 et 60 %.

Il est possible d'interrompre l'horloge externe dans les conditions enregistrées dans le fichier sur carte FE_{CCI}. Le premier octet du corps du fichier FECCI programme les conditions d'application du mode Arrêt d'horloge (cf. EN 726-3 pour plus de détails):

Inférieur	Supérieur		
Bit 3	Bit 2	Bit 1	
0	0	1	Arrêt d'horloge autorisé, pas de niveau préférentiel
0	1	1	Arrêt d'horloge autorisé, avec une préférence pour le niveau supérieur
1	0	1	Arrêt d'horloge autorisé, avec une préférence pour le niveau inférieur
0	0	0	Arrêt d'horloge interdit
0	1	0	Arrêt d'horloge autorisé uniquement au niveau supérieur
1	0	0	Arrêt d'horloge autorisé uniquement au niveau inférieur

Les bits 4 à 8 ne sont pas utilisés.

2.4. **Contacts d'E/S**

Le contact d'E/S C7 autorise la réception et l'émission de données en provenance comme à destination du PIF concerné. En cours d'exploitation, la carte et le PIF ne peuvent opérer simultanément en mode émission. Dans l'éventualité où ces deux composants seraient exploités en mode émission, la carte ne courrait cependant aucun risque de détérioration. Lorsque la carte ne procède à aucune émission, elle passe systématiquement en mode réception.

2.5. **États de la carte**

La carte fonctionne selon deux états lorsque la tension d'alimentation requise est appliquée aux bornes de celle-ci:

— État d'exploitation lors de l'exécution de commandes ou en interfaçage avec une unité numérique

— État de repos dans tous les autres cas de figure; dans cet état, la carte doit mémoriser toutes les données utiles.

▼M1

3. MATÉRIEL ET COMMUNICATION

3.1. **Introduction**

Les fonctions minimales requises par les cartes tachygraphiques et les UV pour garantir des conditions d'exploitation et d'interopérabilité satisfaisantes font l'objet d'une description détaillée dans le présent paragraphe.

Les cartes tachygraphiques doivent être aussi conformes que possible aux normes ISO/CEI en vigueur (et à la norme ISO/CEI 7816 en particulier). Toutefois, les commandes et protocoles font l'objet d'une description détaillée afin de fournir, s'il y a lieu, quelques précisions sur certains usages restreints ou certaines différences éventuelles. Sauf indication contraire, les commandes spécifiées sont toutes conformes aux normes dont il est question.

3.2. **Protocole de transmission**

Le protocole de transmission doit être conforme à la norme ISO/CEI 7816-3. En particulier, l'UV doit être à même de reconnaître les extensions de délai d'attente que lui envoie la carte.

3.2.1. ***Protocoles***

La carte doit être à même de fournir les protocoles T=0 et T=1.

Le protocole T=0 est sélectionné par défaut; par conséquent, le lancement d'une commande STP est indispensable pour adopter le protocole T=1.

Les périphériques doivent prendre en charge la convention directe que comportent ces deux protocoles. En conséquence, la convention directe est obligatoire pour la carte.

La RAR doit présenter l'octet Longueur de la zone d'information réservée à la carte au niveau du caractère TA3. Valeur minimale: ′F0h′ (= 240 octets).

Les restrictions qui suivent s'appliquent aux protocoles:

T=0

— Le périphérique d'interface doit prendre en charge une réponse au niveau de l'E/S après le front montant du signal sur RINIT à partir de 400 ch.

— Le périphérique d'interface doit être à même de lire des caractères séparés par 12 ute.

— Le périphérique d'interface doit être capable de reconnaître un caractère erroné et sa répétition, même s'ils sont séparés par 13 ute. En cas de détection d'un caractère erroné, le signal d'erreur peut se manifester à l'E/S dans un délai compris entre 1 et 2 ute. Le périphérique doit être en mesure de supporter un retard d'une ute.

— Le périphérique d'interface doit accepter une RAR de 33 octets (TS+32).

— Si la RAR présente le caractère TC1, le temps de garde supplémentaire prévu doit être ménagé pour les caractères transmis par le périphérique d'interface bien que les caractères transmis par la carte puissent encore être séparés par 12 ute. Cette disposition s'applique également au caractère d'accusé de réception transmis par la carte après l'émission d'un caractère P3 par le périphérique d'interface.

— Le périphérique d'interface doit prendre un caractère NUL émis par la carte.

— Le périphérique d'interface doit accepter le mode complémentaire pour accusé de réception.

— La commande GET RESPONSE (obtenir une réponse) ne peut s'utiliser en mode chaînage pour obtenir des données dont la longueur pourrait excéder 255 octets.

T=1

— Octet ADN: inutilisé (l'octet ADN doit être mis à ′00′).

— ABANDON du bloc S: inutilisé.

— Erreur d'état VPP affectant le bloc S: inutilisé.

— La longueur totale de chaînage associée à une zone de données ne doit pas dépasser 255 octets (pour être garantie par le PIF).

— Le PIF doit indiquer la longueur de la zone d'information réservée au périphérique (LZIP) immédiatement après la RAR. Le PIF doit émettre la demande de longueur de la zone d'information du bloc S après la RAR et la carte doit lui renvoyer la LZI du bloc S. Il est recommandé d'accorder la valeur suivante à la LZID: 254 octets.

— La carte ne doit pas demander de réajustement de la LZI.

▼**M1**

3.2.2. ***RAR***

Le périphérique procède à un contrôle des octets RAR conformément à la norme ISO/CEI 7816-3. Les caractères historiques de la RAR ne doivent être soumis à aucune vérification.

Exemple de RAR biprotocole de base conforme à la norme ISO/CEI 7816-3

Caractère	Valeur	Remarques
TS	′3Bh′	Indique une convention directe
T0	′85h′	TD1 présent; présence de 5 octets historiques
TD1	′80h′	TD2 présent; T=0 à utiliser
TD2	′11h′	TA3 présent; T=1 à utiliser
TA3	′XXh′ (′F0h′ au moins)	Longueur de la zone d'information réservée à la carte (LZIC)
TH1 à TH5	′XXh′	Caractères historiques
TCK	′XXh′	Vérification de caractère (OU exclusif)

Après la réponse à une réinitialisation (RAR), le fichier maître (FM) est implicitement sélectionné. Il devient le répertoire en cours.

3.2.3. ***STP***

Le protocole par défaut est le suivant: T=0. Pour sélectionner le protocole T=1, le périphérique doit envoyer à la carte un message de STP (également désigné par l'abréviation PPS).

Tout comme les protocoles T=0 et T=1, la STP de base autorisant la permutation des protocoles est également obligatoire pour la carte.

La STP s'utilise, conformément aux dispositions de la norme ISO/CEI 7816-3, pour passer à des débits binaires supérieurs à celui par défaut proposé, le cas échéant, par la carte au niveau de la RAR [octet TA(1)].

L'emploi de débits binaires supérieurs est facultatif pour la carte.

Si la carte n'est compatible qu'avec le débit binaire par défaut (ou si le débit binaire sélectionné est incompatible), la carte doit répondre correctement à la STP en omettant l'octet PPS1, conformément à la norme ISO/CEI 7816-3.

Ci-après figure une série d'exemples de STP de base destinés à la sélection de protocoles:

Caractère	Valeur	Remarques
PPSS	′FFh′	Caractère de lancement
PPS0	′00h′ ou ′01h′	PPS1 à PPS3 sont absents; ′00h′ pour sélectionner T0, ′01h′ pour sélectionner T1
PK	′XXh′	Caractère de contrôle: ′XXh′ = ′FFh′ si PPS0 = ′00h′ ′XXh′ = ′FEh′ si PPS0 = ′01h′

3.3. **Conditions d'accès (CA)**

Les conditions d'accès (CA) aux commandes UPDATE_BINARY et READ_BINARY sont définies pour chaque fichier élémentaire.

Les CA au fichier en cours doivent être satisfaites avant de pouvoir accéder à ce dernier par l'intermédiaire de ces commandes.

Les conditions d'accès envisageables se définissent comme suit:

— TJR: l'action toujours envisageable peut être exécutée sans restriction.

— JAM: l'action n'est jamais envisageable.

▼**M1**

— AUT: les droits correspondant à une authentification externe réussie doivent être ouverts (par la commande EXTERNAL_AUTHENTIFICATION).

— PRO MS: la commande doit être transmise avec un total de contrôle cryptographique en recourant à la messagerie sécurisée (cf. appendice 11).

— AUT et PRO MS (combinées).

Pour ce qui concerne les commandes de traitement (UPDATE_BINARY et READ_BINARY), il est possible de configurer les conditions d'accès suivantes au niveau de la carte:

	UPDATE_BINARY	READ_BINARY
TJR	Oui	Oui
JAM	Oui	Oui
AUT	Oui	Oui
PRO MS	Oui	Non
AUT et PRO MS	Oui	Non

La condition d'accès PRO MS n'est pas disponible pour la commande READ_BINARY. Cela signifie que la présence d'un total de contrôle cryptographique pour une commande READ n'est jamais obligatoire. Toutefois, l'affectation de la valeur ′OC′ à la classe permet d'utiliser la commande READ_BINARY en messagerie sécurisée, conformément à la description fournie au paragraphe 3.6.2.

3.4. **Cryptage**

Lorsqu'il est indispensable de préserver la confidentialité des données qui doivent être extraites d'un fichier, ce dernier est repéré comme étant «Codé». Le cryptage s'opère à l'aide d'une messagerie sécurisée (cf. appendice 11).

3.5. **Vue d'ensemble des commandes et codes d'erreur**

Les commandes et la structure des fichiers découlent de la norme ISO/CEI 7816-4 et sont conformes à ses dispositions.

Les paires commande/réponse UDPA qui suivent font l'objet d'une description détaillée dans ce paragraphe:

Commande	INS
SELECT FILE	A4
READ BINARY	B0
UPDATE BINARY	D6
GET CHALLENGE	84
VERIFY	20
GET RESPONSE	C0
PERFORM SECURITY OPERATION: VERIFY CERTIFICATE COMPUTE DIGITAL SIGNATURE VERIFY DIGITAL SIGNATURE HASH	2A
INTERNAL AUTHENTICATE	88
EXTERNAL AUTHENTICATE	82
MANAGE SECURITY ENVIRONMENT:	22

▼**M1**

Commande	INS
SETTING A KEY	
PERFORM HASH OF FILE	2A

Les mots d'état ME1 et ME2 accompagnent tout message de réponse. Ils indiquent l'état de traitement de la commande correspondante.

ME1	ME2	Signification
90	00	Traitement normal
61	XX	Traitement normal. XX = nombre d'octets de réponse disponibles
62	81	Traitement d'avertissement. XX = nombre d'octets de réponse disponibles
63	CX	IVT erronées (NIP). Compteur de tentatives restantes assuré par 'X'
64	00	Erreur d'exécution. État de la mémoire rémanente inchangé. Erreur d'intégrité.
65	00	Erreur d'exécution. État de la mémoire rémanente changé
65	81	Erreur d'exécution. État de la mémoire rémanente changé. Défaillance de la mémoire
66	88	Erreur de sécurité: Total de contrôle cryptographique erroné (en cours de messagerie sécurisée) Certificat erroné (pendant la vérification du certificat) Cryptogramme erroné (pendant l'authentification externe) Signature erronée (pendant la vérification de la signature)
67	00	Longueur erronée (Lc ou Le erronée)
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 de FE actif)
69	87	Absence des objets informatifs MS prévus
69	88	Objets informatifs MS incorrects
6A	82	Fichier introuvable
6A	86	Paramètres P1-P2 erronés
6A	88	Données désignées introuvables
6B	00	Paramètres erronés (déplacement hors du FE)
6C	XX	Longueur erronée, le ME2 indique la longueur exacte. Aucune zone de données n'est renvoyée
6D	00	Code d'instruction incompatible ou incorrect

▼**M1**

ME1	ME2	Signification
6E	00	Classe incompatible
6F	00	Autres erreurs de contrôle

3.6. **Description des commandes**

Les commandes obligatoires auxquelles doivent réagir les cartes tachygraphiques font l'objet d'une description détaillée dans ce chapitre.

L'appendice 11 (Mécanismes de sécurité communs) constitue une source d'informations pertinentes concernant les opérations cryptographiques en jeu.

Toutes les commandes sont décrites indépendamment du protocole employé (T=0 ou T=1). Les octets UDPA CLA, INS, P1, P2, Lc et Le sont toujours indiqués. Si la commande décrite peut se passer de l'octet Lc ou Le, les cellules longueur, valeur et description associées à celui-ci demeurent vides.

Si la présence des deux octets de longueur (Lc et Le) est requise, la commande décrite doit être scindée en deux parties si le PIF emploie le protocole T=0: le PIF envoie la commande décrite avec P3=Lc + données, puis il envoie une commande GET_RESPONSE (cf. paragraphe 3.6.6) avec P3=Le.

Si la présence des deux octets de longueur est requise et si Le=0 (messagerie sécurisée):

— En cas d'utilisation du protocole T=1, la carte doit répondre à Le=0 en envoyant toutes les données de sortie disponibles.

— En cas d'utilisation du protocole T=0, le PIF doit envoyer la première commande avec P3=Lc + données, la carte doit répondre (à ce Le=0 implicite) en envoyant les octets d'état ′61La′, où La correspond au nombre des octets de réponse disponibles. Ensuite, le PIF doit générer une commande GET RESPONSE avec P3=La pour procéder à la lecture des données.

3.6.1. ***Select File (sélectionner un fichier)***

Cette commande est conforme à la norme ISO/CEI 7816-4, mais elle se caractérise par un usage restreint en comparaison avec la commande analogue définie dans cette norme.

Emploi de la commande SELECT FILE:

— Sélection d'un FS d'application (sélection par nom impérative)

— Sélection d'un fichier élémentaire correspondant à l'ID de fichier présentée

3.6.1.1. *Sélection par nom (IDA)*

Cette commande permet de sélectionner un FS d'application enregistré sur la carte.

Cette commande s'exécute à partir d'un point quelconque de la structure des fichiers (après la RAR ou à tout moment).

La sélection d'une application réinitialise l'environnement de sécurité actif. Après avoir procédé à la sélection de l'application, aucune clé publique active n'est plus sélectionnée et la clé de session antérieure cesse d'être disponible pour la messagerie sécurisée. La condition d'accès AUT est également perdue.

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′00h′	
INS	1	′A4h′	
P1	1	′04h′	Sélection par nom (IDA)
P2	1	′0Ch′	Aucune réponse prévue
Lc	1	′NNh′	Nombre d'octets envoyés à la carte (longueur de l'IDA): ′06h′ pour l'application tachygraphique
#6-#(5+NN)	NN	′XX..XXh′	IDA ′FF 54 41 43 48 4F′ pour l'application tachygraphique

▼**M1**

Le système se passe de réponse à la commande SELECT FILE (Le absent en T=1 ou pas de réponse requise en T=0).

Message de réponse (pas de réponse requise)

Octet	Longueur	Valeur	Description
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si la commande aboutit, la carte renvoie l'état ′9000′.

— Si le logiciel ne parvient pas à trouver l'application correspondant à l'IDA, il renvoie l'état de traitement suivant: ′6A82′.

— En T=1, la présence de l'octet Le entraîne le renvoi de l'état ′6700′.

— En T=0, l'exigence d'une réponse après réception de la commande SELECT FILE entraîne le renvoi de l'état ′6900′.

— Si l'application sélectionnée est considérée comme altérée (une erreur d'intégrité est détectée dans les attributs du fichier), le logiciel renvoie l'état de traitement ′6400′ ou ′6581′.

3.6.1.2. *Sélection d'un fichier élémentaire au moyen de son identificateur de fichier*

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′00h′	
INS	1	′A4h′	
P1	1	′02h′	Sélection d'un FE dépendant du FS actif
P2	1	′0Ch′	Aucune réponse prévue
Lc	1	′02h′	Nombre d'octets envoyés à la carte
#6-#7	2	′XXXXh′	Identificateur de fichier

Le système se passe de réponse à la commande SELECT FILE (Le absent en T=1 ou pas de réponse requise en T=0).

Message de réponse (pas de réponse requise)

Octet	Longueur	Valeur	Description
ME 2	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si la commande aboutit, la carte renvoie l'état ′9000′.

— Si le logiciel ne parvient pas à trouver le fichier correspondant à l'identificateur de fichier, il renvoie l'état de traitement suivant: ′6A82′.

— En T=1, la présence de l'octet Le entraîne le renvoi de l'état ′6700′.

— En T=0, l'exigence d'une réponse après réception de la commande SELECT FILE entraîne le renvoi de l'état ′6900′.

— Si le fichier sélectionné est considéré comme altéré (une erreur d'intégrité est détectée dans les attributs du fichier), le logiciel renvoie l'état de traitement ′6400′ ou ′6581′.

3.6.2. ***Read Binary (lire des données)***

Cette commande est conforme à la norme ISO/CEI 7816-4, mais elle se caractérise par un usage restreint en comparaison avec la commande analogue définie dans cette norme.

La commande READ BINARY permet d'extraire les données enregistrées dans un fichier transparent.

La réponse de la carte consiste à renvoyer les données extraites, en les intégrant, le cas échéant, dans une structure de messagerie sécurisée.

Cette commande ne peut être exécutée qu'à la condition que l'état de sécurité satisfasse aux attributs de sécurité définis pour le FE et pour la fonction READ (lecture, extraction).

▼**M1**

3.6.2.1. *Commande sans messagerie sécurisée*

Cette commande permet au PIF d'extraire des données du FE sélectionné, sans recourir à aucune messagerie sécurisée.

Cette commande ne permet pas d'extraire des données d'un fichier repéré comme étant «Codé».

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′00h′	Aucune messagerie sécurisée n'est requise
INS	1	′B0h′	
P1	1	′XXh′	Décalage en octets à compter du début du fichier: octet le plus significatif
P2	1	′XXh′	Décalage en octets à compter du début du fichier: octet le moins significatif
Le	1	′XXh′	Longueur des données attendues. Nombre des octets à extraire.

Remarque: le bit 8 de l'octet P1 doit être mis à 0.

Message de réponse

Octet	Longueur	Valeur	Description
#1-#X	X	′XX..XXh′	Données extraites
SW	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si la commande aboutit, la carte renvoie l'état ′9000′.

— Si le logiciel ne parvient à sélectionner aucun FE, il renvoie l'état de traitement suivant: ′6986′.

— Si les conditions d'accès au fichier sélectionné ne sont pas remplies, l'exécution de la commande est interrompue par l'état ′6982′.

— Si le décalage n'est pas compatible avec la taille du FE (décalage > taille du FE), le logiciel renvoie l'état de traitement suivant: ′6B00′.

— Si le volume des données à extraire n'est pas compatible avec la taille du FE (décalage + Le > taille du FE) le logiciel renvoie l'état de traitement suivant: ′6700′ ou ′6Cxx′ où ′xx′ indique la longueur exacte.

— Si une erreur d'intégrité est détectée dans les attributs du fichier, la carte considère le fichier comme altéré et non récupérable, et le logieicl renvoie l'état de traitement ′6400′ ou ′6581′.

— Si une erreur d'intégrité est détectée dans les données stockées, la carte renvoie les données demandées et le logiciel renvoie l'état de traitement ′6281′.

3.6.2.2. *Commande avec messagerie sécurisée*

Cette commande permet au PIF d'extraire des données du FE sélectionné avec messagerie sécurisée afin de s'assurer de l'intégrité des données reçues et d'en préserver la confidentialité, dans l'éventualité où le FE considéré serait repéré comme étant «Codé».

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′0Ch′	Messagerie sécurisée requise
INS	1	′B0h′	INS
P1	1	′XXh′	P1 (décalage en octets offset à compter du début du fichier): octet le plus significatif
P2	1	′XXh′	P2 (décalage en octets offset à compter du début du fichier): octet le moins significatif

▼**M1**

Octet	Longueur	Valeur	Description
Lc	1	′09h′	Longueur des données d'entrée pour la messagerie sécurisée
#6	1	′97h′	T_{LE}: balise indiquant la spécification de la longueur attendue
#7	1	′01h′	L_{LE}: longueur de la longueur attendue
#8	1	′NNh′	Spécification de la longueur attendue (Le original): nombre d'octets à extraire
#9	1	′8Eh′	T_{CC}: balise indiquant le total de contrôle cryptographique
#10	1	′04h′	L_{CC}: longueur du total de contrôle cryptographique suivant
#11-#14	4	′XX..XXh′	Total de contrôle cryptographique (les 4 octets les plus significatifs)
Le	1	′00h′	En conformité avec les dispositions de la norme ISO/CEI 7816-4

Message de réponse si le FE n'est pas repéré comme étant «codé» et si le format d'entrée de la messagerie sécurisée est correct:

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	′8Eh′	T_{CC}: balise indiquant un total de contrôle cryptographique
#(3+L+NN)	1	′04h′	L_{CC}: longueur du total de contrôle cryptographique qui suit
#(4+L+NN)-#(7+L+NN)	4	′XX..XXh′	Total de contrôle cryptographique (les 4 octets les plus significatifs)
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

Message de réponse si le FE est repéré comme étant «codé» et si le format d'entrée de la messagerie sécurisée est correct:

Octet	Longueur	Valeur	Description
#1	1	′87h′	$T_{PI\ CG}$: balise indiquant des données codées (cryptogramme)
#2	L	′MMh′ ou ′81 MMh′	$L_{PI\ CG}$: longueur des données codées renvoyées (différentes du Le original de la commande en raison du remplissage). L équivaut à 2 octets si $L_{PI\ CG}$ > 127 octets
#(2+L)-#(1+L+MM)	MM	′01XX..XXh′	Données codées: cryptogramme et indicateur de remplissage

▼**M1**

Octet	Longueur	Valeur	Description
#(2+L+MM)	1	′8Eh′	T_{CC}: balise indiquant un total de contrôle cryptographique
#(3+L+MM)	1	′04h′	L_{CC}: longueur du total de contrôle cryptographique qui suit
#(4+L+MM)-#(7+L+MM)	4	′XX..XXh′	Total de contrôle cryptographique (les 4 octets les plus significatifs)
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

Les données codées renvoyées contiennent un premier octet indiquant le mode de remplissage utilisé. Pour l'application tachygraphique, l'indicateur de remplissage prend toujours la valeur ′01h′ , laquelle indique que le mode de remplissage employé est celui spécifié dans la norme ISO/CEI 7816-4 (un octet possédant la valeur ′80h′ suivi d'une série d'octets nuls: norme ISO/CEI 9797 méthode 1).

Les structures de message de réponse décrites plus haut permettent de renvoyer les états de traitement «normaux» précisés pour la commande READ BINARY sans messagerie sécurisée (cf. paragraphe 3.6.2.1).

Par ailleurs, certaines erreurs propres à la messagerie sécurisée sont susceptibles de se manifester. Dans ce cas, le logiciel se contente de renvoyer l'état de traitement concerné sans impliquer aucune structure de messagerie sécurisée:

Message de réponse si le format d'entrée de la messagerie sécurisée est incorrect

Octet	Longueur	Valeur	Description
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si aucune clé de session active n'est disponible, le logiciel renvoie l'état de traitement ′6A88′. Cet événement se produit si la clé de session n'a pas encore été générée ou si la clé de session est arrivée à expiration (dans ce cas, le PIF doit réexécuter le processus d'authentification mutuel approprié pour définir une nouvelle clé de session).

— Si certains objets informatifs attendus (comme précisé ci-avant) font défaut dans la structure de messagerie sécurisée, le logiciel renvoie l'état de traitement ′6987′: cette erreur se produit si une balise attendue manque à l'appel ou si le corps de la commande n'est pas correctement construit.

— Si certains objets informatiques sont incorrects, le logiciel renvoie l'état de traitement ′6988′: cette erreur se produit si toutes les balises requises sont présentes mais si certaines longueurs diffèrent de celles attendues.

— Si la vérification du total de contrôle cryptographique échoue, le logiciel renvoie l'état de traitement ′6688′.

3.6.3. ***Update Binary (actualisation des données)***

Cette commande est conforme à la norme ISO/CEI 7816-4, mais elle se caractérise par un usage restreint en comparaison avec la commande analogue définie dans cette norme.

Le message de commande UPDATE BINARY lance l'actualisation (effacement + enregistrement) des bits déjà présents dans un FE avec les bits que recèle la commande UDPA.

Cette commande ne peut être exécutée qu'à la condition que l'état de sécurité satisfasse aux attributs de sécurité définis pour le FE et pour la fonction UPDATE (si le contrôle d'accès de la fonction UPDATE comporte une PRO MS, il convient d'adjoindre une structure de messagerie sécurisée à cette commande).

3.6.3.1. *Commande sans messagerie sécurisée*

Cette commande permet au PIF d'enregistrer des données dans le FE sélectionné, sans que la carte s'assure de l'intégrité des données reçues. Ce mode sans détour n'est autorisé qu'à la condition que le fichier correspondant ne soit pas repéré comme étant «codé».

▼**M1**

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′00h′	Aucune messagerie sécurisée n'est requise
INS	1	′D6h′	
P1	1	′XXh′	Décalage en octets à compter du début du fichier: octet le plus significatif
P2	1	′XXh′	Décalage en octets à compter du début du fichier: octet le moins significatif
Lc	1	′NNh′	Longueur Lc des données à mettre à jour. Nombre des octets à enregistrer
#6-#(5+NN)	NN	′XX..XXh′	Données à enregistrer

Remarque: le bit 8 de l'octet P1 doit être mis à 0.

Message de réponse

Octet	Longueur	Valeur	Description
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si la commande aboutit, la carte renvoie l'état de traitement ′9000′.

— Si le logiciel ne parvient à sélectionner aucun FE, il renvoie l'état de traitement suivant: ′6986′.

— Si les conditions d'accès au fichier sélectionné ne sont pas remplies, l'exécution de la commande est interrompue par l'état ′6982′.

— Si le décalage n'est pas compatible avec la taille du FE (décalage > taille du FE), le logiciel renvoie l'état de traitement suivant: ′6B00′.

— Si le volume des données à enregistrer n'est pas compatible avec la taille du FE (décalage + Le > taille du FE) le logiciel renvoie l'état de traitement suivant: ′6700′.

— Si une erreur d'intégrité est détectée dans les attributs du fichier, la carte considère le fichier comme altéré et non récupérable, le logiciel renvoie l'état de traitement ′6400′ ou ′6500′.

— Si l'enregistrement est impossible, le logiciel renvoie l'état de traitement ′6581′.

3.6.3.2. *Commande avec messagerie sécurisée*

Cette commande permet au PIF d'enregistrer des données dans le FE sélectionné, la carte s'assurant de l'intégrité des données reçues. Comme aucune confidentialité n'est requise, les données ne sont pas codées.

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′0Ch′	Messagerie sécurisée requise
INS	1	′D6h′	INS
P1	1	′XXh′	Décalage en octets à compter du début du fichier: octet le plus significatif
P2	1	′XXh′	Décalage en octets à compter du début du fichier: octet le moins significatif
Lc	1	′XXh′	Longueur de la zone de données sécurisée
#6	1	′81h′	T_{PV}: balise indiquant la valeur des données ordinaires
#7	L	′NNh′ ou ′81 NNh′	L_{PV}: longueur des données transmises L équivaut à 2 octets si L_{PV} > 127 octets

▼**M1**

Octet	Longueur	Valeur	Description
#(7+L)-#(6+L+NN)	NN	′XX..XXh′	Valeur des données ordinaires (données à enregistrer)
#(7+L+NN)	1	′8Eh′	T_{CC}: balise indiquant un total de contrôle cryptographique
#(8+L+NN)	1	′04h′	L_{CC}: longueur du total de contrôle cryptographique suivant
#(9+L+NN)-#(12+L+NN)	4	′XX..XXh′	Total de contrôle cryptographique (les 4 octets les plus significatifs)
Le	1	′00h′	En conformité avec les dispositions de la norme ISO/CEI 7816-4

Message de réponse si le format d'entrée de la messagerie sécurisée est correct

Octet	Longueur	Valeur	Description
#1	1	′99h′	T_{SW}: balise indiquant des mots d'état (à protéger par CC)
#2	1	′02h′	L_{SW}: longueur des mots d'état renvoyés
#3-#4	2	′XXXXh′	Mots d'état (ME1, ME2)
#5	1	′8Eh′	T_{CC}: balise indiquant un total de contrôle cryptographique
#6	1	′04h′	L_{CC}: longueur du total de contrôle cryptographique suivant
#7-#10	4	′XX..XXh′	Total de contrôle cryptographique (les 4 octets les plus significatifs)
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

La structure des messages de réponse décrite plus haut permet de renvoyer les états de traitement «normaux» précisés pour la commande UPDATE BINARY sans messagerie sécurisée (cf. paragraphe 3.6.3.1).

Par ailleurs, certaines erreurs propres à la messagerie sécurisée sont susceptibles de se manifester. Dans ce cas, le logiciel se contente de renvoyer l'état de traitement concerné sans impliquer aucune structure de messagerie sécurisée:

Message de réponse en cas d'erreur affectant la messagerie sécurisée

Octet	Longueur	Valeur	Description
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si aucune clé de session active n'est disponible, le logiciel renvoie l'état de traitement ′6A88′.

— Si certains objets informatifs attendus (comme précisé ci-avant) font défaut dans la structure de messagerie sécurisée, le logiciel renvoie l'état de traitement ′6987′ : cette erreur se produit si une balise attendue manque à l'appel ou si le corps de la commande n'est pas correctement construit.

— Si certains objets informatifs sont incorrects, le logiciel renvoie l'état de traitement ′6988′ : cette erreur se produit si toutes les balises requises sont présentes mais si certaines longueurs diffèrent de celles attendues.

— Si la vérification du total de contrôle cryptographique échoue, le logiciel renvoie l'état de traitement ′6688′.

3.6.4. ***Get Challenge (obtenir un challenge)***

Cette commande est conforme à la norme ISO/CEI 7816-4, mais elle se caractérise par un usage restreint en comparaison avec la commande analogue définie dans cette norme.

▼**M1**

La commande GET CHALLENGE demande à la carte d'émettre un challenge afin de l'utiliser dans le cadre d'une procédure liée à la sécurité et comportant l'envoi d'un cryptogramme ou de données codées à la carte.

Le challenge émis par la carte n'est valable que pour la prochaine commande (laquelle a recours à un challenge) envoyée à la carte.

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′00h′	CLA
INS	1	′84h′	INS
P1	1	′00h′	P1
P2	1	′00h′	P2
Le	1	′08h′	Le (longueur du challenge attendu)

Message de réponse

Octet	Longueur	Valeur	Description
#1-#8	8	′XX..XXh′	Challenge
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si la commande aboutit, la carte renvoie l'état de traitement ′9000′.

— Si l'octet Le diffère de ′08h′, le logiciel renvoie l'état de traitement suivant: ′6700′.

— Si les paramètres P1-P2 sont incorrects, le logiciel renvoie l'état de traitement suivant: ′6A86′.

3.6.5. ***Verify (contrôle)***

Cette commande est conforme à la norme ISO/CEI 7816-4, mais elle se caractérise par un usage restreint en comparaison avec la commande analogue définie dans cette norme.

La commande VERIFY lance, au niveau de la carte, la comparaison entre les données IVT (NIP) envoyées et les données IVT de référence enregistrées dans la mémoire de la carte.

Remarque: le PIF doit compléter à droite par une série d'octets ′FFh′ le NIP entré par l'utilisateur jusqu'à ce que ce numéro atteigne une longueur de 8 octets.

Si la commande aboutit, les droits correspondant à la présentation des données IVT sont ouverts et le compteur de tentatives IVT restantes est réinitialisé.

Tout échec de la comparaison entreprise donne lieu à l'enregistrement de données sur la carte dans le but de limiter le nombre des tentatives ultérieures d'utilisation des données IVT de référence.

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′00h′	CLA
INS	1	′20h′	INS
P1	1	′00h′	P1
P2	1	′00h′	P2 (les IVT vérifiées sont implicitement connues)
Lc	1	′08h′	Longueur du code IVT transmis
#6-#13	8	′XX..XXh′	IVT

▼**M1**

Message de réponse

Octet	Longueur	Valeur	Description
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si la commande aboutit, la carte renvoie l'état de traitement ′9000′.

— Si les IVT de référence sont introuvables, le logiciel renvoie l'état de traitement ′6A88′.

— Si les IVT sont bloquées (le compteur de tentatives IVT restantes est nul), le logiciel renvoie l'état de traitement ′6983′. Une fois dans cet état, les IVT ne pourront jamais plus être présentées avec succès.

— Si la comparaison échoue, le compteur de tentatives restantes est décrémenté et le logiciel renvoie l'état ′63CX′ (X > 0 et X correspond au compteur de tentatives IVT restantes. Si X = ′F′, le compteur de tentatives ITV est supérieur à ′F′).

— Si les IVT de référence sont considérées comme altérées, le logiciel renvoie l'état de traitement ′6400′ ou ′6581′.

3.6.6. ***Get Response (obtenir une réponse)***

Cette commande est conforme à la norme ISO/CEI 7816-4.

Cette commande (exclusivement indispensable et disponible pour le protocole T=0) permet d'assurer la transmission de données préparées entre la carte et le périphérique d'interface (cas où une commande aura inclus les deux octets Lc et Le).

La commande GET_RESPONSE doit être émise immédiatement après la commande de préparation des données, sinon la perte de ces dernières est inévitable. Après exécution de la commande GET_RESPONSE (sauf si l'erreur ′61xx′ ou ′6Cxx′ s'est manifestée, cf. ci-après), les données préalablement préparées cessent d'être disponibles.

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′00h′	
INS	1	′C0h′	
P1	1	′00h′	
P2	1	′00h′	
Le	1	′XXh′	Nombre d'octets attendus

Message de réponse

Octet	Longueur	Valeur	Description
#1-#X	X	′XX..XXh′	Données
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si la commande aboutit, la carte renvoie l'état de traitement ′9000′.

— Si la carte n'a préparé aucune donnée, elle renvoie l'état de traitement ′6900′ ou ′6F00′.

— Si l'octet Le dépasse le nombre d'octets disponibles ou si cet octet est nul, le logiciel renvoie l'état de traitement ′6Cxx′, les caractères ′xx′ indiquant le nombre exact d'octets disponibles. Dans ce cas, les données préparées demeurent disponibles pour l'exécution d'une commande GET_RESPONSE ultérieure.

— Si l'octet Le véhicule une valeur non nulle inférieure au nombre des octets disponibles, la carte procède normalement à l'envoi des données requises et elle renvoie l'état de traitement ′61xx′, dans lequel ′xx′ indique un nombre d'octets supplémentaires encore disponibles pour l'exécution d'une commande GET_RESPONSE ultérieure.

— Si la commande n'est pas prise en charge (protocole T=1), la carte renvoie l'état de traitement ′6D00′.

▼M1

3.6.7. ***PSO: Verify Certificate (contrôle de validité)***

Cette commande est conforme à la norme ISO/CEI 7816-8, mais elle se caractérise par un usage restreint en comparaison avec la commande analogue définie dans cette norme.

La carte se sert de la commande VERIFY CERTIFICATE pour obtenir une clé publique provenant du monde extérieur et pour en contrôler la validité.

Lorsqu'une commande VERIFY CERTIFICATE aboutit, la clé publique correspondante est mémorisée dans l'environnement de sécurité, aux fins d'utilisation ultérieure. Cette clé doit être explicitement configurée pour être utilisée, dans le cadre de commandes touchant à la sécurité (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE ou VERIFY CERTIFICATE), par la commande MSE (cf. paragraphe 3.6.10) en usant de son identificateur de clé.

En tout état de cause, la commande VERIFY CERTIFICATE se sert de la clé publique préalablement sélectionnée par la commande MSE pour ouvrir le certificat. Cette clé publique doit être celle d'un État membre ou de l'Europe.

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′00h′	CLA
INS	1	′2Ah′	Exécution d'une opération de sécurité
P1	1	′00h′	P1
P2	1	′AEh′	P2: données codées non BER-TLV (concaténation d'éléments d'information)
Lc	1	′CEh′	Lc: Longueur du certificat, 194 octets
#6-#199	194	′XX..XXh′	Certificat: concaténation d'éléments d'information (conformément à la description fournie dans l'appendice 11)

Message de réponse

Octet	Longueur	Valeur	Description
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si la commande aboutit, la carte renvoie l'état de traitement ′9000′.

— Si la vérification du certificat échoue, le logiciel renvoie l'état de traitement ′6688′. Le processus de vérification et de dévoilement du certificat fait l'objet d'une description détaillée à l'appendice 11.

— Si aucune clé publique n'est présente dans l'environnement de sécurité, le logiciel renvoie l'état de traitement ′6A88′.

— Si la clé publique sélectionnée (et utilisée pour dévoiler le certificat) est considérée comme altérée, le logiciel renvoie l'état de traitement ′6400′ ou ′6581′.

— Si la clé publique sélectionnée (utilisée pour dévoiler le certificat) possède un CHA.LSB (CertificateHolderAuthorisation.equipmentType) différent de ′00′ (donc n'est pas celle d'un État membre ni de l'Europe), le logiciel renvoie l'état de traitement ′6985′.

3.6.8. ***Internal Authenticate (authentification interne)***

Cette commande est conforme à la norme ISO/CEI 7816-4.

La commande INTERNAL AUTHENTICATE permet au PIF d'authentifier la carte.

Le processus d'authentification fait l'objet d'une description détaillée à l'appendice 11. Il comprend les instructions suivantes:

La commande INTERNAL AUTHENTICATE se sert de la clé privée de la carte (implicitement sélectionnée) pour signer des données d'authentification, K1 (premier élément indiquant la concordance des clés de session) et RND1 inclus, et elle a recours à la clé publique sélectionnée (par le biais de la dernière commande MSE) pour coder la signature et constituer le jeton d'authentification (pour plus de détails, reportez-vous à l'appendice 11).

▼**M1**

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′00h′	CLA
INS	1	′88h′	INS
P1	1	′00h′	P1
P2	1	′00h′	P2
Lc	1	′10h′	Longueur des données transmises à la carte
#6-#13	8	′XX..XXh′	Challenge utilisé pour authentifier la carte
#14-#21	8	′XX..XXh′	UV.CTC (cf. appendice 11)
Le	1	′80h′	Longueur des données attendues en provenance de la carte

Message de réponse

Octet	Longueur	Valeur	Description
#1-#128	128	′XX..XXh′	Jeton d'authentification de carte (cf. appendice 11)
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si la commande aboutit, la carte renvoie l'état de traitement ′9000′.

— Si aucune clé publique n'est présente dans l'environnement de sécurité, le logiciel renvoie l'état de traitement ′6A88′.

— Si aucune clé privée n'est présente dans l'environnement de sécurité, le logiciel renvoie l'état de traitement ′6A88′.

— Si l'UV.CTC ne correspond pas à l'identificateur de clé publique actif, le logiciel renvoie l'état de traitement ′6A88′.

— Si la clé privée sélectionnée est considérée comme altérée, le logiciel renvoie l'état de traitement ′6400′ ou ′6581′.

Si la commande INTERNAL_AUTHENTICATE aboutit, la clé de session active, pour autant qu'elle existe, est effacée et cesse d'être disponible. Pour disposer d'une nouvelle clé de session, il convient d'exécuter avec succès la commande EXTERNAL_AUTHENTICATE.

3.6.9. ***External Authenticate (authentification externe)***

Cette commande est conforme à la norme ISO/CEI 7816-4.

La commande EXTERNAL AUTHENTICATE permet à la carte d'authentifier le PIF.

Le processus d'authentification fait l'objet d'une description détaillée à l'appendice 11. Il comprend les instructions suivantes:

Il faut qu'une commande GET CHALLENGE précède immédiatement la commande EXTERNAL_AUTHENTICATE. La carte émet un challenge vers le monde extérieur (RND3).

La fonction de vérification du cryptogramme se sert du challenge RND3 (émis par la carte), de la clé privée de la carte (implicitement sélectionnée) et de la clé publique préalablement sélectionnée par le biais de la commande MSE.

La carte vérifie le cryptogramme; s'il est correct, la condition d'accès AUT est ouverte.

Le cryptogramme d'entrée véhicule le second élément K2 indiquant la concordance des clés de session.

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′00h′	CLA
INS	1	′82h′	INS

▼**M1**

Octet	Longueur	Valeur	Description
P1	1	′00h′	P1
P2	1	′00h′	P2 (la clé publique à utiliser est implicitement connue; elle a été préalablement sélectionnée par la commande MSE)
Lc	1	′80h′	Lc (longueur des données envoyées à la carte)
#6-#133	128	′XX..XXh′	Cryptogramme (cf. appendice 11)

Message de réponse

Octet	Longueur	Valeur	Description
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si la commande aboutit, la carte renvoie l'état de traitement ′9000′.

— Si aucune clé publique n'est présente dans l'environnement de sécurité, le logiciel renvoie l'état de traitement ′6A88′.

— Si l'ATC de la Cl2 publique sélectionnée ne correspond pas à la concaténation de l'IDA de l'application tachygraphique et d'un type d'UV, le logiciel renvoie l'état de traitement ′6F00′ (cf. appendice 11).

— Si aucune clé privée n'est présente dans l'environnement de sécurité, le logiciel renvoie l'état de traitement ′6A88′.

— Si la vérification du cryptogramme est erronée, le logiciel renvoie l'état de traitement ′6688′.

— Si la commande n'est pas immédiatement précédée par une commande GET CHALLENGE, le logiciel renvoie l'état de traitement ′6985′.

— Si la clé privée sélectionnée est considérée comme altérée, le logiciel renvoie l'état de traitement ′6400′ ou ′6581′.

Si la commande EXTERNAL AUTHENTICATE aboutit et si la première partie de la clé de session est disponible consécutivement à la réussite d'une commande INTERNAL AUTHENTICATE récemment exécutée, la clé de session est prête pour l'exécution de futures commandes recourant à la messagerie sécurisée.

Si la première partie de la clé de session n'est pas disponible en dépit de l'exécution d'une commande INTERNAL AUTHENTICATE, la seconde partie de cette clé de session, envoyée par le PIF, ne sera pas enregistrée dans la mémoire de la carte. Ce mécanisme permet de garantir que le déroulement du processus d'authentification mutuelle respecte l'ordre précisé dans l'Appendice 11.

3.6.10. ***Manage Security Environment (gestion de l'environnement de sécurité)***

Cette commande permet de définir une clé publique aux fins d'authentification.

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

La clé désignée dans la zone de données MSE s'applique à tous les fichiers du FS d'application tachygraphique.

La clé désignée dans la zone de données MSE demeure la clé publique active jusqu'à la prochaine commande MSE correcte.

Si la clé mentionnée n'est pas (encore) présente dans la mémoire de la carte, l'environnement de sécurité demeure inchangé.

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′00h′	CLA
INS	1	′22h′	INS
P1	1	′C1h′	P1: clé mentionnée valable pour l'ensemble des opérations cryptographiques
P2	1	′B6h′	P2 (données mentionnées concernant la signature numérique)

▼**M1**

Octet	Longueur	Valeur	Description
Lc	1	′0Ah′	Lc: longueur de la zone de données subséquente
#6	1	′83h′	Balise indiquant une clé publique en cas d'asymétrie
#7	1	′08h′	Longueur de la référence (identificateur de clé)
#8-#15	08h	′XX..XXh′	Identificateur de clé conforme aux dispositions énoncées à l'appendice 11

Message de réponse

Octet	Longueur	Valeur	Description
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si la commande aboutit, la carte renvoie l'état de traitement ′9000′.

— Si la clé mentionnée n'est pas présente dans la mémoire de la carte, le logiciel renvoie l'état de traitement ′6A88′.

— Si certains objets informatifs attendus font défaut dans la structure de messagerie sécurisée, le logiciel renvoie l'état de traitement ′6987′ Cet événement est susceptible de se produire si la balise ′83h′ manque à l'appel.

— Si certains objets informatifs sont incorrects, le logiciel renvoie l'état de traitement ′6988′. Cet événement est susceptible de se produire si la longueur de l'identificateur de clé ne correspond pas à ′08h′.

— Si la clé sélectionnée est considérée comme altérée, le logiciel renvoie l'état de traitement ′6400′ ou ′6581′.

3.6.11. ***PSO: Hash (hachage)***

Cette commande permet de transférer vers la carte le résultat du calcul de hachage auquel certaines données pourraient être soumises. Cette commande s'emploie lors de la vérification de signatures numériques. La valeur de hachage est enregistrée dans une mémoire morte effaçable programmable électriquement (EEPROM) en vue de la prochaine commande de vérification de signatures numériques.

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

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′00h′	CLA
INS	1	′2Ah′	Exécution d'une opération de sécurité
P1	1	′90h′	Renvoi d'un code de hachage
P2	1	′A0h′	Balise: zone de données contenant les DO appropriés pour le hachage
Lc	1	′16h′	Longueur Lc de la zone de données ultérieure
#6	1	′90h′	Balise indiquant le code de hachage
#7	1	′14h′	Longueur du code de hachage
#8-#27	20	′XX..XXh′	Code de hachage

Message de réponse

Octet	Longueur	Valeur	Description
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si la commande aboutit, la carte renvoie l'état de traitement ′9000′.

▼M1

— Si certains objets informatifs attendus font défaut, le logiciel renvoie l'état de traitement ′6987′. Cet événement est susceptible de se produire si l'une des balises ′90h′ manque à l'appel.

— Si certains objets informatifs sont incorrects, le logiciel renvoie l'état de traitement ′6988′. Cette erreur est susceptible de se manifester si la balise requise est présente mais si sa longueur diffère de ′14h′.

3.6.12. ***Perform Hash of File (hachage d'un fichier)***

Cette commande n'est pas conforme à la norme ISO/CEI 7816-8. Par conséquent, l'octet CLA de cette commande indique un usage exclusif de la commande PERFORM SECURITY OPERATION/HASH.

La commande PERFORM HASH OF FILE s'utilise pour hacher la zone de données du FE transparent sélectionné.

Le résultat de l'opération de hachage est enregistré dans la mémoire de la carte. Par la suite, son utilisation permettra d'obtenir une signature numérique du fichier en recourant à la commande PSO: COMPUTE_DIGITAL_SIGNATURE. Ce résultat demeure disponible pour la commande COMPUTE DIGITAL SIGNATURE jusqu'à l'exécution réussie d'une prochaine commande PERFORM HASH OF FILE.

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′80h′	CLA
INS	1	′2Ah′	Exécution d'une opération de sécurité
P1	1	′90h′	Balise: hachage
P2	1	′00h′	P2: hachage des données enregistrées dans le fichier transparent sélectionné

Message de réponse

Octet	Longueur	Valeur	Description
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si la commande aboutit, la carte renvoie l'état de traitement ′9000′.

— Si aucune application n'est sélectionnée, le logiciel renvoie l'état de traitement ′6985′.

— Si le FE sélectionné est considéré comme altéré (erreurs d'intégrité sur les attributs du fichier ou les données stockées), le logiciel renvoie l'état de traitement ′6400′ ou ′6581′.

— Si le fichier sélectionné n'est pas un fichier transparent, le logiciel renvoie un état de traitement ′6986′.

3.6.13. ***PSO: Compute Digital Signature (calcul de la signature numérique)***

Cette commande permet de calculer la signature numérique du code de hachage préalablement calculé (cf. commande PERFORM HASH OF FILE, paragraphe 3.6.12).

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

La clé privée de la carte permet de calculer la signature numérique. La carte connaît implicitement cette clé.

La carte exécute une signature numérique en recourant à une méthode de remplissage conforme à la norme PKCS1 (pour plus de détails, il convient de se référer à l'appendice 11).

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′00h′	CLA
INS	1	′2Ah′	Exécution d'une opération de sécurité
P1	1	′9Eh′	Signature numérique à renvoyer

▼**M1**

Octet	Longueur	Valeur	Description
P2	1	′9Ah′	Balise: zone de données contenant les données à signer. Comme aucune zone de données n'est incluse, les données sont supposées être déjà présentes sur la carte (hachage du fichier)
Le	1	′80h′	Longueur de la signature attendue

Message de réponse

Octet	Longueur	Valeur	Description
#1-#128	128	′XX..XXh′	Signature du hachage préalablement calculé
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si la commande aboutit, la carte renvoie l'état de traitement ′9000′.

— Si la clé privée implicitement sélectionnée est considérée comme altérée, le logiciel renvoie l'état de traitement ′6400′ ou ′6581′.

3.6.14. ***Verify Digital Signature (contrôle de la signature numérique)***

Cette commande permet de vérifier la signature numérique, fournie comme une entrée, en conformité avec la PKCS1 d'un message dont le hachage est connu de la carte. La carte connaît implicitement l'algorithme de signature.

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

La commande VERIFY DIGITAL SIGNATURE se sert toujours de la clé publique sélectionnée par l'intermédiaire de la précédente commande MANAGE SECURITY ENVIRONMENT et du code de hachage antérieur introduit par le biais d'une commande PSO: HASH.

Message de commande

Octet	Longueur	Valeur	Description
CLA	1	′00h′	CLA
INS	1	′2Ah′	Exécution d'une opération de sécurité
P1	1	′00h′	
P2	1	′A8h′	Balise: zone de données contenant les DO appropriés pour la vérification
Lc	1	′83h′	Longueur Lc de la zone de données subséquente
#28	1	′9Eh′	Balise indiquant une signature numérique
#29-#30	2	′8180h′	Longueur de la signature numérique (128 octets, codés conformément à la norme ISO/CEI 7816-6)
#31-#158	128	′XX..XXh′	Contenu de la signature numérique

Message de réponse

Octet	Longueur	Valeur	Description
ME	2	′XXXXh′	Mots d'état (ME1, ME2)

— Si la commande aboutit, la carte renvoie l'état de traitement ′9000′.

— Si la vérification de la signature échoue, le logiciel renvoie l'état de traitement ′6688′. Le processus de vérification fait l'objet d'une description détaillée à l'appendice 11.

— Si aucune clé publique n'est sélectionnée, le logiciel renvoie l'état de traitement ′6A88′.

▼M1

— Si certains objets informatifs attendus font défaut, le logiciel renvoie l'état de traitement ′6987′ Cet événement est susceptible de se produire si l'une des balises requises manque à l'appel.

— Si aucun code de hachage n'est disponible pour traiter la commande (en raison du traitement d'une commande PSO: HASH antérieure), le logiciel renvoie l'état de traitement ′6985′.

— Si certains objets informatifs sont incorrects, le logiciel renvoie l'état de traitement ′6988′. Cette erreur est susceptible de se manifester si la longueur de l'un des objets informatifs requis est incorrecte.

— Si la clé publique sélectionnée est considérée comme altérée, le logiciel renvoie l'état de traitement ′6400′ ou ′6581′.

4. STRUCTURE DES CARTES TACHYGRAPHIQUES

Ce paragraphe traite de la structure logique des fichiers que les cartes tachygraphiques affectent à la mémorisation des données accessibles.

Il n'apporte aucune précision quant à leur structure interne, laquelle dépend du fabricant (en-têtes de fichier par exemple). Il n'aborde pas non plus l'archivage et le traitement d'éléments d'information à usage interne tels que les EuropeanPublicKey, CardPrivateKey, TDesSessionKey ou WorkshopCardPin.

La capacité de mémoire utile des cartes tachygraphiques doit être au moins égale à 11 Ko. Rien ne s'oppose à l'emploi de capacités supérieures. En pareil cas, la structure de la carte demeure inchangée, mais le nombre de relevés de certains éléments structurels augmente. Les valeurs minimale et maximale que la numérotation de ces relevés est susceptible d'atteindre sont précisées dans ce paragraphe.

4.1. **Structure des cartes de conducteur**

Après sa personnalisation, toute carte de conducteur doit présenter la structure logique permanente et les conditions d'accès aux fichiers qui suivent:

Fichier	ID de fichier	Condition d'accès		
		Lecture	Actualisation	Cryptage
MF	3F00			
├─EF ICC	0002	TJR	JAM	Non
├─EF IC	0005	TJR	JAM	Non
└─DF Tachograph	0500			
├─EF Application_Identification	0501	TJR	JAM	Non
├─EF Card_Certificate	C100	TJR	JAM	Non
├─EF CA_Certificate	C108	TJR	JAM	Non
├─EF Identification	0520	TJR	JAM	Non
├─EF Card_Download	050E	TJR	TJR	Non
├─EF Driving_Licence_Info	0521	TJR	JAM	Non
├─EF Events_Data	0502	TJR	PRO M5 ∣ AUT	Non
├─EF Faults_Data	0503	TJR	PRO M5 ∣ AUT	Non
├─EF Driver_Activity_Data	0504	TJR	PRO M5 ∣ AUT	Non
├─EF Vehicles_Used	0505	TJR	PRO M5 ∣ AUT	Non
├─EF Places	0506	TJR	PRO M5 ∣ AUT	Non
├─EF Current_Usage	0507	TJR	PRO M5 ∣ AUT	Non
├─EF Control_Activity_Data	0508	TJR	PRO M5 ∣ AUT	Non
└─EF Specific_Conditions	0522	TJR	PRO M5 ∣ AUT	Non

La structure de tous les FE doit être transparente.

La lecture avec messagerie sécurisée doit être envisageable pour tous les fichiers incorporés dans le fichier spécialisé Tachograph.

Toute carte de conducteur doit présenter la structure de données suivante:

▼**M1**

Fichier / Élément d'information	Nr de relevés	Taille (octets) Min.	Max.	Valeurs par défaut
MF		*11411*	*24959*	
├─EF ICC		*25*	*25*	
│ └─CardIccIdentification		*25*	*25*	
│ ├─clockStop		1	1	[00]
│ ├─cardExtendedSerialNumber		8	8	[00..00]
│ ├─cardApprovalNumber		8	8	[20..20]
│ ├─cardPersonaliserID		1	1	[00]
│ ├─embedderIcAssemblerId		5	5	[00..00]
│ └─icIdentifier		2	2	[00 00]
├─EF IC		*8*	*8*	
│ └─CardChipIdentification		*8*	*8*	
│ ├─icSerialNumber		4	4	[00..00]
│ └─icManufacturingReferences		4	4	[00..00]
└─DF Tachograph		*11378*	*24926*	
├─EF Application_Identification		*10*	*10*	
│ └─DriverCardApplicationIdentification		*10*	*10*	
│ ├─typeOfTachographCardId		1	1	[00]
│ ├─cardStructureVersion		2	2	[00 00]
│ ├─noOfEventsPerType		1	1	[00]
│ ├─noOfFaultsPerType		1	1	[00]
│ ├─activityStructureLength		2	2	[00 00]
│ ├─noOfCardVehicleRecords		2	2	[00 00]
│ └─noOfCardPlaceRecords		1	1	[00]
├─EF Card_Certificate		*194*	*194*	
│ └─CardCertificate		194	194	[00..00]
├─EF CA_Certificate		*194*	*194*	
│ └─MemberStateCertificate		194	194	[00..00]
├─EF Identification		*143*	*143*	
│ ├─CardIdentification		65	65	
│ │ ├─cardIssuingMemberState		1	1	[00]
│ │ ├─cardNumber		16	16	[20..20]
│ │ ├─cardIssuingAuthorityName		36	36	[20..20]
│ │ ├─cardIssueDate		4	4	[00..00]
│ │ ├─cardValidityBegin		4	4	[00..00]
│ │ └─cardExpiryDate		4	4	[00..00]
│ └─DriverCardHolderIdentification		78	78	
│ ├─cardHolderName		72	72	
│ │ ├─holderSurname		36	36	[00, 20..20]
│ │ └─holderFirstNames		36	36	[00, 20..20]
│ ├─cardHolderBirthDate		4	4	[00..00]
│ └─cardHolderPreferredLanguage		2	2	[20 20]

▼**M1**

EF Card_Download		4	4	
LastCardDownload		4	4	
EF Driving_Licence_Info		53	53	
CardDrivingLicenceInformation		53	53	
drivingLicenceIssuingAuthority		36	36	(00, 20..20)
drivingLicenceIssuingNation		1	1	(00)
drivingLicenceNumber		16	16	(20..20)
EF Events_Data		864	1728	
CardEventData		864	1728	
cardEventRecords	6	144	288	
CardEventRecord	n_1	24	24	
eventType		1	1	(00)
eventBeginTime		4	4	(00..00)
eventEndTime		4	4	(00..00)
eventVehicleRegistration				
vehicleRegistrationNation		1	1	(00)
vehicleRegistrationNumber		14	14	(00, 20..20)
EF Faults_Data		576	1152	
CardFaultData		576	1152	
cardFaultRecords	2	288	576	
CardFaultRecord	n_2	24	24	
faultType		1	1	(00)
faultBeginTime		4	4	(00..00)
faultEndTime		4	4	(00..00)
faultVehicleRegistration				
vehicleRegistrationNation		1	1	(00)
vehicleRegistrationNumber		14	14	(00, 20..20)
EF Driver_Activity_Data		5548	13780	
CardDriverActivity		5548	13780	
activityPointerOldestDayRecord		2	2	(00 00)
activityPointerNewestRecord		2	2	(00 00)
activityDailyRecords	n_4	5544	13776	(00..00)
EF Vehicles_Used		2606	6202	
CardVehiclesUsed		2606	6202	
vehiclePointerNewestRecord		2	2	(00 00)
cardVehicleRecords		2604	6200	
CardVehicleRecord	n_3	31	31	
vehicleOdometerBegin		3	3	(00..00)
vehicleOdometerEnd		3	3	(00..00)
vehicleFirstUse		4	4	(00..00)
vehicleLastUse		4	4	(00..00)
vehicleRegistration				
vehicleRegistrationNation		1	1	(00)
vehicleRegistrationNumber		14	14	(00, 20..20)
vuDataBlockCounter		2	2	(00 00)
EF Places		841	1121	
CardPlaceDailyWorkPeriod		841	1121	
placePointerNewestRecord		1	1	(00)
placeRecords		840	1120	
PlaceRecord	n_5	10	10	
entryTime		4	4	(00..00)
entryTypeDailyWorkPeriod		1	1	(00)
dailyWorkPeriodCountry		1	1	(00)
dailyWorkPeriodRegion		1	1	(00)
vehicleOdometerValue		3	3	(00..00)
EF Current_Usage		19	19	
CardCurrentUse		19	19	
sessionOpenTime		4	4	(00..00)
sessionOpenVehicle				
vehicleRegistrationNation		1	1	(00)
vehicleRegistrationNumber		14	14	(00, 20..20)
EF Control_Activity_Data		46	46	
CardControlActivityDataRecord		46	46	
controlType		1	1	(00)
controlTime		4	4	(00..00)
controlCardNumber				
cardType		1	1	(00)
cardIssuingMemberState		1	1	(00)
cardNumber		16	16	(20..20)
controlVehicleRegistration				
vehicleRegistrationNation		1	1	(00)
vehicleRegistrationNumber		14	14	(00, 20..20)
controlDownloadPeriodBegin		4	4	(00..00)
controlDownloadPeriodEnd		4	4	(00..00)
EF Specific_Conditions		280	280	
SpecificConditionRecord	56	5	5	
entryTime		4	4	(00..00)
SpecificConditionType		1	1	(00)

Employées pour indiquer des tailles dans la table ci-avant, les valeurs qui suivent correspondent aux nombres minimal et maximal de relevés que la structure de données d'une carte de conducteur doit respecter:

▼**M1**

		Min.	Max.
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 octets (28 jours * 93 chang. d'activité)	13 776 octets (28 jours * 240 chang. d'activité)

4.2. **Structure des cartes d'atelier**

Après sa personnalisation, toute carte d'atelier doit présenter la structure logique permanente et les conditions d'accès aux fichiers qui suivent:

Fichier	ID de fichier	Condition d'accès		
		Lecture	Actualisation	Cryptage
MF	3F00			
├─EF ICC	0002	T|R	JAM	Non
├─EF IC	0005	T|R	JAM	Non
└─DF Tachograph	0500			
├─EF Application_Identification	0501	T|R	JAM	Non
├─EF Card_Certificate	C100	T|R	JAM	Non
├─EF CA_Certificate	C108	T|R	JAM	Non
├─EF Identification	0520	T|R	JAM	Non
├─EF Card_Download	0509	T|R	T|R	Non
├─EF Calibration	050A	T|R	PRO MS | AUT	Non
├─EF Sensor_Installation_Data	050B	T|R	JAM	Oui
├─EF Events_Data	0502	T|R	PRO MS | AUT	Non
├─EF Faults_Data	0503	T|R	PRO MS | AUT	Non
├─EF Driver_Activity_Data	0504	T|R	PRO MS | AUT	Non
├─EF Vehicles_Used	0505	T|R	PRO MS | AUT	Non
├─EF Places	0506	T|R	PRO MS | AUT	Non
├─EF Current_Usage	0507	T|R	PRO MS | AUT	Non
├─EF Control_Activity_Data	0508	T|R	PRO MS | AUT	Non
└─EF Specific_Conditions	0522	T|R	PRO MS | AUT	Non

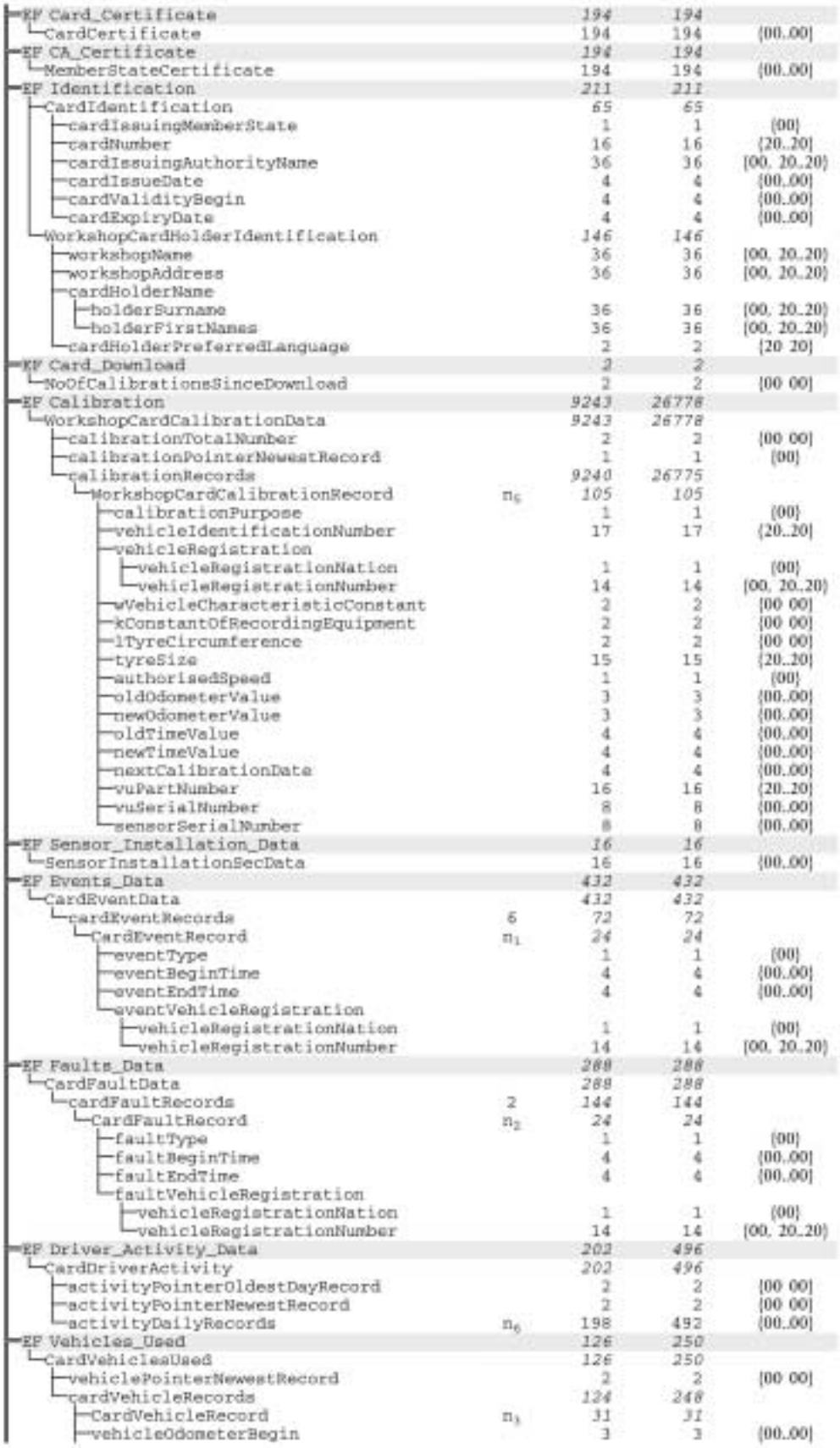
La structure de tous les FE doit être transparente.

La lecture avec messagerie sécurisée doit être envisageable pour tous les fichiers incorporés dans le fichier spécialisé Tachograph.

Toute carte d'atelier doit présenter la structure de données suivante:

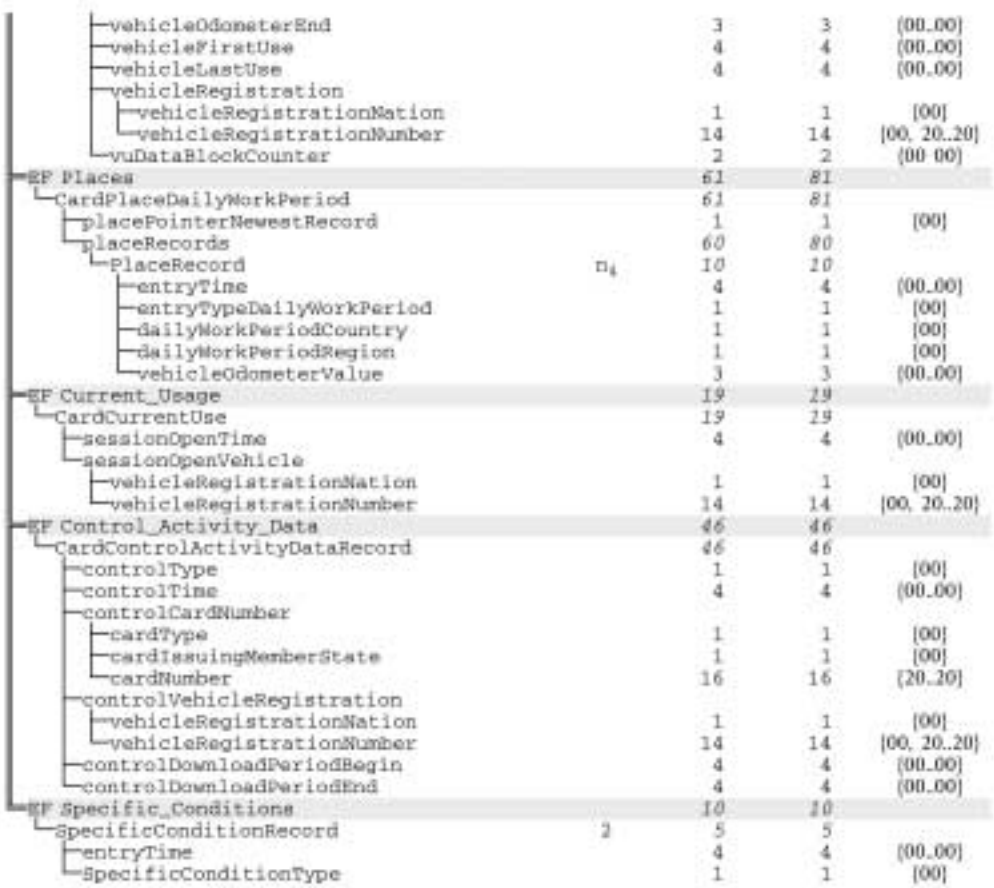
Fichier|Élément d'information	Nb de relevés	Taille (octets) Min.	Taille (octets) Max.	Valeurs par défaut
MF		*11088*	*29061*	
├─EF ICC		*25*	*25*	
│ └─CardIccIdentification		*25*	*25*	
│ ├─clockStop		1	1	{00}
│ ├─cardExtendedSerialNumber		8	8	{00..00}
│ ├─cardApprovalNumber		8	8	{20..20}
│ ├─cardPersonaliserID		1	1	{00}
│ ├─embedderIcAssemblerId		5	5	{00..00}
│ └─icIdentifier		2	2	{00 00}
├─EF IC		*8*	*8*	
│ └─CardChipIdentification		*8*	*8*	
│ ├─icSerialNumber		4	4	{00..00}
│ └─icManufacturingReferences		4	4	{00..00}
└─DF Tachograph		*11055*	*29028*	
├─EF Application_Identification		*11*	*11*	
│ └─WorkshopCardApplicationIdentification		*11*	*11*	
│ ├─typeOfTachographCardId		1	1	{00}
│ ├─cardStructureVersion		2	2	{00 00}
│ ├─noOfEventsPerType		1	1	{00}
│ ├─noOfFaultsPerType		1	1	{00}
│ ├─activityStructureLength		2	2	{00 00}
│ ├─noOfCardVehicleRecords		2	2	{00 00}
│ ├─noOfCardPlaceRecords		1	1	{00}
│ └─noOfCalibrationRecords		1	1	{00}

▼**M1**



EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	(00..00)
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	(00..00)
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	(00)
cardNumber		16	16	(20..20)
cardIssuingAuthorityName		36	36	(00, 20..20)
cardIssueDate		4	4	(00..00)
cardValidityBegin		4	4	(00..00)
cardExpiryDate		4	4	(00..00)
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	(00, 20..20)
workshopAddress		36	36	(00, 20..20)
cardHolderName				
holderSurname		36	36	(00, 20..20)
holderFirstNames		36	36	(00, 20..20)
cardHolderPreferredLanguage		2	2	(20 20)
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	(00 00)
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	(00 00)
calibrationPointerNewestRecord		1	1	(00)
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_6	*105*	*105*	
calibrationPurpose		1	1	(00)
vehicleIdentificationNumber		17	17	(20..20)
vehicleRegistration				
vehicleRegistrationNation		1	1	(00)
vehicleRegistrationNumber		14	14	(00, 20..20)
wVehicleCharacteristicConstant		2	2	(00 00)
kConstantOfRecordingEquipment		2	2	(00 00)
lTyreCircumference		2	2	(00 00)
tyreSize		15	15	(20..20)
authorisedSpeed		1	1	(00)
oldOdometerValue		3	3	(00..00)
newOdometerValue		3	3	(00..00)
oldTimeValue		4	4	(00..00)
newTimeValue		4	4	(00..00)
nextCalibrationDate		4	4	(00..00)
vuPartNumber		16	16	(20..20)
vuSerialNumber		8	8	(00..00)
sensorSerialNumber		8	8	(00..00)
EF Sensor_Installation_Data		*16*	*16*	
SensorInstallationSecData		16	16	(00..00)
EF Events_Data		*432*	*432*	
CardEventData		*432*	*432*	
cardEventRecords	6	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	(00)
eventBeginTime		4	4	(00..00)
eventEndTime		4	4	(00..00)
eventVehicleRegistration				
vehicleRegistrationNation		1	1	(00)
vehicleRegistrationNumber		14	14	(00, 20..20)
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	(00)
faultBeginTime		4	4	(00..00)
faultEndTime		4	4	(00..00)
faultVehicleRegistration				
vehicleRegistrationNation		1	1	(00)
vehicleRegistrationNumber		14	14	(00, 20..20)
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	(00 00)
activityPointerNewestRecord		2	2	(00 00)
activityDailyRecords	n_6	198	492	(00..00)
EF Vehicles_Used		*126*	*250*	
CardVehiclesUsed		*126*	*250*	
vehiclePointerNewestRecord		2	2	(00 00)
cardVehicleRecords		*124*	*248*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	(00..00)

▼**M1**



├─vehicleOdometerEnd		3	3	[00..00]
├─vehicleFirstUse		4	4	[00..00]
├─vehicleLastUse		4	4	[00..00]
├─vehicleRegistration				
│ ├─vehicleRegistrationNation		1	1	[00]
│ └─vehicleRegistrationNumber		14	14	[00, 20..20]
└─vuDataBlockCounter		2	2	[00 00]
EF Places		61	81	
└─CardPlaceDailyWorkPeriod		61	81	
├─placePointerNewestRecord		1	1	[00]
└─placeRecords		60	80	
└─PlaceRecord	n_4	10	10	
├─entryTime		4	4	[00..00]
├─entryTypeDailyWorkPeriod		1	1	[00]
├─dailyWorkPeriodCountry		1	1	[00]
├─dailyWorkPeriodRegion		1	1	[00]
└─vehicleOdometerValue		3	3	[00..00]
EF Current_Usage		19	19	
└─CardCurrentUse		19	19	
├─sessionOpenTime		4	4	[00..00]
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	[00]
└─vehicleRegistrationNumber		14	14	[00, 20..20]
EF Control_Activity_Data		46	46	
└─CardControlActivityDataRecord		46	46	
├─controlType		1	1	[00]
├─controlTime		4	4	[00..00]
├─controlCardNumber				
│ ├─cardType		1	1	[00]
│ ├─cardIssuingMemberState		1	1	[00]
│ └─cardNumber		16	16	[20..20]
├─controlVehicleRegistration				
│ ├─vehicleRegistrationNation		1	1	[00]
│ └─vehicleRegistrationNumber		14	14	[00, 20..20]
├─controlDownloadPeriodBegin		4	4	[00..00]
└─controlDownloadPeriodEnd		4	4	[00..00]
EF Specific_Conditions		10	10	
└─SpecificConditionRecord	2	5	5	
├─entryTime		4	4	[00..00]
└─SpecificConditionType		1	1	[00]

Employées pour indiquer des tailles dans la table ci-avant, les valeurs qui suivent correspondent aux nombres minimal et maximal de relevés que la structure de données d'une carte d'atelier se doit de respecter:

		Min.	Max.
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 octets (1 jour * 93 chang. d'activité)	492 octets (1 jour * 240 chang. d'activité)

▼**M1**

4.3. **Structure des cartes de contrôleur**

Après sa personnalisation, toute carte de contrôleur doit présenter la structure logique permanente et les conditions d'accès aux fichiers qui suivent:

Fichier	ID de fichier	Condition d'accès		
		Lecture	Actualisation	Cryptage
MF	3F00			
├─EF ICC	0002	T/R	JAM	Non
├─EF IC	0005	T/R	JAM	Non
└─DF Tachograph	0500			
├─EF Application_Identification	0501	T/R	JAM	Non
├─EF Card_Certificate	C100	T/R	JAM	Non
├─EF CA_Certificate	C108	T/R	JAM	Non
├─EF Identification	0520	AUT	JAM	Non
└─EF Controller_Activity_Data	050C	T/R	PRO MS / AUT	Non

La structure de tous les FE doit être transparente.

La lecture avec messagerie sécurisée doit être envisageable pour tous les fichiers incorporés dans le fichier spécialisé Tachograph.

Toute carte de contrôleur doit présenter la structure de données suivante:

Fichier/Élément d'information	Nb de relevés	Taille (octets)		Valeurs par défaut
		Min.	Max.	
MF		*11219*	*24559*	
├─EF ICC		*25*	*25*	
│ └─CardIccIdentification		*25*	*25*	
│ ├─clockStop		1	1	(00)
│ ├─cardExtendedSerialNumber		8	8	(00..00)
│ ├─cardApprovalNumber		8	8	(20..20)
│ ├─cardPersonaliserID		1	1	(00)
│ ├─embedderIcAssemblerId		5	5	(00..00)
│ └─icIdentifier		2	2	(00 00)
├─EF IC		*8*	*8*	
│ └─CardChipIdentification		*8*	*8*	
│ ├─icSerialNumber		4	4	(00..00)
│ └─icManufacturingReferences		4	4	(00..00)
└─DF Tachograph		*11186*	*24526*	
├─EF Application_Identification		5	5	
│ └─ControlCardApplicationIdentification		5	5	
│ ├─typeOfTachographCardId		1	1	(00)
│ ├─cardStructureVersion		2	2	(00 00)
│ └─noOfControlActivityRecords		2	2	(00 00)
├─EF Card_Certificate		*194*	*194*	
│ └─CardCertificate		194	194	(00..00)
├─EF CA_Certificate		*194*	*194*	
│ └─MemberStateCertificate		194	194	(00..00)
├─EF Identification		*211*	*211*	
│ ├─CardIdentification		*65*	*65*	
│ │ ├─cardIssuingMemberState		1	1	(00)
│ │ ├─cardNumber		16	16	(20..20)
│ │ ├─cardIssuingAuthorityName		36	36	(00, 20..20)
│ │ ├─cardIssueDate		4	4	(00..00)
│ │ ├─cardValidityBegin		4	4	(00..00)
│ │ └─cardExpiryDate		4	4	(00..00)
│ └─ControlCardHolderIdentification		*146*	*146*	
│ ├─controlBodyName		36	36	(00, 20..20)
│ ├─controlBodyAddress		36	36	(00, 20..20)
│ ├─cardHolderName				
│ │ ├─holderSurname		36	36	(00, 20..20)
│ │ └─holderFirstNames		36	36	(00, 20..20)
│ └─cardHolderPreferredLanguage		2	2	(20 20)
└─EF Controller_Activity_Data		*10582*	*23922*	
└─ControlCardControlActivityData		*10582*	*23922*	
├─controlPointerNewestRecord		2	2	(00 00)
└─controlActivityRecords		*10580*	*23920*	
└─controlActivityRecord	n_7	*46*	*46*	
├─controlType		1	1	(00)
├─controlTime		4	4	(00..00)
├─controlledCardNumber				
│ ├─cardType		1	1	(00)
│ ├─cardIssuingMemberState		1	1	(00)
│ └─cardNumber		16	16	(20..20)
├─controlledVehicleRegistration				
│ ├─vehicleRegistrationNation		1	1	(00)
│ └─vehicleRegistrationNumber		14	14	(00, 20..20)
├─controlDownloadPeriodBegin		4	4	(00..00)
└─controlDownloadPeriodEnd		4	4	(00..00)

▼**M1**

Employées pour indiquer des tailles dans la table ci-avant, les valeurs qui suivent correspondent aux nombres minimal et maximal de relevés que la structure de données d'une carte de contrôleur se doit de respecter:

		Min.	Max.
n_7	NoOfControlActivityRecords	230	520

4.4. **Structure des cartes d'entreprise**

Après sa personnalisation, toute carte d'entreprise doit présenter la structure logique permanente et les conditions d'accès aux fichiers qui suivent:

Fichier	ID de fichier	Condition d'accès: Lecture	Actualisation	Cryptage
MF	3F00			
├EF ICC	0002	TJR	JAM	Non
├EF IC	0005	TJR	JAM	Non
└DF Tachograph	0500			
├EF Application_Identification	0501	TJR	JAM	Non
├EF Card_Certificate	C100	TJR	JAM	Non
├EF CA_Certificate	C108	TJR	JAM	Non
├EF Identification	0520	AUT	JAM	Non
└EF Company_Activity_Data	050D	TJR	PRO MS ∣ AUT	Non

La structure de tous les FE doit être transparente.

La lecture avec messagerie sécurisée doit être envisageable pour tous les fichiers incorporés dans le fichier spécialisé Tachograph.

Toute carte d'entreprise doit présenter la structure de données suivante:

Fichier/Élément d'information	Nb de relevés	Taille (octets) Min.	Max.	Valeurs par défaut
MF		*11147*	*24487*	
├EF ICC		*25*	*25*	
│└CardIccIdentification		*25*	*25*	
│ ├clockStop		1	1	[00]
│ ├cardExtendedSerialNumber		8	8	[00..00]
│ ├cardApprovalNumber		8	8	[20..20]
│ ├cardPersonaliserID		1	1	[00]
│ ├embedderIcAssemblerId		5	5	[00..00]
│ └icIdentifier		2	2	[00 00]
├EF IC		*8*	*8*	
│└CardChipIdentification		*8*	*8*	
│ ├icSerialNumber		4	4	[00..00]
│ └icManufacturingReferences		4	4	[00..00]
└DF Tachograph		*11114*	*24454*	
├EF Application_Identification		*5*	*5*	
│└CompanyCardApplicationIdentification		5	5	
│ ├typeOfTachographCardId		1	1	[00]
│ ├cardStructureVersion		2	2	[00 00]
│ └noOfCompanyActivityRecords		2	2	[00 00]
├EF Card_Certificate		*194*	*194*	
│└CardCertificate		194	194	[00..00]
├EF CA_Certificate		*194*	*194*	
│└MemberStateCertificate		194	194	[00..00]
├EF Identification		*139*	*139*	
│├CardIdentification		*65*	*65*	
││ ├cardIssuingMemberState		1	1	[00]
││ ├cardNumber		16	16	[20..20]
││ ├cardIssuingAuthorityName		36	36	[00, 20..20]
││ ├cardIssueDate		4	4	[00..00]
││ ├cardValidityBegin		4	4	[00..00]
││ └cardExpiryDate		4	4	[00..00]
│└CompanyCardHolderIdentification		74	74	
│ ├companyName		36	36	[00, 20..20]
│ ├companyAddress		36	36	[00, 20..20]
│ └cardHolderPreferredLanguage		2	2	[20 20]
└EF Company_Activity_Data		*10582*	*23922*	
└CompanyActivityData		*10582*	*23922*	
├companyPointerNewestRecord		2	2	[00 00]
└companyActivityRecords		*10580*	*23920*	
└companyActivityRecord	n_{69}	46	46	
├companyActivityType		1	1	[00]
├companyActivityTime		4	4	[00..00]
├cardNumberInformation				
│ ├cardType		1	1	[00]
│ ├cardIssuingMemberState		1	1	[00]
│ └cardNumber		16	16	[20..20]
└vehicleRegistrationInformation				
├vehicleRegistrationNation		1	1	[00]
└vehicleRegistrationNumber		14	14	[00, 20..20]

▼**M1**

cardNumberInformation			
├─cardType	1	1	[00]
├─cardIssuingMemberState	1	1	[00]
└─cardNumber	16	16	[20..20]
├─downloadPeriodBegin	4	4	[00..00]
└─downloadPeriodEnd	4	4	[00..00]

Employées pour indiquer des tailles dans la table ci-avant, les valeurs qui suivent correspondent aux nombres minimal et maximal de relevés que la structure de données d'une carte d'entreprise se doit de respecter:

		Min.	Max.
n_8	NoOfCompanyActivityRecords	230	520

▼M1

Appendice 3

PICTOGRAMMES

▼**M1**

L'appareil de contrôle est susceptible d'employer les pictogrammes et combinaisons de pictogrammes qui suivent:

1. PICTOGRAMMES DE BASE

	Personnes	**Actions**	**Modes de fonctionnement**
	Entreprise		Mode entreprise
	Contrôleur	Contrôle	Mode de contrôle
	Conducteur	Conduite	Mode opérationnel
	Atelier/Poste d'essai	Inspection/Étalonnage	Mode étalonnage
	Constructeur		

	Activités	**Durée**
	Disponibilité	Période de disponibilité en cours
	Conduite	Temps de conduite continue
	Repos	Période de repos en cours
	Travail	Période de travail en cours
	Pause	Temps de pause cumulé
?	Inconnu	

	Équipement	**Fonctions**
1	Lecteur de carte du conducteur	
2	Lecteur de carte du convoyeur	
	Carte	
	Horloge	
	Affichage	Affichage
	Mémoire externe	Téléchargement
	Alimentation électrique	
	Imprimante/Tirage	Impression
	Capteur	
	Dimensions des pneumatiques	
	Véhicule/Unité embarquée sur le véhicule (UEV)	

	Conditions particulières
OUT	Hors limites
	Traversée sur ferry-boat/en train

	Divers		
!	Événements		Anomalies
	Début de la période journalière de travail		Fin de la période journalière de travail
	Lieu	M	Saisie manuelle des activités du conducteur
	Sécurité		Vitesse
	Heure	Σ	Total/Synthèse

	Qualificatifs
24h	Journalier
|	Hebdomadaire
||	Bihebdomadaire
	De ou vers

2. COMBINAISONS DE PICTOGRAMMES

	Divers		
	Poste de contrôle		
	Site de début de la période de travail quotidienne		Site de fin de la période de travail quotidienne
	De heures		À heures
	Du véhicule		
OUT	Hors limites, début	OUT	Hors limites, fin

▼**M1**

Cartes

Carte du conducteur
Carte d'entreprise
Carte de contrôleur
Carte d'atelier
Pas de carte

Conduite

Conduite en équipage
Temps de conduite hebdomadaire
Temps de conduite bihebdomadaire

Tirages

Tirage quotidien des activités du conducteur extraites de la carte
Tirage quotidien des activités du conducteur extraites de l'UV
Tirage des événements et anomalies éventuelles extraits de la carte
Tirage des événements et anomalies éventuelles extraits de l'UV
Tirage des données techniques
Tirage des dépassements de la vitesse autorisée

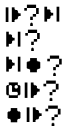
Événements

Insertion d'une carte erronée
Conflit de carte
Dépassement du temps imparti
Conduite sans carte appropriée
Insertion d'une carte en cours de route
Clôture incorrecte de la dernière session
Dépassement de la vitesse autorisée
Coupure d'alimentation électrique
Erreur au niveau des données de mouvement
Atteinte à la sécurité
Réglage de l'heure (en atelier)
Contrôle de dépassement de la vitesse autorisée

Anomalies

Carte défectueuse (logement de carte du conducteur)
Carte défectueuse (logement de carte du convoyeur)
Affichage défectueux
Erreur de téléchargement
Imprimante défectueuse
Capteur défectueux
Défaillance interne de l'UV

Procédure de saisie manuelle



Même période journalière de travail?
Fin de la période de travail antérieure?
Confirmation ou saisie du lieu de fin de la période de travail
Saisie de l'heure de départ
Saisie du lieu de début de la période de travail.

Remarque: diverses combinaisons de pictogrammes supplémentaires associées à autant d'identificateurs d'enregistrement ou de blocs d'impression sont définies à l'appendice 4.

▼**M1**

Appendice 4

TIRAGES PAPIER

TABLE DES MATIÈRES

▼**M1**

1. GÉNÉRALITÉS

Toute sortie imprimée se compose d'une succession de blocs de données séquencés, susceptibles d'être désignés par un identificateur de bloc.

Un bloc de données contient un ou plusieurs enregistrements désignés, le cas échéant, par un identificateur d'enregistrement.

Si un identificateur de bloc précède immédiatement un identificateur d'enregistrement, ce dernier n'est pas imprimé.

Si un élément d'information est inconnu ou ne doit pas être imprimé en raison de l'existence de droits d'accès aux données, le système imprime des espaces en lieu et place de ces éléments.

Si le contenu d'une ligne complète est inconnu ou ne nécessite aucune impression, la ligne correspondante est omise.

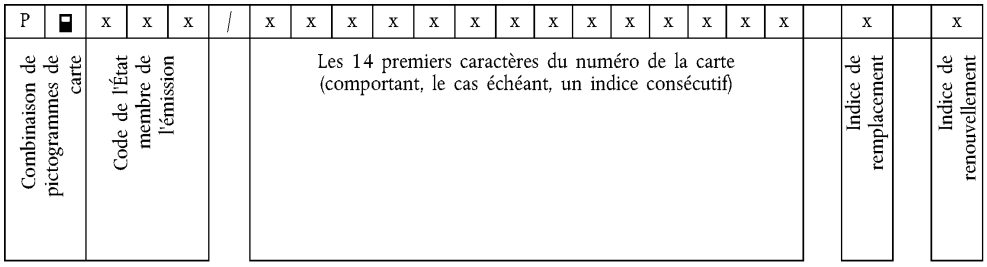
Les champs de données numériques sont justifiés à droite au tirage, leur impression s'accompagnant d'espaces de séparation marquant le passage des centaines aux milliers et des milliers aux millions, sans comporter de zéros en tête.

Les champs constitués de chaînes de caractères sont justifiés à gauche au tirage et, le cas échéant, complétés d'espaces pour atteindre la longueur élémentaire requise ou tronqués pour la même raison (noms et adresses).

2. CARACTÉRISTIQUES DES BLOCS DE DONNÉES

Dans ce chapitre, les conventions de notation suivantes ont été appliquées:

— les caractères affichés en *gras* identifient le texte en clair à imprimer (au tirage, les caractères sont normaux),
— les caractères normaux indiquent à l'affichage des variables (pictogrammes ou données) remplacées au tirage par leurs valeurs respectives,
— les noms de variable s'accompagnent de traits de soulignement indiquant la longueur élémentaire disponible pour la variable considérée,
— les dates respectent par défaut le format «jj/mm/aaaa» (jour, mois, année). L'application du format «jj.mm.aaaa» est également envisageable,
— la rubrique «identification de carte» se compose des éléments suivants: type de carte indiqué par une combinaison de pictogrammes, code de l'État membre d'émission de la carte, barre oblique suivie du numéro de la carte, puis d'un indice de remplacement et d'un indice de renouvellement séparés tous deux de l'élément qui les précède par un espace:



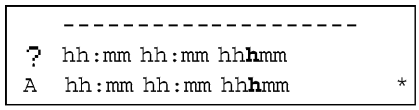
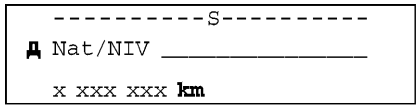
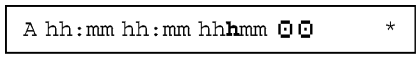
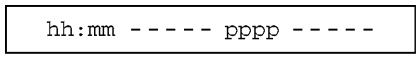
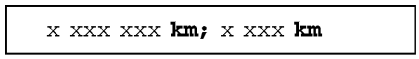
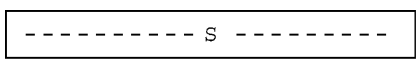
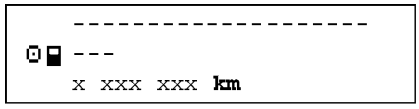
Les tirages se composeront des blocs et/ou enregistrements de données qui suivent, ces derniers se devant d'être conformes aux significations et formats suivants:

Numéro de bloc ou d'enregistrement Signification	Structure des données
1 **Date et heure d'impression du document**	▼ jj/mm/aaaa hh:mm
2 **Type de sortie imprimée** Identificateur de bloc Combinaison de pictogrammes d'impression (cf. appendice 3); réglage du dispositif limiteur de vitesse (impression uniquement en cas de dépassement de la vitesse autorisée)	----------▼ ---------- Picto xxx **km/h**

▼**M1**

Numéro de bloc ou d'enregistrement Signification	Structure des données
3 **Identification du titulaire de la carte** Identificateur de bloc. P = pictogramme individuel Nom du titulaire de la carte Prénom(s) du titulaire de la carte (le cas échéant) Identification de carte Date d'expiration de la carte (le cas échéant) Si la carte considérée n'est pas individuelle et ne contient aucun nom de titulaire, le nom de l'entreprise, de l'atelier ou de l'organisme de contrôle concerné sera imprimé en lieu et place de celui-ci.	----------P---------- P Nom _____ Prénom _____ Identification_carte _____ jj/mm/aaaa
4 **Identification du véhicule** Identificateur de bloc NIdV État membre dans lequel le véhicule est immatriculé et numéro d'immatriculation du véhicule	----------🚗---------- 🚗 NIdV _____ Nat/NIV _____
5 **Identification de l'UEV** Identificateur de bloc Nom du fabricant de l'UEV Numéro de référence de l'UEV	----------⊟---------- ⊟ Fabricant_UEV _____ Numéro_Référence_UEV ____
6 **Dernier étalonnage de l'équipement d'enregistrement** Identificateur de bloc Nom de l'atelier Identification de carte de l'atelier Date de l'étalonnage	----------🔧---------- 🔧 Nom _____ Identification_carte _____ 🔧 jj/mm/aaaa
7 **Dernier contrôle (contrôleur)** Identificateur de bloc Identification de carte du contrôleur Date, heure et type de contrôle Type de contrôle: combinaison composée de quatre pictogrammes au maximum. Le type de contrôle est susceptible de correspondre à l'un des pictogrammes suivants (ou à leur combinaison): 🖳: Téléchargement à partir d'une carte, 🖳↓: Téléchargement à partir de l'UEV, 🖨: Impression, □: Affichage	----------□---------- Identification_carte _____ □ jj/mm/aaaa hh:mm pppp
8 **Activités du conducteur enregistrées par ordre chronologique sur une carte** Identificateur de bloc Date de consultation (jour civil dont les données font l'objet du tirage) + compteur de présence quotidienne de la carte	----------🗀---------- jj/mm/aaaa xxx

▼**M1**

Numéro de bloc ou d'enregistrement Signification	Structure des données
8.1 *Période pendant laquelle la carte n'était pas présente dans son lecteur* 8.1a Identificateur d'enregistrement (début de la période) 8.1b *Période inconnue*. Heure de début et heure de fin, durée 8.1c *Activité entrée manuellement* Pictogramme d'activité, heure de début et de fin (incluse), durée; les périodes de repos dont la durée s'élève à une heure au moins sont repérées par un astérisque.	
8.2 *Insertion de la carte dans le lecteur S* État membre dans lequel le véhicule est immatriculé et numéro d'immatriculation du véhicule Kilométrage indiqué au compteur du véhicule lors de l'insertion de la carte	
8.3 *Activité (lors de l'insertion de la carte)* Pictogramme d'activité, heure de début et de fin (incluse), durée, situation de l'équipage (pictogramme d'équipage s'il comporte plusieurs membres, espaces s'il n'en comprend qu'un); les périodes de repos dont la durée s'élève à une heure au moins sont repérées par un astérisque.	
8.3a *Conditions particulières*. Heures d'introduction, pictogramme (ou combinaison de pictogrammes) associé aux conditions particulières.	
8.4 *Retrait de carte* Kilométrage indiqué au compteur du véhicule et distance parcourue depuis la dernière insertion de la carte, compte tenu du kilométrage affiché alors	
9 **Activités du conducteur enregistrées sur une UEV par ordre chronologique et par lecteur de carte** Identificateur de bloc Date de consultation (jour civil dont les données font l'objet du tirage) Kilométrage indiqué au compteur du véhicule à 00:00 et 24:00	
10 **Activités menées dans le lecteur S** Identificateur de bloc	
10.1 *Période pendant laquelle aucune carte n'était présente dans le lecteur S* Identificateur d'enregistrement Lecteur vide de carte Kilométrage indiqué au compteur du début de la période considérée	

▼**M1**

Numéro de bloc ou d'enregistrement Signification	Structure des données
10.2 *Insertion de carte* Identificateur d'enregistrement d'insertion de carte Nom du conducteur Prénom du conducteur Identification de carte du conducteur Date d'expiration de la carte du conducteur État membre dans lequel le précédent véhicule utilisé est immatriculé et numéro d'immatriculation de ce véhicule Date et heure de retrait de la carte introduite sur le précédent véhicule Ligne vierge Kilométrage indiqué au compteur lors de l'insertion de la carte, entrée manuelle du drapeau d'activité du conducteur (M dans l'affirmative, vierge dans la négative).	---------- O Nom _____ Prénom _____ Identification_carte _____ jj/mm/aaaa Nat/NIV _____ jj/mm/aaaa hh:mm x xxx xxx **km** M
10.3 *Activité* Pictogramme d'activité, heure de début et de fin (incluse), durée, situation de l'équipage (pictogramme d'équipage s'il comporte plusieurs membres, espaces s'il n'en comprend qu'un); les périodes de repos dont la durée s'élève à une heure au moins sont repérées par un astérisque.	A hh:mm hh:mm hh**h**mm 00 *
10.3a *Conditions particulières.* Heures d'introduction, pictogramme (ou combinaison de pictogrammes) associé aux conditions particulières.	hh:mm ----- pppp -----
10.4 *Retrait de carte ou fin de période «Sans carte»* Kilométrage indiqué au compteur du véhicule lors du retrait de la carte ou à la fin de la période «Sans carte» et distance parcourue depuis l'insertion de la carte ou depuis le début de la période «Sans carte».	x xxx xxx **km;** x xxx **km**
11 **Synthèse quotidienne** Identificateur de bloc	----------Σ----------
11.1 *Synthèse UEV des périodes sans carte dans le lecteur du conducteur* Identificateur de bloc	10■ - - -
11.2 *Synthèse UEV des périodes sans carte dans le lecteur du convoyeur* Identificateur de bloc	20■ - - -
11.3 *Synthèse UEV quotidienne par conducteur* Identificateur d'enregistrement Nom du conducteur Prénom(s) du conducteur Identification de carte du conducteur	---------- O Nom _____ Prénom _____ Identification_carte _____

▼**M1**

Numéro de bloc ou d'enregistrement Signification	Structure des données
11.4 *Saisie du site où une période de travail quotidienne débute et/ou prend fin* pi = pictogramme du site de départ/ d'arrivée, heure, pays, région, Kilométrage indiqué au compteur	pihh:mm Pay Rég x xxx xxx **km**
11.5 *Totaux par activité (extraits d'une carte)* Durée totale du temps de conduite, distance parcourue Durée totale de la période de travail et de disponibilité effective Durée totale de la période de repos et d'activité non répertoriée Durée totale des activités de l'équipage	hh**h**mm x xxx **km** hh**h**mm hh**h**mm hh**h**mm hh**h**mm hh**h**mm
11.6 *Totaux par activité (périodes sans carte insérée dans le lecteur conducteur)* Durée totale du temps de conduite, distance parcourue Durée totale de la période de travail et de disponibilité effective Durée totale de la période de repos	hh**h**mm x xxx **km** hh**h**mm hh**h**mm hh**h**mm
11.7 *Totaux par activité (périodes sans carte insérée dans le lecteur convoyeur)* Durée totale de la période de travail et de disponibilité effective Durée totale de la période de repos	hh**h**mm hh**h**mm hh**h**mm
11.8 *Totaux par activité (et par conducteur, les deux lecteurs étant inclus dans leur calcul)* Durée totale du temps de conduite, distance parcourue Durée totale de la période de travail et de disponibilité effective Durée totale de la période de repos Durée totale des activités de l'équipage Si un tirage quotidien s'impose, l'établissement des informations de synthèse s'effectue à partir des données disponibles à l'heure de l'impression.	hh**h**mm x xxx **km** hh**h**mm hh**h**mm hh**h**mm hh**h**mm
12 **Événements et/ou anomalies enregistrés sur une carte**	
12.1 Identificateur de bloc; 5 derniers «Événements et anomalies» extraits d'une carte	-------- !x▪ --------
12.2 Identificateur de bloc; ensemble des «Événements» enregistrés sur une carte	--------- !▪---------
12.3 Identificateur de bloc; ensemble des «Anomalies» enregistrées sur une carte	--------- x▪---------

▼**M1**

Numéro de bloc ou d'enregistrement Signification	Structure des données
12.4 *Enregistrement d'événement et/ou d'anomalie* Identificateur d'enregistrement Pictogramme d'événement/anomalie, motif d'enregistrement, date et heure de début Code d'événement/anomalie supplémentaire (le cas échéant), durée État membre dans lequel le véhicule est immatriculé et numéro d'immatriculation du véhicule sur lequel l'événement ou l'anomalie s'est manifesté	---------- Pic jj/mm/aaaa hh:mm ! xxx hhhmm Nat/NIV _____
13 **Événements et/ou anomalies enregistrés ou en cours au sein d'une UEV**	
13.1 Identificateur de bloc; 5 derniers «Événements et anomalies» extraits d'une UEV	-------- ! x --------
13.2 Identificateur de bloc; ensemble des «Événements» enregistrés ou en cours au sein d'une UEV	--------- ! ---------
13.3 Identificateur de bloc; ensemble des «Anomalies» enregistrées ou en cours au sein d'une UEV	--------- x ---------
13.4 *Enregistrement d'événement et/ou d'anomalie* Identificateur d'enregistrement Pictogramme d'événement/anomalie, motif d'enregistrement, date et heure de début Code d'événement/anomalie supplémentaire (le cas échéant), Nb. d'événements analogues le même jour, durée Identification des cartes insérées au début ou à la fin de l'événement ou de l'anomalie considéré (jusqu'à 4 lignes sans répéter aucun numéro de carte) Cas où les lecteurs n'accueillent aucune carte Le motif d'enregistrement (p) prend la forme d'un code numérique indiquant la raison pour laquelle l'événement ou l'anomalie constaté a été enregistré et codé en conformité avec l'élément d'information *MotifEnregistrementÉvénementAnomalie*.	---------- Pic (p) jj/mm/aaaa hh:mm ! xxx (xxx) hhhmm Identification_carte _____ Identification_carte _____ Identification_carte _____ Identification_carte _____ ----
14 **Identification de l'UEV** Identificateur de bloc Nom du fabricant de l'UEV Adresse du fabricant de l'UEV Numéro de référence de l'UEV Numéro d'homologation de l'UEV Numéro de série de l'UEV Année de fabrication de l'UEV	---------- Nom _____ Adresse _____ NuméroRéférence _____ Homolog _____ N/S _____ aaaa v xx.xx.xx jj/mm/aaaa

▼**M1**

Numéro de bloc ou d'enregistrement Signification	Structure des données
Version du logiciel d'exploitation de l'UEV et date d'installation	
15 **Identification d'un capteur**	
Identificateur de bloc	----------Л----------
Numéro de série du capteur	Л N/S _____
Numéro d'homologation du capteur	Homolog _____
Date d'installation initiale du capteur	jj/mm/aaaa
16 **Données d'étalonnage**	
Identificateur de bloc	---------- ----------
16.1 *Enregistrement d'étalonnage*	
Identificateur d'enregistrement	----------
Atelier responsable de l'étalonnage	Nom_atelier _____
Adresse de l'atelier	Adresse_atelier _____
Identification de carte de l'atelier	Identification_carte _____
Date d'expiration de la carte de l'atelier	jj/mm/aaaa
Ligne vierge	jj/mm/aaaa (p)
Date d'étalonnage + motif d'étalonnage	NIdV _____
NidV	Nat/NIV _____
État membre dans lequel le véhicule est immatriculé et numéro d'immatriculation du véhicule	w xx xxx **Imp/km**
Coefficient caractéristique du véhicule	k xx xxx **Imp/km**
Constante de l'équipement d'enregistrement	l xx xxx **mm**
Circonférence effective des pneumatiques	DimensionPneu _____
Dimensions des pneumatiques montés	xxx **km/h**
Réglage du dispositif limiteur de vitesse	x xxx xxx – x xxx xxx **km**
Ancien et nouveau kilométrages indiqués au compteur	
Le motif d'enregistrement (p) prend la forme d'un code numérique indiquant la raison pour laquelle ces paramètres d'étalonnage ont été enregistrés et codés en conformité avec l'élément d'information MotifÉtalonnage.	
17 **Réglage de l'heure**	
Identificateur de bloc	---------- ----------
17.1 *Enregistrement du réglage de l'heure*	
Identificateur d'enregistrement	----------
Anciennes date et heure	! jj/mm/aaaa hh:mm
Nouvelles date et heure	jj/mm/aaaa hh:mm
Atelier ayant procédé au réglage de l'heure	Nom_atelier _____
Adresse de l'atelier	Adresse_atelier _____
Identification de carte de l'atelier	Identification_carte _____
	jj/mm/aaaa

▼**M1**

Numéro de bloc ou d'enregistrement Signification	Structure des données
Date d'expiration de la carte de l'atelier	
18 **Événements et anomalies les plus récents enregistrés au sein de l'UEV**	---------- ! ✕ 🚗 ---------- ! jj/mm/aaaa hh:mm ✕ jj/mm/aaaa hh:mm
Identificateur de bloc	
Date et heure de l'événement le plus récent	
Date et heure de l'anomalie la plus récente	
19 **Informations relatives au contrôle de dépassement de la vitesse autorisée**	----------»» ---------- »🗎 jj/mm/aaaa hh:mm »» jj/mm/aaaa hh:mm (nnn)
Identificateur de bloc	
Date et heure du dernier CONTRÔLE DE DÉPASSEMENT DE LA VITESSE AUTORISÉE	
Date/heure du premier dépassement de la vitesse autorisée et nombre des événements de cette nature enregistrés depuis lors	
20 **Enregistrement des dépassements de la vitesse autorisée**	
20.1 Identificateur de bloc «Premier dépassement de la vitesse autorisée après le dernier étalonnage»	-------- »»1 --------
20.2 Identificateur de bloc «Les 5 dépassements les plus sérieux relevés au cours des 365 derniers jours écoulés»	------- »»(365) -------
20.3 Identificateur de bloc «Le dépassement le plus sérieux pour chacune des périodes coïncidant avec les dix derniers jours de manifestation»	------- »»(10) -------
20.4 Identificateur d'enregistrement	------------------ »» jj/mm/aaaa hh:mm hh**h**mm xxx **km/h** xxx **km/h** (xxx) 🙍 Nom _____ Prénom _____ Identification_carte _____
Date, heure et durée	
Vitesses maximale et moyenne, Nb. d'événements similaires le même jour	
Nom du conducteur	
Prénom(s) du conducteur	
Identification de carte du conducteur	
20.5 Si un bloc est dépourvu de tout enregistrement de dépassement de la vitesse autorisée	»» - - -
21 **Informations saisies au clavier**	---------- 🗎● ..... 🗎 ..... 🕒+ ..... +🕒 ..... 🙍 .....
Identificateur de bloc	
21.1 Poste de contrôle	
21.2 Signature du contrôleur	
21.3 De heures	
21.4 À heures	
21.5 Signature du conducteur	
«Informations entrées manuellement»: introduisez suffisamment de lignes vierges	

▼**M1**

Numéro de bloc ou d'enregistrement Signification	Structure des données

en amont de toute rubrique entrée manuellement afin de pouvoir rédiger les informations requises ou d'apposer une signature.

3. CARACTÉRISTIQUES DES TIRAGES PAPIER

Dans ce chapitre, les conventions de notation suivantes ont été appliquées:

N	Impression du bloc ou de l'enregistrement numéro N
N X/Y	Impression du bloc ou de l'enregistrement numéro N répété autant de fois que l'exige la situation Impression des blocs ou enregistrements X et/ou Y selon les besoins, et répétition de l'opération autant de fois que l'exige la situation.

3.1. **Tirage quotidien des activités du conducteur extraites d'une carte**

Le tirage quotidien des activités du conducteur extraites d'une carte doit respecter le format suivant:

1	Date et heure d'impression du document
2	Type de document imprimé
3	Identification du contrôleur (en cas d'insertion d'une carte de contrôle dans l'UEV)
3	Identification du conducteur (extraite de la carte faisant l'objet de l'impression)
4	Identification du véhicule (à partir duquel le tirage est exécuté)
5	Identification de l'UEV (à partir de laquelle le tirage est exécuté)
6	Dernier étalonnage de cette UEV
7	Dernier contrôle auquel le conducteur inspecté a été soumis
8	Délimiteur des activités du conducteur
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Activités du conducteur par ordre chronologique
11	Délimiteur de synthèse quotidienne
11.4	Sites introduits par ordre chronologique
11.5	Totaux par activité
12.1	Délimiteur des événements et anomalies extraits d'une carte
12.4	Enregistrements d'événement/anomalie (5 derniers événements ou anomalies enregistrés sur la carte)
13.1	Délimiteur des événements ou anomalies extraits de l'UEV
13.4	Enregistrements d'événement/anomalie (5 derniers événements ou anomalies enregistrés ou en cours au sein de l'UEV)
21.1	Poste de contrôle
21.2	Signature du contrôleur
21.5	Signature du conducteur

3.2. **Tirage quotidien des activités du conducteur extraites de l'UEV**

Le tirage quotidien des activités du conducteur extraites de l'UEV doit respecter le format suivant:

1	Date et heure d'impression du document

▼**M1**

2	Type de document imprimé	
3	Identification du titulaire de la carte (pour toutes les cartes insérées dans l'UEV)	
4	Identification du véhicule (à partir duquel le tirage est exécuté)	
5	Identification de l'UEV (à partir de laquelle le tirage est exécuté)	
6	Dernier étalonnage de cette UEV	
7	Dernier contrôle auquel cet équipement d'enregistrement a été soumis	
9	Délimiteur des activités du conducteur	
10	Délimiteur de lecteur de carte du conducteur (lecteur 1)	
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)	
10.1 / 10.2 / 10.3 /10.3a / 10.4	Activités par ordre chronologique (lecteur conducteur)	
11	Délimiteur de synthèse quotidienne	
11.1	Synthèse des périodes sans carte dans le lecteur du conducteur	
11.4	Sites introduits par ordre chronologique	
11.6	Totaux par activité	
11.2	Synthèse des périodes sans carte dans le lecteur du convoyeur	
11.4	Sites introduits par ordre chronologique	
11.7	Totaux par activité	
11.3	Synthèse des activités par conducteur, les deux lecteurs étant inclus	
11.4	Sites introduits par ce conducteur et par ordre chronologique	
11.7	Totaux par activité pour ce conducteur	
13.1	Délimiteur d'événements et d'anomalies	
13.4	Enregistrements d'événement/anomalie (5 derniers événements ou anomalies enregistrés ou en cours au sein de l'UEV)	
21.1	Poste de contrôle	
21.2	Signature du contrôleur	
21.3	De heures	(espace disponible pour un conducteur dépourvu de carte lui permettant d'indiquer les périodes qui correspondent à ses prestations)
21.4	À heures	
21.5	Signature du conducteur	

3.3. **Tirage des anomalies et événements extraits d'une carte**

Le tirage quotidien des activités du conducteur extraites de l'UEV doit respecter le format suivant:

1	Date et heure d'impression du document
2	Type de document imprimé
3	Identification du contrôleur (en cas d'insertion d'une carte de contrôle dans l'UEV)
3	Identification du conducteur (extraite de la carte faisant l'objet de l'impression)
4	Identification du véhicule (à partir duquel le tirage est exécuté)
12.2	Délimiteur des événements
12.4	Enregistrements d'événements (tous les événements enregistrés sur la carte)
12.3	Délimiteur des anomalies

▼**M1**

12.4	Enregistrements d'anomalies (toutes les anomalies enregistrées sur la carte)
21.1	Poste de contrôle
21.2	Signature du contrôleur
21.5	Signature du conducteur

3.4. **Tirage des anomalies et événements extraits de l'UEV**

Le tirage des anomalies et événements extraits de l'UEV doit respecter le format suivant:

1	Date et heure d'impression du document
2	Type de document imprimé
3	Identification du titulaire de la carte (pour toutes les cartes insérées dans l'UEV)
4	Identification du véhicule (à partir duquel le tirage est exécuté)
13.2	Délimiteur des événements
13.4	Enregistrements d'événements (tous les événements enregistrés ou en cours au sein de l'UEV)
13.3	Délimiteur des anomalies
13.4	Enregistrements d'anomalies (toutes les anomalies enregistrées ou en cours au sein de l'UEV)
21.1	Poste de contrôle
21.2	Signature du contrôleur
21.5	Signature du conducteur

3.5. **Tirage des données techniques**

Tirage des données techniques doit respecter le format suivant:

1	Date et heure d'impression du document
2	Type de document imprimé
3	Identification du titulaire de la carte (pour toutes les cartes insérées dans l'UEV)
4	Identification du véhicule (à partir duquel le tirage est exécuté)
14	Identification de l'UEV
15	Identification des capteurs
16	Délimiteur des données d'étalonnage
16.1	Enregistrement d'étalonnage (ensemble des enregistrements disponibles par ordre chronologique)
17	Délimiteur du réglage de l'heure
17.1	Enregistrement du réglage de l'heure (ensembles des enregistrements disponibles, extraits des enregistrements du réglage de l'heure et des données d'étalonnage)
18	Événements et anomalies les plus récents enregistrés au sein de l'UEV

3.6. **Tirage des dépassements de la vitesse autorisée**

Le tirage des dépassements de la vitesse autorisée doit respecter le format suivant:

1	Date et heure d'impression du document
2	Type de document imprimé
3	Identification du titulaire de la carte (pour toutes les cartes insérées dans l'UEV)
4	Identification du véhicule (à partir duquel le tirage est exécuté)

▼**M1**

19	Informations relatives au contrôle de dépassement de la vitesse autorisée
20.1	Identificateur des données de dépassement de la vitesse autorisée
20.4 / 20.5	Premier dépassement de la vitesse autorisée après le dernier étalonnage
20.2	Identificateur des données de dépassement de la vitesse autorisée
20.4 / 20.5	Les 5 dépassements les plus sérieux relevés au cours des 365 derniers jours écoulés
20.3	Identificateur des données de dépassement de la vitesse autorisée
20.4 / 20.5	Le dépassement le plus sérieux pour chacune des périodes coïncidant avec les dix derniers jours de manifestation
21.1	Poste de contrôle
21.2	Signature du contrôleur
21.5	Signature du conducteur

▼**M1**

Appendice 5

AFFICHAGE

▼**M1**

Les conventions de présentation qui suivent sont d'application dans le présent appendice:

— les caractères **gras** indiquent le texte à afficher (l'affichage demeure en caractères normaux),
— les caractères normaux indiquent des variables (pictogrammes ou données) à remplacer par leurs valeurs respectives à l'affichage:

jj mm aaaa:	jour, mois, année,
hh:	heures
mm:	minutes
D:	pictogramme de durée
EF:	combinaison de pictogrammes d'événement ou d'anomalie
O:	pictogramme de mode d'exploitation.

L'équipement d'enregistrement est susceptible d'employer les formats d'affichage des données suivants:

Données	Format
Affichage par défaut	
Heure locale	hh:mm
Mode d'exploitation	O
Informations relatives au conducteur	1 Jhhhmm ▮▮hhhmm
Informations relatives au convoyeur	2 Jhhhmm
Condition hors limites	OUT
Affichage d'avertissements	
Dépassement du temps de conduite continue	10 hhhmm ▮▮hhhmm
Événement ou anomalie	EF
Autres affichages	
Date TUC	TUC jj/mm/aaaa ou TUC jj.mm.aaaa
Heure	hh:mm
Temps de conduite continue et temps de pause cumulé du conducteur	10 hhhmm ▮▮hhhmm
Temps de conduite continue et temps de pause cumulé du convoyeur	20 hhhmm ▮▮hhhmm
Temps de conduite cumulé du conducteur, enregistré pendant la semaine en cours et la semaine précédente	10 ‖ hhhhmm
Temps de conduite cumulé du convoyeur, enregistré pendant la semaine en cours et la semaine précédente	20 ‖ hhhhmm

▼**M1**

Appendice 6

INTERFACES EXTERNES

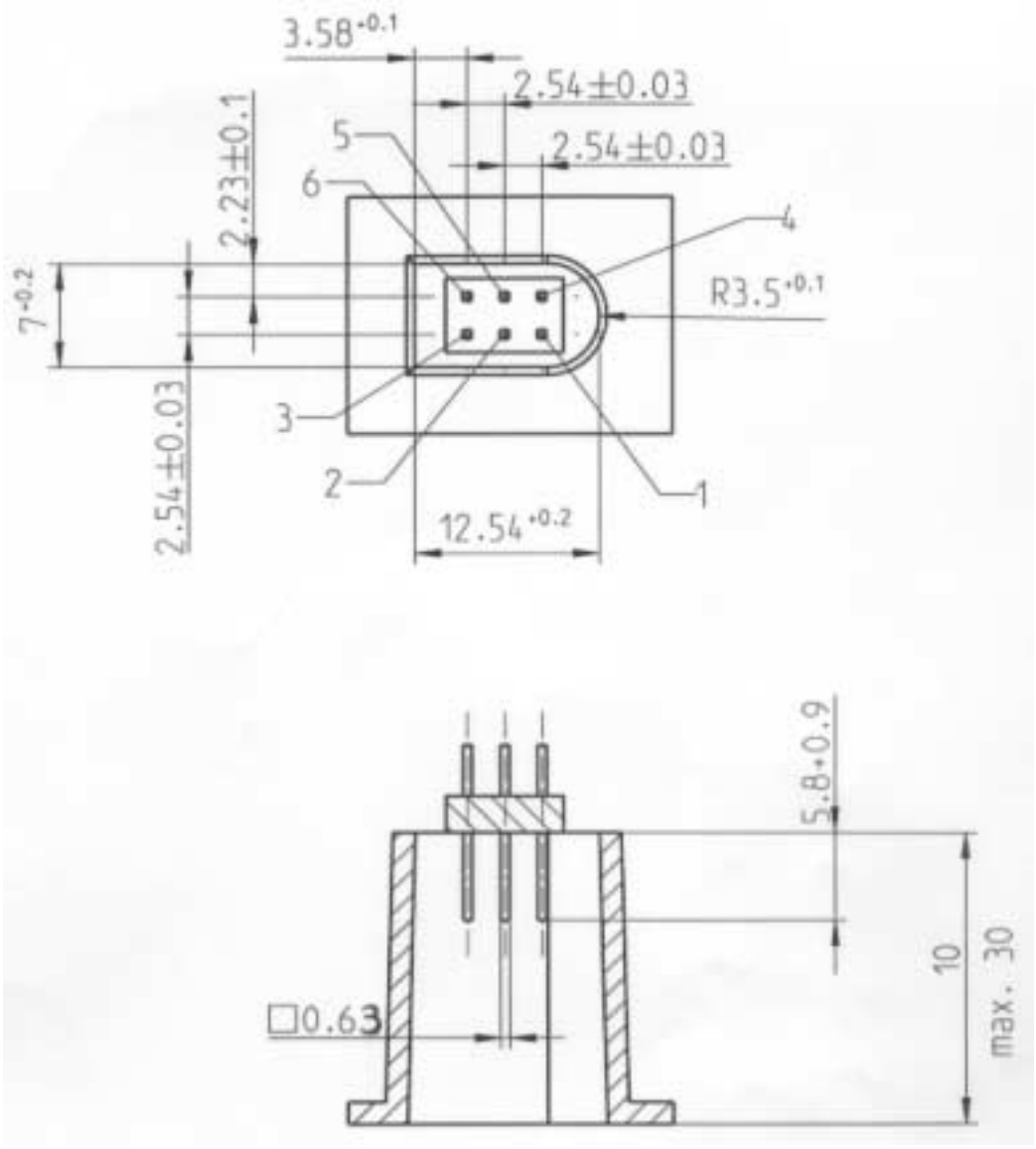
TABLE DES MATIÈRES

▼**M1**

1. MATÉRIEL

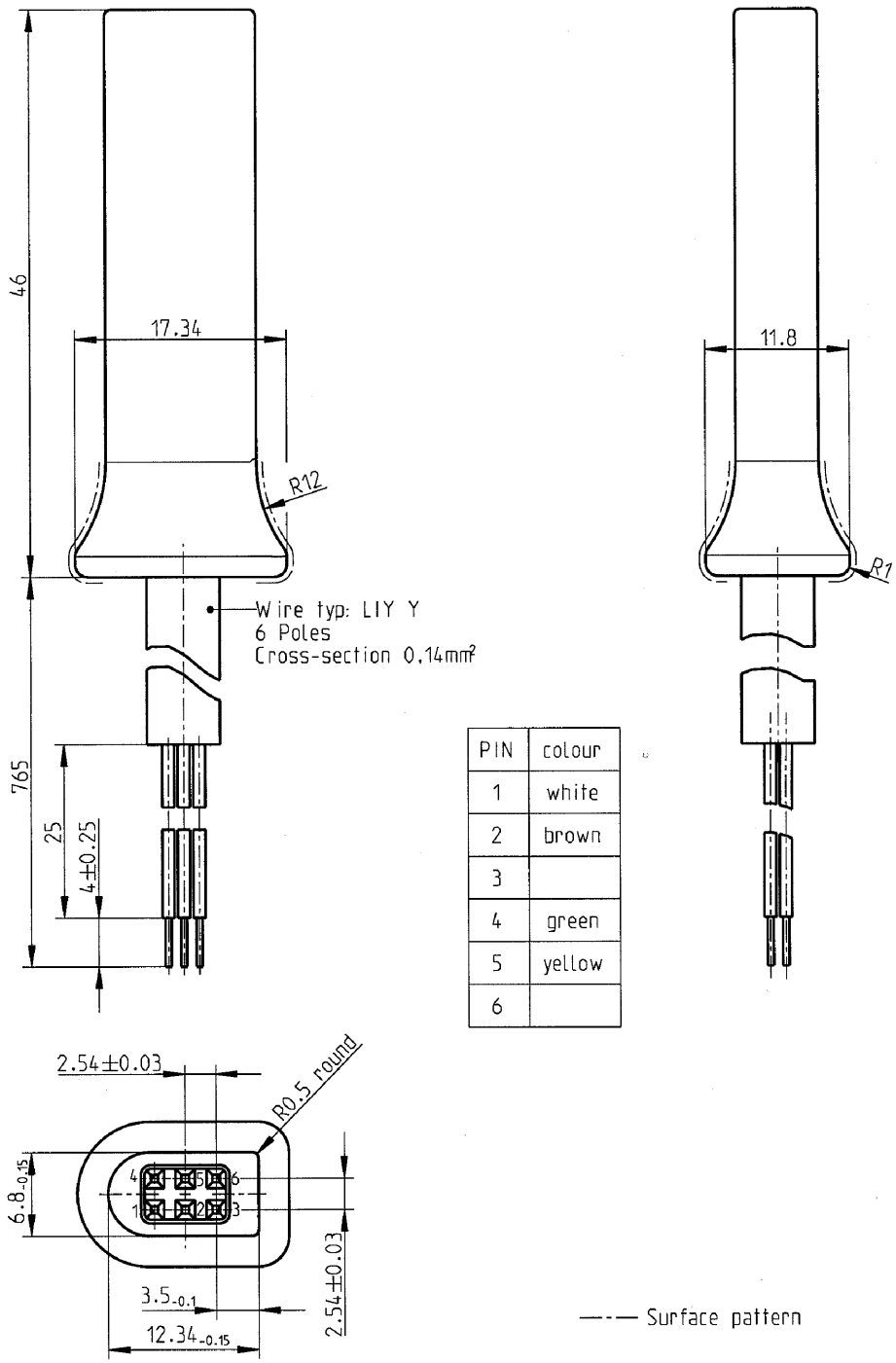
1.1. **Connecteur**

Le connecteur de téléchargement/étalonnage doit se présenter sous la forme d'un connecteur à 6 broches, accessible sur la face avant sans nécessiter la déconnexion d'aucun organe du matériel de contrôle. Il doit se conformer au plan qui suit (toutes les cotes sont en millimètres):



▼**M1**

Le schéma suivant illustre une fiche usuelle d'accouplement à 6 broches:



PIN	colour
1	white
2	brown
3	
4	green
5	yellow
6	

▼M1

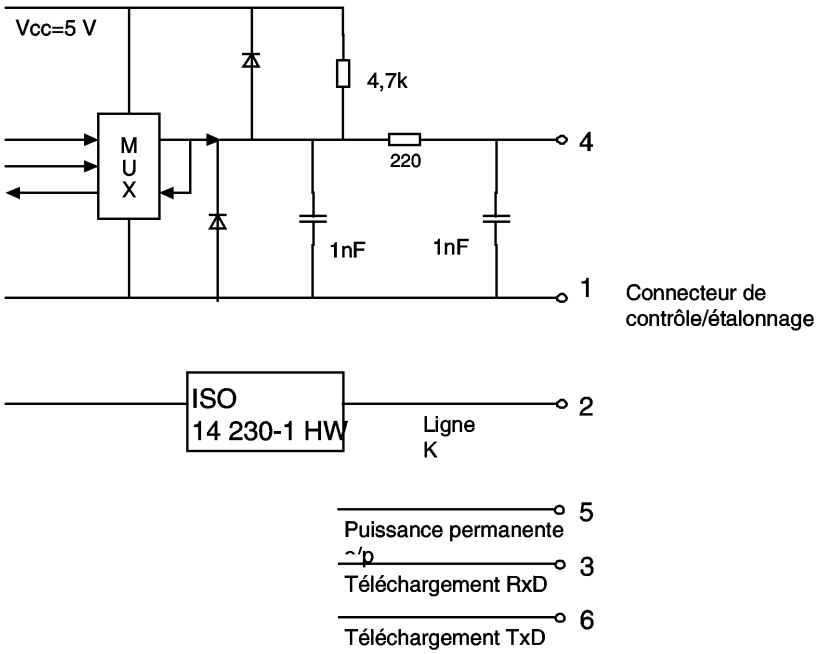
1.2. **Affectation des contacts**

L'affectation des contacts doit être conforme à la table qui suit:

Pin	Description	Remarque
1	Pôle négatif de la batterie	Raccordée à la borne négative de la batterie montée sur le véhicule
2	Communication de données	Ligne K (ISO 14230-1)
3	RxD — Téléchargement	Entrée de données à destination du matériel de contrôle
4	Signal d'entrée/sortie	Étalonnage
5	Puissance de sortie permanente	La plage de tensions doit être identique à celle de l'alimentation électrique du véhicule diminuée de 3 V afin de tenir compte de la chute de tension inhérente au passage du courant à travers les circuits de protection Sortie 40 mA
6	TxD — Téléchargement	Sortie de données émanant de l'équipement d'enregistrement

1.3. **Schéma fonctionnel**

Le schéma fonctionnel doit être conforme aux indications suivantes:



2. INTERFACE DE TÉLÉCHARGEMENT

L'interface de téléchargement doit être conforme aux spécifications de la norme RS232.

L'interface de téléchargement doit recourir à un bit de départ, huit bits d'information (bit le moins significatif en tête), un bit de parité pair et un bit d'arrêt.

Agencement d'un octet d'information

Bit de départ: un bit de niveau logique 0;

▼**M1**

Bits d'information: transmis avec le bit le moins significatif en tête;

Bit de parité: parité paire

Bit d'arrêt: un bit de niveau logique 1

En cas de transmission de données numériques composées de plus d'un octet, l'octet le plus significatif est transmis en premier lieu, l'octet le moins significatif en dernier lieu.

Les débits de transmission doivent être réglables dans une plage comprise entre 9 600 et 115 200 bits par seconde. Toute transmission doit s'opérer à la vitesse de transmission la plus élevée possible, le débit initial étant égal à 9 600 bits par seconde immédiatement après le début d'une communication.

3. INTERFACE D'ÉTALONNAGE

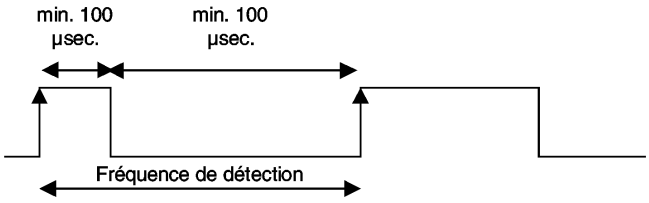
La communication de données doit être conforme aux spécifications de la norme ISO 14230-1 Véhicules routiers — Systèmes de diagnostic — Protocole à mots clés 2000 — Partie 1: Couche physique. Première édition: 1999.

Le signal d'entrée/sortie doit se conformer aux spécifications électriques qui suivent:

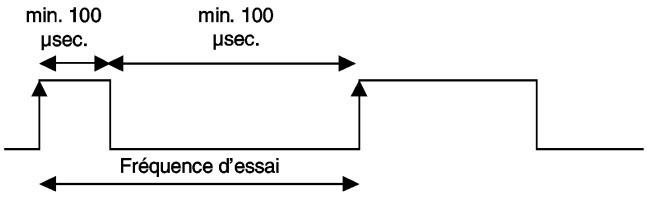
Paramètre	Minimum	Caractéristique	Maximum	Remarque
U_{low} (entrée)			1,0 V	I = 750 µA
U_{high} (entrée)	4 V			I = 200 µA
Fréquence			4 kHz	
U_{low} (sortie)			1,0 V	I = 1 mA
U_{high} (sortie)	4 V			I = 1 mA

Le signal d'entrée/sortie doit se conformer aux chronogrammes qui suivent:

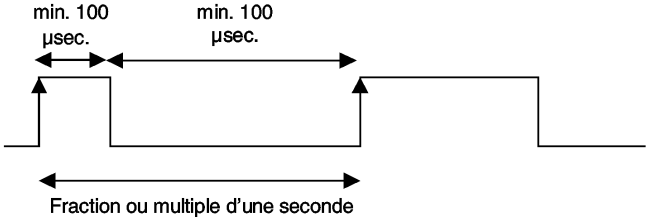
Signal détecteur (sortie)



Signal d'essai (entrée)



Signal d'horloge TUC (sortie)



▼**M1**

Appendice 7

PROTOCOLES DE TÉLÉCHARGEMENT DE DONNÉES

TABLE DES MATIÈRES

▼**M1**

▼M1

1. INTRODUCTION

Cet appendice traite des procédures qu'il convient d'appliquer pour exécuter les différents types de téléchargement de données vers un support de mémoire externe (SME). Il traite également des protocoles qu'il y a lieu de mettre en œuvre pour assurer un transfert de données correct et garantir la parfaite compatibilité des données téléchargées afin de permettre à tout contrôleur d'inspecter ces données en s'assurant de leur authenticité et de leur intégrité avant de procéder à leur analyse éventuelle.

1.1. **Portée**

Certaines données sont susceptibles d'être téléchargées vers un support de mémoire externe:

— à partir d'une unité embarquée sur véhicule par l'intermédiaire d'un équipement spécialisé intelligent (ESI) raccordé à l'UEV

— à partir d'une carte tachygraphique par l'intermédiaire d'un équipement spécialisé intelligent (ESI) équipé d'un périphérique de lecture de carte (PIF)

— à partir d'une carte tachygraphique par l'intermédiaire d'une unité embarquée sur véhicule et par le biais d'un équipement ESI raccordé à l'UEV.

Afin de donner la possibilité à certains contrôleurs de vérifier l'authenticité et l'intégrité des données téléchargées qui auraient été sauvegardées sur un support de mémoire externe, ces données s'accompagnent d'une signature aux termes de l'Appendice 11 (Mécanismes de sécurité communs). L'identification de l'équipement source (UEV 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 au cours d'une session de téléchargement doivent être enregistrées dans un même fichier sur leur support de mémoire externe.

1.2. **Abréviations et notations**

Les abréviations qui suivent apparaissent dans le présent appendice:

CCI	carte à circuit(s) intégré(s)
CIB	octet cible
EOpS	exécution d'une opération de sécurité
ESI	équipement spécialisé intelligent [équipement utilisé pour procéder au téléchargement de données vers le support de mémoire externe (p. ex. ordinateur individuel)]
FE	fichier élémentaire
FMT	octet de structure (premier octet de l'en-tête d'un message)
FS	fichier spécialisé
IDA	identificateur d'application
IDF	identificateur de fichier
IDS	identificateur de service
LON	octet de longueur (dernier octet de l'en-tête d'un message)
PIF	périphérique d'interface
PMC	protocole à mots clés 2000
PDT	paramètre de demande de transfert
PRT	paramètre de réponse pour le transfert
RAR	réponse à une réinitialisation
SD	session de diagnostic
SME	support de mémoire externe
SPP	sélection des paramètres de protocole
SRC	octet source
TC	octet total de contrôle
UEV	unité embarquée sur le véhicule
VLB	valeur d'une longueur de balise

▼M1

2. TÉLÉCHARGEMENT DE DONNÉES SUR L'UEV

2.1. **Procédure de téléchargement**

Pour procéder au téléchargement de données sur l'UEV, l'opérateur doit exécuter les opérations suivantes:

— Introduire la carte de tachygraphe qu'il détient dans la fente de l'un des lecteurs de carte de l'unité embarquée sur véhicule ([1])

— Raccorder l'ESI au connecteur de téléchargement de l'UEV

— Établir la liaison entre l'ESI et l'UEV

— Sélectionner sur l'ESI les données à télécharger et envoyer la demande requise à l'UEV

— Clôturer la session de téléchargement.

2.2. **Protocole de téléchargement des données**

La structure du protocole repose sur une relation maître-esclave, l'ESI jouant le rôle du maître et l'UEV celui de l'unité asservie.

La structure des messages, leur type et leur acheminement sont essentiellement basés sur le protocole à mots clés 2000 (PMC) (ISO 14230-2 Véhicules routiers — Systèmes de diagnostic — Protocole à mots clés 2000 — Partie 2: Couche liaison de données).

La couche d'application est principalement basée sur le projet actuel de norme ISO 14229-1 (Véhicules routiers — systèmes de diagnostic — Partie 1: services de diagnostic, version 6 du 22 février 2001).

2.2.1. ***Structure des messages***

Tous les messages échangés entre l'ESI et l'UEV se caractérisent par une structure à trois éléments:

— En-tête composé des octets suivants: octet de structure (FMT), octet cible (CIB), octet source (SRC) et, le cas échéant, octet de longueur (LON).

— Champ de données composé d'un octet d'identification de service (IDS) et d'un nombre variable d'octets d'information qui peuvent comprendre un octet optionnel de session de diagnostic (SD) ou un octet optionnel de paramètre de transfert (PDT ou PRT).

— Total de contrôle composé d'un octet total de contrôle (TC).

En-tête				Champ de données					Total de contrôle
FMT	CIB	SRC	LON	IDS	DON-NÉES	…	…	…	TC
4 octets				255 octets max.					1 octet

Les octets CIB et SRC représentent les adresses physiques du destinataire et de l'expéditeur du message. Ils prennent les valeurs F0 Hex pour l'ESI et EE Hex pour l'UEV.

L'octet LON indique la longueur du champ de données.

L'octet total de contrôle correspond à une série de sommes de 8 bits modulo 256 représentant tous les octets du message à l'exclusion du TC lui-même.

Les octets FMT, IDS, SD, PDT et PRT font également l'objet d'une définition présentée plus loin dans ce document.

Si la longueur des données que le message est censé véhiculer est supérieure à l'espace disponible dans la partie champ de données, l'envoi de ce message prend la forme de plusieurs sous-messages. Chacun de ces sous-messages comporte un en-tête, les mêmes IDS et PRT ainsi qu'un compteur de sous-messages de 2 octets indiquant le numéro d'ordre de chaque sous-message au sein du message global. Afin de permettre le contrôle d'erreur et l'abandon éventuel d'un échange de données, l'ESI accuse réception de chaque sous-message. L'ESI est à même d'accepter le sous-message, d'en demander la réémission et de demander à l'UEV d'en reprendre ou d'en abandonner la transmission.

Si le champ de données du dernier sous-message contient exactement 255 octets, il est indispensable d'adjoindre à l'ensemble un sous-message final

([1]) L'insertion de la carte déclenche l'activation des droits d'accès appropriés tant aux données qu'à la fonction de téléchargement.

▼**M1**

comportant un champ de données vide (à l'exception des IDS, PRT et compteur de sous-messages) pour indiquer la fin du message.

Exemple:

En-tête	IDS	PRT	Message	TC
4 octets	Longueur supérieure à 255 octets			

Transmis sous la forme suivante:

En-tête	IDS	PRT	00	01	Sous-message 1	TC
4 octets	255 octets					

En-tête	IDS	PRT	00	02	Sous-message 2	TC
4 octets	255 octets					

…

En-tête	IDS	PRT	xx	yy	Sous-message n	TC
4 octets	Longueur inférieure à 255 octets					

Ou sous la forme:

En-tête	IDS	PRT	00	01	Sous-message 1	TC
4 octets	255 octets					

En-tête	IDS	PRT	00	02	Sous-message 2	TC
4 octets	255 octets					

…

En-tête	IDS	PRT	xx	yy	Sous-message n	TC
4 octets	255 octets					

En-tête	IDS	PRT	xx	yy+1	TC
4 octets	4 octets				

2.2.2. ***Types de message***

Le protocole de communication qui s'applique au téléchargement de données entre l'UEV et l'ESI réclame l'échange de 14 types de message distincts.

La table qui suit en présente une synthèse.

▼**M1**

Structure du message	En-tête de 4 octets max.				Données de 255 octets max.			Total de contrôle d'un octet
ESI -> <- UEV	FMT	CIB	SRC	LON	IDS	SD/ PRT	DONNÉES	TC
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		8F,EA	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
Liaison avec le service de contrôle								
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	ED
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Réponse positive à une demande de vérification du débit en bauds	80	F0	EE	02	C7		01	28
Débit de transition en bauds (étape 2)	80	EE	F0	03	87		02,03	ED
Demande de téléchargement (upload)	80	EE	F0	0A	35		00,00,00,-00,00,FF,-FF,FF,FF	99
Réponse positive à une demande de téléchargement	80	F0	EE	03	75		00,FF	D5
Demande de transfert de données								
Récapitulatif	80	EE	F0	02	36	01		97
Activités	80	EE	F0	06	36	02	Date	CS
Événements et anomalies	80	EE	F0	02	36	03		99
Vitesse instantanée	80	EE	F0	02	36	04		9A
Données techniques	80	EE	F0	02	36	05		9B
Téléchargement (download) d'une carte	80	EE	F0	02	36	06		9C

▼**M1**

Structure du message	En-tête de 4 octets max.				Données de 255 octets max.			Total de contrôle d'un octet
ESI -> <- UEV	FMT	CIB	SRC	LON	IDS	SD/ PRT	DONNÉE-S	TC
Réponse positive à une demande de transfert de données	80	F0	EE	Len	76	TREP	Data	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		Data	CS
Réponses négatives								
Téléchargement 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 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

Notes:

— IDS Dem = IDS de la demande correspondante, IDL Dem = IDL de la demande correspondante.
— PRT = le PDT de la demande correspondante.
— La présence de cellules noires indique une absence de transmission.
— L'utilisation du terme «upload» [téléchargement d'un satellite vers le central] (considéré à partir de l'ESI) s'impose pour garantir la compatibilité du système avec la norme ISO 14229. Ce terme possède la même signification que «download» [téléchargement du central vers un satellite] (considéré à partir de l'UEV).
— Cette table ne présente aucun compteur potentiel de sous-messages de 2 octets.

▼**M1**

2.2.2.1. *Demande d'établissement de la communication (IDS 81)*

Ce message est émis par l'ESI pour établir la liaison d'intercommunication avec l'UEV. Les communications initiales sont toujours effectuées à 9 600 bauds (jusqu'à ce que ce débit soit modifié à l'aide des services appropriés de contrôle des liaisons).

2.2.2.2. *Réponse positive à une demande d'établissement de la communication (IDS C1)*

L'UEV émet ce message pour répondre positivement à une demande d'établissement de la communication. Il comporte les deux octets clés ′8F′ ′EA′ indiquant que l'unité correspondante prend en charge le protocole concerné, l'en-tête de chaque message incluant les octets cible, source et longueur.

2.2.2.3. *Demande d'ouverture d'une session de diagnostic (IDS 10)*

L'ESI émet un message de demande d'ouverture de session de diagnostic dans le but de solliciter une nouvelle session de diagnostic avec l'UEV. La sous-fonction ′session par défaut′ (81 Hex) indique qu'une session de diagnostic standard va être ouverte.

2.2.2.4. *Réponse positive à une demande d'ouverture de session de diagnostic (IDS 50)*

L'UEV émet un message de réponse positive à une demande de diagnostic pour répondre positivement à une demande d'ouverture d'une session de diagnostic.

2.2.2.5. *Service de contrôle de liaison (IDS 87)*

Le service de contrôle de liaison est utilisé par l'ESI pour initier une modification du débit en bauds. Cette opération comporte deux étapes. Dans la première étape, l'ESI propose une modification du débit en bauds, en indiquant le nouveau débit. À réception d'un message positif de l'UEV, l'ESI envoie la confirmation du changement du débit en bauds à l'UEV (deuxième étape). L'ESI passe alors au nouveau débit en bauds. Après réception de la confirmation, l'UEV passe au nouveau débit en bauds.

2.2.2.6. *Réponse positive au contrôle de liaison (IDS C7)*

La réponse positive au contrôle de liaison est délivrée par l'UEV sur demande du service de contrôle de liaison (première étape). À noter qu'aucune réponse n'est donnée à la demande de confirmation (deuxième étape).

2.2.2.7. *Demande de téléchargement (IDS 35)*

L'ESI émet un message de demande de téléchargement afin de préciser à l'UEV qu'il réclame l'exécution d'une opération de téléchargement. Afin de satisfaire aux exigences de la norme ISO 14229, des données sont incluses concernant l'adresse, la taille et les caractéristiques de format des données demandées. Ces informations n'étant pas connues de l'ESI avant le téléchargement, l'adresse de mémoire est mise à 0, la structure est décryptée et décompressée et la taille de la mémoire est mise au maximum.

2.2.2.8. *Réponse positive à une demande de téléchargement (IDS 75)*

L'UEV émet un message de réponse positive à une demande de téléchargement pour signifier à l'ESI que l'UEV est prête à télécharger des données. Afin de satisfaire aux exigences de la norme ISO 14229, le message de réponse positive comprend des données indiquant à l'ESI que les messages ultérieurs de réponse positive à une demande de transfert de données comporteront au maximum 00FF hex octets.

2.2.2.9. *Demande de transfert de données (IDS 36)*

L'ESI émet une demande de transfert de données afin de préciser à l'UEV la nature des données à télécharger. Un paramètre de demande de transfert (PDT) d'un octet indique de quel type de transfert il s'agit.

Il existe six types de transfert de données:

— Récapitulatif (PDT 01)
— Activités associées à une date précise (PDT 02)
— Événements et anomalies (PDT 03)
— Vitesse instantanée (PDT 04)
— Données techniques (PDT 05)
— Téléchargement de carte (PDT 06).

▼**M1**

Il est obligatoire pour l'ESI de demander un transfert de données du type «récapitulatif» (PDT 01) au cours d'une session de téléchargement, car cela seul garantit que les certificats de l'UEV sont enregistrés sur le fichier téléchargé (et permet ainsi la vérification de la signature numérique).

Dans le deuxième cas de figure (PDT 02), le message de demande de transfert de données comporte l'indication du jour civil (format TimeReal) auquel le téléchargement est associé.

2.2.2.10. *Réponse positive à une demande de transfert de données (IDS 76)*

L'UEV émet un message de réponse positive à une demande de transfert de données en réponse à une demande de cette nature. Ce message contient les données réclamées ainsi qu'un paramètre de réponse à une demande de transfert (PRT) correspondant à celui de la demande.

Dans le premier cas (PDT 01), l'UEV enverra des données destinées à aider l'opérateur de l'ESI 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 actuels sur l'UEV

— date la plus précoce et la plus tardive pour le téléchargement (données de l'UEV)

— indications concernant la présence de cartes dans l'UEV

— téléchargements antérieurs vers une entreprise

— verrouillages d'entreprise

— contrôles précédents.

2.2.2.11. *Demande de fin de transfert (IDS 37)*

L'ESI émet un message de demande de fin de transfert pour informer l'UEV que la session de téléchargement est terminée.

2.2.2.12. *Réponse positive à une demande de fin de transfert (IDS 77)*

L'UEV émet un message de réponse positive à une demande de fin de transfert pour accuser réception de la demande de fin de transfert.

2.2.2.13. *Demande d'arrêt de la communication (IDS 82)*

L'ESI émet un message de demande d'arrêt de la communication dans le but de rompre la liaison d'intercommunication avec l'UEV.

2.2.2.14. *Réponse positive à une demande d'arrêt de la communication (IDS C2)*

L'UEV émet un message de réponse positive à une demande d'arrêt de la communication pour accuser réception de la demande d'arrêt de la communication.

2.2.2.15. *Accusé de réception d'un sous-message (IDS 83)*

L'ESI émet un accusé de réception de sous-message pour confirmer la réception des différentes parties d'un message transmis sous forme de sous-messages. Le champ de données contient l'IDS transmis par l'UEV ainsi qu'un code de 2 octets qui s'énonce comme suit:

— MsgC + 1 accuse la réception correcte du sous-message numéro MsgC.

  Demande d'envoi du sous-message suivant adressée à l'UEV par l'ESI.

— MsgC indique la manifestation d'un problème affectant la réception du sous-message numéro MsgC.

  Demande de renvoi du sous-message concerné adressée à l'UEV par l'ESI.

— FFFF réclame l'interruption du message en cours de transmission.

  L'ESI peut recourir à ce code pour mettre un terme à la transmission du message envoyé par l'UEV et ce, quelle qu'en soit la raison.

Le système permet d'accuser (ou non) réception du dernier sous-message d'un message quelconque (octet LON < 255) en recourant ou non à l'un quelconque de ces codes.

Composée de plusieurs sous-messages, la réponse de l'UEV s'énonce comme suit:

— réponse positive à une demande de transfert de données (IDS 76).

▼**M1**

2.2.2.16. *Réponse négative (IDS 7F)*

L'UEV émet le message de réponse négative en réponse aux messages ci-dessus si elle s'avère dans l'impossibilité de satisfaire à la demande transmise. Les champs de données du message contiennent l'IDS de la réponse (7F), l'IDS de la demande, et un code précisant le motif de la réponse négative. Les codes suivants sont d'application:

— 10 rejet général

L'opération ne peut être exécutée pour une raison qui n'est pas abordée ci-après.

— 11 service incompatible

L'IDS de la demande n'est pas intelligible à l'UEV.

— 12 sous-fonction incompatible

Le SD ou le PDT de la demande ne sont pas intelligibles à l'UEV ou la transmission des sous-messages est arrivée à son terme.

— 13 longueur de message incorrecte

La longueur du message reçu est incorrecte.

— 22 conditions non correctes ou erreur affectant la séquence d'interrogation

Le service demandé n'est pas disponible ou la séquence des messages de demande est incorrecte.

— 31 demande non recevable

Le relevé (champ de données) du paramètre de la demande n'est pas valable.

— 50 téléchargement refusé

La demande ne peut être exécutée (l'UEV est exploitée dans un mode inapproprié ou elle présente une anomalie interne).

— 78 réponse en suspens

L'action réclamée ne peut être achevée dans le temps imparti et l'UEV n'est pas prête à accepter une autre demande.

— Données FA indisponibles

L'objet d'une demande de transfert de données n'est pas accessible au sein de l'UEV (p. ex. absence d'insertion de carte, …).

2.2.3. ***Acheminement des messages***

Pendant une procédure de téléchargement normale, l'acheminement des messages s'effectue habituellement comme suit:

ESI		UEV
Demande d'établissement de la communication	⇨	
	⇦	Réponse positive
Demande d'ouverture d'une session de diagnostic	⇨	
	⇦	Réponse positive
Demande de téléchargement	⇨	
	⇦	Réponse positive
Demande de transfert de données #1 Récapitulatif	⇨	
	⇦	Réponse positive

▼**M1**

ESI		UEV
Demande de transfert de données #2	⇨	
	⇦	Réponse positive #1
Accusé de réception d'un sous-message #1	⇨	
	⇦	Réponse positive #2
Accusé de réception d'un sous-message #2	⇨	
	⇦	Réponse positive #m
Accusé de réception d'un sous-message #m	⇨	
	⇦	Réponse positive (champ de données < 255 octets)
Accusé de réception d'un sous-message (facultatif)	⇨	
…		
Demande de transfert de données #n	⇨	
	⇦	Réponse positive
Demande de fin de transfert	⇨	
	⇦	Réponse positive
Demande d'arrêt de la communication	⇨	
	⇦	Réponse positive

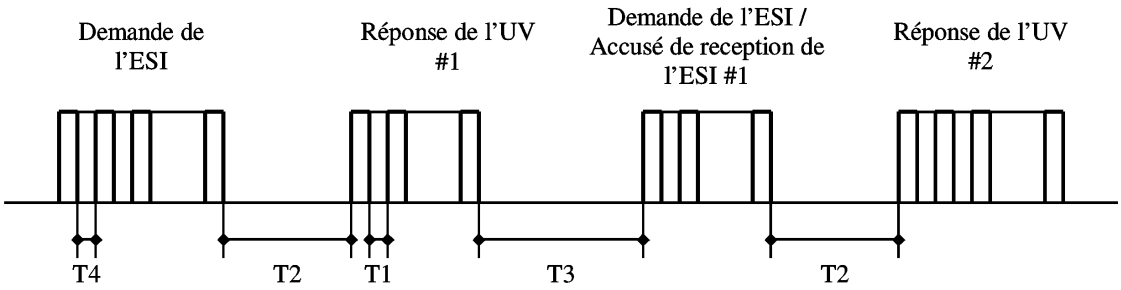
▼M1

2.2.4. ***Synchronisation***

Dans des conditions d'exploitation normales, les paramètres de synchronisation dont la figure ci-après fournit l'illustration sont d'application:

Figure 1

Acheminement des messages, synchronisation



Où:

P1 = Temps interoctet caractérisant une réponse de l'UEV.

P2 = Temps ménagé entre la fin d'une demande de l'ESI et le début de la réponse de l'UEV ou entre la fin d'un accusé de réception de l'ESI et le début de la prochaine réponse de l'UEV.

P3 = Temps ménagé entre la fin d'une réponse de l'UEV et le début d'une nouvelle demande de l'ESI, entre la fin d'une réponse de l'UEV et le début d'un accusé de réception de l'ESI ou entre la fin d'une demande de l'ESI et le début d'une nouvelle demande de l'ESI dans l'éventualité où l'UEV manquerait à répondre.

P4 = Temps interoctet caractérisant une demande de l'ESI.

P5 = Valeur étendue de P3 pour le téléchargement de cartes.

Le tableau ci-après présente les valeurs que les paramètres de synchronisation sont susceptibles de prendre (jeu étendu de paramètres de synchronisation PMC, utilisés en cas d'adressage physique visant à accroître la vitesse des communications).

Paramètre de synchronisation	Limite inférieure (en ms)	Limite supérieure (en ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10 minutes	20 minutes

(*) Si l'UEV réagit en émettant une réponse négative contenant un code qui possède la signification suivante: «réception correcte de la demande, réponse en suspens», cette valeur est portée à la même limite supérieure que celle de P3.

2.2.5. ***Traitement des erreurs***

Si une erreur se manifeste pendant l'échange de messages, le plan d'acheminement des messages est modifié en fonction de l'équipement qui a décelé l'erreur et du message à l'origine de celle-ci.

Les figures 2 et 3 illustrent les procédures de traitement d'erreur appliquées respectivement à l'UEV et à l'ESI.

2.2.5.1. *Phase d'établissement de la communication*

Si l'ESI détecte une erreur au cours de la phase d'établissement de la communication, tant au niveau de la synchronisation qu'au niveau du train de bits, celui-ci temporise alors pendant une période T3min avant d'émettre à nouveau la même demande.

▼M1

Si l'UEV détecte une erreur dans la séquence provenant de l'ESI, celle-ci n'envoie aucune réponse; elle attend un autre message de demande d'établissement de la communication dans un délai P3max.

2.2.5.2. *Phase de communication*

Deux procédures de traitement d'erreur distinctes peuvent être définies:

1. L'UEV détecte une erreur de transmission de l'ESI

L'UEV procède à l'analyse de chaque message reçu afin de déceler toute erreur éventuelle de synchronisation, de structure des octets (p. ex. violations affectant les bits de départ et d'arrêt) ou de perte de verrouillage de trame (réception d'un nombre erroné d'octets, octet total de contrôle erroné).

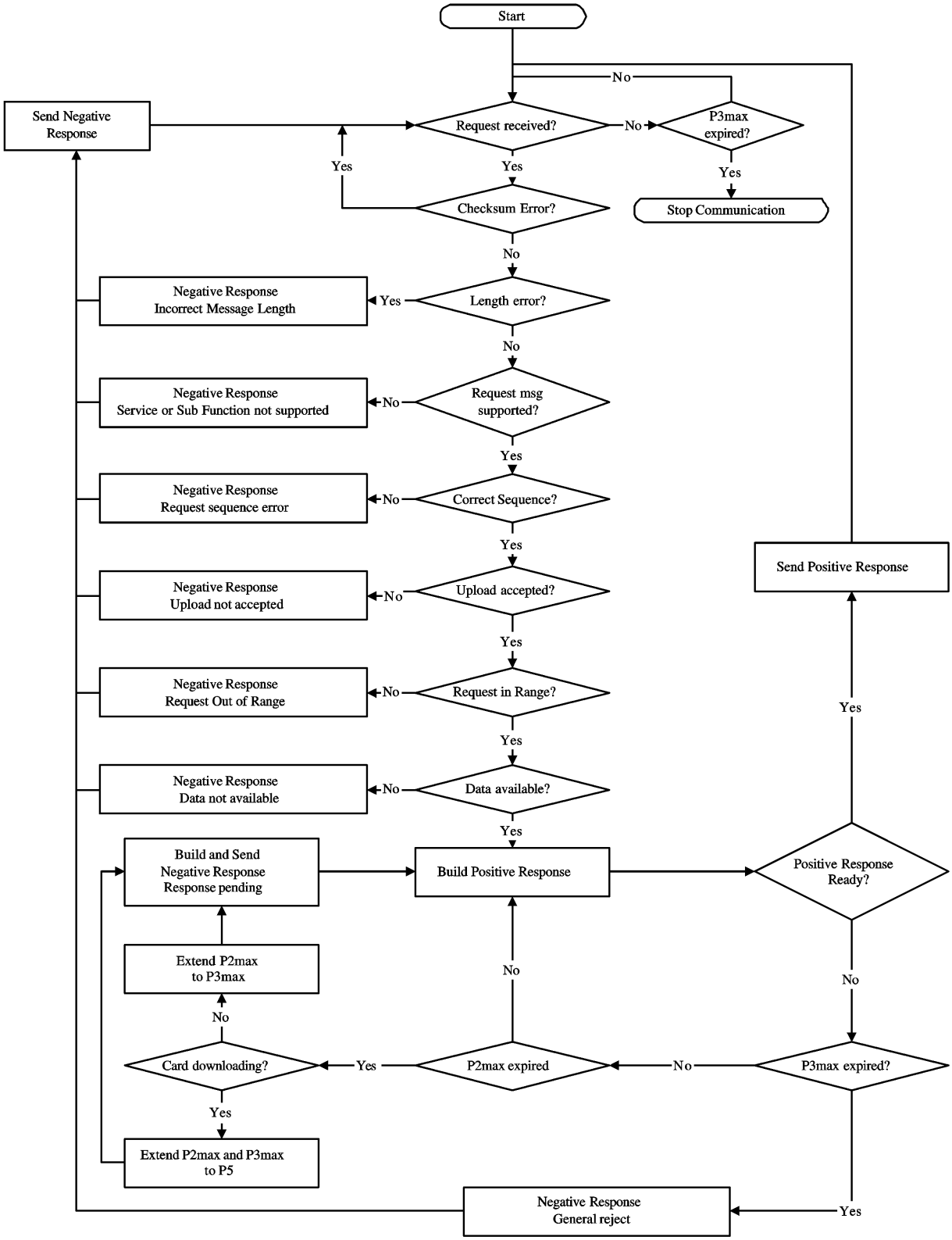
Si l'UEV détecte l'une des erreurs susmentionnées, elle n'envoie aucune réponse et ne tient aucun compte du message reçu.

L'UEV est susceptible de détecter d'autres erreurs affectant la structure ou le contenu du message reçu (p. ex. message incompatible) même si le message satisfait aux critères de longueur et de contrôle requis; en pareil cas, l'UEV doit répondre à l'ESI en lui adressant un message de réponse négatif spécifiant la nature de l'erreur.

▼M1

Figure 2

Traitement d'erreur au niveau de l'UEV



▼M1

2. L'ESI détecte une erreur de transmission de l'UEV

L'ESI procède à l'analyse de chaque message reçu afin de déceler toute erreur éventuelle de synchronisation, de structure des octets (p. ex. violations affectant les bits de départ et d'arrêt) ou de perte de verrouillage de trame (réception d'un nombre erroné d'octets, octet total de contrôle erroné).

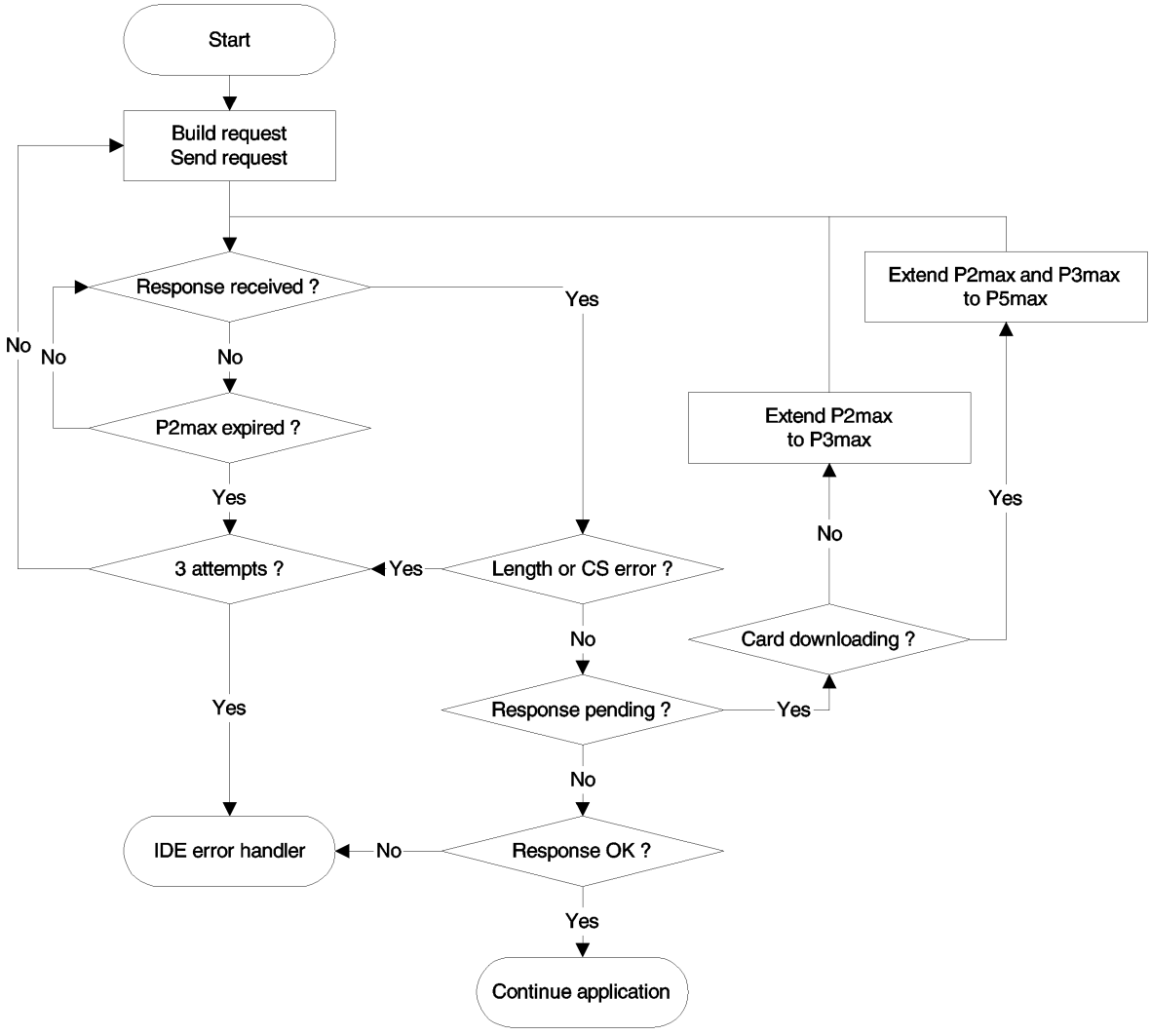
L'ESI détecte les erreurs de séquence telles que l'incrémentation incorrecte du compteur de sous-messages que comportent les messages successifs reçus.

Si l'ESI détecte une erreur ou si l'UEV ne lui envoie aucune réponse dans un délai P2max, le message de demande concerné sera renvoyé à trois reprises au maximum à l'unité destinataire. Aux fins de cette détection d'erreurs, tout accusé de réception d'un sous-message quelconque sera considéré comme une demande adressée à l'UEV.

L'ESI doit temporiser pendant un laps de temps P3min avant d'entreprendre toute transmission; le délai de temporisation se mesure à partir de la dernière occurrence d'un bit d'arrêt relevée après la détection de l'erreur dont il est question.

Figure 3

Traitement d'erreur au niveau de l'ESI



▼M1

2.2.6. ***Contenu des messages de réponse***

Ce paragraphe traite du contenu des champs de données que comportent les différents messages de réponse positive.

Les éléments d'information sont définis dans l'appendice 1 (Dictionnaire de données).

2.2.6.1. *Réponse positive à un récapitulatif de transfert de données*

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 IDS 76 Hex, PRT 01 Hex et critères appropriés de séparation et de comptage des sous-messages:

Élément d'information	Longueur (en octets)	Commentaire
MemberStateCertificate VUCertificate	194 194	Certificats de sécurité de l'UEV
VehicleIdentificationNumber VehicleRegistrationIdentification vehicleRegistrationNation vehicleRegistrationNumber	17 1 14	Identification du véhicule
CurrentDateTime	4	Date et heure actuelles de l'UEV
VuDownloadablePeriod minDownloadableTime maxDownloadableTime	 4 4	Période téléchargeable
CardSlotsStatus	1	Nature des cartes insérées dans les lecteurs de l'UEV
VuDownloadActivityData downloadingTime fullCardNumber companyOrWorkshopName	 4 18 36	Téléchargement antérieur de l'UEV
VuCompanyLocksData noOfLocks	 1	Enregistrement de tous les verrouillages d'entreprise. Si cette section est vide, seule est transmise l'information noOfLocks = 0
...	(98)	
Vu Company Locks Record: lockInTime	4	
Vu Company Locks Record: lockOutTime	4	
Vu Company Locks Record: companyName	36	
Vu Company Locks Record: companyAddress	36	
Vu Company Locks Record: companyCardNumber	18	
...		
VuControlActivityData noOfControls	 1	Enregistrement de tous les relevés de contrôle au sein de l'UEV. Si cette section est vide, seule est transmise l'information noOfControls = 0
...	(31)	
Vu Control Activity Record: controlType	1	
Vu Control Activity Record: controlTime	4	
Vu Control Activity Record: controlCardNumber	18	
Vu Control Activity Record: downloadPeriodBeginTime	4	
Vu Control Activity Record: downloadPeriodEndTime	4	
...		
Signature	128	Signature RSA de toutes les données (à l'exception des certificats); du numéro d'identification du véhicule au dernier octet du dernier relevé d'activité de contrôle de l'UEV

▼**M1**

2.2.6.2. *Réponse positive à une demande de transfert de données relatives aux activités*

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 IDS 76 Hex, PRT 02 Hex et critères appropriés de séparation et de comptage des sous-messages:

Élément d'information	Longueur (en octets)	Commentaire
TimeReal	4	Date du jour téléchargé
OdometerValueMidnight	3	Kilométrage affiché à la fin du jour téléchargé
VuCardIWData		Données relatives aux cycles d'insertion et de retrait des cartes. — Si cette section ne contient aucune donnée disponible, seule est transmise l'information noOfVuCardIWRecords = 0 — Si un relevé d'insertion/retrait de carte au sein de l'UEV couvre une période débutant avant 00h00 (insertion de carte le jour précédent) ou prenant fin après 24h00 (retrait de carte le jour suivant), il apparaît dans son intégralité dans les répertoires relatifs aux deux jours impliqués
noOfVuCardIWRecords	2	
...	(129)	
VuCardIWRecord		
cardHolderName		
holderSurname	36	
holderFirstNames	36	
fullCardNumber	18	
cardExpiryDate	4	
cardInsertionTime	4	
vehicleOdometerValueAtInsertion	3	
cardSlotNumber	1	
cardWithdrawalTime	4	
vehicleOdometerValueAtWithdrawal	3	
previousVehicleInfo		
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
cardWithdrawalTime	4	
manualInputFlag	1	
...		
VuActivityDailyData		État des lecteurs à 00:00 et changements d'activité enregistrés pour le jour téléchargé
noOfActivityChanges	2	
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData		Lieux et sites en rapport avec les données enregistrées pour le jour téléchargé. Si cette section est vide, seule est transmise l'information noOfPlaceRecords = 0
noOfPlaceRecords	1	
...	(28)	
VuPlaceDailyWorkPeriodRecord		
fullCardNumber	18	
placeRecord		
entryTime	4	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		
VuSpecificConditionData		Données relatives aux conditions particulières enregistrées pour le jour téléchargé. Si cette section est vide, seule est transmise l'information noOfSpecificConditionRecords = 0
noOfSpecificConditionRecords	2	
...	(5)	
SpecificConditionRecord		
EntryTime	4	
specificConditionType	1	
...		
Signature	128	Signature RSA de toutes les données; de l'élément Temps réel au dernier octet du dernier relevé relatif aux conditions particulières

▼**M1**

2.2.6.3. *Réponse positive à une demande de transfert de données relatives aux événements et anomalies*

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 IDS 76 Hex, PRT 03 Hex et critères appropriés de séparation et de comptage des sous-messages:

Élément d'information	Longueur (en octets)	Commentaire
VuFaultData		Toutes les anomalies enregistrées ou en cours au sein de l'UEV. Si cette section est vide, seule est transmise l'information noOfVuFaults = 0
NoOfVuFaults	1	
...	(82)	
VuFaultRecord: FaultType	1	
VuFaultRecord: FaultRecordPurpose	1	
VuFaultRecord: FaultBeginTime	4	
VuFaultRecord: FaultEndTime	4	
VuFaultRecord: CardNumberDriverSlotBegin	18	
VuFaultRecord: cardNumberCodriverSlotBegin	18	
VuFaultRecord: CardNumberDriverSlotEnd	18	
VuFaultRecord: CardNumberCodriverSlotEnd	18	
...		
VuEventData		Tous les événements (à l'exception des excès de vitesse) enregistrés ou en cours au sein de l'UEV. Si cette section est vide, seule est transmise l'information noOfVuEvents = 0
NoOfVuEvents	1	
...	(83)	
VuEventRecord: EventType	1	
VuEventRecord: EventRecordPurpose	1	
VuEventRecord: EventBeginTime	4	
VuEventRecord: EventEndTime	4	
VuEventRecord: CardNumberDriverSlotBegin	18	
VuEventRecord: cardNumberCodriverSlotBegin	18	
VuEventRecord: CardNumberDriverSlotEnd	18	
VuEventRecord: CardNumberCodriverSlotEnd	18	
VuEventRecord: SimilarEventsNumber	1	
...		
VuOverSpeedingControlData		Données relatives au dernier contrôle d'excès de vitesse (valeur par défaut en l'absence de données)
LastOverspeedControlTime	4	
FirstOverspeedSince	4	
NumberOfOverspeedSince	1	
VuOverSpeedingEventData		Tous les événements du type excès de vitesse enregistrés au sein de l'UEV. Si cette section est vide, seule est transmise l'information noOfVuOverSpeedingEvents = 0
NoOfVuOverSpeedingEvents	1	
...	(31)	
VuOverSpeedingEventRecord: EventType	1	
VuOverSpeedingEventRecord: EventRecordPurpose	1	
VuOverSpeedingEventRecord: EventBeginTime	4	
VuOverSpeedingEventRecord: EventEndTime	4	
VuOverSpeedingEventRecord: MaxSpeedValue	1	
VuOverSpeedingEventRecord: AverageSpeedValue	1	
VuOverSpeedingEventRecord: CardNumberDriverSlotBegin	18	
VuOverSpeedingEventRecord: SimilarEventsNumber	1	
...		
VuTimeAdjustmentData		Tous les événements de réglage temporel enregistrés au sein de l'UEV (hors du cadre d'un étalonnage complet). Si cette section est vide, seule est transmise l'information noOfVuTimeAdjRecords = 0
NoOfVuTimeAdjRecords	1	
...	(98)	
VuTimeAdjustmentRecord: OldTimeValue	4	
VuTimeAdjustmentRecord: NewTimeValue	4	
VuTimeAdjustmentRecord: WorkshopName	36	
VuTimeAdjustmentRecord: WorkshopAddress	36	
VuTimeAdjustmentRecord: WorkshopCardNumber	18	
...		
Signature	128	Signature RSA de toutes les données; du nombre d'anomalies affectant l'UEV au dernier octet du dernier relevé de réglage temporel

▼**M1**

2.2.6.4. *Réponse positive à une demande de transfert de données relatives à la vitesse du véhicule*

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 IDS 76 Hex, PRT 04 Hex et critères appropriés de séparation et de comptage des sous-messages:

Élément d'information	Longueur (en octets)	Commentaire
VuDetailedSpeedData		Toutes les données relatives à la vitesse instantanée enregistrées au sein de l'UEV (un bloc de vitesse par minute pendant laquelle le véhicule était en mouvement). À raison de 60 vitesses instantanées par minute (une par seconde)
NoOfSpeedBlocks	2	
...		
VuDetailedSpeedBlock		
SpeedBlockBeginDate	4	
speedsPerSecond	60	
...		
Signature	128	Signature RSA de toutes les données; du nombre de blocs de données relatives à la vitesse au dernier octet du dernier bloc de vitesse

2.2.6.5. *Réponse positive à une demande de transfert de données techniques*

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 IDS 76 Hex, PRT 05 Hex et critères appropriés de séparation et de comptage des sous-messages:

Élément d'information	Longueur (octets)	Commentaire
VuIdentification		
vuManufacturerName	36	
vuManufacturerAddress	36	
vuPartNumber	16	
vuSerialNumber	8	
vuSoftwareIdentification		
vuSoftwareVersion	4	
vuSoftInstallationDate	4	
vuManufacturingDate	4	
vuApprovalNumber	8	
SensorPaired		
sensorSerialNumber	8	
sensorApprovalNumber	8	
sensorPairingDateFirst	4	
VuCalibrationData		Tous les relevés d'étalonnage enregistrés au sein de l'UEV
noOfVuCalibrationRecords	1	
...	(164)	
VuCalibrationRecord		
calibrationPurpose	1	
workshopName	36	
workshopAddress	36	
workshopCardNumber	18	
workshopCardExpiryDate	4	
vehicleIdentificationNumber	17	
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
wVehicleCharacteristicConstant	2	
kConstantOfRecordingEquipment	2	
lTyreCircumference	2	
tyreSize	15	
authorisedSpeed	1	
oldOdometerValue	3	
newOdometerValue	3	
oldTimeValue	4	
newTimeValue	4	
nextCalibrationDate	4	
...		
Signature	128	Signature RSA de toutes les données; du nom du fabricant de l'UEV au dernier octet du dernier relevé d'étalonnage de l'UEV

▼M1

2.3. **Archivage de fichiers sur un support de mémoire externe**

Si une session de téléchargement a comporté une opération de transfert de données à partir de l'UEV, l'ESI doit enregistrer au sein d'un seul fichier physique toutes les données transmises par l'UEV pendant cette session de téléchargement dans des messages de réponse positive concernant le transfert de données. La sauvegarde de ces données en exclut les en-têtes de message, compteurs de sous-messages, sous-messages vides et totaux de contrôle; mais elle inclut les IDS et PRT (du premier sous-message dans l'éventualité où leur nombre serait supérieur à l'unité).

3. PROTOCOLE DE TÉLÉCHARGEMENT DES CARTES TACHYGRAPHIQUES

3.1. **Portée**

Ce paragraphe comporte une description du téléchargement direct vers un ESI des données de carte mémorisées sur une carte tachygraphique. L'ESI ne fait pas partie de l'environnement sécurisé; par conséquent, le système n'exécute aucune procédure d'authentification de la carte et de l'ESI.

3.2. **Définitions**

Session de téléchargement: Chaque fois que le système procède à une opération de téléchargement des données enregistrées sur une carte à circuit(s) intégré(s). Cette session couvre l'ensemble de la procédure, de la réinitialisation de la CCI par un PIF à la désactivation de la CCI (retrait de la carte ou réinitialisation suivante).

Fichier de données signé: Fichier enregistré sur la CCI. Ce fichier est transféré en clair vers le PIF. Sur la CCI, le fichier est haché et signé; la signature est transférée vers le PIF.

3.3. **Téléchargement d'une carte**

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

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

— Téléchargement des FE 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 FE de données d'application (dans le FS Tachograph) sauf le FE Card_Download. Ces informations sont protégées par une signature numérique.

  — Il y a lieu de télécharger au moins les FE Application_Identification et ID lors de toute session de téléchargement.

  — Lors du téléchargement d'une carte de conducteur, il faut également procéder obligatoirement au téléchargement des FE suivants:

    — Events_Data,
    — Faults_Data,
    — Driver_Activity_Data,
    — Vehicles_Used,
    — Places,
    — Control_Activity_Data,
    — Specific_Conditions.

— Lors du téléchargement d'une carte de conducteur, il convient de mettre à jour la date du dernier téléchargement dans le FE Card_Download.

— Lors du téléchargement d'une carte d'atelier, il convient de réinitialiser le compteur d'étalonnage enregistré dans le FE Card_Download.

3.3.1. ***Séquence d'initialisation***

L'ESI doit lancer la séquence en procédant comme suit:

Carte	Sens	ESI/PIF	Signification/Remarques
	⇦	Réinitialisation matérielle	
RAR	⇨		

▼**M1**

L'utilisateur a l'option de recourir à la SPP pour passer à un débit supérieur à condition que la CCI en assure la prise en charge.

3.3.2. ***Séquence de téléchargement des fichiers de données non signés***

La séquence de téléchargement des FE ICC, IC, Card_Certificate y CA_Certificate se présente comme suit:

Carte	Sens	ESI/PIF	Signification/Remarques
	⇦	SELECT FILE	Sélection par le biais d'identificateurs de fichier
OK	⇨		
	⇦	READ BINARY	Si le volume des données que contient le fichier est supérieur à la capacité de la mémoire tampon du lecteur ou de la carte, la commande doit être réitérée jusqu'à ce que les données que contient ce fichier aient été extraites dans leur intégralité
Données OK	⇨	Sauvegarder les données sur le SME	En conformité avec le paragraphe 3.4 Format d'archivage des données

Remarque: avant de sélectionner le FE Card_Certificate il convient de sélectionner préalablement l'application tachygraphique (sélection opérée par IDA).

3.3.3. ***Séquence de téléchargement des fichiers de données signés***

Il y a lieu de recourir à la séquence ci-après pour procéder au téléchargement de chacun des fichiers qui suivent accompagnés de leur signature:

Carte	Sens	ESI/PIF	Signification/Remarques
	⇦	SELECT FILE	
OK	⇨		
	⇦	PERFORM HASH OF FILE	Permet de calculer la valeur de hachage par rapport au contenu du fichier sélectionné en appliquant l'algorithme de hachage prescrit en conformité avec l'appendice 11. Cette commande n'est pas une commande ISO
Calculer le hachage du fichier et enregistrer temporairement la valeur de hachage retenue			
OK	⇨		
	⇦	READ BINARY	Si le fichier contient plus de données que le tampon ou la carte ne peut en contenir, la commande doit être réitérée jusqu'à ce que les données que contient ce fichier aient été extraites dans leur intégralité
Données OK	⇨	Sauvegarder les données sur le SME	En conformité avec le paragraphe 3.4 Format d'archivage des données

▼**M1**

Carte	Sens	ESI/PIF	Signification/Remarques
	⇦	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 le SME	En conformité avec le paragraphe 3.4 Format d'archivage des données

3.3.4. ***Séquence de réinitialisation d'un compteur d'étalonnage***

La séquence de réinitialisation du compteur NoOfCalibrationsSinceDownload qui contient le FE Card_Download d'une carte d'atelier se présente comme suit:

Carte	Sens	ESI/PIF	Signification/Remarques
	⇦	SELECT FILE EF Card_Download	Sélection par le biais d'identificateurs de fichier
OK	⇨		
	⇦	UPDATE BINARY NoOfCalibrationsSinceDownload = '00 00'	
réinitialise le nombre de téléchargements de la carte			
OK	⇨		

3.4. **Format d'archivage des données**

3.4.1. ***Introduction***

Les données téléchargées doivent être enregistrées dans les conditions suivantes:

— L'enregistrement des données doit être transparent. En d'autres termes, l'ordre dans lequel se présentent les octets et les bits constitutifs de ces octets doit être préservé lors de l'opération d'archivage exécutée après leur transfert de la carte.

— Tous les fichiers de la carte téléchargés dans le cadre d'une session de téléchargement doivent être enregistrés au sein d'un seul et même fichier sur le SME.

3.4.2. ***Format des fichiers***

Le format des fichiers se présente comme la concaténation de plusieurs objets VLB.

La balise associée à un FE doit prendre la forme de l'IDF du fichier assorti de l'appendice «00».

La balise associée à la signature d'un FE doit prendre la forme de l'IDF du fichier assorti de l'appendice «01».

La longueur correspond à une valeur exprimée par deux octets. Cette valeur détermine le nombre d'octets affectés au champ valeur. La valeur «FF FF» que contient le champ longueur est réservée à un usage ultérieur.

▼M1

Faute de téléchargement, aucune information relative à un fichier déterminé ne sera sauvegardée (pas de balise et pas de longueur zéro).

Toute signature doit être sauvegardée sous forme d'objet VLB immédiatement après l'objet VLB qui contient les données que recèle le fichier concerné.

Définition	Signification	Longueur
IDF (2 octets) || «00»	Balise pour FE (IDF)	3 octets
IDF (2 octets) || «01»	Balise pour signature de FE (IDF)	3 octets
xx xx	Longueur du champ valeur	2 octets

Exemple de données enregistrées dans un fichier de téléchargement sur un SME:

Balise	Longueur	Valeur
00 02 00	00 11	Données du FE ICC
C1 00 00	00 C2	Données du FE Card_Certificate
		…
05 05 00	0A 2E	Données du FE Vehicles_Used
05 05 01	00 80	Signature du FE Vehicles_Used

4. TÉLÉCHARGEMENT D'UNE CARTE TACHYGRAPHIQUE PAR L'INTERMÉDIAIRE D'UNE UNITÉ EMBARQUÉE SUR VÉHICULE

L'UEV doit autoriser le téléchargement du contenu d'une carte de conducteur insérée dans le lecteur d'un ESI connecté.

Cet ESI doit envoyer un message «Demande de transfert de données du type téléchargement de carte» à l'UEV pour lancer ce mode de transmission (cf. 2.2.2.9).

À ce stade, l'UEV 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'ESI de toutes les données extraites de la carte dans le format de fichier VLB approprié (cf. 3.4.2) et encapsulées dans un message «Réponse positive à une demande de transfert de données».

L'ESI doit extraire les données de la carte intégrées au message «Réponse positive à une demande de transfert de données» (en éliminant tous les en-têtes, IDS, PRT, compteurs de sous-messages et totaux de contrôle) et les enregistrer dans un fichier physique conformément à la description présentée au paragraphe 2.3.

Ensuite, l'UEV doit, selon le cas, procéder à une actualisation du fichier de données des activités de contrôle ou de téléchargement de cartes sur la carte du conducteur.

▼**M1**

Appendice 8

PROTOCOLE D'ÉTALONNAGE

TABLE DES MATIÈRES

▼M1

1. INTRODUCTION

Cet appendice traite des modalités d'échange des données entre un appareil d'essai et une unité embarquée sur véhicule par l'intermédiaire de la ligne K. Cette ligne fait partie intégrante de l'interface d'étalonnage décrite à l'appendice 6. Le présent appendice traite aussi du contrôle de la ligne de signalisation d'entrée/sortie exercé au niveau du connecteur d'étalonnage.

L'établissement de communications sur la ligne K est décrit au chapitre 4 «Services de communication».

Le présent appendice s'appuie sur le concept de «sessions de diagnostic» pour déterminer la portée du contrôle de la ligne K au gré de l'évolution des modalités d'échange. La session par défaut est la «StandardDiagnosticSession», où toutes les données que contient une unité embarquée sur véhicule sont susceptibles d'en être extraites, mais aucune donnée ne peut être enregistrée sur cette unité.

La sélection de l'option «session de diagnostic» fait l'objet d'une description détaillée au chapitre 5 «Services de gestion».

La «ECUProgrammingSession» autorise l'entrée de données au sein de l'unité embarquée sur véhicule. En cas d'entrée de données d'étalonnage (exigences 097 et 098), l'unité embarquée sur véhicule doit en outre être exploitée en mode ÉTALONNAGE.

Le transfert de données par l'intermédiaire de la ligne K fait l'objet d'une description détaillée au chapitre 6 «Services de transmission de données». Les formats des données transférées sont décrits en détail au chapitre 8 «Structures des relevés de données».

La session de réglage «ECUAdjustmentSession» permet de sélectionner le mode de la ligne de signalisation d'entrée/sortie d'étalonnage par le biais de l'interface avec la ligne K. Le contrôle de la ligne de signalisation d'entrée/sortie d'étalonnage fait l'objet d'une description détaillée au chapitre 7 «Contrôle des impulsions d'essai — Unité fonctionnelle de contrôle des entrées/sorties».

Tout au long de ce document, l'appareil d'essai possède l'adresse suivante: ′tt′. Bien que certaines adresses d'appareil d'essai soient privilégiées, l'UEV doit réagir correctement à toute adresse d'appareil d'essai. L'adresse physique de l'UEV s'énonce comme suit: 0xEE.

2. TERMINOLOGIE, DÉFINITIONS ET RÉFÉRENCES

Les protocoles, messages et codes d'erreur sont principalement basés sur la version actuelle du projet de norme ISO 14229-1 (Véhicules routiers — systèmes de diagnostic — Partie 1: services de diagnostic, version 6 du 22 février 2001).

Des codages d'octets et autres valeurs hexadécimales s'utilisent lors de la définition des identificateurs de service, de l'élaboration des demandes et réponses de service et de la configuration des paramètres standard.

Le terme «appareil d'essai» fait référence à l'équipement utilisé pour entrer des données de programmation/étalonnage dans l'UEV.

Les termes «client» et «serveur» font respectivement référence à l'appareil d'essai et à l'unité embarquée sur véhicule.

Le terme UCE signifie «unité de commande électronique» et s'applique à l'UEV.

Références:

ISO 14230-2: Véhicules routiers — Systèmes de diagnostic — Protocole à mots clés 2000 — Partie 2: Couche liaison de données. Première édition: 1999. Véhicules routiers — Systèmes de diagnostic

3. VUE D'ENSEMBLE DES SERVICES

3.1. **Services disponibles**

Le tableau qui suit présente une vue d'ensemble des services définis dans le présent document et auxquels se doit de pourvoir l'appareil de contrôle.

Ce tableau indique quels sont les services disponibles lors d'une session de diagnostic active.

— La 1re colonne répertorie les services disponibles

— La 2e colonne indique le numéro du paragraphe qui présente une description détaillée du service considéré dans le présent appendice.

— La 3e colonne indique la valeur affectée à l'identificateur de service concerné dans les messages de demande de service.

▼M1

— La 4e colonne précise quels sont les services de la «StandardDiagnosticSession» (SD) dont la mise en œuvre au sein de l'UEV est indispensable.

— La 5e colonne précise quels sont les services de la «ECUAdjustmentSession» (ECUAS) dont la mise en œuvre est indispensable pour permettre un contrôle adéquat de la ligne de signalisation d'entrée/sortie au niveau du connecteur d'étalonnage monté sur la face avant de l'UEV.

— La 6e colonne précise quels sont les services de la «ECUProgrammingSession» (ECUPS) dont la mise en œuvre est indispensable pour procéder à la programmation des paramètres d'exploitation au sein de l'UEV.

Tableau 1

Tableau récapitulatif des valeurs affectées aux identificateurs de service

Noms des services de diagnostic	Paragraphes	Valeurs affectées aux identificateurs de services	Sessions de diagnostic		
			SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Ce symbole rappelle le caractère obligatoire du service correspondant pendant cette session de diagnostic.Aucun symbole n'indique que l'exécution du service correspondant n'est pas autorisée pendant cette session de diagnostic.

3.2. **Codes de réponse**

Des codes de réponse sont définis pour chaque service.

4. SERVICES DE COMMUNICATION

Certains services sont nécessaires à l'établissement et au maintien des communications. Ils n'apparaissent pas dans la couche application. Le tableau qui suit répertorie les différents services disponibles:

Tableau 2

Services de communication

Noms des services	Description
StartCommunication	Le client demande le lancement d'une session de communication avec un ou plusieurs serveurs
StopCommunication	Le client demande l'arrêt de la session de communication en cours
TesterPresent	Le client indique au serveur qu'il est encore présent

Le service StartCommunication s'utilise pour établir une communication. L'exécution de tout service suppose l'établissement d'une communication et la sélection de paramètres adaptés au mode d'exploitation souhaité.

4.1. **Service StartCommunication**

À la réception d'une primitive d'indication StartCommunication, l'UEV vérifie si l'établissement de la liaison d'intercommunication requise est envisageable dans les conditions en vigueur. Les conditions d'établissement d'une liaison d'inter-

▼M1

communication font l'objet d'une description détaillée dans le document ISO 14230-2.

Ensuite, l'UEV doit exécuter toutes les actions nécessaires à l'établissement de la liaison d'intercommunication requise et envoyer une primitive de réponse Start-Communication avec les paramètres de réponse positive sélectionnés.

Si une UEV déjà initialisée (et entrée en session de diagnostic) reçoit une nouvelle demande d'établissement d'une liaison d'intercommunication (p.ex. en raison d'une reprise sur incident au niveau de l'appareil d'essai), cette demande doit être acceptée et l'UEV réinitialisée.

Si, pour une raison quelconque, l'établissement de la liaison d'intercommunication s'avère impossible, l'UEV doit continuer à fonctionner dans les mêmes conditions qu'immédiatement avant la tentative d'établissement d'une liaison d'intercommunication.

Le message de demande d'établissement d'une communication doit être adressé physiquement.

L'initialisation de l'UEV pour les services est réalisée par la méthode d'initialisation rapide:

— Temps d'occupation/inoccupation préalable à toute activité

— Transmission d'une configuration d'initialisation par l'appareil d'essai

— Toutes les informations nécessaires à l'établissement d'une communication sont contenues dans la réponse de l'UEV.

Après initialisation,

— Les valeurs attribuées à l'ensemble des paramètres de communication sont celles définies dans le tableau 4 en fonction des octets clés.

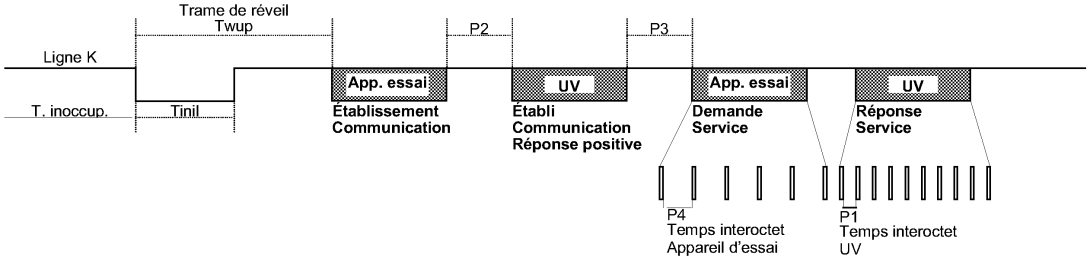
— L'UEV attend la première demande en provenance de l'appareil d'essai.

— L'UEV est exploitée en mode de diagnostic par défaut, autrement dit le mode StandardDiagnosticSession.

— La ligne de signalisation d'E/S d'étalonnage est dans son état d'exploitation par défaut, à savoir, désactivée.

Le débit de données sur la ligne K est de 10 400 bauds.

L'initialisation rapide est lancée par l'appareil d'essai, lequel émet une trame de réveil (Wup) sur la ligne K. Cette trame débute au terme d'un délai d'inoccupation de la ligne K suivi d'un temps de Tinil. L'appareil d'essai émet le premier bit du StartCommunicationService au terme d'un délai de Twup suivi du premier front descendant.



Les valeurs de synchronisation propres à l'initialisation rapide et aux communications en général font l'objet d'une description détaillée dans les tableaux ci-après. Pour ce qui concerne le temps d'inoccupation, trois possibilités sont envisageables:

— Première transmission après la mise sous tension, T. inoccup. = 300 ms

— Après clôture d'un StopCommunicationService, T. inoccup. = P3 min.

— Après interruption d'une communication pour cause de dépassement du temps imparti P3 max, T. inoccup. = 0.

Tableau 3

Valeurs de synchronisation propres à l'initialisation rapide

Paramètre		Valeur min.	Valeur max.
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

▼**M1**

Tableau 4

Valeurs accordées aux paramètres de synchronisation des communications

Paramètre de synchronisation	Synchronisation	Valeurs minimales admises (ms)	Valeurs maximales admises (ms)
		min.	max.
P1	Délai interoctet à respecter dans l'attente d'une réponse de l'UEV	0	20
P2	Laps de temps entre une demande de l'appareil d'essai et une ou deux réponses de l'UEV	25	250
P3	Laps de temps entre la fin des réponses de l'UEV et le début d'une nouvelle demande émise par l'appareil d'essai	55	5 000
P4	Délai interoctet à respecter dans l'attente d'une demande émise par l'appareil d'essai	5	20

La structure des messages transmis dans le cadre d'une initialisation rapide fait l'objet d'une description détaillée dans les tableaux qui suivent.

Tableau 5

Message de demande d'établissement de communication

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	81	FMT
#2	Octet d'adresse de la cible	EE	CIB
#3	Octet d'adresse de la source	tt	SRC
#4	ID du service Demande d'établissement de communication	81	DEC
#5	Total de contrôle	00-FF	TC

Tableau 6

Message de réponse positive à une demande d'établissement de communication

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	CIB
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LON
#5	ID du service Réponse positive à une demande d'établissement de communication	C1	RPDEC
#6	Octet clé 1	EA	OC1
#7	Octet clé 2	8F	OC2
#8	Total de contrôle	00-FF	TC

Il n'y a pas de réponse négative au message de demande d'établissement de communication. Faute de message de réponse positive à transmettre, l'UEV n'est pas initialisée, aucune donnée n'est émise et le système demeure en mode d'exploitation normal.

▼M1

4.2. **Service StopCommunication**

4.2.1. ***Description des messages***

Ce service portant sur la couche communication vise à mettre un terme à toute session de communication.

À la réception d'une primitive d'indication StopCommunication, l'UEV doit vérifier si les conditions en vigueur permettent d'interrompre la communication en cours. Si tel est le cas, l'UEV doit exécuter toutes les opérations requises pour mettre un terme à cette communication.

Si une interruption de la communication est envisageable, l'UEV doit émettre une primitive de réponse StopCommunication en recourant aux paramètres de réponse positive sélectionnés, avant de clore la communication.

Si, pour une raison quelconque, il s'avère impossible d'interrompre la communication concernée, l'UEV doit émettre une primitive de réponse StopCommunication en recourant au paramètre de réponse négative sélectionné.

Si l'UEV détecte un dépassement du délai P3max, la communication est interrompue sans s'accompagner de l'émission d'aucune primitive de réponse.

4.2.2. ***Structure des messages***

La structure des messages associés aux primitives StopCommunication fait l'objet d'une description détaillée dans les tableaux ci-après.

Tableau 7

Message de demande d'interruption de communication

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	CIB
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	01	LON
#5	ID du service Demande d'interruption de communication	82	DIC
#6	Total de contrôle	00-FF	TC

Tableau 8

Message de réponse positive à une demande d'interruption de communication

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	CIB
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	01	LON
#5	ID du service Réponse positive à une demande d'interruption de communication	C2	RPDIC
#6	Total de contrôle	00-FF	CS

Tableau 9

Message de réponse négative à une demande d'interruption de communication

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	CIB

▼M1

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LON
#5	ID du service Réponse négative	7F	RN
#6	ID du service Demande d'interruption de communication	82	DIC
#7	Code de réponse = generalReject	10	CR_GR
#8	Total de contrôle	00-FF	TC

4.2.3. ***Définition des paramètres***

Ce service ne nécessite la définition d'aucun paramètre.

4.3. **Service TesterPresent**

4.3.1. ***Description du message***

Le service TesterPresent est utilisé par l'appareil d'essai pour indiquer au serveur qu'il est encore présent, afin d'empêcher que le serveur ne retourne automatiquement en fonctionnement normal et ne coupe éventuellement la communication. Ce service, envoyé périodiquement, maintient en activité la session de diagnostic et la communication en remettant à zéro le compteur P3 à chaque demande de prestation.

4.3.2. ***Format du message***

La structure des messages associés aux primitives TesterPresent fait l'objet d'une description détaillée dans les tableaux ci-après.

Tableau 10

Message de demande d'indication de présence de l'appareil d'essai

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	CIB
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	02	LON
#5	ID du service Demande d'indication de présence de l'appareil d'essai	3E	IPAE
#6	Sous-fonction = responseRequired (réponse requise) = [yes (oui) no (non)]	01 02	RESPREQ_-Y RESPREQ_-NO
#7	Total de contrôle	00-FF	CS

Si le paramètre responseRequired est «oui», le serveur répondra par le message positif suivant. Si le paramètre est «non», le serveur n'envoie pas de réponse.

Tableau 11

Message de réponse positive de l'indicateur de présence de l'appareil d'essai

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT

▼**M1**

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#2	Octet d'adresse de la cible	tt	CIB
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	01	LON
#5	ID du service Réponse positive de l'indicateur de présence de l'appareil d'essai	7E	RPIPAE
#6	Total de contrôle	00-FF	CS

Le service accepte les codes de réponse négative suivants:

Tableau 12

Message de réponse négative de l'indicateur de présence de l'appareil d'essai

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	CIB
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LON
#5	ID du service Réponse négative	7E	RN
#6	ID du service Demande de l'indicateur de présence	3E	TP
#7	Code réponse = [SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_-IF
	incorrectMessageLength] (sous-fonction non acceptée-format non valable-longueur de message incorrecte)	13	RC_IML
#8	Total de contrôle	00-FF	CS

5. SERVICES DE GESTION

Le tableau qui suit répertorie les différents services disponibles:

Tableau 13

Services de gestion

Noms des services	Description
StartDiagnosticSession	Le client demande le lancement d'une session de diagnostic avec une UEV
SecurityAccess	Le client demande l'accès à certaines fonctions réservées aux utilisateurs autorisés

5.1. **Service StartDiagnosticSession**

5.1.1. ***Description des messages***

Le service StartDiagnosticSession permet d'activer différentes sessions de diagnostic au sein du serveur. Une session de diagnostic autorise l'exploitation d'un jeu de services spécifique, conformément aux indications fournies au tableau 17. Une session peut permettre des services spécifiques du constructeur du véhicule

▼M1

qui ne font pas partie du présent document. Les règles de mise en œuvre doivent satisfaire aux exigences suivantes:

— il doit toujours y avoir exactement une session de diagnostic en cours dans l'UEV;

— l'UEV doit toujours ouvrir la session standard de diagnostic lorsqu'elle est mise sous tension; si aucune autre session de diagnostic n'est ouverte, la session standard de diagnostic doit rester ouverte aussi longtemps que l'UEV est sous tension;

— si une session de diagnostic déjà ouverte a été demandée par l'appareil d'essai, l'UEV envoie un message de réponse positive;

— lorsque l'appareil d'essai demande une nouvelle session de diagnostic, l'UEV envoie d'abord un message de réponse positive à la demande d'ouverture d'une session de diagnostic avant que la nouvelle session ne s'ouvre dans l'UEV. Si l'UEV n'a pu ouvrir la nouvelle session de diagnostic demandée, il envoie un message de réponse négative à la demande d'ouverture d'une session de diagnostic, et la session en cours se poursuit.

Le lancement d'une session de diagnostic n'est envisageable qu'à la condition qu'une communication ait été préalablement établie entre le client et l'UEV.

Les paramètres de synchronisation définis dans le tableau 4 deviendront actifs au terme de l'exécution réussie d'un service StartDiagnosticSession, pour autant que le message de demande comporte le paramètre de session de diagnostic «Session standard» dans l'éventualité où une autre session de diagnostic aurait été préalablement active.

5.1.2. ***Structure des messages***

La structure des messages associés aux primitives StartDiagnosticSession fait l'objet d'une description détaillée dans les tableaux ci-après.

Tableau 14

Message de demande de lancement d'une session de diagnostic

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	CIB
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	02	LON
#5	ID du service Demande de lancement d'une session de diagnostic	10	DLSD
#6	Session de diagnostic = [une valeur extraite du tableau 17]	xx	SD_ …
#7	Total de contrôle	00-FF	TC

Tableau 15

Message de réponse positive à une demande de lancement d'une session de diagnostic

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	CIB
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	02	LON
#5	ID du service Réponse positive à une demande de lancement d'une session de diagnostic	50	RPDLSD
#6	Session de diagnostic = [même valeur que l'octet #6 du tableau 14]	xx	SD_ …

▼M1

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#7	Total de contrôle	00-FF	TC

Tableau 16

Message de réponse négative à une demande de lancement d'une session de diagnostic

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	CIB
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LON
#5	ID du service Réponse négative	7F	RN
#6	ID du service Demande de lancement d'une session de diagnostic	10	DLSD
#7	Code réponse = [subFunctionNotSupported — (sous-fonction non acceptée) ([a])	12	RC_SFNS
	incorrectMessageLength — (longueur de message incorrecte) ([b])	13	RC_IML
	conditionsNotCorrect — (conditions non correctes) ([c])]	22	RC_CNC
#8	Total de contrôle	00-FF	TC

([a]) La valeur introduite dans l'octet #6 du message de demande n'est pas prise en charge, c.-à-d. pas dans le tableau 17.

([b]) La longueur du message est incorrecte.

([c]) Les critères pour la demande d'ouverture d'une session de diagnostic (StartDiagnosticSession) ne sont pas remplis.

5.1.3. ***Définition des paramètres***

Le service StartDiagnosticSession a recours au paramètre Session de diagnostic (SDC_) pour sélectionner le comportement particulier du ou des serveurs. Les sessions de diagnostic qui suivent sont précisées dans le présent document:

Tableau 17

Définition des valeurs affectées aux sessions de diagnostic

Hex	Description	Mnémonique
81	Session standard de diagnostic (StandardDiagnosticSession) Cette session de diagnostic permet d'activer tous les services indiqués dans le tableau 1 colonne 4 «SD». Ces services autorisent l'extraction de données enregistrées sur un serveur (UEV). Cette session de diagnostic ne devient active qu'après la réussite de la phase d'initialisation entre client (appareil d'essai) et serveur (UEV). Cette session est susceptible d'être écrasée par d'autres sessions de diagnostic spécifiées dans ce chapitre.	SD
85	Session de programmation de l'UCE (ECUProgrammingSession) Cette session de diagnostic permet d'activer tous les services répertoriés dans tableau 1 colonne 6 «ECUPS». Ces services prennent en charge la programmation de la mémoire d'un serveur (UEV). Cette session de diagnostic est susceptible d'être écrasée par d'autres sessions de diagnostic spécifiées dans ce chapitre.	SPUCE

▼M1

Hex	Description	Mnémonique
87	Session de réglage de l'UCE (ECUAdjustmentSession) Cette session de diagnostic permet d'activer tous les services répertoriés dans le tableau 1 colonne 5 «ECUAS». Ces services prennent en charge le contrôle des entrées/sorties d'un serveur (UEV). Cette session de diagnostic est susceptible d'être écrasée par d'autres sessions de diagnostic spécifiées dans ce chapitre.	SRUCE

5.2. **Service SecurityAccess**

Pour que l'enregistrement de données d'étalonnage et l'accès à la ligne d'entrée/sortie d'étalonnage soient envisageables, il faut que l'UEV soit exploitée en mode ÉTALONNAGE. Outre l'insertion d'une carte d'atelier valide dans le lecteur approprié de l'UEV, il est indispensable d'entrer le numéro d'identification individuel adéquat dans l'UEV pour avoir accès au mode ÉTALONNAGE.

Le service SecurityAccess permet d'introduire le numéro d'identification individuel et d'indiquer à l'appareil d'essai si l'UEV est exploitée ou non en mode ÉTALONNAGE.

Le système permet de recourir à d'autres méthodes pour entrer ce numéro d'identification individuel.

5.2.1. ***Descriptions des messages***

Le service SecurityAccess comporte l'exécution d'un message «requestSeed» (demande de germe), suivi le cas échéant d'un message «sendKey» (demande d'envoi d'une clé). Le service SecurityAccess doit être exécuté après le service StartDiagnosticSession.

L'appareil d'essai doit recourir au message SecurityAcess "requestSeed" pour vérifier si l'unité embarquée sur véhicule est prête à accepter un numéro d'identification individuel.

Si l'unité embarquée sur véhicule est déjà en mode ÉTALONNAGE, elle répond à la demande qui lui est adressée par l'envoi d'un «germe» de 0x0000 en utilisant le service Réponse positive à la demande SecurityAccess.

Si l'unité embarquée sur véhicule est prête à accepter un numéro d'identification individuel en vue d'une opération de vérification par le biais d'une carte d'atelier, elle doit répondre à la demande qui lui est adressée par l'envoi d'un «germe» d'une valeur supérieure à 0x0000 en utilisant le service Réponse positive à la demande SecurityAccess.

Si l'unité embarquée sur véhicule n'est pas prête à accepter un numéro d'identification individuel émanant de l'appareil d'essai parce que la carte d'atelier insérée dans le lecteur n'est pas valable, parce que ce dernier n'en contient aucune ou que l'unité embarquée sur véhicule attend la transmission du numéro d'identification individuel requis par une autre méthode, celle-ci doit répondre à la demande qui lui est adressée par l'envoi d'une réponse négative accompagnée d'un code de réponse conditionsNotCorrect ou ResquestSequenceError.

En définitive, l'appareil d'essai devra recourir au message SecurityAcess «sendKey» pour transmettre un numéro d'identification individuel à l'unité embarquée sur véhicule. Pour ménager le temps nécessaire à l'exécution du processus d'authentification de la carte, l'UEV devra recourir au code de réponse négative requestCorrectlyReceived-ResponsePending (demande bien reçue — réponse suit) afin de prolonger le temps de réponse. Le temps de réponse ne devra cependant pas dépasser 5 minutes. Dès que le service demandé est exécuté, l'UEV envoie un message de réponse positive ou négative avec un code de réponse différent du code précité. Le code de réponse négative requestCorrectlyReceived-ResponsePending peut être répété par l'UEV jusqu'à ce que le service demandé soit exécuté et le message de réponse finale envoyé.

L'unité embarquée sur véhicule ne doit répondre à cette demande en recourant au service Réponse positive à la demande SecurityAccessRequest#2 qu'à la condition d'être exploitée en mode ÉTALONNAGE.

Dans les cas énumérés ci-après, l'unité embarquée sur véhicule doit répondre à cette demande par une réponse négative accompagnée de l'un des codes de réponse suivants:

— SubFunctionNotSupported: format non valable pour le paramètre de la sous-fonction (accessType)

— conditionsNotCorrectorRequestSequenceError: unité embarquée sur véhicule pas prête à accepter l'entrée d'un numéro d'identification individuel

— InvalidKey: Numéro d'identification individuel non valable sans dépassement du nombre de tentatives de vérification de ce numéro

▼M1

— ExceedNumberOfAttempts: Numéro d'identification individuel non valable et dépassement du nombre de tentatives de vérification de ce numéro

— generalReject: Numéro d'identification individuel correct, mais échec de la tentative d'authentification mutuelle avec la carte d'atelier utilisée.

5.2.2. ***Structure des messages — SecurityAccessRequest#1***

La structure des messages associés aux primitives SecurityAccess "requestSeed" fait l'objet d'une description détaillée dans les tableaux ci-après.

Tableau 18

Message de demande SecurityAccess — requestSeed

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	CIB
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	02	LON
#5	ID du service Demande SecurityAccess	27	SA
#6	Mode d'accès — demande de germe (resquest-Seed)	7D	MA_DG
#7	Total de contrôle	00-FF	TC

Tableau 19

Message de réponse positive à une demande SecurityAccess — requestSeed

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	CIB
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	04	LON
#5	ID du service Réponse positive à une demande SecurityAccess	67	RPAS
#6	Mode d'accès — demande de germe	7D	MA_DG
#7	Germe supérieur	00-FF	GERMSUP
#8	Germe inférieur	00-FF	GERMINF
#9	Total de contrôle	00-FF	TC

Tabelle 20

Message de réponse négative à une demande SecurityAccess

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	CIB
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LON
#5	ID du service Réponse négative	7F	RN

▼M1

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#6	ID du service Demande SecurityAccess	27	AS
#7	Codederéponse=[conditionsNotCorrectOrRequestSequenceError	22	CR_CNC
	incorrectMessageLength]	13	RC_IML
#8	Total de contrôle	00-FF	TC

5.2.3. ***Structure des messages — SecurityAccess — sendKey***

La structure des messages associés aux primitives SecurityAccess «sendKey» fait l'objet d'une description détaillée dans les tableaux ci-après.

Tableau 21

Message de demande SecurityAccess — sendKey

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	CIB
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	m+2	LON
#5	ID du service Demande SecurityAccess	27	AS
#6	Mode d'accès — envoi d'une clé (sendKey)	7E	MA_EC
#7 a #m+6	Clé#1 (sup)	xx	CLE
	…	…	
	Clé #m (inf, la valeur de m doit être comprise entre 4 et 8 inclus)	xx	
#m+7	Total de contrôle	00-FF	TC

Tableau 22

Message de réponse positive à une demande SecurityAccess — sendKey

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	CIB
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	02	LON
#5	ID du service Réponse positive à une demande SecurityAccess	67	RPAS
#6	Mode d'accès — envoi d'une clé (sendKey)	7E	MA_EC
#7	Total de contrôle	00-FF	TC

▼**M1**

Tableau 23

Message de réponse négative à une demande SecurityAccess

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	CIB
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LON
#5	ID du service Réponse négative	7F	NR
#6	ID du service SecurityAccess	27	AS
#7	Code de réponse = [generalReject	10	CR_GR
	subFunctionNotSupported	12	CR_SFNS
	incorrectMessageLength	13	CR_IML
	conditionsNotCorrectOrRequestSequenceError	22	CR_CNC
	invalidKey	35	CR_IK
	exceededNumberOfAttempts	36	CR_ENA
	requestCorrectlyReceived-ResponsePending]	78	CR_RCR_-RP
#8	Total de contrôle	00-FF	TC

6. SERVICES DE TRANSMISSION DE DONNÉES

Les services disponibles font l'objet d'une description détaillée dans le tableau ci-après:

Tableau 24

Services de transmission de données

Noms des services	Description
ReadDataByIdentifier	Le client demande la transmission de la valeur actuelle d'un relevé auquel un identificateur commun permet d'accéder
WriteDataByIdentifier	Le client demande l'enregistrement d'un relevé auquel un identificateur a permis d'accéder

6.1. **Service ReadDataByIdentifier**

6.1.1. ***Description des messages***

Le message de demande ReadDataByIdentifier est utilisé par le client pour demander l'extraction de valeurs enregistrées sur un serveur. Les données sont identifiées par un Identificateur de relevés. Il incombe au fabricant de l'UEV de veiller à ce que les conditions du serveur soient remplies lors de l'exécution de ce service.

6.1.2. ***Structure des messages***

La structure des messages associés aux primitives ReadDataByIdentifier fait l'objet d'une description détaillée dans les tableaux ci-après.

▼M1

Tableau 25

Message de demande de lecture de données par un identificateur

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	CIB
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	03	LON
#5	ID du service Demande ReadDataByIdentifier	22	RDBI
#6 à #7	Identificateur de relevés = [une valeur extraite du tableau 28]	xxxx	IRL_ …
#8	Total de contrôle	00-FF	TC

Tableau 26

Message de réponse positive à une demande de lecture de données par un identificateur

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	CIB
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	m+3	LON
#5	ID du service Réponse positive à une demande ReadDataByIdentifier	62	RPDRDBI
#6 et #7	Identificateur local de relevés = [même valeur que les octets #6 et #7 du tableau 25]	xxxx	ILR_ …
#8 à #m+7	Valeur de relevé#1 : valeur de relevé#m	xx : xx	VR_ … : VR_ …
#m+8	Total de contrôle	00-FF	TC

Tableau 27

Message de réponse négative à une demande de lecture de données par un identificateur

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	CIB
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LON
#5	ID du service Réponse négative	7F	RN
#6	ID du service Demande ReadDataByIdentifier	22	RDBI

▼**M1**

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#7	Code de réponse = [requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect]	22	RC_CNC
#8	Total de contrôle	00-FF	TC

6.1.3. ***Définition des paramètres***

Le paramètre Identificateur de relevés (IR_) dans le message de demande ReadDataByIdentifier identifie un relevé de données.

Les valeurs qu'un identificateur de relevés (recordDataIdentifier) est susceptible de prendre sont indiquées dans le tableau ci-après.

Ce tableau des identificateurs de relevés se compose de quatre colonnes et d'un certain nombre de lignes.

— La 1re colonne (Hex.) indique la «Valeur hex.» affectée à l'identificateur de relevés spécifié dans la 3e colonne.

— La 2e colonne (Élément de donnée) indique l'élément de donnée de l'appendice 1 sur lequel est basé l'identificateur de relevés (un transcodage est parfois nécessaire).

— La 3e colonne (Description) indique le nom de l'identificateur de relevés correspondant.

— La 4e colonne (Mnémonique) indique le mnémonique associé à cet identificateur de relevés.

Tableau 28

Définition des valeurs attribuées aux identificateurs de relevés

Hex.	Élément de donnée	Nom de l'identificateur de relevés (voir la structure indiquée au chapitre 8, partie 2)	Mnémonique
F90B	CurrentDateTime	Date et heure	IR_DH
F912	HighResOdometer	Kilométrage total du véhicule en haute définition	IR_KTVHD
F918	K-ConstantOfRecordingEquipment	Facteur K	IR_FK
F91C	L-TyreCircumference	Circonférence des pneus Facteur L	IR_FL
F91D	W-VehicleCharacteristicConstant	Coefficient W caractéristique du véhicule	IR_CWCV
F921	TyreSize	Dimensions des pneumatiques	IR_DP
F922	nextCalibrationDate	Date du prochain étalonnage	IR_DPE
F92C	SpeedAuthorised	Vitesse autorisée	IR_VA
F97D	vehicleRegistrationNation	État membre d'immatriculation	IR_EMI
F97E	VehicleRegistrationNumber	Numéro d'immatriculation du véhicule	IR_NIMV
F190	VehicleIdentificationNumber	Numéro d'identification du véhicule	IR_NIDV

Le paramètre Valeur de relevé (VR_) est utilisé pour le message de réponse positive ReadDataByIdentifier pour fournir au client (appareil d'essai) le relevé de données identifié par l'identificateur de relevés. Les structures de données sont indiquées au chapitre 8. D'autres relevés de données, telles que les entrées propres à l'UEV ainsi que les données de sortie internées et externes, peuvent

▼M1

être obtenus au choix de l'utilisateur, mais ils ne sont pas définis dans le présent document.

6.2. **Service WriteDataByIdentifier**

6.2.1. ***Description des messages***

Le client a recours au service WriteDataByIdentifier pour procéder à l'enregistrement de valeurs associées aux relevés de données sur un serveur. Les données sont identifiées par un identificateur de relevés. C'est au fabricant de l'UEV qu'incombe la responsabilité de s'assurer que les conditions d'exploitation normale du serveur sont réunies lors de l'exécution de ce service. Pour procéder à l'actualisation des paramètres répertoriés au tableau 28, il faut que l'UEV soit exploitée en mode ÉTALONNAGE.

6.2.2. ***Structure des messages***

La structure des messages associés aux primitives WriteDataByIdentifier fait l'objet d'une description détaillée dans les tableaux ci-après.

Tableau 29

Message de demande d'écriture de données par un identificateur

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	CIB
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	m+3	LON
#5	ID du service Demande WriteDataByIdentifier	2E	WDBI
#6 à #7	Identificateur de relevés = [une valeur extraite du tableau 28]	xxxx	IR_ …
#8 à #m+7	Valeur de relevé#1 : Valeur de relevé#m	xx : xx	VR_V1 : VR_Vm
#m+8	Total de contrôle	00-FF	TC

Tableau 30

Message de réponse positive à une demande d'écriture de données par un identificateur

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	CIB
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LON
#5	ID du service Réponse positive à une demande WriteDataByIdentifier	6E	WDBIPR
#6 à #7	Identificateur local de relevés = [même valeur que les octets #6 et #7 tableau 29]	xxxx	IR_ …
#8	Total de contrôle	00-FF	TC

▼M1

Tableau 31

Message de réponse négative à une demande d'écriture de données par un identificateur

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	CIB
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LON
#5	ID du service Réponse négative	7F	RN
#6	ID du service Demande WriteDataByIdentifier	2E	WDBLI
#7	Code de réponse = [requestOutOfRange	31	CR_ROOR
	incorrectMessageLength	13	CR_IML
	conditionsNotCorrect]	22	CR_CNC
#8	Total de contrôle	00-FF	TC

6.2.3. ***Définition des paramètres***

Le paramètre Identificateur de relevés (ILR_) est défini au tableau 28.

Le paramètre Valeur de relevé (VR) est utilisé pour le message de demande WriteDataByIdentifier afin de fournir au serveur (UEV) les valeurs de relevé identifiées par le recordDataIdentifier. Les structures des données sont indiquées au chapitre 8.

7. CONTRÔLE DES IMPULSIONS D'ESSAI — UNITÉ FONCTIONNELLE DE CONTRÔLE DES ENTRÉES/SORTIES

Les services disponibles font l'objet d'une description détaillée dans le tableau ci-après:

Tableau 32

Unité fonctionnelle de contrôle des entrées/sorties

Nom du service	Description
InputOutputControlByIdentifier	Le client demande le contrôle d'une entrée/sortie propre au serveur

7.1. **Service InputOutputControlByIdentifier**

7.1.1. ***Description des messages***

La connexion réalisée par l'intermédiaire du connecteur frontal permet de contrôler ou de surveiller les impulsions d'essai au moyen d'un testeur approprié.

Il est possible de configurer cette ligne de signalisation d'entrée/sortie par le biais d'une commande lancée sur la ligne K en recourant au service InputOutputControlByIdentifier pour sélectionner la fonction d'entrée ou de sortie requise pour la ligne considérée. Les états disponibles sur la ligne sont les suivants:

— désactivé;

— speedSignalInput, où la ligne de signalisation d'entrée/sortie est utilisée pour entrer un signal de vitesse (signal d'essai) en remplacement du signal de vitesse du détecteur de mouvement;

— realTimeSpeedSignalOutputSensor, où la ligne de signalisation d'entrée/sortie est utilisée pour la sortie du signal de vitesse du détecteur de mouvement;

— RTCOutput, où la ligne de signalisation d'entrée/sortie est utilisée pour la sortie du signal de l'horloge TUC.

▼M1

Pour être en mesure de configurer l'état de la ligne, il faut que l'unité embarquée sur véhicule soit entrée en session de réglage et qu'elle soit exploitée en mode ÉTALONNAGE. Lorsque l'opérateur met un terme à une session de réglage ou décide de sortir du mode ÉTALONNAGE, l'unité embarquée sur véhicule doit s'assurer que la ligne de signalisation d'entrée/sortie est revenue à son état de désactivation (par défaut).

En cas de réception d'impulsions de vitesse sur la ligne d'entrée du signal de vitesse instantanée de l'UEV alors que la ligne de signalisation d'E/S est exploitée en mode entrée, cette ligne de signalisation passera en mode sortie ou sera ramenée à son état de désactivation.

Voici la séquence des opérations:

— Établissement d'une liaison d'intercommunication par le biais du service StartCommunication

— Entrée en session de réglage par le biais du service StartDiagnosticSession et passage en mode d'exploitation ÉTALONNAGE (l'ordre d'exécution de ces deux opérations est sans importance)

— Modification de l'état de la sortie par le biais du service InputOutputControl-Bydentifier.

7.1.2. ***Structure des messages***

La structure des messages associés aux primitives InputOutputControlByIdentifier fait l'objet d'une description détaillée dans les tableaux ci-après.

Tableau 33

Message de demande de contrôle d'entrée/sortie par un identificateur

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	EE	CIB
#3	Octet d'adresse de la source	tt	SRC
#4	Octet de longueur supplémentaire	xx	LON
#5	ID du service Demande InputOutputControlByIdentifier	2F	IOCBLI
#6 et #7	Identificateur local d'entrée/sortie = [CalibrationInputOutput]	F960	ILES_CIO
#8 ou #8 à #9	Option de contrôle = [		OC_ …
	Paramètre de contrôle d'entrée/sortie — une valeur extraite du tableau 36	xx	PCES_ …
	État de contrôle — une valeur extraite du tableau 37 (cf. remarque ci-après)]	xx	ETC_ …
#9 ou #10	Total de contrôle	00-FF	TC

Remarque: Le paramètre État de contrôle n'apparaît que dans certains cas (cf. para. 7.1.3).

Tableau 34

Message de réponse positive à une demande de contrôle d'entrée/sortie par un identificateur

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	CIB
#3	Octet d'adresse de la source	EE	SRC

▼**M1**

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#4	Octet de longueur supplémentaire	xx	LON
#5	ID du service Réponse positive à une demande inputOutputControlByIdentifier	6F	RPIOCBI
#6 et #7	Identificateur local d'entrée/sortie = [CalibrationInputOutput]	F960	ILES_CIO
8 ou #8 à #9	Situation de contrôle = [		STC_
	Paramètre de contrôle d'entrée/sortie (même valeur que l'octet #7 du tableau 33)	xx	PCES_ …
	État de contrôle (même valeur que l'octet #8 du tableau 33]	xx	ETC_ …
#9	Total de contrôle	00-FF	TC

Tableau 35

Message de réponse négative à une demande de contrôle d'entrée/sortie par un identificateur

Octet #	Nom de paramètre	Valeur hex.	Mnémonique
#1	Octet de structure — adressage physique	80	FMT
#2	Octet d'adresse de la cible	tt	CIB
#3	Octet d'adresse de la source	EE	SRC
#4	Octet de longueur supplémentaire	03	LON
#5	ID du service Réponse négative	7F	RN
#6	ID du service Demande inputOutputControlByIdentifier	2F	IOCBI
#7	Code de réponse = [		
	incorrectMessageLength	13	CR_IML
	conditionsNotCorrect	22	CR_CNC
	requestOutOfRange	31	CR_ROOR
	deviceControlLimitsExceeded]	7A	CR_DCLE
#8	Total de contrôle	00-FF	TC

7.1.3. ***Définition des paramètres***

Le paramètre Paramètre de contrôle d'entrée/sortie (PCES_) est défini dans le tableau ci-après.

Tableau 36

Définition des valeurs accordées aux paramètres de contrôle d'entrée/sortie

Hex	Description	Mnémonique
00	Retour de commande à l'UCE Cette valeur doit indiquer au serveur (UEV) que l'appareil d'essai ne commande plus la ligne de signalisation d'E/S.	RCUCE

▼M1

Hex	Description	Mnémonique
01	Rétablissement de la configuration par défaut Cette valeur doit indiquer au serveur (UEV) qu'il est tenu de ramener à son état initial le signal d'entrée, le paramètre interne ou le signal de sortie désigné par l'identificateur local d'entrée/sortie.	RCD
03	Réglage à court terme Cette valeur doit indiquer au serveur (UEV) qu'il est tenu de régler le signal d'entrée, le paramètre interne ou le signal de sortie désigné par l'identificateur local d'entrée/sortie dans la mémoire vive en lui attribuant l'une des valeurs incluses dans les paramètres d'état de contrôle.	RCT

Le paramètre État de contrôle n'apparaît que lorsque le paramètre de contrôle d'entrée/sortie est configuré comme paramètre de réglage à court terme et défini dans le tableau ci-après:

Tableau 37

Définition des valeurs accordées au paramètre État de contrôle

Mode	Valeur hex.	Description
Désactivation	00	Ligne d'E/S désactivée (par défaut)
Activation	01	Ligne d'E/S activée pour l'entrée de signaux de vitesse (speedSignalInput)
Activation	02	Ligne d'E/S activée pour la sortie du capteur de signal de vitesse en temps réel (realTimeSpeedSignalOutputSensor)
Activation	03	Ligne d'E/S activée pour RTCOutput

8. STRUCTURES DES RELEVÉS DE DONNÉES

Le présent chapitre expose en détail:

— les règles générales applicables aux gammes de paramètres transmises par l'unité embarquée sur le véhicule à l'appareil d'essai,

— les structures qui sont utilisées pour les données transférées par l'intermédiaire des services de transmission de données au chapitre 6.

Tous les paramètres indiqués sont pris en charge par l'UEV.

Les données transmises par l'UEV à l'appareil d'essai en réponse à une demande sont du type mesurées (c.-à-d. la valeur actuelle du paramètre demandé telle que mesurée ou observée par l'UEV).

8.1. **Gammes des paramètres transmis**

Le tableau 38 définit les gammes utilisées pour déterminer la validité d'un paramètre transmis.

Les valeurs de la gamme «indicateur d'erreur» permettent à l'unité embarquée sur le véhicule d'indiquer immédiatement qu'aucune donnée paramétrique valable n'est actuellement disponible en raison d'une erreur quelconque au niveau de l'appareil de contrôle.

Les valeurs de la gamme «non disponible» permettent à l'unité embarquée sur le véhicule de transmettre un message contenant un paramètre non disponible ou non pris en charge dans le module en cause. Les valeurs de la gamme «non demandé» permettent la transmission d'une message de commande et mettent en lumière les paramètres pour lesquels le récepteur n'attend pas de réponse.

Lorsqu'une défaillance d'un composant empêche la transmission de données valables pour un paramètre, il convient d'utiliser l'indicateur d'erreur tel que décrit dans le tableau 38 à la place des données de ce paramètre. Toutefois, si les données mesurées ou calculées donnent une valeur valable mais qui se situe en dehors de la gamme fixée pour ce paramètre, l'indicateur d'erreur ne devrait pas être utilisé. Il convient dans ce cas de transmettre les données en utilisant la valeur paramétrique minimale ou maximale appropriée.

▼M1

Tableau 38

Gammes des relevés de données

Nom de la gamme	1 octet (valeur hex.)	2 octets (valeur hex.)	4 octets (valeur hex.)	ASCII
Signal valable	00 à FA	0000 à FAFF	00000000 à FAFFFFFF	1 à 254
Indicateur propre au paramètre	FB	FB00 à FBFF	FB000000 à FBFFFFFF	néant
Gamme réservée aux futurs octets de l'indicateur	FC à FD	FC00 à FDFF	FC000000 à FDFFFFFF	néant
Indicateur d'erreur	FE	FE00 à FEFF	FE000000 à FEFFFFFF	0
Non disponible ou non demandée	FF	FF00 à FFFF	FF000000 à FFFFFFFF	FF

Pour les paramètres encodés en ASCII, le caractère ASCII «*» est réservé comme délimiteur.

8.2. **Structures des relevés de données**

Les tableaux 39 à 42 ci-après exposent en détail les structures à utiliser par l'intermédiaire des services ReadDataByIdentifier et WriteDataByIdentifier.

Le tableau 39 indique la longueur, la résolution et la gamme opérationnelle de chaque paramètre identifié par son identificateur de relevé (recordDataIdentifier):

Tableau 39

Structure des relevés

Nom de paramètre	Longueur des données (en octets)	Résolution	Gamme opérationnelle
Date et heure	8	Pour plus de précisions voir le tableau 40	
Kilométrage total du véhicule en haute définition	4	gain 5 m/bit, décalage 0 m	0 à + 21 055 406 km
Facteur K	2	gain 0,001 impulsion/m/bit, décalage 0	0 à 64,255 impulsion/m
Circonférence des pneus Facteur L	2	gain 0,125 10^{-3} m/bit, décalage 0	0 à 8 031 m
Coefficient W caractéristique du véhicule	2	gain 0,001 impulsion/m/bit, décalage 0	0 à 64,255 impulsion/m
Taille des pneumatiques	15	ASCII	ASCII
Date du prochain étalonnage	3	Pour plus de précisions voir le tableau 41	
Vitesse autorisée	2	gain 1/256 km/h/bit, décalage 0	0 à 250,996 km/h
État membre d'immatriculation	3	ASCII	ASCII
Numéro d'immatriculation du véhicule	14	Pour plus de précisions voir le tableau 42	
Numéro d'identification du véhicule	17	ASCII	ASCII

▼M1

Le tableau 40 expose en détail les structures des différents octets du paramètre «date et heure»:

Tableau 40

Structure détaillée du paramètre «date et heure» (valeur de l'identificateur de relevé # F00B)

Octet	Définition du paramètre	Résolution	Gamme opérationnelle
1	Secondes	gain 0,25 s/bit, décalage 0 s	0 à 59,75 s
2	Minutes	gain 1 mn/bit, décalage 0 mn	0 à 59 mn
3	Heures	gain 1 h/bit, décalage 0 h	0 à 23 h
4	Mois	gain 1 mois/bit, décalage 0 mois	1 à 12 mois
5	Jour	gain 0,25 jour/bit, décalage 0 jour (voir ci-après la note du tableau 41)	0,25 à 31,75 jours
6	Année	gain 1 année/bit, décalage + 1985 (voir ci-après la note du tableau 41)	1985 à 2235
7	Correction locale des minutes	gain 1 mn/bit, décalage - 125 mn	- 59 à 59 mn
8	Correction locale des heures	gain 1 h/bit, décalage - 125 h	- 23 à + 23 h

Le tableau 41 expose en détail la structure des différents octets du paramètre «Date du prochain étalonnage».

Tableau 41

Structure détaillée du paramètre «Date du prochain étalonnage» (valeur de l'identificateur de relevé # F022)

Octet	Définition du paramètre	Résolution	Gamme opérationnelle
1	Mois	gain 1 mois/bit, décalage 0 mois	1 à 12 mois
2	Jour	gain 0,25 jour/bit, décalage 0 jour (voir la note ci-après)	0,25 à 31,75 jours
3	Année	gain 1 année/bit, décalage + 1985 (voir la note ci-après)	1985 à 2235

Note concernant l'utilisation du paramètre «jour»:
1) Une valeur de 0 pour la date est nulle. Les valeurs 1, 2, 3, et 4 sont utilisées pour identifier le premier jour du mois; les valeurs 5, 6, 7 et 8 indiquent le deuxième jour du mois; etc.
2) Ce paramètre n'influence pas ni ne modifie le paramètre des heures.

Note concernant l'utilisation de l'octet du paramètre «année»:
Une valeur de 0 pour l'année correspond à l'année 1985; une valeur de 1 correspond à l'année 1986, et ainsi de suite.

▼**M1**

Le tableau 42 expose en détail la structure des différents octets du paramètre «Numéro d'immatriculation du véhicule».

Tableau 42

Structure détaillée du paramètre «Numéro d'immatriculation du véhicule» (valeur de l'identificateur de relevé # F07E)

Octet	Définition du paramètre	Résolution	Gamme opérationnelle
1	Page de code (telle que définie à l'appendice 1)	ASCII	01 à 0A
2 à 14	Numéro d'immatriculation du véhicule (tel que défini à l'appendice 1)	ASCII	ASCII

▼**M1**

Appendice 9

HOMOLOGATION DE TYPE — LISTE DES ESSAIS MINIMAUX REQUIS

TABLE DES MATIÈRES

▼M1

1. INTRODUCTION

1.1. **Homologation de type**

L'homologation de type CEE d'un appareil de contrôle (d'un composant de cet appareil) ou d'une carte tachygraphique repose sur les certifications suivantes:

— Certification de sécurité exécutée par l'un des organismes compétents de l'ITSEC contre une cible de sécurité parfaitement conforme à l'appendice 10 de la présente annexe;

— Certification de fonctionnement exécutée par les autorités compétentes d'un État membre et certifiant que l'élément testé satisfait aux exigences de la présente annexe sur le plan des fonctions exécutées, de la précision des mesures et des caractéristiques environnementales;

— Certification d'interopérabilité exécutée par l'organisme compétent chargé de certifier l'interopérabilité de l'appareil de contrôle (ou la carte tachygraphique) visé avec la carte tachygraphique (ou l'appareil de contrôle) indispensable (cf. chapitre VIII de la présente annexe).

Le présent appendice précise les tests minimaux auxquels les autorités compétentes d'un État membre doivent se livrer pendant une série d'essais de fonctionnement ainsi que les tests minimaux que l'organisme compétent se doit d'effectuer pendant les essais d'interopérabilité. Ni les procédures d'exécution de ces essais ni leur type ne font l'objet d'explications plus détaillées.

Le présent appendice ne traite pas des différents aspects de la certification de sécurité. Si certains essais d'homologation de type sont exécutés pendant le processus d'évaluation et de certification de la sécurité, leur réexécution ultérieure est superflue. En pareil cas, seuls les résultats de ces essais de sécurité sont sujets à vérification. À titre informatif, les exigences qui doivent faire l'objet d'essais (ou sont étroitement liées avec les essais qu'il y a lieu d'exécuter) pendant la certification de sécurité sont repérées par un astérisque («*») dans le présent appendice.

Le présent appendice traite séparément de l'homologation de type du détecteur de mouvement et de celle de l'unité embarquée sur le véhicule, respectivement considérés comme deux composants distincts de l'appareil de contrôle. L'interopérabilité entre chaque modèle de détecteur de mouvement et chaque modèle d'unité embarquée sur le véhicule n'est pas obligatoire; par conséquent, l'homologation de type d'un détecteur de mouvement ne peut être accordée qu'en association avec l'homologation de type d'une unité embarquée sur le véhicule et réciproquement.

1.2. **Références**

Le présent appendice fait référence aux documents qui suivent:

CEI 68-2-1	Essais environnementaux — Partie 2: Essais — Essais A: Froid. 1990 + amendement 2: 1994.
CEI 68-2-2	Essais environnementaux — Partie 2: Essais — Essais B: Chaleur sèche. 1974 + amendement 2: 1994.
CEI 68-2-6	Procédures fondamentales d'essai environnemental — Méthodes d'essai — Test Fc et directives: Vibrations (sinusoïdales). 6e édition: 1985.
CEI 68-2-14	Procédures fondamentales d'essai environnemental — Méthodes d'essai — Test N: Changement de température. Modification 1: 1986.
CEI 68-2-27	Procédures fondamentales d'essai environnemental — Méthodes d'essai - Test Ea et directives: Chocs. Édition 3: 1987.
CEI 68-2-30	Procédures fondamentales d'essai environnemental — Méthodes d'essai — Test Db et directives: Chaleur humide, cyclique (12 + 12 — cycle temporel). Modification 1: 1985.
CEI 68-2-35	Procédure fondamentale d'essai environnemental — Méthodes d'essai — Test Fda: Vibrations aléatoires en large bande — Reproductibilité élevée. Modification 1: 1983.
CEI 529	Degrés de protection assurés par les boîtiers (code IP). Édition 2: 1989.
CEI 61000-4-2	Compatibilité électromagnétique (CEM) — Techniques d'essai et de mesure — Essai d'immunité aux décharges électrostatiques: 1995/Amendement 1: 1998:
ISO 7637-1	Véhicules routiers — Perturbations radio-électriques par conduction et couplage — Partie 1: Voitures particulières et véhicules utilitaires légers équipés d'une alimentation électrique dont la tension nominale s'élève à 12 V —

▼**M1**

Conduction électrique transitoire exclusivement le long des lignes d'alimentation. Seconde édition: 1990.

ISO 7637-2 Véhicules routiers — Perturbations radio-électriques par conduction et couplage — Partie 2: Véhicules utilitaires équipés d'une alimentation électrique dont la tension nominale s'élève à 12 ou 24 V — Conduction électrique transitoire exclusivement le long des lignes d'alimentation. Première édition: 1990.

ISO 7637-3 Véhicules routiers — Perturbations radio-électriques par conduction et couplage — Partie 3: Véhicules équipés d'une alimentation électrique dont la tension nominale s'élève à 12 ou 24 V — Émission électrique transitoire par couplage capacitif et inductif le long d'autres lignes que celles d'alimentation. Première édition: 1995 + Cor 1: 1995.

ISO/CEI 7816-1 Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 1: Caractéristiques physiques. Première édition: 1998.

ISO/CEI 7816-2 Informatique — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 2: Dimensions et emplacement des contacts. Première édition: 1999.

ISO/CEI 7816-3 Informatique — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 3: Signaux électroniques et protocole de transmission. Seconde édition: 1997.

ISO/CEI 10373 Cartes d'identification — Méthodes d'essai. Première édition: 1993.

2. ESSAIS DE FONCTIONNEMENT DE L'UNITÉ EMBARQUÉE SUR LE VÉHICULE

Nº	Essai	Description	Exigences connexes
1.	**Inspection administrative**		
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.	070, 071, 073
2.	**Inspection visuelle**		
2.1.	Conformité à la documentation		
2.2.	Identification/marquage		168, 169
2.3.	Matériaux		163 à 167
2.4	Scellement		251
2.5.	Interfaces externes		
3.	**Essais de fonctionnement**		
3.1.	Fonctions prévues		002, 004, 244
3.2.	Modes d'exploitation		006*, 007*, 008*, 009*, 106, 107
3.3.	Droits d'accès aux fonctions et données		010*, 011*, 240, 246, 247
3.4.	Surveillance de l'insertion et du retrait des cartes		013, 014, 015*, 016*, 106
3.5.	Mesure de la vitesse et de la distance		017 à 026
3.6.	Chronométrage (essai exécuté à 20 ºC)		027 à 032
3.7.	Surveillance des activités du conducteur		033 à 043, 106

▼**M1**

Nº	Essai	Description	Exigences connexes
3.8.	Surveillance de l'état de conduite		044, 045, 106
3.9.	Entrées manuelles		046 à 050 *ter*
3.10.	Gestion des dispositifs de verrouillage de l'entreprise		051 à 055
3.11.	Suivi des activités de contrôle		056, 057
3.12.	Détection d'événements et/ou d'anomalies		059 à 069, 106
3.13.	Données d'identification des équipements		075*, 076*, 079
3.14.	Données d'insertion et de retrait de la carte du conducteur		081* à 083*
3.15.	Données relatives aux activités du conducteur		084* à 086*
3.16.	Données relatives aux lieux		087* à 089*
3.17.	Données relatives aux kilométrages		090* à 092*
3.18.	Données détaillées relatives à la vitesse		093*
3.19.	Données relatives aux événements		094*, 095
3.20.	Données relatives aux anomalies		096*
3.21.	Données d'étalonnage		097*, 098*
3.22.	Données de réglage de l'heure		100*, 101*
3.23.	Données relatives aux activités de contrôle		102*, 103*
3.24.	Données relatives aux dispositifs de verrouillage de l'entreprise		104*
3.25.	Téléchargement de données relatives aux activités		105*
3.26.	Données relatives aux conditions particulières		105 *bis**, 105 *ter**
3.27.	Enregistrement et mémorisation sur les cartes tachygraphiques		108, 109*, 109 *bis**, 110*, 111, 112
3.28.	Affichage		072, 106, 113 à 128, PIC_001, DIS_001
3.29.	Impression		072, 106, 129 à 138, PIC_001, PRT_001 à PRT_012
3.30.	Avertissement		106, 139 à 148, PIC_001
3.31.	Téléchargement de données à destination de supports externes		072, 106, 149 à 151
3.32.	Données de sortie à destination de périphériques externes supplémentaires		152, 153
3.33.	Étalonnage		154*, 155*, 156*, 245
3.34.	Réglage de l'heure		157*, 158*
3.35.	Absence d'interférence des fonctions supplémentaires		003, 269

▼M1

Nº	Essai	Description	Exigences connexes
4.	**Essais environnementaux**		
4.1.	Température	S'assurer de la fonctionnalité en exécutant les essais suivants: — CEI 68-2-1, test Ad, en appliquant une durée d'essai de 72 heures à basse température (− 20 ºC), le matériel testé alternant les phases d'exploitation et de repos d'une heure — CEI 68-2-2, test Bd, en appliquant une durée d'essai de 72 heures à haute température (+ 70 ºC), le matériel testé alternant les phases d'exploitation et de repos d'une heure Cycles de température: s'assurer que l'unité embarquée sur le véhicule est capable de résister à une évolution rapide de la température ambiante en exécutant l'essai CEI 68-2-14 test Na, comportant 20 cycles pendant lesquels la température oscille entre une température minimale (− 20 ºC) et une température maximale (+ 70 ºC) ainsi qu'un cycle de maintien de 2 heures à ces deux températures extrêmes 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	159
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 68-2-30, test Db, comportant six cycles de 24 heures, la température variant de + 25 ºC à + 55 ºC et le taux d'humidité relative atteignant 97 % à + 25 ºC et 93 % à + 55 ºC	160
4.3.	Vibration	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 68-2-6, test 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) 2. Vibrations aléatoires: S'assurer que l'unité embarquée sur le véhicule est capable de résister à des vibrations aléatoires possédant les caractéristiques suivantes: fréquence 5 à 150 Hz, niveau 0,02 g^2/Hz L'essai CEI 68-2-35, test Ffda, permet de vérifier la satisfaction de cette exigence. La durée minimale de cet essai s'élève à 3 × 12 heures (12 heures par essieu), le matériel testé alternant les phases d'exploitation et de repos d'une heure. Il convient d'exécuter les deux essais décrits ci-avant sur deux échantillons distincts du type d'équipement testé	163

▼**M1**

Nº	Essai	Description	Exigences connexes
4.4.	Protection contre l'eau et les corps étrangers	S'assurer que l'indice de protection de l'unité embarquée sur le véhicule conforme à la norme CEI 529 s'élève à IP 40 au moins, lorsque cette unité embarquée sur le véhicule est montée pour fonctionner dans des conditions d'exploitation normales	164, 165
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 ºC pendant 1 heure Versions 12 V: 17 V à + 40 ºC pendant 1 heure	161
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	161
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	161
5.	**Essais de compatibilité électromagnétique**		
5.1.	Émission rayonnée et susceptibilité	Conformité avec la directive 95/54/CE	162
5.2.	Décharge électrostatique	Conformité avec la norme CEI 61000-4-2, ± 2 kV (niveau 1)	162
5.3.	Susceptibilité transitoire par conduction au niveau de l'alimentation	Pour les versions 24 V: conformité avec la norme ISO 7637-2: impulsion 1a: Vs = − 100 V, Ri = 10 ohms impulsion 2: Vs = + 100 V, Ri = 10 ohms impulsion 3a: Vs = − 100 V, Ri = 50 ohms impulsion 3b: Vs = + 100 V, Ri = 50 ohms impulsion 4: Vs = − 16 V Va = − 12 V, t6=100 ms impulsion 5: Vs = + 120 V, Ri = 2,2 ohms, td = 250 ms Pour les versions 12 V: conformité avec la norme ISO 7637-1: impulsion 1: Vs = − 100 V, Ri = 10 ohms impulsion 2: Vs = + 100 V, Ri = 10 ohms impulsion 3a: Vs = − 100 V, Ri = 50 ohms impulsion 3b: Vs = + 100 V, Ri = 50 ohms impulsion 4: Vs = − 6 V, Va = − 5 V, t6 = 15 ms impulso 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 de protection externe contre le déversement des chargements transportés	162

▼**M1**

3. ESSAIS DE FONCTIONNEMENT DU DÉTECTEUR DE MOUVEMENT

N°	Essai	Description	Exigences connexes
1.	**Inspection administrative**		
1.1.	Documentation	Exactitude de la documentation	
2.	**Inspection visuelle**		
2.1.	Conformité avec la documentation		
2.2.	Identification/marquage		169, 170
2.3.	Matériaux		163 à 167
2.4.	Scellement		251
3.	**Essais de fonctionnement**		
3.1.	Données d'identification du détecteur		077*
3.2.	Détecteur de mouvement — appariement à l'unité embarquée sur le véhicule		099*, 155
3.3.	Détection de mouvement		
	Précision de la mesure des mouvements		022 à 026
4.	**Essais environnementaux**		
4.1.	Température d'exploitation	S'assurer de la fonctionnalité de ce composant (telle qu'elle est définie dans le test n° 3.3) pour la plage de températures [− 40 °C + 135 °C] en exécutant les essais suivants: — CEI 68-2-1 test Ad, en appliquant une durée d'essai de 96 heures à la température minimale To_{min} — CEI 68-2-2 test Bd, en appliquant une durée d'essai de 96 heures à la température maximale To_{max}	159
4.2.	Cycles de température	S'assurer de la fonctionnalité de ce composant (telle qu'elle est définie dans le test n° 3.3) en exécutant l'essai CEI 68-2-14 test Na, comportant 20 cycles pendant lesquels la température oscille entre une température minimale (- 40 °C) et une température maximale (+ 135 °C) ainsi qu'un cycle de maintien de 2 heures à ces deux températures extrêmes Il est possible de se livrer à un nombre limité d'essais (parmi ceux définis dans le test 3.3) aux températures minimale et maximale indiquées ainsi que pendant les cycles de variation de la température	159
4.3.	Cycles humides	S'assurer de la fonctionnalité de ce composant (telle qu'elle est définie dans le test n° 3.3) en exécutant l'essai CEI 68-2-30, test 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	160
4.4.	Vibration	S'assurer de la fonctionnalité de ce composant (telle qu'elle est définie dans le test n° 3.3) en exécutant l'essai CEI 68-2-6, test Fc, en appliquant une durée d'essai de 100 cycles de changement de fréquences:	163

▼**M1**

Nº	Essai	Description	Exigences connexes
		Déplacement constant entre 10 et 57 Hz: 1,5 mm max. Accélération constante comprise entre 57 et 500 Hz: 20 g	
4.5.	Chocs mécaniques	S'assurer de la fonctionnalité de ce composant (telle qu'elle est définie dans le test nº 3.3) en exécutant l'essai CEI 68-2-27, test Ea, 3 chocs dans les deux directions des trois axes de référence perpendiculaires	163
4.6.	Protection contre l'eau et les corps étrangers	S'assurer que l'indice de protection du détecteur de mouvement conforme à la norme CEI 529 s'élève à IP 64 au moins, lorsque ce détecteur de mouvement est monté sur un véhicule pour fonctionner dans des conditions d'exploitation normales	165
4.7.	Protection contre les inversions de polarité	S'assurer que le détecteur de mouvement est capable de supporter une inversion de polarité au niveau de son alimentation électrique	161
4.8.	Protection contre les courts-circuits	S'assurer que les signaux d'entrée et de sortie sont protégés contre les courts-circuits à l'alimentation électrique et à la terre	161
5.	**Essais de compatibilité électromagnétique**		
5.1.	Émission rayonnée et susceptibilité	S'assurer de la conformité avec la directive 95/54/CE	162
5.2.	Décharge électrostatique	Conformité avec la norme CEI 61000-4-2, ± 2 kV (niveau 1)	162
5.3.	Susceptibilité transitoire par conduction au niveau des lignes de transmission de données)	Conformité avec la norme ISO 7637-3 (niveau III)	162

4. ESSAIS DE FONCTIONNEMENT DES CARTES DE TACHYGRAPHE

Nº	Essai	Description	Exigences connexes
1.	**Inspection administrative**		
1.1.	Documentation	Exactitude de la documentation	
2.	**Inspection visuelle**		
2.1.		S'assurer de la conformité et de la qualité d'impression de toutes les fonctions de protection et données visibles	171 à 181
3.	**Essais mécaniques**		
3.1.	Vérifier les dimensions de la carte ainsi que l'emplacement des contacts		184 ISO/CEI 7816-1 ISO/CEI 7816-2

▼**M1**

Nº	Essai	Description	Exigences connexes
4.	**Essais de protocole**		
4.1.	ATR	S'assurer de la conformité de l'ATR	ISO/CEI 7816-3 TCS 304, 307, 308
4.2.	T=0	S'assurer de la conformité du protocole T=0	ISO/CEI 7816-3 TCS 302, 303, 305
4.3.	PTS	S'assurer de la conformité de la commande PTS en passant de T=0 à T=1	ISO/CEI 7816-3 TCS 309 à 311
4.4.	T=1	S'assurer de la conformité du protocole T=1	ISO/CEI 7816-3 TCS 303, / 306
5.	**Structure de la carte**		
5.1.		S'assurer de la conformité de la structure des fichiers enregistrée sur la carte en contrôlant la présence des fichiers obligatoires sur la carte ainsi que leurs conditions d'accès	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	**Essais de fonctionnement**		
6.1.	Fonctionnement normal	Il convient de tester une fois au moins chaque usage autorisé pour chaque commande (ex.: essayer la commande UPDATE BINARY avec CLA = ′00′, CLA = ′0C′ pour des paramètres P1, P2 et Lc distincts). S'assurer que les opérations voulues ont été correctement exécutées sur la carte (ex.: en extrayant le fichier sur lequel la commande considérée a été exécutée)	TCS 313 à TCS 379
6.2.	Messages d'erreur	Il convient de tester une fois au moins chaque message d'erreur (comme indiqué à l'appendice 2) pour chaque commande. Il faut tester une fois au moins chaque erreur générique (à l'exception des erreurs d'intégrité ′6400′ contrôlées pendant la phase de certification de sécurité)	
7.	**Essais environnementaux**		
7.1.		S'assurer du bon fonctionnement des cartes dans les conditions limites définies en conformité avec la norme ISO/CEI 10373	185 à 188 ISO/CEI 7816-1

5. ESSAIS D'INTEROPÉRABILITÉ

Nº	Essai	Description
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 au départ de 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 de FE que présente la carte

▼**M1**

Nº	Essai	Description
		Procéder à un téléchargement sur carte pour s'assurer de la bonne exécution de tous les enregistrements correspondants S'assurer de l'extraction correcte de tous les enregistrements correspondants par l'impression quotidienne des données que contient une carte

▼**M1**

Appendice 10

OBJECTIFS GÉNÉRAUX DE SÉCURITÉ

Le présent appendice spécifie le contenu minimal requis des objectifs de sécurité du détecteur de mouvement, de l'unité embarquée sur le véhicule et des cartes tachygraphiques.

Pour formuler les objectifs de sécurité en vue de l'obtention de certificats de sécurité, les fabricants seront habilités à peaufiner et, le cas échéant, à compléter les documents, sans supprimer ni apporter aucune modification aux caractéristiques des menaces, objectifs, ressources procédurales et fonctions dédiées à la sécurité qu'ils recèlent.

TABLE DES MATIÈRES

Objectifs généraux de sécurité pour le détecteur de mouvement

▼**M1**

Objectifs généraux de sécurité pour l'unité embarquée sur le véhicule

▼**M1**

▼**M1**

▼M1

OBJECTIFS GÉNÉRAUX DE SÉCURITÉ POUR LE DÉTECTEUR DE MOUVEMENT

1. **Introduction**

Le présent document comporte une description du détecteur de mouvement, des menaces qu'il doit être capable de neutraliser et des objectifs de sécurité qu'il se doit d'atteindre. Il spécifie la nature des fonctions dédiées à la sécurité que requiert le système. De plus, il précise la puissance minimale des mécanismes de sécurité ainsi que le niveau de garantie requis tant en ce qui concerne le développement que l'évaluation du matériel considéré.

Les exigences dont il est fait état dans le présent document sont celles qui apparaissent dans le corps de l'annexe I B. Les exigences énoncées, pour plus de clarté, dans le corps de l'annexe I B font parfois double emploi avec les exigences requises en matière d'obectifs de sécurité. En cas d'ambiguïté entre l'une des exigences requises en matière d'objectifs de sécurité et l'exigence de l'annexe I B à laquelle la première fait référence, l'exigence énoncée dans le corps de l'annexe I B prévaudra.

Les exigences énoncées dans le corps de l'annexe I B auxquelles les objectifs de sécurité ne font aucune allusion sont sans rapport avec les fonctions dédiées à la sécurité.

Aux fins de traçabilité, des labels individuels ont été affectés aux menaces, objectifs, ressources procédurales et spécifications des fonctions dédiées à la sécurité qui apparaissent dans la documentation de développement et d'évaluation.

2. **Abréviations, définitions et références**

2.1. ***Abréviations***

ROM	Mémoire morte
SEF	Fonction dédiée à la sécurité
TBD	À définir
TOE	Cible d'évaluation
UEV	Unité embarquée sur le véhicule

2.2. ***Définitions***

Tachygraphe numérique	Appareil de contrôle
Entité	Périphérique connecté au détecteur de mouvement
Données de mouvement	Données échangées avec l'UEV et rendant compte de la vitesse du véhicule et de la distance parcourue
Pièces séparées physiquement	Composants matériels du détecteur de mouvement disséminés dans le véhicule par opposition aux composants matériels regroupés dans le boîtier du détecteur de mouvement
Données de sécurité	Données particulières indispensables à l'exécution des fonctions dédiées à la sécurité (p. ex. clés cryptographiques)
Système	Équipement, personnel ou entreprises entretenant un rapport quelconque avec l'équipement d'enregistrement
Utilisateur	Utilisateur humain du détecteur de mouvement (lorsque ce terme n'entre pas dans la composition de l'expression «données utilisateur»)
Données utilisateur	Toutes les données autres que les données de mouvement ou de sécurité qui sont enregistrées ou mémorisées par le détecteur de mouvement.

2.3. ***Références***

ITSEC	Information Technology Security Evaluation Criteria 1991 [Critères d'évaluation de la sécurité informatique]

▼M1

3. **Argumentaire de produit**

3.1. ***Description du détecteur de mouvement et méthode d'utilisation***

Le détecteur de mouvement est conçu pour être installé sur des véhicules de transport routier. Il a pour fonction de transmettre à une UEV des données de mouvement sécurisées, représentatives de la vitesse du véhicule et de la distance parcourue.

Le détecteur de mouvement est mécaniquement couplé à un élément mobile du véhicule dont le mouvement permet de déduire la vitesse du véhicule ou la distance parcourue. Il se monte dans la boîte de vitesses ou en tout autre point du véhicule.

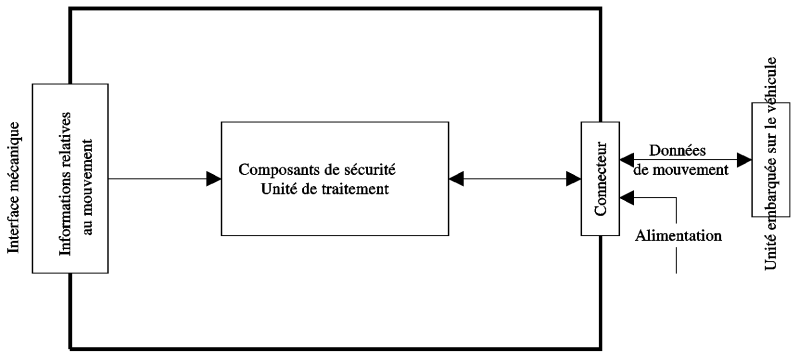
En mode opérationnel, le détecteur de mouvement est connecté à une UEV.

Ce détecteur est également susceptible d'être connecté à un équipement spécifique aux fins de gestion (à définir par le fabricant)

La figure ci-après illustre le fonctionnement d'un détecteur de mouvement classique:

Figure 1

Détecteur de mouvement classique



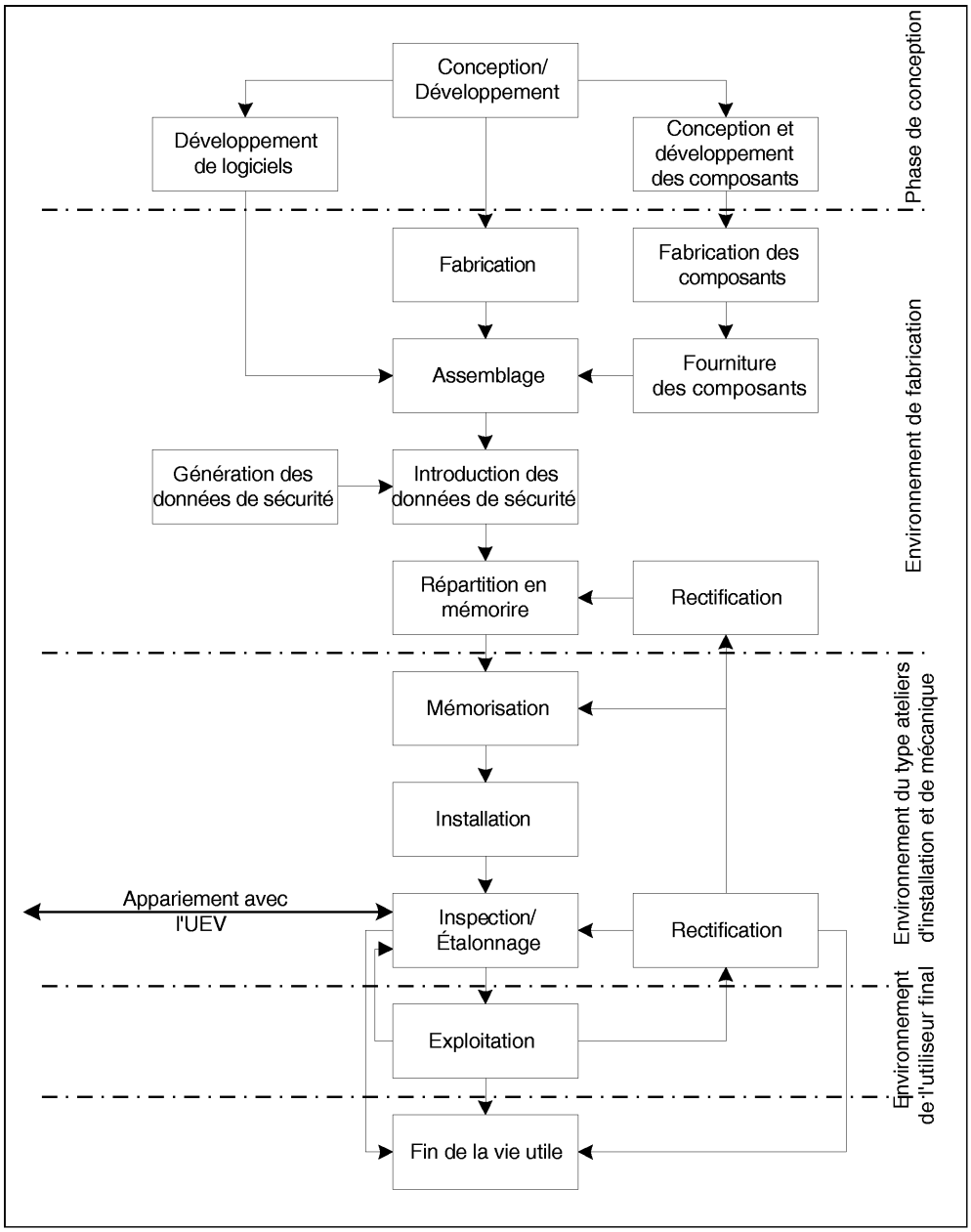
▼M1

3.2. ***Cycle de vie du détecteur de mouvement***

La figure ci-après illustre le cycle de vie caractéristique du détecteur de mouvement:

Figure 2

Cycle de vie caractéristique du détecteur de mouvement



3.3. ***Menaces***

Ce paragraphe présente une description des menaces qui pèsent sur le détecteur de mouvement.

3.3.1. *Menaces pesant sur les politiques de contrôle d'accès*

M.Accès	Certains utilisateurs pourraient tenter d'accéder à des fonctions qui leur sont interdites

3.3.2. *Menaces inhérentes à la conception*

M.Défauts	Certaines anomalies affectant les matériels, logiciels et procédures de communication pourraient mettre le détecteur de mouvement dans une situ-

▼**M1**

	ation imprévue susceptible d'en compromettre la sécurité
M.Essais	Le recours à des modes d'essai non invalidés ou à des portes dérobées pourrait compromettre la sécurité du détecteur de mouvement
M.Conception	Certains utilisateurs pourraient être tentés de se procurer de manière illicite des données confidentielles concernant la conception dudit détecteur en les extrayant du matériel dont dispose le fabricant (vol, corruption, etc.) ou en procédant par ingénierie inverse

3.3.3. *Menaces pesant sur l'exploitation*

M.Environnement	Certains utilisateurs pourraient compromettre la sécurité du détecteur de mouvement par des agressions à caractère environnemental (agressions thermiques, électromagnétiques, optiques, chimiques, mécaniques, etc.)
M.Matériel	Certains utilisateurs pourraient tenter d'altérer le matériel constitutif du détecteur de mouvement
M.Origine_Mécanique	Certains utilisateurs pourraient tenter de manipuler l'entrée du détecteur de mouvement (p. ex. en procédant à sa dépose de la boîte de vitesses, etc.)
M.Données_Mouvement	Certains utilisateurs pourraient tenter d'apporter des modifications aux données de mouvement du véhicule (adjonction, modification, suppression, restitution du signal)
M.Alimentation	Certains utilisateurs pourraient tenter d'aller à l'encontre des objectifs de sécurité du détecteur de mouvement en modifiant son alimentation (coupure, réduction, augmentation)
M.Données_Sécurité	Certains utilisateurs pourraient être tentés de se procurer de manière illicite des données de sécurité confidentielles lors de leur génération, de leur transfert ou de leur enregistrement au sein de l'équipement
M.Logiciel	Certains utilisateurs pourraient tenter d'apporter des modifications au logiciel du détecteur de mouvement
M.Données_Mémorisées	Certains utilisateurs pourraient tenter de modifier les données mémorisées (données utilisateur ou de sécurité)

3.4. ***Objectifs de sécurité***

Le principal objectif de sécurité du système tachygraphique numérique s'énonce comme suit:

O.Principal	Les données que les services de contrôle sont censés vérifier se doivent d'être disponibles et de refléter fidèlement et avec la précision requise les activités des conducteurs contrôlés et de leurs véhicules tant en ce qui concerne la vitesse du véhicule considéré que les périodes de conduite, de travail, de disponibilité et de repos

Par conséquent, l'objectif de sécurité du détecteur de mouvement contribuant à l'objectif de sécurité global s'énonce comme suit:

O.Principal_Détecteur	L'UEV doit avoir accès aux données transmises par le détecteur de mouvement pour être en mesure de reconstituer dans leur intégralité et avec la précision requise les déplacements du véhicule tant sur le plan de la vitesse que sur celui de la distance parcourue

3.5. ***Objectifs de sécurité informatique***

Les objectifs de sécurité informatique du détecteur de mouvement contribuant à l'objectif de sécurité global s'énoncent comme suit:

O.Accèss	Le détecteur de mouvement doit contrôler l'accès des entités connectées aux fonctions et données

▼**M1**

O.Analyse	Le détecteur de mouvement se doit de surveiller les tentatives d'affaiblissement de sa sécurité et de remonter jusqu'aux entités impliquées dans ces opérations
O.Authentification	Le détecteur de mouvement doit authentifier les entités connectées
O.Traitement	Le détecteur de mouvement doit s'assurer que le traitement des entrées dont découlent les données de mouvement est d'une précision satisfaisante
O.Fiabilité	Le détecteur de mouvement doit assurer un service d'une fiabilité satisfaisante
O.Échanges_Don._Protégés	Le détecteur de mouvement doit protéger les échanges de données avec l'UEV

3.6. ***Ressources matérielles, procédurales et en personnel***

Ce paragraphe présente une description des ressources matérielles, procédurales et en personnel qui contribuent à la sécurité du détecteur de mouvement.

3.6.1. *Conception de l'équipement*

R.Développement	Les concepteurs du détecteur de mouvement doivent veiller à ce que la répartition des responsabilités pendant la phase de développement ne mette pas en péril la sécurité informatique du projet
R.Fabrication	Les fabricants de détecteurs de mouvement doivent veiller à ce que la répartition des responsabilités pendant la phase de fabrication ne mette pas en péril la sécurité informatique du projet et à ce que le détecteur de mouvement considéré soit protégé contre le risque d'agressions physiques susceptibles d'en compromettre la sécurité informatique pendant le processus de fabrication

3.6.2. *Livraison de l'équipement*

R.Livraison	Les fabricants de détecteurs de mouvement, les constructeurs automobiles ainsi que les ateliers d'installation ou de mécanique doivent veiller à ce qu'aucune intervention ne compromette la sécurité informatique du détecteur de mouvement

3.6.3. *Génération et livraison des données de sécurité*

R.Génération_Don._Sécur.	Les algorithmes de génération des données de sécurité ne doivent être accessibles qu'à des personnes autorisées et dignes de confiance
R.Transport_Don._Sécur.	Les données de sécurité doivent être générées, acheminées et introduites dans le détecteur de mouvement de telle manière que leur confidentialité et leur intégrité soient préservées

3.6.4. *Installation, étalonnage et inspection de l'équipement d'enregistrement*

R.Ateliers_Agréés	L'installation, l'étalonnage et la réparation de l'équipement d'enregistrement doivent être confiés à des ateliers d'installation ou de mécanique agréés et dignes de confiance
R.Interface_Mécanique	L'équipement doit être pourvu de dispositifs de détection des tentatives d'altération de l'interface mécanique (pose de scellés p. ex.)
R.Inspections_Régulières	L'équipement d'enregistrement doit faire l'objet d'inspections et d'étalonnages périodiques

3.6.5. *Contrôle d'application de la loi*

R.Contrôles	L'équipement doit être soumis régulièrement et de manière aléatoire à des contrôles d'application de la loi. Ces contrôles doivent s'accompagner d'analyses de sécurité

▼M1

3.6.6. *Mises à niveau logicielles*

R.Actualisation_Logiciel	Toute révision logicielle doit s'être vue octroyer un certificat de sécurité avant toute mise en œuvre au sein d'un détecteur de mouvement

4. **Fonctions dédiées à la sécurité**

4.1. ***Identification et authentification***

Le détecteur de mouvement doit être à même d'établir, lors de chaque interaction, l'identité de toute entité à laquelle il pourrait être connecté.

L'identité d'une entité connectée se composera des éléments suivants:

— Un groupe d'entités:
  — UEV
  — Périphérique de gestion
  — Divers
— Une ID d'entité (UEV uniquement).

L'ID d'entité d'une UEV connectée se composera du numéro d'homologation et du numéro de série de l'UEV.

Le détecteur de mouvement sera en mesure d'authentifier toute UEV ou périphérique de gestion auquel il pourrait être connecté:

— lors de la connexion de toute entité
— lors de tout rétablissement de l'alimentation électrique

Le détecteur de mouvement sera capable de procéder à une authentification renouvelée de l'UEV à laquelle il est connecté.

Le détecteur de mouvement détectera et préviendra toute tentative d'utilisation de données d'authentification copiées ou reconstituées.

Après la détection de X tentatives (c'est au fabricant qu'il appartient d'en déterminer le nombre, celui-ci devant demeurer inférieur à 20) d'authentification successives mais infructueuses, la fonction dédiée à la sécurité (SEF) devra:

— générer un rapport d'analyse de l'événement
— avertir l'entité appropriée
— poursuivre l'exportation de données de mouvement dans un mode non protégé

4.2. ***Gestion des accès***

Les contrôles d'accès garantissent que l'extraction d'informations à partir de la cible d'évaluation, leur création au sein de celle-ci ou l'apport de modifications à ces données sont des opérations auxquelles seules les personnes dûment autorisées sont à même de procéder.

4.2.1. *Politique de contrôle des accès*

Le détecteur de mouvement contrôlera les droits d'accès aux fonctions et données.

4.2.2. *Droits d'accès aux données*

Le détecteur de mouvement devra garantir que ses données d'identification ne peuvent faire l'objet que d'une seule opération d'enregistrement (exigence 078).

Le détecteur de mouvement n'acceptera et/ou n'enregistrera que des données utilisateur émanant d'entités authentifiées.

Le détecteur de mouvement appliquera aux données de sécurité les droits d'accès en lecture et en écriture qui s'imposent.

4.2.3. *Structure des fichiers et conditions d'accès*

La structure des fichiers d'application et de données ainsi que les conditions d'accès à ces fichiers seront définies pendant le processus de fabrication, puis verrouillées afin de décourager toute tentative de modification ou de suppression.

4.3. ***Responsabilité***

Le détecteur de mouvement sauvegardera dans sa mémoire les données d'identification du détecteur de mouvement (exigence 077).

▼M1

Le détecteur de mouvement enregistrera dans sa mémoire les données d'installation utiles (exigence 099).

Le détecteur de mouvement sera à même de transférer des données d'activité vers les entités authentifiées à la demande de ces dernières.

4.4. ***Analyse***

Le détecteur de mouvement générera des rapports d'analyse couvrant les événements qui portent atteinte à sa sécurité.

Les événements qui affectent la sécurité du détecteur de mouvement sont les suivants:

— Tentatives d'atteinte à la sécurité:
  — échec de la procédure d'authentification
  — défaut d'intégrité des données enregistrées
  — erreur de transfert de données internes
  — ouverture illicite d'un boîtier
  — sabotage du matériel
— Défaillance du détecteur

Les rapports d'analyse devront comporter les données suivantes:

— date et heure de l'événement
— type d'événement
— identité de l'entité connectée

Si les données requises ne sont pas disponibles, ces rapports se devront néanmoins de fournir une indication d'anomalie appropriée (à définir par le fabricant).

Le détecteur de mouvement transmettra les rapports d'analyse générés à l'UEV dès leur production. Il pourra également les enregistrer dans sa mémoire.

Si le détecteur de mouvement est conçu pour enregistrer des rapports d'analyse, il doit également l'être pour sauvegarder 20 rapports d'analyse, quel que soit le degré de saturation de la mémoire affectée à l'enregistrement de ces rapports, et pour transmettre les rapports d'analyse mémorisés aux entités authentifiées à la demande de ces dernières.

4.5. ***Précision***

4.5.1. *Politique de contrôle des flux d'informations*

Le détecteur de mouvement doit présenter toutes les garanties que les données de mouvement traitées proviennent exclusivement de l'entrée mécanique du détecteur.

4.5.2. *Transferts de données internes*

Les exigences énoncées dans ce paragraphe ne sont d'application que si le détecteur de mouvement a recours à des pièces séparées physiquement.

Si des données doivent être transférées entre des pièces séparées physiquement du détecteur de mouvement, il faut que celles-ci soient à l'abri de toute tentative de modification.

En cas de détection d'une erreur de transfert de données pendant un transfert interne, le détecteur devra procéder à une nouvelle transmission tandis que la fonction dédiée à la sécurité devra générer un rapport d'analyse de l'événement.

4.5.3. *Intégrité des données enregistrées*

Le détecteur de mouvement vérifiera les données utilisateur enregistrées dans sa mémoire afin de déceler tout défaut d'intégrité éventuel.

En cas de détection d'un défaut d'intégrité affectant les données utilisateur mémorisées, la fonction dédiée à la sécurité générera un rapport d'analyse.

4.6. ***Fiabilité du service***

4.6.1 *Essais*

Toutes les commandes, actions ou points d'essai propres aux besoins d'essai de la phase de fabrication seront désactivés ou supprimés avant la fin de la phase de fabrication. Il ne sera pas possible de les rétablir aux fins d'utilisation ultérieure.

▼M1

Le détecteur de mouvement procédera à des essais automatiques durant sa phase de mise en route initiale ainsi qu'en cours d'exploitation normale afin de s'assurer de son bon fonctionnement. Les essais automatiques du détecteur de mouvement comporteront une vérification de l'intégrité des données de sécurité ainsi qu'une vérification de l'intégrité du code exécutable enregistré (pour autant qu'il ne soit pas enregistré dans la mémoire morte).

En cas de détection d'une anomalie interne pendant un essai automatique, la fonction dédiée à la sécurité générera un rapport d'analyse (défaillance du détecteur).

4.6.2. *Logiciel*

Le logiciel du détecteur de mouvement sera impossible à analyser ou dépanner sur site.

Les entrées provenant de sources externes ne seront en aucun cas acceptées comme des codes exécutables.

4.6.3. *Protection matérielle*

Si le boîtier du détecteur de mouvement est conçu pour être ouvert, le détecteur doit être à même de déceler toute ouverture de ce boîtier pendant une période minimale de 6 mois, même s'il est privé d'alimentation externe. En pareil cas, la fonction dédiée à la sécurité générera un rapport d'analyse couvrant l'événement (il est admis que les rapports d'analyse de cette nature soient générés et mémorisés après le rétablissement éventuel de l'alimentation électrique).

Si le boîtier du détecteur de mouvement se veut inviolable, le détecteur doit être ainsi conçu que toute tentative de violation soit aisément décelable (p. ex. en procédant à une inspection visuelle).

Le détecteur de mouvement devra détecter certaines tentatives de sabotage du matériel (à définir par le fabricant).

Dans l'éventualité d'une tentative de sabotage, la fonction dédiée à la sécurité générera un rapport d'analyse et le détecteur de mouvement procédera à l'intervention suivante: (à définir par le fabricant).

4.6.4. *Coupures d'alimentation*

Le détecteur de mouvement se mettra dans un état de sécurisation satisfaisant pendant les coupures ou les variations d'alimentation.

4.6.5. *Conditions de réinitialisation*

En cas de coupure d'alimentation, d'interruption d'une transaction avant terme ou de toute autre situation requérant sa réinitialisation, le détecteur de mouvement se réinitialisera sans heurt.

4.6.6. *Disponibilité des données*

Le détecteur de mouvement se devra de garantir l'accès aux ressources lorsque cela s'impose, sans que celles-ci soient sollicitées ou retenues inutilement.

4.6.7. *Applications multiples*

Si le détecteur de mouvement comporte des applications autres que l'application tachygraphique, toutes ces applications devront être séparées les unes des autres au niveau physique et/ou logique. Ces applications ne partageront aucune donnée de sécurité. Seule une tâche à la fois sera activée.

4.7. ***Échange de données***

Le détecteur de mouvement exportera des données de mouvement vers l'UEV en les accompagnant des attributs de sécurité qui leur sont associés de telle sorte que l'UEV soit en mesure d'en vérifier l'intégrité et l'authenticité.

4.8. ***Soutien cryptographique***

Les exigences énoncées dans ce paragraphe ne sont d'application qu'en cas de nécessité, en fonction des mécanismes de sécurité employés et des solutions adoptées par le fabricant.

Toute opération cryptographique exécutée par le détecteur de mouvement doit être en conformité avec un algorithme précis et un format de clé déterminé.

Si le détecteur de mouvement génère des clés cryptographiques, il doit s'acquitter de cette tâche en conformité avec certains formats et algorithmes de génération de clés cryptographiques.

▼M1

Si le détecteur de mouvement distribue des clés cryptographiques, il doit s'acquitter de cette tâche en conformité avec certaines méthodes de distribution des clés cryptographiques.

Si le détecteur de mouvement accède à des clés cryptographiques, il doit s'acquitter de cette tâche en conformité avec certaines méthodes d'accès aux clés cryptographiques.

Si le détecteur de mouvement détruit des clés cryptographiques, il doit s'acquitter de cette tâche en conformité avec certaines méthodes de destruction des clés cryptographiques.

5. **Définition des mécanismes de sécurité**

Les mécanismes de sécurité qui remplissent les fonctions dédiées à la sécurité sont définis par les fabricants de détecteurs de mouvement.

6. **Puissance minimale des mécanismes de sécurité**

La puissance minimale requise des mécanismes de sécurité du détecteur de mouvement est élevée, conformément aux critères définis dans le document de référence de l'ITSEC.

7. **Niveau de garantie**

Le niveau de garantie visé pour le détecteur de mouvement correspond au niveau E3, conformément aux critères définis dans le document de référence de l'ITSEC.

8. **Analyse raisonnée**

Les matrices qui suivent présentent une analyse raisonnée des fonctions dédiées à la sécurité en mettant en évidence les éléments suivants:

— les FDS et autres moyens de neutralisation des diverses menaces

— les FDS qui remplissent les différents objectifs de sécurité informatique.

▼**M1**

	Menaces												Objectifs de sécurité informatique					
	M.Accès	M.Défauts	M.Essais	M.Conception	M.Environnement	M.Matériel	M.Origine_Mécanique	M.Données_Mouvement	M.Alimentation	M.Données_Sécurité	M.Logiciel	M.Données_Mémorisées	O.Accès	O.Analyse	O.Authentification	O.Traitement	O.Fiabilité	O.Échanges_Don._Protég.
Ressources matérielles, procédurales et ou personnel																		
Développement		x	x	x														
Fabrication			x	x														
Livraison						x					x	x						
Génération de données de sécurité										x								
Acheminement des données de sécurité										x								
Ateliers agréés							x											
Interface mécanique							x											
Inspection régulière						x	x		x		x							
Contrôles d'application de la loi					x	x	x		x	x	x							
Mises à niveau logicielles											x							
Fonctions dédiées à la sécurité																		
Identification et authentification																		
UIA_101 Identification des entités	x							x					x		x			x
UIA_102 Identité des entités	x												x		x			

▼M1

	Menaces												Objectifs de sécurité informatique					
	M.Accès	M.Défauts	M.Essais	M.Conception	M.Environnement	M.Matériel	M.Origine_Mécanique	M.Données_Mouvement	M.Alimentation	M.Données_Sécurité	M.Logiciel	M.Données_Mémorisées	O.Accès	O.Analyse	O.Authentification	O.Traitement	O.Fiabilité	O.Échanges_Don._Protég.
UIA_103 Identité de l'UEV														x				
UIA_104 Authentification des entités	x							x					x		x			x
UIA_105 Authentification renouvelée	x							x					x		x			x
UIA_106 Authentification infalsifiable	x							x					x		x			
UIA_107 Échec d'une authentification								x						x			x	
Gestion des accès																		
ACC_101 Politique de contrôle d'accès	x									x		x	x					
ACC_102 ID du détecteur de mouvement												x	x					
ACC_103 Données utilisateur												x	x					
ACC_104 Données de sécurité										x		x	x					
ACC_105 Structure des fichiers et conditions d'accès	x									x		x	x					
Responsabilité																		
ACT_101 Données d'ID du détecteur de mouvement														x				
ACT_102 Données d'appariement														x				

▼M1

	Menaces												Objectifs de sécurité informatique					
	M.Accès	M.Défauts	M.Essais	M.Conception	M.Environnement	M.Matériel	M.Origine_Mécanique	M.Données_Mouvement	M.Alimentation	M.Données_Sécurité	M.Logiciel	M.Données_Mémorisées	O.Accès	O.Analyse	O.Authentification	O.Traitement	O.Fiabilité	O.Échanges_Don._Protég.
ACT_103 Données d'activité														x				
Analyse																		
AUD_101 Rapports d'analyse														x				
AUD_102 Liste des événements à rapporter	x				x	x						x		x				
AUD_103 Données d'analyse														x				
AUD_104 Outils d'analyse														x				
AUD_105 mémorisation des rapports d'analyse														x				
Précision																		
ACR_101 politique de contrôle des flux d'informations								x								x	x	
ACR_102 Transferts internes																x	x	
ACR_103 Transferts internes														x				
ACR_104 Intégrité des données enregistrées												x					x	
ACR_105 Intégrité des données enregistrées												x		x				

▼M1

	Menaces												Objectifs de sécurité informatique					
	M.Accès	M.Défauts	M.Essais	M.Conception	M.Environnement	M.Matériel	M.Origine_Mécanique	M.Données_Mouvement	M.Alimentation	M.Données_Sécurité	M.Logiciel	M.Données_Mémorisées	O.Accès	O.Analyse	O.Authentification	O.Traitement	O.Fiabilité	O.Échanges_Don._Protég.
Fiabilité																		
RLB_101 Essais de fabrication			x	x													x	
RLB_102 Essais automatiques		x				x			x		x						x	
RLB_103 Essais automatiques						x			x		x			x				
RLB_104 Analyse logicielle				x							x						x	
RLB_105 Entrée logicielle											x					x	x	
RLB_106 Ouverture de boîtier				x	x	x				x	x	x					x	
RLB_107 Sabotage du matériel						x											x	
RLB_108 Sabotage du matériel						x								x				
RLB_109 Coupures d'alimentation									x								x	
RLB_110 Réinitialisation		x															x	
RLB_111 Disponibilité des données																x	x	
RLB_112 Applications multiples																	x	
Échange de données																		

▼M1

	Menaces												Objectifs de sécurité informatique					
	M.Accès	M.Défauts	M.Essais	M.Conception	M.Environnement	M.Matériel	M.Origine_Mécanique	M.Données_Mouvement	M.Alimentation	M.Données_Sécurité	M.Logiciel	M.Données_Mémorisées	O.Accès	O.Analyse	O.Authentification	O.Traitement	O.Fiabilité	O.Échanges_Don._Protég.
DEX_101 Exportation sécurisée des données de mouvement								x										x
Soutien cryptographique																		
CSP_101 Algorithmes																	x	x
CSP_102 Génération de clés																	x	x
CSP_103 Distribution de clés																	x	x
CSP_104 Accès aux clés																	x	x
CSP_105 Destruction de clés																	x	x

▼M1

OBJECTIFS GÉNÉRAUX DE SÉCURITÉ POUR L'UNITÉ EMBARQUÉE SUR LE VÉHICULE

1. **Introduction**

Le présent document comporte une description de l'unité embarquée sur le véhicule, des menaces qu'elle doit être capable de neutraliser et des objectifs de sécurité qu'elle se doit d'atteindre. Il spécifie la nature des fonctions dédiées à la sécurité que requiert le système. De plus, il précise la puissance minimale des mécanismes de sécurité ainsi que le niveau de garantie requis tant en ce qui concerne le développement que l'évaluation du matériel considéré.

Les exigences dont il est fait état dans le présent document sont celles qui apparaissent dans le corps de l'annexe I B. Les exigences énoncées, pour plus de clarté, dans le corps de l'annexe I B font parfois double emploi avec les exigences requises en matière d'objectifs de sécurité. En cas d'ambiguïté entre l'une des exigences requises en matière d'objectifs de sécurité et l'exigence de l'annexe I B à laquelle la première fait référence, l'exigence énoncée dans le corps de l'annexe I B prévaudra.

Les exigences énoncées dans le corps de l'annexe I B auxquelles les objectifs de sécurité ne font aucune allusion sont sans rapport avec les fonctions dédiées à la sécurité.

Aux fins de traçabilité, des labels individuels ont été affectés aux menaces, objectifs, ressources procédurales et spécifications des fonctions dédiées à la sécurité qui apparaissent dans la documentation de développement et d'évaluation.

2. **Abréviations, définitions et références**

2.1. ***Abréviations***

PIN	Numéro d'identification personnel
ROM	Mémoire morte
SEF	Fonction dédiée à la sécurité
TBD	À définir
TOE	Cible d'évaluation
UEV	Unité embarquée sur le véhicule

2.2. ***Définitions***

Tachygraphe numérique	Équipement d'enregistrement
Données de mouvement	Données échangées avec le détecteur de mouvement et rendant compte de la vitesse du véhicule et de la distance parcourue
Pièces séparées physiquement	Composants matériels de l'unité embarquée sur le véhicule disséminés dans le véhicule par opposition aux composants matériels regroupés dans le boîtier de l'UEV
Données de sécurité	Données particulières indispensables à l'exécution des fonctions dédiées à la sécurité (p. ex. clés cryptographiques)
Système	Équipement, personnel ou entreprises entretenant un rapport quelconque avec l'équipement d'enregistrement
Utilisateur	Utilisateurs humains de l'équipement. Utilisateurs normaux de l'unité embarquée sur le véhicule: conducteurs, contrôleurs, ateliers et entreprises
Données utilisateur	Toutes les données autres que les données de sécurité qui sont enregistrées ou mémorisées par l'unité embarquée sur le véhicule, conformément aux dispositions énoncées au chapitre III.12

2.3. ***Références***

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991 [Critères d'évaluation de la sécurité informatique]

▼M1

3. **Argumentaire de produit**

3.1. ***Description de l'unité embarquée sur le véhicule et méthode d'utilisation***

L'unité embarquée sur le véhicule est conçue pour être installée sur des véhicules de transport routier. Elle a pour fonction d'enregistrer, mémoriser, afficher, imprimer et sortir des données se rapportant aux activités du ou des conducteurs.

L'UEV est raccordée à un détecteur de mouvement avec lequel elle échange des données de mouvement relatives au véhicule considéré.

Les utilisateurs s'identifient auprès de l'UEV au moyen de cartes de tachygraphe.

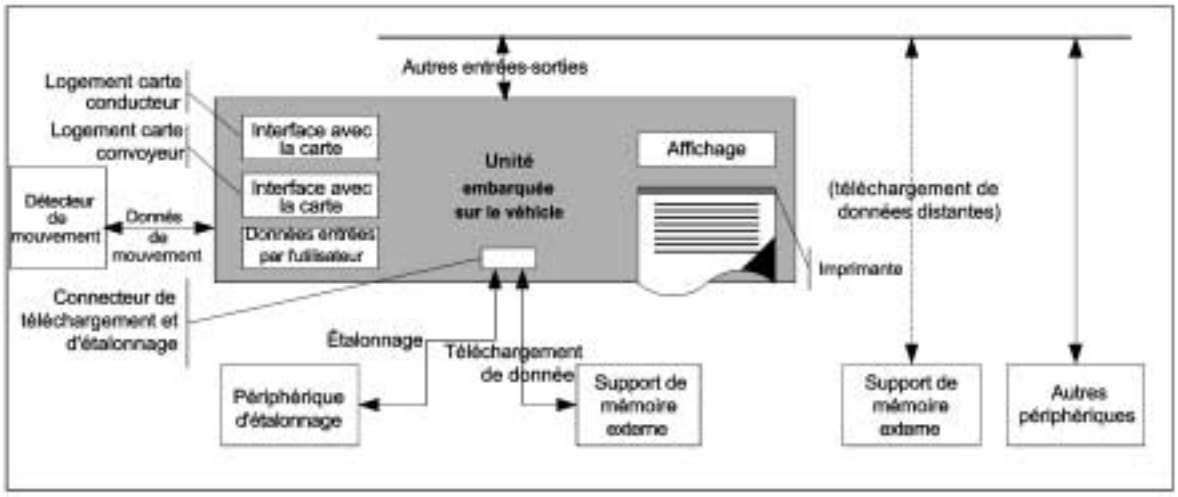
L'UEV enregistre et mémorise les données d'activité utilisateur dans sa mémoire de données; elle enregistre également les données d'activité utilisateur enregistrées sur les cartes de tachygraphe.

L'UEV procède à la sortie de données à destination de son écran d'affichage, d'une imprimante et de périphériques externes.

La figure ci-après illustre l'environnement opérationnel de l'unité embarquée sur le véhicule lorsqu'elle est installée sur un véhicule:

Figure 2

Environnement opérationnel de l'unité embarquée sur le véhicule



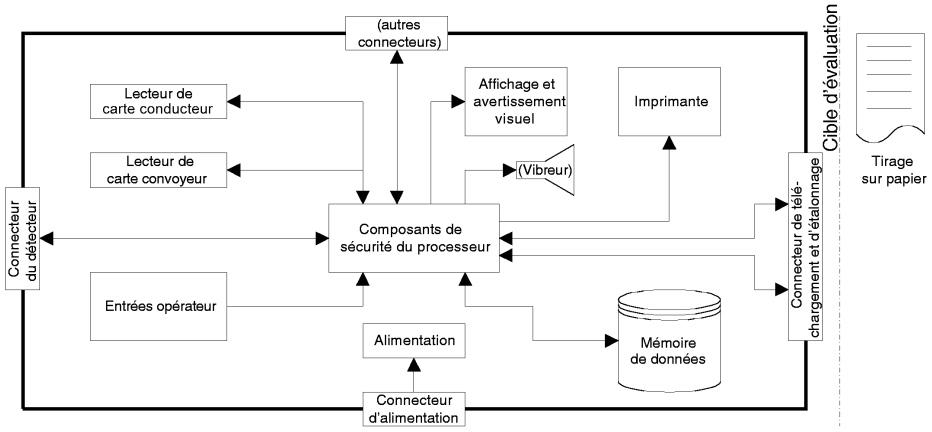
Le Chapitre II de l'Annexe I (B) présente une description détaillée des caractéristiques, fonctions et modes d'exploitation de l'UEV.

Les exigences fonctionnelles auxquelles doit satisfaire l'UEV sont spécifiées au chapitre III de l'annexe I B.

La figure ci-après illustre une UEV classique:

Figure 3

UEV classique (…) en option



▼**M1**

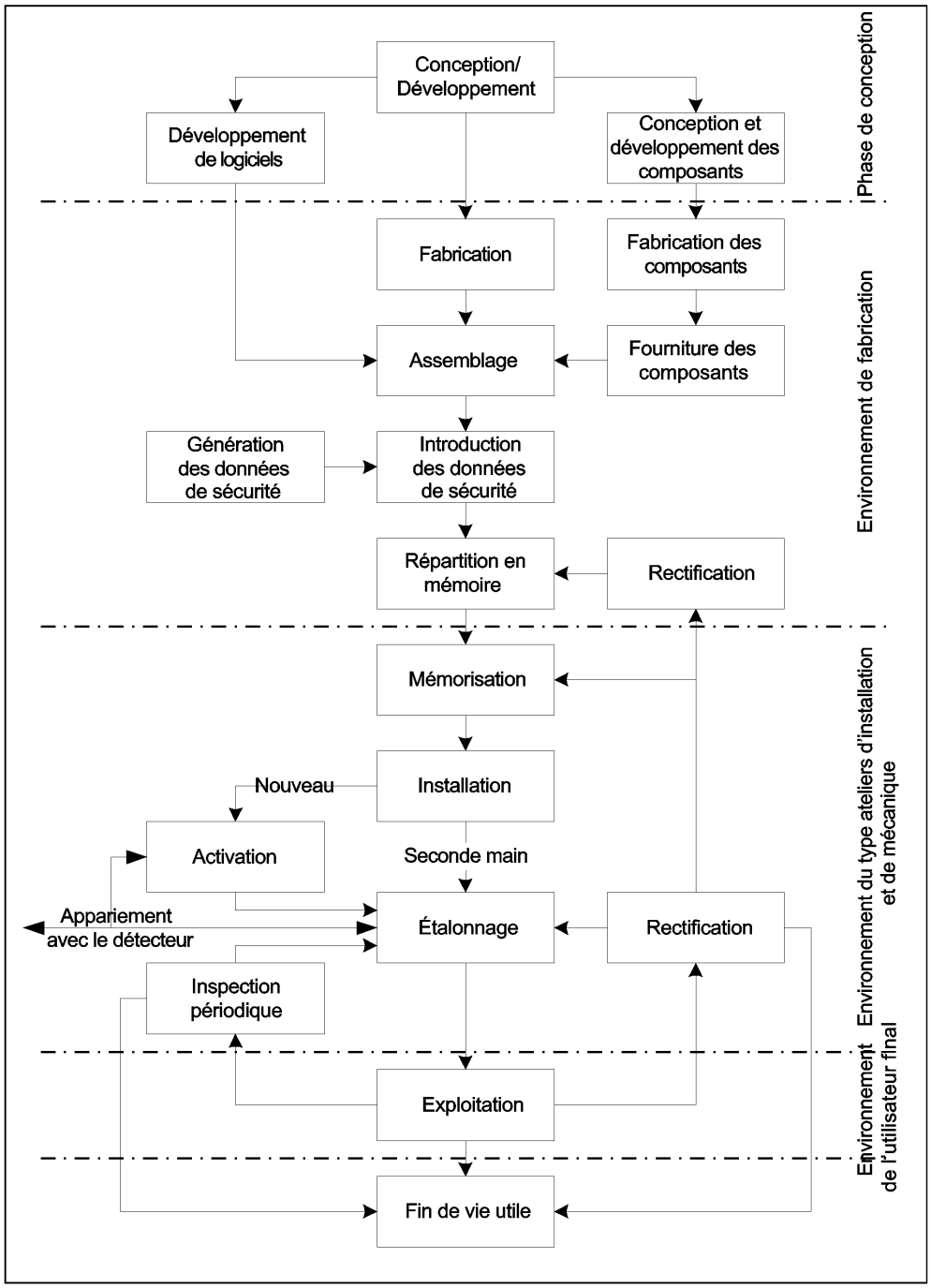
Il convient d'observer qu'en dépit de l'appartenance du mécanisme d'impression à la cible d'évaluation, le document tiré sur papier cesse de l'être après impression.

3.2. ***Cycle de vie de l'unité embarquée sur le véhicule***

La figure ci-après illustre le cycle de vie caractéristique de l'UEV:

Figure 4

Cycle de vie caractéristique de l'UEV



▼**M1**

3.3. ***Menaces***

Ce paragraphe présente une description des menaces qui pèsent sur l'UEV.

3.3.1. *Menaces pesant sur les politiques d'identification et de contrôle d'accès*

M.Accès	Certains utilisateurs pourraient tenter d'accéder à des fonctions qui leur sont interdites (p. ex. conducteurs accédant à la fonction d'étalonnage)
M.Identification	Certains utilisateurs pourraient tenter de se servir de plusieurs identifications ou de n'en utiliser aucune

3.3.2. *Menaces inhérentes à la conception*

M.Défauts	Certaines anomalies affectant les matériels, logiciels et procédures de communication pourraient mettre l'UEV dans une situation imprévue susceptible d'en compromettre la sécurité
M.Essais	Le recours à des modes d'essai non invalidés ou à des portes dérobées pourrait compromettre la sécurité de l'UEV
M.Conception	Certains utilisateurs pourraient être tentés de se procurer de manière illicite des données confidentielles concernant la conception de ladite unité embarquée sur le véhicule en les extrayant du matériel dont dispose le fabricant (vol, corruption, etc.) ou en procédant par ingénierie inverse

3.3.3. *Menaces pesant sur l'exploitation*

M.Paramètres_Étalonnage	Certains utilisateurs pourraient tenter d'utiliser des équipements dont l'étalonnage est erroné (par l'apport de modifications aux données d'étalonnage ou en raison de faiblesses structurelles)
M. Échange_Don._Carte	Certains utilisateurs pourraient tenter de modifier des données pendant leur échange entre l'UEV et des cartes de tachygraphe (adjonction, modification, suppression, restitution du signal)
M.Horloge	Certains utilisateurs pourraient tenter de modifier l'horloge interne
M.Environnement	Certains utilisateurs pourraient compromettre la sécurité de l'UEV par des agressions à caractère environnemental (agressions thermiques, électromagnétiques, optiques, chimiques, mécaniques, etc.)
M.Périphériques_Factice	Certains utilisateurs pourraient tenter de raccorder des périphériques factices (détecteur mouvement, cartes à mémoire) à l'UEV
M.Matériel	Certains utilisateurs pourraient tenter d'altérer le matériel constitutif de l'UEV
M.Données_Mouvement	Certains utilisateurs pourraient tenter d'apporter des modifications aux données de mouvement du véhicule (adjonction, modification, suppression, restitution du signal)
M.Non_Activation	Certains utilisateurs pourraient se servir d'équipements non activés
M.Sortie_Données	Certains utilisateurs pourraient tenter de modifier la sortie de données (impression, affichage ou téléchargement)
M.Alimentation	Certains utilisateurs pourraient tenter d'aller à l'encontre des objectifs de sécurité de l'UEV en modifiant son alimentation (coupure, réduction, augmentation)
M.Données_Sécurité	Certains utilisateurs pourraient être tentés de se procurer de manière illicite des données de sécurité confidentielles lors de leur génération, de leur transfert ou de leur enregistrement au sein de l'équipement
M.Logiciel	Certains utilisateurs pourraient tenter d'apporter des modifications au logiciel de l'UEV

▼**M1**

M.Données_Mémorisées	Certains utilisateurs pourraient tenter de modifier les données mémorisées (données utilisateur ou de sécurité)

3.4. ***Objectifs de sécurité***

Le principal objectif de sécurité du système tachygraphique numérique s'énonce comme suit:

O.Principal	Les données que les services de contrôle sont censés vérifier se doivent d'être disponibles et de refléter fidèlement et avec la précision requise les activités des conducteurs contrôlés et de leurs véhicules tant en ce qui concerne la vitesse du véhicule considéré que les périodes de conduite, de travail, de disponibilité et de repos

Par conséquent, les objectifs de sécurité de l'UEV contribuant à l'objectif de sécurité global s'énoncent comme suit:

O.Principal_UEV	Les données que l'UEV doit mesurer et enregistrer pour que les services de contrôle puissent procéder aux vérifications nécessaires se doivent d'être disponibles et de refléter fidèlement et avec la précision requise les activités des conducteurs contrôlés et de leurs véhicules tant en ce qui concerne la vitesse du véhicule considéré que les périodes de conduite, de travail, de disponibilité et de repos
O.UEV_Exportation	L'UEV doit être à même d'exporter des données vers des supports de mémoire externes afin de permettre à qui de droit d'en vérifier l'intégrité et l'authenticité

3.5. ***Objectifs de sécurité informatique***

Les objectifs de sécurité informatique spécifiques de l'UEV contribuant à ses objectifs de sécurité globaux s'énoncent comme suit:

O.Accès	L'UEV doit contrôler l'accès des utilisateurs aux fonctions et données
O.Responsabilité	L'UEV doit recueillir des données d'activité précises
O.Analyse	L'UEV se doit de surveiller les tentatives d'affaiblissement de la sécurité du système et remonter jusqu'aux utilisateurs impliqués dans ces opérations
O.Authentification	L'UEV doit authentifier les utilisateurs et les entités connectées (lorsqu'il faut établir une voie de confiance entre diverses entités)
O.Intégrité	L'UEV doit préserver l'intégrité des données enregistrées
O.Sortie	L'UEV doit garantir que les sorties de données reflètent avec la précision requise les données mesurées ou enregistrées
O.Traitement	L'UEV doit s'assurer que le traitement des entrées dont découlent les données utilisateur est d'une précision satisfaisante
O.Fiabilité	L'UEV doit assurer un service d'une fiabilité satisfaisante
O.Échange_Don._Protég.	L'UEV doit protéger les échanges de données avec le détecteur de mouvement et les cartes de tachygraphe

3.6. ***Ressources matérielles, procédurales et en personnel***

Ce paragraphe présente une description des ressources matérielles, procédurales et en personnel qui contribuent à la sécurité de l'UEV

3.6.1. *Conception de l'équipement*

R.Développement	Les concepteurs de l'UEV doivent veiller à ce que la répartition des responsabilités pendant la phase de développement ne mette pas en péril la sécurité informatique du projet

▼**M1**

R.Fabrication	Les fabricants d'UEV doivent veiller à ce que la répartition des responsabilités pendant la phase de fabrication ne mette pas en péril la sécurité informatique du projet et à ce que l'UEV considérée soit protégée contre le risque d'agressions physiques susceptibles d'en compromettre la sécurité informatique pendant le processus de fabrication

3.6.2. *Livraison et activation de l'équipement*

R.Livraison	Les fabricants d'UEV, les constructeurs automobiles ainsi que les ateliers d'installation ou de mécanique doivent veiller à ce qu'aucune intervention sur les UEV non activées n'en compromette la sécurité informatique
R.Activation	Les constructeurs automobiles ainsi que les ateliers d'installation ou de mécanique doivent activer les UEV considérées après leur installation, mais avant que les véhicules concernés quittent les locaux où cette installation a eu lieu

3.6.3. *Génération et livraison des données de sécurité*

R.Génération_Don._Sécur.	Les algorithmes de génération des données de sécurité ne doivent être accessibles qu'à des personnes autorisées et dignes de confiance
R.Transport_Don._Sécur.	Les données de sécurité doivent être générées, acheminées et introduites dans l'UEV de telle manière que leur confidentialité et leur intégrité soient préservées

3.6.4. *Livraison des cartes*

R.Disponibilité_Carte	Les cartes de tachygraphe doivent être disponibles et n'être livrées qu'à des personnes dûment autorisées
R.Unicité_Carte_Conduc.	Les conducteurs doivent posséder une et une seule carte de conducteur valable
R.Traçabilité_Carte	La livraison des cartes doit être aisée à reconstituer (listes blanches, listes noires) et les listes noires utilisées lors des analyses de sécurité

3.6.5. *Installation, étalonnage et inspection de l'équipement d'enregistrement*

R.Ateliers_Agréés	L'installation, l'étalonnage et la réparation de l'équipement d'enregistrement doivent être confiés à des ateliers d'installation ou de mécanique agréés et dignes de confiance
R.Inspections_Régulières	L'équipement d'enregistrement doit faire l'objet d'inspections et d'étalonnages périodiques
R.Étalonnage_Précis	Les ateliers d'installation et de mécanique agréés se doivent d'entrer des paramètres de véhicule appropriés dans l'équipement d'enregistrement au cours de l'étalonnage

3.6.6. *Exploitation de l'équipement*

R.Conducteurs_Fiables	Les conducteurs doivent respecter la règle du jeu et faire preuve de sérieux (p. ex. se servir de leurs cartes de conducteur, sélectionner correctement leur activité parmi celles dont la sélection s'opère manuellement, etc.)

3.6.7. *Contrôle d'application de la loi*

R.Contrôles	L'équipement doit être soumis régulièrement et de manière aléatoire à des contrôles d'application de la loi. Ces contrôles doivent s'accompagner d'analyses de sécurité.

3.6.8. *Mises à niveau logicielles*

R.Actualisation_Logiciel	Toute révision logicielle doit s'être vue octroyer un certificat de sécurité avant toute mise en œuvre au sein d'une UEV

▼M1

4. **Fonctions dédiées à la sécurité**

4.1. ***Identification et authentification***

4.1.1. *Identification et authentification du détecteur de mouvement*

L'UEV doit être à même d'établir, lors de chaque interaction, l'identité du détecteur de mouvement auquel elle est raccordée

L'identité du détecteur de mouvement se composera des numéros d'homologation et de série du détecteur

L'UEV authentifiera le détecteur de mouvement auquel elle est raccordée:

— lors de la connexion du détecteur de mouvement
— lors de chaque étalonnage de l'équipement d'enregistrement
— lors de tout rétablissement de l'alimentation

Ce processus d'authentification mutuel sera lancé par l'UEV

L'UEV exécutera périodiquement (période à définir par le constructeur, cette dernière devant toutefois être inférieure à une heure) une procédure d'identification et d'authentification renouvelées du détecteur de mouvement auquel elle est raccordée. L'UEV devra s'assurer que personne n'a remplacé par un autre instrument le détecteur de mouvement identifié lors du dernier étalonnage de l'équipement d'enregistrement

L'UEV détectera et préviendra toute tentative d'utilisation de données d'authentification copiées ou reconstituées

Après la détection de X tentatives (c'est au fabricant qu'il appartient d'en déterminer le nombre, celui-ci devant demeurer inférieur à 20) d'authentification successives mais infructueuses et/ou après la détection d'un changement d'identité non autorisé (autrement dit, alors que l'équipement d'enregistrement n'est pas en cours d'étalonnage) du détecteur de mouvement, la fonction dédiée à la sécurité (SEF) devra:

— générer un rapport d'analyse de l'événement
— avertir l'utilisateur
— continuer à accepter et utiliser les données de mouvement non sécurisées que lui envoie le détecteur de mouvement.

4.1.2. *Identification et authentification de l'utilisateur*

L'UEV assurera en permanence et de manière sélective le suivi de l'identité de deux utilisateurs, en surveillant les cartes de tachygraphe respectivement introduites dans les lecteurs conducteur et convoyeur de l'appareil.

L'identité de chaque utilisateur se composera des éléments suivants:

— un groupe d'utilisateurs:
  — CONDUCTEUR (carte de conducteur)
  — CONTRÔLEUR (carte de contrôle)
  — ATELIER (carte d'atelier)
  — ENTREPRISE (carte d'entreprise)
  — INCONNU (pas de carte insérée)
— une ID d'utilisateur se composera des éléments suivants:
  — le code de l'État membre émetteur de la carte et le numéro de la carte
  — INCONNU si le groupe d'utilisateurs est INCONNU.

Les identités INCONNUES peuvent être implicitement ou explicitement connues.

L'UEV procédera à l'authentification de ses utilisateurs lors de toute insertion de carte.

L'UEV procédera à une authentification renouvelée de ses utilisateurs:

— lors de tout rétablissement de l'alimentation
— périodiquement ou après la manifestation de certains événements (période à définir par le fabricant, cette dernière devant toutefois être inférieure à 24 heures).

La procédure d'authentification consistera à démontrer que la carte introduite est une carte tachygraphique valable sur laquelle sont enregistrées des données de sécurité qui émanent obligatoirement du système considéré. Ce processus d'authentification mutuel sera lancé par l'UEV.

Outre les prescriptions énoncées ci-avant, les ateliers seront tenus de se laisser authentifier par le biais d'un contrôle de leur numéro d'identification personnel. Ces numéros d'identification devront comporter 4 caractères au moins.

▼M1

Remarque: si ce numéro d'identification personnel est communiqué à l'UEV par l'intermédiaire d'un équipement externe situé à proximité de celle-ci, la confidentialité du numéro concerné ne doit pas obligatoirement faire l'objet d'une protection particulière pendant l'opération de transfert.

L'UEV détectera et préviendra toute tentative d'utilisation de données d'authentification copiées ou reconstituées.

Après la détection de 5 tentatives d'authentification successives mais infructueuses, la fonction dédiée à la sécurité (SEF) devra:

— générer un rapport d'analyse de l'événement

— avertir l'utilisateur

— considérer l'utilisateur comme INCONNU et la carte comme non valable [définition z) et exigence 007].

4.1.3. *Identification et authentification de l'entreprise connectée à distance*

L'installation d'une capacité de connexion à distance est une option facultative. Par conséquent, le paragraphe qui suit n'est d'application qu'à la condition que cette fonction soit implémentée.

Lors de toute interaction avec une entreprise connectée à distance, l'UEV devra être à même d'établir l'identité de cette entreprise.

L'identité de l'entreprise connectée à distance se composera des éléments suivants: code de l'État membre émetteur de la carte et le numéro de la carte de l'entreprise.

L'UEV procédera à une authentification probante de l'entreprise connectée à distance avant d'autoriser l'exportation de données à destination de celle-ci.

La procédure d'authentification consistera à démontrer que l'entreprise concernée possède une carte d'entreprise valable sur laquelle sont enregistrées des données de sécurité qui émanent obligatoirement du système considéré.

L'UEV détectera et préviendra toute tentative d'utilisation de données d'authentification copiées ou reconstituées.

Après la détection de 5 tentatives d'authentification successives mais infructueuses, la fonction dédiée à la sécurité (SEF) devra:

— avertir l'entreprise connectée à distance.

4.1.4. *Identification et authentification de l'unité de gestion*

Les fabricants d'UEV doivent prévoir le développement et la fabrication de périphériques spécialisés autorisant l'exécution de fonctions de gestion supplémentaires de l'UEV (p. ex. mise à niveau de logiciels, rechargement des données de sécurité, etc.). Par conséquent, le paragraphe qui suit n'est d'application qu'à la condition que cette fonction soit implémentée.

Lors de toute interaction avec une unité de gestion, l'UEV devra être à même d'établir l'identité de cette unité.

L'UEV procédera à une authentification probante de l'unité de gestion considérée avant d'autoriser toute interaction ultérieure avec cette dernière.

L'UEV détectera et préviendra toute tentative d'utilisation de données d'authentification copiées ou reconstituées.

4.2. ***Gestion des accès***

Les contrôles d'accès garantissent que l'extraction d'informations à partir de la cible d'évaluation, leur création au sein de celle-ci ou l'apport de modifications à ces données sont des opérations auxquelles seules les personnes dûment autorisées sont à même de procéder.

Il convient d'observer qu'en dépit de la sensibilité commerciale ou du caractère privé de certaines données utilisateur enregistrées par l'UEV, celles-ci ne sont pas d'une nature confidentielle. Par conséquent, l'exigence fonctionnelle relative aux droits d'accès en lecture aux données (exigence 011) ne fait l'objet d'aucune fonction dédiée à la sécurité.

4.2.1. *Politique de contrôle d'accès*

L'UEV gérera et contrôlera les droits d'accès aux fonctions et données.

4.2.2. *Droits d'accès aux fonctions*

L'UEV appliquera les règles de sélection du mode d'exploitation (exigences 006 à 009).

L'UEV recourra au mode d'exploitation approprié pour appliquer les règles de contrôle d'accès aux fonctions (exigence 010).

▼M1

4.2.3. *Droits d'accès aux données*

L'UEV appliquera les règles d'accès en écriture aux données d'identification de l'UEV (exigence 076)

L'UEV appliquera les règles d'accès en écriture aux données d'identification du détecteur de mouvement associé (exigences 079 et 155).

Après son activation, l'UEV veillera à ce que l'introduction de données d'étalonnage et leur enregistrement dans sa mémoire de données ne soient possibles qu'en mode étalonnage (exigences 154 et 156).

Après son activation, l'UEV appliquera les règles d'accès en écriture et en suppression aux données d'étalonnage (exigence 097).

Après son activation, l'UEV veillera à ce que l'introduction de données de réglage temporel et leur enregistrement dans sa mémoire de données ne soient possibles qu'en mode étalonnage (cette exigence ne s'applique pas aux petits réglages temporels autorisés par les exigences 157 et 158).

Après son activation, l'UEV appliquera les règles d'accès en écriture et en suppression aux données de réglage temporel (exigence 100).

L'UEV appliquera aux données de sécurité les droits d'accès en lecture et en écriture qui s'imposent (exigence 080).

4.2.4. *Structure des fichiers et conditions d'accès*

La structure des fichiers d'application et de données ainsi que les conditions d'accès à ces fichiers seront définies pendant le processus de fabrication, puis verrouillées afin de décourager toute tentative de modification ou de suppression.

4.3. ***Responsabilité***

L'UEV veillera à ce que les conducteurs soient comptables de leurs activités (exigences 081, 084, 087, 105 *bis*, 105 *ter*, 109 et 109 *bis*).

L'UEV sauvegardera dans sa mémoire des données d'identification permanentes (exigence 075).

L'UEV veillera à ce que les ateliers soient comptables de leurs activités (exigences 098, 101 et 109).

L'UEV veillera à ce que les contrôleurs soient comptables de leurs activités (exigences 102, 103 et 109).

L'UEV enregistrera des données odométriques (exigence 090) ainsi que des données détaillées sur la vitesse (exigence 093).

L'UEV veillera à ce que les données utilisateur en rapport avec les exigences 081 à 093 et 102 à 105 ter incluses ne subissent aucune modification après leur enregistrement, si ce n'est lorsqu'elles deviennent les données mémorisées les plus anciennes auxquelles seront amenées à se substituer des données plus récentes.

L'UEV doit s'abstenir d'apporter des modifications aux données déjà mémorisées sur une carte tachygraphique (exigences 109 et 109*bis*) si ce n'est pour remplacer les données les plus anciennes par de nouvelles données (exigence 110) ou si le système se trouve dans le cas de figure décrit dans la remarque du paragraphe 2.1 de l'appendice 1.

4.4. ***Analyse***

Les fonctions d'analyse ne doivent s'appliquer qu'aux événements susceptibles d'indiquer une tentative de manipulation ou d'atteinte à la sécurité. Leur application est superflue dans le cadre de l'exercice normal des droits même s'ils entretiennent un rapport avec la sécurité.

L'UEV enregistrera les événements qui portent atteinte à sa sécurité en accompagnant leur enregistrement des données s'y rapportant (exigences 094, 096 et 109).

Les événements qui affectent la sécurité de l'UEV sont les suivants:

— Tentatives d'atteinte à la sécurité:
  — échec de la procédure d'authentification du détecteur de mouvement
  — échec de la procédure d'authentification des cartes de tachygraphe
  — remplacement illicite du détecteur de mouvement
  — défaut d'intégrité de l'entrée des données enregistrées sur une carte
  — défaut d'intégrité des données utilisateur enregistrées
  — erreur de transfert de données internes

▼M1

— ouverture illicite d'un boîtier

— sabotage du matériel

— Clôture incorrecte de la dernière session de carte

— Événement erreur affectant les données de mouvement

— Événement erreur affectant l'alimentation

— Défaillance interne de l'UEV.

L'UEV appliquera les règles d'archivage des rapports d'analyse (exigences 094 et 096).

L'UEV enregistrera dans sa mémoire de données les rapports d'analyse générés par le détecteur de mouvement.

Le système autorisera l'impression, l'affichage et le téléchargement de rapports d'analyse.

4.5. ***Réutilisation d'objets***

L'UEV devra permettre la réutilisation des objets de stockage temporaire sans que celle-ci se traduise par la génération de flux d'informations inadmissibles.

4.6. ***Précision***

4.6.1. *Politique de contrôle des flux d'informations*

L'UEV devra veiller à ce que les données utilisateur relevant des exigences 081, 084, 087, 090, 093, 102, 104, 105, 105 **bis** et 109 ne puissent être traitées qu'à partir des sources d'entrée appropriées:

— données de mouvement du véhicule

— horloge temps réel de l'UEV

— paramètres d'étalonnage de l'équipement d'enregistrement

— cartes de tachygraphe

— données introduites par l'utilisateur.

L'UEV devra veiller à ce que les données utilisateur relevant de l'exigence 109 *bis* ne puissent être entrées que pour la période comprise entre le dernier retrait de la carte et l'introduction actuelle (exigence 050 *bis*).

4.6.2. *Transferts de données internes*

Les exigences énoncées dans ce paragraphe ne sont d'application que si l'UEV a recours à des pièces séparées physiquement.

Si des données doivent être transférées entre des pièces séparées physiquement de l'UEV, il faut que celles-ci soient à l'abri de toute tentative de modification.

En cas de détection d'une erreur de transfert de données pendant un transfert interne, l'UEV devra procéder à une nouvelle transmission tandis que la fonction dédiée à la sécurité devra générer un rapport d'analyse de l'événement.

4.6.3. *Intégrité des données enregistrées*

L'UEV vérifiera les données utilisateur enregistrées dans sa mémoire de données afin de déceler tout défaut d'intégrité éventuel.

En cas de détection d'un défaut d'intégrité affectant les données utilisateur mémorisées, la fonction dédiée à la sécurité générera un rapport d'analyse.

4.7. ***Fiabilité du service***

4.7.1. *Essais*

Toutes les commandes, actions ou points d'essai propres aux besoins d'essai de la phase de fabrication de l'UEV seront désactivés ou supprimés avant l'activation de l'UEV. Il ne sera pas possible de les rétablir aux fins d'utilisation ultérieure.

L'UEV procédera à des essais automatiques durant sa phase de mise en route initiale ainsi qu'en cours d'exploitation normale afin de s'assurer de son bon fonctionnement. Les essais automatiques de l'UEV comporteront une vérification de l'intégrité des données de sécurité ainsi qu'une vérification de l'intégrité du code exécutable enregistré (pour autant qu'il ne soit pas enregistré dans la mémoire morte).

▼M1

En cas de détection d'une anomalie interne pendant un essai automatique, la fonction dédiée à la sécurité devra:

— générer un rapport d'analyse (sauf en mode étalonnage) (anomalie interne de l'UEV)

— préserver l'intégrité des données mémorisées.

4.7.2. *Logiciel*

Après activation de l'UEV, son logiciel d'exploitation sera impossible à analyser ou dépanner sur site.

Les entrées provenant de sources externes ne seront en aucun cas acceptées comme des codes exécutables.

4.7.3. *Protection matérielle*

Si le boîtier de l'UEV est conçu pour être ouvert, l'UEV doit être à même, sauf en mode étalonnage, de déceler toute ouverture de ce boîtier pendant une période minimale de 6 mois, même si elle est privée d'alimentation externe. En pareil cas, la fonction dédiée à la sécurité générera un rapport d'analyse (il est admis que les rapports d'analyse de cette nature soient générés et mémorisés après le rétablissement éventuel de l'alimentation électrique).

Si le boîtier de l'UEV se veut inviolable, l'UEV doit être ainsi conçue que toute tentative de violation soit aisément décelable (p. ex. par une inspection visuelle).

Après son activation, l'UEV devra détecter certaines tentatives de sabotage du matériel (à définir par le fabricant).

Dans l'éventualité d'une tentative de sabotage, la fonction dédiée à la sécurité générera un rapport d'analyse et l'UEV procédera à l'intervention suivante: (à définir par le fabricant).

4.7.4. *Coupures d'alimentation*

L'UEV décèlera tout écart par rapport aux valeurs prescrites, y compris les coupures d'alimentation.

En pareil cas, la fonction dédiée à la sécurité devra:

— générer un rapport d'analyse (sauf en mode étalonnage)

— préserver l'état de sécurisation de l'UEV

— assurer le maintien des fonctions de sécurité qui s'appliquent à des composants ou processus encore opérationnels

— préserver l'intégrité des données enregistrées.

4.7.5. *Conditions de réinitialisation*

En cas de coupure d'alimentation, d'interruption d'une transaction avant terme ou de toute autre situation requérant sa réinitialisation, l'UEV se réinitialisera sans heurt.

4.7.6. *Disponibilité des données*

L'UEV se devra de garantir l'accès aux ressources lorsque cela s'impose, sans que celles-ci soient sollicitées ou retenues inutilement.

L'UEV doit interdire toute libération des cartes avant d'avoir procédé à l'enregistrement des données requises sur celles-ci (exigences 015 et 016)

En pareil cas, la fonction dédiée à la sécurité générera un rapport d'analyse couvrant l'événement.

4.7.7. *Applications multiples*

Si l'UEV comporte des applications autres que l'application tachygraphique, toutes ces applications devront être séparées les unes des autres au niveau physique et/ou logique. Ces applications ne partageront aucune donnée de sécurité. Seule une tâche à la fois sera activée.

4.8. ***Échange de données***

Ce paragraphe traite de l'échange de données entre l'UEV et les périphériques raccordés.

4.8.1. *Échange de données avec le détecteur de mouvement*

L'UEV procédera à une vérification de l'intégrité et de l'authenticité des données de mouvement importées à partir du détecteur de mouvement

▼M1

En cas de détection d'un défaut d'intégrité ou d'authenticité affectant certaines données de mouvement, la fonction dédiée à la sécurité devra:

— générer un rapport d'analyse

— continuer à utiliser les données importées.

4.8.2. *Échange de données avec les cartes de tachygraphe*

L'UEV procédera à une vérification de l'intégrité et de l'authenticité des données de mouvement importées à partir des cartes de tachygraphe.

En cas de détection d'un défaut d'intégrité ou d'authenticité affectant certaines données enregistrées sur une carte, l'UEV devra:

— générer un rapport d'analyse

— s'abstenir d'utiliser les données concernées.

L'UEV exportera des données vers les cartes de tachygraphe en les accompagnant des attributs de sécurité qui leur sont associés de telle sorte que la ou les cartes concernées soient en mesure d'en vérifier l'intégrité et l'authenticité.

4.8.3. *Échange de données avec les supports de mémoire externes (fonction de téléchargement)*

L'UEV générera une preuve d'origine pour les données téléchargées vers des supports de mémoire externes.

L'UEV fournira au destinataire le moyen de vérifier l'authenticité de la preuve d'origine des données téléchargées.

L'UEV procédera au téléchargement de données vers des supports de mémoire externes en les accompagnant des attributs de sécurité qui leur sont associés de telle sorte que le ou les supports concernés soient en mesure de vérifier l'intégrité et l'authenticité des données téléchargées.

4.9. ***Soutien cryptographique***

Les exigences énoncées dans ce paragraphe ne sont d'application que dans les situations où leur usage s'impose, en fonction des mécanismes de sécurité employés et des solutions adoptées par le fabricant.

Toute opération cryptographique exécutée par l'UEV doit être en conformité avec un algorithme précis et un format de clé déterminé.

Si l'UEV génère des clés cryptographiques, elle doit s'acquitter de cette tâche en conformité avec certains formats et algorithmes de génération de clés cryptographiques.

Si l'UEV distribue des clés cryptographiques, elle doit s'acquitter de cette tâche en conformité avec certaines méthodes de distribution des clés cryptographiques.

Si l'UEV accède à des clés cryptographiques, elle doit s'acquitter de cette tâche en conformité avec certaines méthodes d'accès aux clés cryptographiques.

Si l'UEV détruit des clés cryptographiques, elle doit s'acquitter de cette tâche en conformité avec certaines méthodes de destruction des clés cryptographiques.

5. **Définition des mécanismes de sécurité**

Les mécanismes de sécurité requis font l'objet d'une description précise à l'appendice 11.

Les autres mécanismes de sécurité doivent être définis par les fabricants.

6. **Puissance minimale des mécanismes de sécurité**

La puissance minimale requise des mécanismes de sécurité de l'unité embarquée sur le véhicule est élevée, conformément aux critères définis dans le document de référence de l'ITSEC.

7. **Niveau de garantie**

Le niveau de garantie visé pour l'unité embarquée sur le véhicule correspond au niveau E3, conformément aux critères définis dans le document de référence de l'ITSEC.

▼M1

8. **Analyse raisonnée**

Les matrices qui suivent présentent une analyse raisonnée des fonctions dédiées à la sécurité en mettant en évidence les éléments suivants:

— les FDS et autres moyens de neutralisation des diverses menaces

— les FDS qui remplissent les différents objectifs de sécurité informatique.

▼M1

	Menaces																			Objectifs de sécurité informatique									
	M. Accès	M.Identification	M.Défauts	M.Essais	M.Conception	M.Paramètres_Étalonnage	M.Échange_Don._Carte	M.Horloge	M.Environnement	M.Périphériques_Factices	M.Matériel	M.Données_Mouvement	M.Désactivé	M.Données_Sortie	M.Alimentation	M.Saturation	M.Données_Sécurité	M.Logiciel	M.Données_Enregistrées	O.Accès	O.Responsabilité	O.Analyse	O.Authentification	O.Intégrité	O.Sortie	O.Traitement	O.Fiabilité	O.Échanges_Don._Protég.
Ressources matérielles, procédurales ou en personnel																													
Développement			x	x	x																								
Fabrication				x	x																								
Livraison													x																
Activation	x												x																
Génération de données de sécurité																	x												
Acheminement des données de sécurité																	x												
Disponibilité des cartes		x																											
Carte individuelle par conducteur		x																											
Traçabilité des cartes		x																											
Ateliers agréés						x		x																					
Inspection régulière étalonnage						x		x				x	x			x													
Ateliers fiables						x		x																					
Conducteurs fiables		x																											
Contrôles d'application de la loi		x				x		x	x		x		x		x			x	x										

▼M1

	Menaces																			Objectifs de sécurité informatique								
	M. Accès	M.Identification	M.Défauts	M.Essais	M.Conception	M.Paramètres_Étalonnage	M.Échange_Don._Carte	M.Horloge	M.Environnement	M.Périphériques_Factices	M.Matériel	M.Données_Mouvement	M.Désactivé	M.Données_Sortie	M.Alimentation	M.Saturation	M.Données_Sécurité	M.Logiciel	M.Données_Enregistrées	O.Accès	O.Responsabilité	O.Analyse	O.Authentification	O.Intégrité	O.Sortie	O.Traitement	O.Fiabilité	O.Échanges_Don._Protég.
Mises à niveau logicielles																			x									
Fonctions dédiées à la sécurité																												
Identification et authentification																												
UIA_201 Identification du détecteur										x		x											x					x
UIA_202 Identité du détecteur										x		x											x					x
UIA_203 Authentification du détecteur										x		x											x					x
UIA_204 Identification et authentification renouvelées du détecteur										x		x											x					x
UIA_205 Authentification infalsifiable										x		x											x					
UIA_206 Échec d'une authentification										x		x										x					x	
UIA_207 Identification des utilisateurs	x	x								x										x			x					x
UIA_208 Identité d'un utilisateur	x	x								x										x			x					x
UIA_209 Authentification d'un utilisateur	x	x								x										x			x					x
UIA_210 Authentification renouvelée d'un utilisateur	x	x								x										x			x					x
UIA_211 Moyens d'authentification	x	x								x										x			x					

▼**M1**

	Menaces																			Objectifs de sécurité informatique								
	M. Accès	M.Identification	M.Défauts	M.Essais	M.Conception	M.Paramètres_Étalonnage	M.Échange_Don._Carte	M.Horloge	M.Environnement	M.Périphériques_Factices	M.Matériel	M.Données_Mouvement	M.Désactivé	M.Données_Sortie	M.Alimentation	M.Saturation	M.Données_Sécurité	M.Logiciel	M.Données_Enregistrées	O.Accès	O.Responsabilité	O.Analyse	O.Authentification	O.Intégrité	O.Sortie	O.Traitement	O.Fiabilité	O.Échanges_Don._Protég.
UIA_212 Contrôles de PIN	x	x				x		x												x			x					
UIA_213 Authentification infalsifiable	x	x								x										x			x					
UIA_214 Échec d'une authentification	x	x								x												x						
UIA_215 Authentification d'un utilisateur distant	x	x																		x			x					x
UIA_216 Identité d'un utilisateur distant	x	x																		x			x					
UIA_217 Authentification d'un utilisateur distant	x	x																		x			x					x
UIA_218 Moyens d'authentification	x	x																		x			x					
UIA_219 Authentification infalsifiable	x	x																		x			x					
UIA_220 Échec d'une authentification	x	x																										
UIA_221 Identification d'un périphérique de gestion	x	x																		x			x					
UIA_222 Authentification d'un périphérique de gestion	x	x																		x			x					
UIA_223 Authentification infalsifiable	x	x																		x			x					
Gestion des accès																												
ACC_201 Politique de contrôle d'accès	x					x		x									x		x	x								

▼M1

	Menaces																			Objectifs de sécurité informatique								
	M. Accès	M.Identification	M.Défauts	M.Essais	M.Conception	M.Paramètres_Étalonnage	M.Échange_Don._Carte	M.Horloge	M.Environnement	M.Périphériques_Factices	M.Matériel	M.Données_Mouvement	M.Désactivé	M.Données_Sortie	M.Alimentation	M.Saturation	M.Données_Sécurité	M.Logiciel	M.Données_Enregistrées	O.Accès	O.Responsabilité	O.Analyse	O.Authentification	O.Intégrité	O.Sortie	O.Traitement	O.Fiabilité	O.Échanges_Don._Protég.
ACC_202 Droits d'accès aux fonctions	x					x		x												x								
ACC_203 Droits d'accès aux fonctions	x					x		x												x								
ACC_204 ID de l'UEV																			x	x								
ACC_205 ID du détecteur connecté										x									x	x								
ACC_206 Données d'étalonnage	x					x													x	x								
ACC_207 Données d'étalonnage						x													x	x								
ACC_208 Données de réglage temporel								x											x	x								
ACC_209 Données de réglage temporel								x											x	x								
ACC_210 Données de sécurité																	x		x	x								
ACC_211 Structure des fichiers et conditions d'accès	x					x											x		x	x								
Responsabilité																												
ACT_201 Responsabilité des conducteurs																					x							
ACT_202 Données d'ID de l'UEV																					x	x						
ACT_203 Responsabilité des ateliers																					x							
ACT_204 Responsabilité des contrôleurs																					x							

▼M1

	Menaces																			Objectifs de sécurité informatique								
	M. Accès	M.Identification	M.Défauts	M.Essais	M.Conception	M.Paramètres_Étalonnage	M.Échange_Don._Carte	M.Horloge	M.Environnement	M.Périphériques_Factices	M.Matériel	M.Données_Mouvement	M.Désactivé	M.Données_Sortie	M.Alimentation	M.Saturation	M.Données_Sécurité	M.Logiciel	M.Données_Enregistrées	O.Accès	O.Responsabilité	O.Analyse	O.Authentification	O.Intégrité	O.Sortie	O.Traitement	O.Fiabilité	O.Échanges_Don._Protég.
ACT_205 Détail des déplacements du véhicule																					x							
ACT_206 Modification des données d'activité																			x					x			x	
ACT_207 Modification des données d'activité																			x					x			x	
Analyse																												
AUD_201 Rapports d'analyse																						x						
AUD_202 Liste des événements à rapporter	x						x				x	x		x	x				x			x						
AUD_203 Règles d'enregistrement des rapports d'analyse																						x						
AUD_204 Rapports d'analyse du détecteur																						x						
AUD_205 Outils d'analyse																						x						
Réutilisation																												
REU_201 Réutilisation																	x									x	x	
Précision																												
ACR_201 Politique de contrôle des flux d'informations						x			x		x															x	x	

▼M1

	Menaces																			Objectifs de sécurité informatique								
	M. Accès	M.Identification	M.Défauts	M.Essais	M.Conception	M.Paramètres_Étalonnage	M.Échange_Don._Carte	M.Horloge	M.Environnement	M.Périphériques_Factices	M.Matériel	M.Données_Mouvement	M.Désactivé	M.Données_Sortie	M.Alimentation	M.Saturation	M.Données_Sécurité	M.Logiciel	M.Données_Enregistrées	O.Accès	O.Responsabilité	O.Analyse	O.Authentification	O.Intégrité	O.Sortie	O.Traitement	O.Fiabilité	O.Échanges_Don._Protég.
ACR_202 Transferts internes														x											x	x	x	
ACR_203 Transferts internes														x								x						
ACR_204 Intégrité des données enregistrées																			x					x			x	
ACR_205 Intégrité des données enregistrées																			x			x						
Fiabilité																												
RLB_201 Essais de fabrication				x	x																						x	
RLB_202 Essais automatiques			x								x				x			x									x	
RLB_203 Essais automatiques											x				x			x				x						
RLB_204 Analyse logicielle					x													x									x	
RLB_205 Entrée logicielle																		x						x	x	x		
RLB_206 Ouverture de boîtier					x				x		x			x			x	x	x					x		x		
RLB_207 Sabotage du matériel											x																x	
RLB_208 Sabotage du matériel											x											x						
RLB_209 Coupures d'alimentation															x												x	
RLB_210 Coupures d'alimentation															x							x						

▼M1

	Menaces																			Objectifs de sécurité informatique								
	M. Accès	M.Identification	M.Défauts	M.Essais	M.Conception	M.Paramètres_Étalonnage	M.Échange_Don._Carte	M.Horloge	M.Environnement	M.Périphériques_Factices	M.Matériel	M.Données_Mouvement	M.Désactivé	M.Données_Sortie	M.Alimentation	M.Saturation	M.Données_Sécurité	M.Logiciel	M.Données_Enregistrées	O.Accès	O.Responsabilité	O.Analyse	O.Authentification	O.Intégrité	O.Sortie	O.Traitement	O.Fiabilité	O.Échanges_Don._Protég.
RLB_211 Réinitialisation			x																								x	
RLB_212 Disponibilité des données																										x	x	
RLB_213 Libération de carte																											x	
RLB_214 Clôture incorrecte d'une session de carte																							x					
RLB_215 Applications multiples																											x	
Échange de données																												
DEX_201 Importation de données de mouvement sécurisées												x																x
DEX_202 Importation de données de mouvement sécurisées												x							x									
DEX_203 Importation de données de carte sécurisées							x																					x
DEX_204 Importation de données de carte sécurisées							x															x						
DEX_205 Exportation de données sécurisées vers les cartes							x																					x
DEX_206 Preuve d'origine																								x	x			

▼M1

	Menaces																			Objectifs de sécurité informatique								
	M. Accès	M.Identification	M.Défauts	M.Essais	M.Conception	M.Paramètres_Étalonnage	M.Échange_Don._Carte	M.Horloge	M.Environnement	M.Périphériques_Factices	M.Matériel	M.Données_Mouvement	M.Désactivé	M.Données_Sortie	M.Alimentation	M.Saturation	M.Données_Sécurité	M.Logiciel	M.Données_Enregistrées	O.Accès	O.Responsabilité	O.Analyse	O.Authentification	O.Intégrité	O.Sortie	O.Traitement	O.Fiabilité	O.Échanges_Don._Protég.
DEX_207 Preuved'origine																								x	x			
DEX_208 Exportation de données sécurisées vers des supports de mémoire externes																								x	x			
Soutien cryptographique																												
CSP_201 Algorithmes																											x	x
CSP_202 Génération de clés																											x	x
CSP_203 Distribution de clés																											x	x
CSP_204 Accès aux clés																											x	x
CSP_205 Destruction de clés																											x	x

▼M1

OBJECTIFS GÉNÉRAUX DE SÉCURITÉ POUR LES CARTES TACHYGRAPHIQUES

1. **Introduction**

Le présent document comporte la description d'une carte tachygraphique, des menaces qu'elle doit être capable de neutraliser et des objectifs de sécurité qu'elle se doit d'atteindre. Il spécifie la nature des fonctions dédiées à la sécurité que requiert le système. De plus, il précise la puissance minimale des mécanismes de sécurité ainsi que le niveau de garantie requis tant en ce qui concerne le développement que l'évaluation du matériel considéré.

Les exigences dont il est fait état dans le présent document sont celles qui apparaissent dans le corps de l'annexe I B. Les exigences énoncées, pour plus de clarté, dans le corps de l'annexe I B font parfois double emploi avec les exigences requises en matière d'objectifs de sécurité. En cas d'ambiguïté entre l'une des exigences requises en matière d'objectifs de sécurité et l'exigence de l'annexe I B à laquelle la première fait référence, l'exigence énoncée dans le corps de l'annexe I B prévaudra.

Les exigences énoncées dans le corps de l'annexe I B auxquelles les objectifs de sécurité ne font aucune allusion sont sans rapport avec les fonctions dédiées à la sécurité.

Une carte tachygraphique est une carte à puce standard qui véhicule une application tachygraphique spécialisée. Elle doit satisfaire aux exigences qui s'appliquent aux cartes de cette nature tant sur le plan fonctionnel que sur celui de leur niveau de garantie et de sécurité. Par conséquent, cet objectif de sécurité n'intègre que les exigences de sécurité supplémentaires requises par l'application tachygraphique.

Aux fins de traçabilité des labels individuels ont été affectés aux menaces, objectifs, ressources procédurales et spécifications des fonctions dédiées à la sécurité qui apparaissent dans la documentation de développement et d'évaluation.

2. **Abréviations, définitions et références**

2.1. ***Abréviations***

IC	Circuit intégré (composant électronique conçu pour exécuter des fonctions de traitement et/ou de mémoire)
OS	Système d'exploitation
PIN	Numéro d'identification personnel
ROM	Mémoire morte
SFP	Politique de définition des fonctions dédiées à la sécurité
TBD	À définir
TOE	Cible d'évaluation
TSF	Fonction de sécurité de la cible d'évaluation
UEV	Unité embarquée sur le véhicule.

2.2. ***Définitions***

Tachygraphe numérique	Équipement d'enregistrement
Données sensibles	Données mémorisées sur la carte tachygraphique dont il convient de protéger l'intégrité et la confidentialité (lorsque de telles mesures s'appliquent aux données de sécurité) tout en interdisant l'apport de modifications illicites. Les données de sécurité et les données utilisateur sont considérées comme des données sensibles
Données de sécurité	Données particulières indispensables à l'exécution des fonctions dédiées à la sécurité (p. ex. clés cryptographiques)
Système	Équipement, personnel ou entreprises entretenant un rapport quelconque avec l'équipement d'enregistrement
Utilisateur	Toute entité (utilisateur humain ou entité informatique externe) indépendante de la cible d'évaluation qui entre en interaction avec celle-ci (lorsque ce terme n'entre pas dans la composition de l'expression «données utilisateur»)

▼**M1**

Données utilisateur	Données sensibles (autres que les données de sécurité) enregistrées sur la carte tachygraphique considérée. Les données d'identification et d'activité font partie intégrante des données utilisateur
Données d'identification	Données d'identification regroupant les données d'identification de carte et d'identification des titulaires de carte
Don. d'identif. de carte	Données utilisateur en rapport avec l'identification de carte aux termes des exigences 190, 191, 192, 194, 215, 231 et 235
Don. d'identif. des titulaires	Données utilisateur en rapport avec l'identification des titulaires aux termes des exigences 195, 196, 216, 232 et 236
Données d'activité	Données d'activité regroupant les données d'activité du titulaire de la carte, les données d'événement et d'anomalie ainsi que les données d'activité de contrôle
Don. d'activité des titulaires	Données utilisateur en rapport avec les activités menées par le titulaire de la carte aux termes des exigences 197, 199, 202, 212, 212 *bis*, 217, 219, 221, 226, 227, 229, 230 *bis*, 233 et 237
Don. d'évén. et d'anomalie	Données utilisateur en rapport avec les événements ou anomalies aux termes des exigences 204, 205, 207, 208 et 223
Don. d'activité de contrôle	Données utilisateur en rapport avec les contrôles d'application de la loi aux termes des exigences 210 et 225

2.3. ***Références***

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991 [Critères d'évaluation de la sécurité informatique]
IC PP	Smartcard Integrated Circuit Protection Profile — version 2.0 — septembre 1998. Déposé auprès de l'organisme de certification national français sous le numéro d'enregistrement PP/9806
ES PP	Smart Card Integrated Circuit With Embedded Software Protection Profile — version 2.0 — juin 99. Déposé auprès de l'organisme de certification national français sous le numéro d'enregistrement PP/9911

3. **Argumentaire de produit**

3.1. ***Description d'une carte tachygraphique et méthode d'utilisation***

Une carte tachygraphique est une carte à puce satisfaisant aux critères énoncés dans les documents de référence IC PP et ES PP. En outre, cette carte se doit de véhiculer une application conçue pour être utilisée avec l'équipement d'enregistrement.

Les fonctions élémentaires d'une carte tachygraphique s'énoncent comme suit:

— mémoriser les données d'identification de la carte et de son titulaire. L'unité embarquée sur le véhicule utilise ces données pour identifier le titulaire de la carte, accorder en conséquence des droits d'accès aux fonctions et données et veiller à ce que le titulaire de la carte assume la responsabilité des activités auxquelles il se livre

— enregistrer les données d'activité du titulaire de la carte, les données d'événement et d'anomalie ainsi que les données d'activité de contrôle qui se rapportent au titulaire de la carte.

Par conséquent, une carte tachygraphique est conçue pour être utilisée en interaction avec le dispositif d'interface de carte d'une unité embarquée sur le véhicule. Elle doit également pouvoir s'employer avec tout lecteur de cartes (équipant, p. ex. un ordinateur individuel) pour autant que ce matériel jouisse de droits d'accès en lecture portant sur l'ensemble des données utilisateur.

Pendant la phase d'utilisation finale du cycle de vie d'une carte tachygraphique (phase 7 du cycle de vie aux termes du document de référence ES PP), seules les unités sur véhicule sont habilitées à enregistrer des données utilisateur sur la carte considérée.

▼**M1**

Les exigences fonctionnelles auxquelles doit satisfaire une carte tachygraphique sont spécifiées dans le corps de l'annexe I B et de l'appendice 2.

3.2. ***Cycle de vie d'une carte tachygraphique***

Le cycle de vie d'une carte tachygraphique est conforme au cycle de vie des cartes à puce décrit dans le document de référence ES PP.

3.3. ***Menaces***

Outre les menaces générales qui pèsent sur les cartes à puce, menaces répertoriées dans les documents de référence ES PP et IC PP, une carte tachygraphique risque également d'être confrontée aux menaces suivantes:

3.3.1. *Objectifs finaux*

L'objectif final des agresseurs sera de modifier les données utilisateur enregistrées au sein de la cible d'évaluation.

M.Données_Identification	L'apport de modifications aux données d'identification enregistrées au sein de la cible d'évaluation (portant p. ex. sur le type de carte, la date d'expiration de la carte ou les données d'identification du titulaire) autoriserait un usage frauduleux de la cible d'évaluation et représenterait une menace sérieuse pour l'objectif de sécurité global du système
M.Données_Activité	L'apport de modifications aux données d'activité enregistrées au sein de la cible d'évaluation représenterait une menace sérieuse pour la sécurité de cette dernière
M.Échange_Données	L'apport de modifications aux données d'activité (adjonction, suppression, modification) pendant leur importation ou leur exportation représenterait une menace sérieuse pour la sécurité de la cible d'évaluation.

3.3.2. *Voies de pénétration*

Les éléments constitutifs de la cible d'évaluation peuvent être attaqués de diverses manières:

— tentatives d'obtention illicite de données confidentielles concernant la conception des matériels et logiciels de la cible d'évaluation et ses fonctions ou données de sécurité en particulier. Pour obtenir ces informations illicites, les malfaiteurs sont susceptibles de s'en prendre directement au matériel développé par les concepteurs ou fabricants (vol, corruption, etc.) ou de procéder à un examen direct de la cible d'évaluation (sondages d'exploration, analyse d'inférence, etc.)

— exploitation des faiblesses éventuelles que pourrait présenter la conception ou la réalisation de la cible d'évaluation (exploitation des erreurs matérielles, erreurs logicielles, défauts de transmission, erreurs induites au sein de la cible d'évaluation par diverses agressions environnementales ou exploitation des faiblesses que pourraient présenter certaines fonctions de sécurité telles que les procédures d'authentification, le contrôle d'accès aux données, les opérations cryptographiques, etc.)

— apport de modifications à la cible d'évaluation ou à ses fonctions de sécurité par le biais d'agressions physiques, électriques ou logiques, qu'elles soient combinées ou non.

3.4. ***Objectifs de sécurité***

Le principal objectif de sécurité du système tachygraphique numérique dans son ensemble s'énonce comme suit:

O.Principal	Les données que les services de contrôle sont censés vérifier se doivent d'être disponibles et de refléter fidèlement et avec la précision requise les activités des conducteurs contrôlés et de leurs véhicules tant en ce qui concerne la vitesse du véhicule considéré que les périodes de conduite, de travail, de disponibilité et de repos.

Par conséquent, les principaux objectifs de la cible d'évaluation contribuant à cet objectif de sécurité global s'énoncent comme suit:

O.Don._Identif._Carte	La cible d'évaluation doit préserver les données d'identification de la carte et de son titulaire enre-

▼M1

	gistrées au cours du processus de personnalisation de la carte.
O.Enregis._Activité_Carte	La cible d'évaluation doit préserver les données enregistrées sur la carte par les unités sur véhicule.

3.5. ***Objectifs de sécurité informatique***

Outre les objectifs de sécurité généraux répertoriés dans les documents de référence ES PP et IC PP, les objectifs de sécurité informatique spécifiques de la cible d'évaluation qui contribuent à ses objectifs de sécurité globaux pendant la phase d'utilisation finale de son cycle de vie s'énoncent comme suit:

O.Accès_Données	La cible d'évaluation doit limiter aux unités sur véhicules authentifiées l'octroi de droits d'accès en écriture aux données utilisateur
O.Com._Sécurisées	La cible d'évaluation doit être capable de prendre en charge des procédures et protocoles de communication sécurisés entre la carte et le dispositif d'interface lorsque l'application l'impose.

3.6. ***Ressources matérielles, procédurales et en personnel***

Les documents de référence ES PP et IC PP répertorient les ressources matérielles, procédurales et en personnel qui contribuent à la sécurité de la cible d'évaluation (chapitres consacrés aux objectifs de sécurité en matière d'environnement).

4. **Fonctions dédiées à la sécurité**

Ce paragraphe traite de manière plus approfondie quelques-unes des opérations permises telles que l'affectation ou la sélection d'ES PP de référence et fournit des exigences fonctionnelles supplémentaires auxquelles doivent satisfaire les fonctions dédiées à la sécurité.

4.1. ***Conformité avec les profils de protection***

La cible d'évaluation devra satisfaire aux exigences énoncées dans le document de référence IC PP.

La cible d'évaluation devra satisfaire aux exigences énoncées dans le document de référence ES PP après avoir subi certaines améliorations ultérieures.

4.2. ***Identification et authentification de l'utilisateur***

La carte doit être à même d'identifier l'entité dans laquelle elle est introduite et de vérifier s'il s'agit ou non d'une unité embarquée sur le véhicule authentifiée. La carte est susceptible de procéder à l'exportation de données utilisateur quelle que soit l'entité à laquelle elle est raccordée, à l'exception de la carte de contrôle qui ne peut exporter de données d'identification du titulaire de la carte qu'à destination d'une unité embarquée sur le véhicule authentifiée (de telle sorte que le contrôleur concerné puisse avoir la certitude que l'unité embarquée sur le véhicule considérée n'est pas factice parce que les coordonnées de celle-ci apparaissent sur l'écran ou les tirages de contrôle).

4.2.1. *Identification de l'utilisateur*

Mission (FIA_UID.1.1) *Liste des actions modifiées avec modération par les fonctions de sécurité de la cible d'évaluation*: néant.

Mission (FIA_ATD.1.1) *Liste des attributs de sécurité*:

— GROUPE_UTILISATEUR: UNITÉ_VÉHICULE, UNITÉ_SANS_VÉHICULE,

— ID_UTILISATEUR: Numéro d'immatriculation du véhicule (NIV) et code de l'État membre dans lequel le véhicule est immatriculé (ID_UTILISATEUR connue uniquement du GROUPE_UTILISATEUR = UNITÉ_VÉHICULE).

4.2.2. *Authentification de l'utilisateur*

Mission (FIA_UAU.1.1) Liste des actions modifiées avec modération par les fonctions de sécurité de la cible d'évaluation:

— Cartes de conducteur et d'atelier: exportation des données utilisateur accompagnées des attributs de sécurité appropriés (fonction de téléchargement des données enregistrées sur la carte)

▼**M1**

— Carte de contrôle: exportation des données utilisateur sans attributs de sécurité, à l'exception des données d'identification du titulaire de la carte concernée.

La procédure d'authentification d'une unité embarquée sur le véhicule consistera à démontrer qu'elle détient des données de sécurité qui émanent obligatoirement du système considéré.

Sélection (FIA_UAU.3.1 et FIA_UAU.3.2): prévention.

Mission (FIA_UAU.4.1) *Mécanisme(s) d'authentification identifié(s)*: tout mécanisme d'authentification.

La carte d'atelier comportera un mécanisme d'authentification supplémentaire lui permettant de vérifier un numéro d'identification personnel (ce mécanisme permet à l'unité embarquée sur le véhicule de s'assurer de l'identité du détenteur de la carte; il n'est pas conçu pour protéger le contenu de la carte d'atelier).

4.2.3. *Échecs de la procédure d'authentification*

Les missions qui suivent décrivent la réaction d'une carte lors de tout échec de la procédure d'authentification d'un utilisateur.

Mission (FIA_AFL.1.1) *Numéro*: 1, *liste des événements d'authentification*: authentification d'un dispositif d'interface.

Mission (FIA_AFL.1.2) Liste des actions:

— avertir l'entité connectée

— considérer l'utilisateur comme une UNITÉ_SANS_VÉHICULE.

Les missions qui suivent décrivent la réaction d'une carte en cas d'échec du mécanisme d'authentification supplémentaire indiqué au point UIA_302.

Mission (FIA_AFL.1.1) *Numéro*: 5, *liste des événements d'authentification*: contrôles des numéros d'identification personnels (carte d'atelier).

Mission (FIA_AFL.1.2) Liste des actions:

— avertir l'entité connectée

— bloquer la procédure de contrôle du numéro d'identification individuel de telle sorte que toute tentative de vérification ultérieure échoue

— être à même d'indiquer aux utilisateurs ultérieurs la raison du blocage imposé.

4.3. ***Gestion des accès***

4.3.1. *Politique de contrôle des accès*

Pendant la phase d'utilisation finale de son cycle de vie, la carte tachygraphique n'est soumise qu'à une seule politique de contrôle d'accès découlant des fonctions dédiées à la sécurité (SFP) et portant le nom de AC_SFP.

Mission (FDP_ACC.2.1) *Contrôle des accès SFP*: AC_SFP.

4.3.2. *Fonctions de contrôle des accès*

Mission (FDP_ACF.1.1) *Contrôle des accès SFP*: AC_SFP.

Mission (FDP_ACF.1.1) *Groupe nommé d'attributs de sécurité*: GROUPE_UTILISATEUR.

Mission (FDP_ACF.1.2) *Règles régissant l'accès aux sujets et objets contrôlés par le biais d'opérations contrôlées*:

— LECTURE_GÉNÉRALE: Les données utilisateur peuvent être extraites de la cible d'évaluation par tout utilisateur, à l'exception des données d'identification du titulaire de la carte concernée dont la lecture sur les cartes de contrôle est réservée aux UNITÉS_VÉHICULE

— ÉCRITURE_IDENTIF: Les données d'identification ne peuvent être enregistrées qu'une seule fois et ce avant la fin de la phase 6 du cycle de vie de la carte. Aucun utilisateur n'est habilité à enregistrer ou modifier des données d'identification pendant la phase d'utilisation finale du cycle de vie de la carte considérée

— ÉCRITURE_ACTIVITÉ: Seules les UNITÉ_VÉHICULE sont habilitées à enregistrer des données d'activité au sein de la cible d'évaluation

— ACTU._LOGICIEL: Aucun utilisateur n'est habilité à procéder à une actualisation quelconque du logiciel de la cible d'évaluation

▼**M1**

— STRUCTURE_FICHIER: La structure des fichiers ainsi que les conditions d'accès seront définies avant la fin de la phase 6 du cycle de vie de la cible d'évaluation, puis verrouillées afin de décourager toute tentative de modification ou de suppression par un utilisateur quelconque

4.4. ***Responsabilité***

La cible d'évaluation sauvegardera dans sa mémoire des données d'identification permanentes.

L'heure et la date de personnalisation de la cible d'évaluation feront l'objet d'une indication qui se devra d'être inaltérable.

4.5. ***Analyse***

La cible d'évaluation doit surveiller les événements qui indiquent une atteinte potentielle à sa sécurité.

Mission (FAU_SAA.1.2) Sous-ensemble défini d'événements analysables:

— échec de la procédure d'authentification du titulaire de la carte (échec de 5 contrôles successifs du numéro d'identification personnel du titulaire)

— erreur d'essai automatique

— erreur d'intégrité des données enregistrées

— erreur d'intégrité relevée lors de l'entrée de données d'activité

4.6. ***Précision***

4.6.1. *Intégrité des données enregistrées*

Mission (FDP_SDI.2.2) *Actions à entreprendre*: avertir l'entité connectée

4.6.2. *Authentification des données de base*

Mission (FDP_DAU.1.1) *Liste des objets ou types d'information*: Données d'activité.

Mission (FDP_DAU.1.2) *Liste des sujets*: Tout sujet.

4.7. ***Fiabilité du service***

4.7.1. *Essais*

Sélection (FPT_TST.1.1): pendant la phase de mise en route initiale et régulièrement en cours d'exploitation normale.

Remarque: dans le cas présent, l'expression «pendant la phase de mise en route initiale» signifie avant l'exécution du code [et pas nécessairement pendant la procédure Answer To Reset (réponse à une réinitialisation)].

Les essais automatiques de la cible d'évaluation comporteront une vérification de l'intégrité de tout code logiciel non enregistré dans la mémoire morte.

En cas de détection d'une erreur d'essai automatique, la fonction de sécurité de la cible d'évaluation avertira l'entité connectée.

Aux termes des essais auxquels le système d'exploitation se doit d'être soumis, toutes les commandes et actions propres à leur exécution seront désactivées ou supprimées. Il ne sera possible ni de remplacer ni de rétablir ces commandes aux fins d'utilisation ultérieure. Les commandes exclusivement associées à une phase déterminée du cycle de vie demeureront inaccessibles pendant les autres phases de ce même cycle.

4.7.2. *Logiciel*

Le logiciel d'exploitation de la cible d'évaluation sera impossible à analyser, modifier ou dépanner sur site.

Les entrées provenant de sources externes ne seront en aucun cas acceptées comme des codes exécutables.

4.7.3. *Alimentation*

La cible d'évaluation se mettra dans un état de sécurisation satisfaisant pendant les coupures ou les variations d'alimentation.

▼M1

4.7.4. *Conditions de réinitialisation*

En cas de coupure d'alimentation (ou de variations de la tension d'alimentation) affectant la cible d'évaluation, en cas d'interruption d'une transaction avant terme ou de toute autre situation requérant sa réinitialisation, la cible d'évaluation se réinitialisera sans heurt.

4.8. ***Échange de données***

4.8.1. *Échange de données avec une unité embarquée sur le véhicule*

La cible d'évaluation procédera à une vérification de l'intégrité et de l'authenticité des données importées à partir d'une unité embarquée sur le véhicule.

En cas de détection d'un défaut d'intégrité des données importées, la cible d'évaluation devra:

— avertir l'entité émettrice

— s'abstenir d'utiliser les données concernées.

La cible d'évaluation exportera des données utilisateur vers l'unité embarquée sur le véhicule en les accompagnant des attributs de sécurité qui leur sont associés, de telle sorte que cette unité embarquée sur le véhicule soit en mesure de vérifier l'intégrité et l'authenticité des données qu'elle aura reçues.

4.8.2. *Exportation de données vers une unité indépendante (fonction de téléchargement)*

La cible d'évaluation sera en mesure de générer une preuve d'origine pour les données téléchargées vers des supports de mémoire externes.

La cible d'évaluation sera en mesure de fournir au destinataire le moyen de vérifier l'authenticité de la preuve d'origine des données téléchargées.

La cible d'évaluation sera en mesure de procéder au téléchargement de données vers des supports de mémoire externes en les accompagnant des attributs de sécurité qui leur sont associés, de telle sorte que le ou les supports concernés soient en mesure de vérifier l'intégrité des données téléchargées.

4.9. ***Soutien cryptographique***

Si la fonction de sécurité de la cible d'évaluation génère des clés cryptographiques, elle doit s'acquitter de cette tâche en conformité avec certains formats et algorithmes de génération de clés cryptographiques. Les clés de session cryptographiques générées se caractériseront par un nombre d'utilisations limité (à définir par le fabricant, ce nombre devant toutefois être inférieur à 240).

Si la fonction de sécurité de la cible d'évaluation distribue des clés cryptographiques, elle doit s'acquitter de cette tâche en conformité avec certaines méthodes de distribution des clés cryptographiques.

5. **Définition des mécanismes de sécurité**

Les mécanismes de sécurité requis font l'objet d'une description précise à l'appendice 11.

Les autres mécanismes de sécurité doivent être définis par le fabricant de la cible d'évaluation.

6. **Puissance minimale des mécanismes de sécurité**

La puissance minimale requise des mécanismes de sécurité conçus pour une carte tachygraphique est élevée, conformément aux critères définis dans le document de référence de l'ITSEC.

7. **Niveau de garantie**

Le niveau de garantie visé pour les cartes de tachygraphe correspond au niveau E3, conformément aux critères définis dans le document de référence de l'ITSEC.

8. **Analyse raisonnée**

Les matrices qui suivent présentent une analyse raisonnée des fonctions dédiées à la sécurité en mettant en évidence les éléments suivants:

— les FDS capables de neutraliser les diverses menaces

— les FDS qui remplissent les différents objectifs de sécurité informatique.

▼**M1**

	Menaces											Objectifs de sécurité informatique								
	T.CLON*	T.DIS_ES2	M.T_ES	M.T_CMD	T.MOD_SOFT*	T.MOD_LOAD	T.MOD_EXE	T.MOD_SHARE	M.Données_Identification	M.Données_Activité	M.Échange_Données	O.TAMPER_ES	O.CLON*	O.OPERATE*	O.FLAW*	O.DIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	O.Accès_Données	O.Communication_Sécurisée
UIA_301 Moyens d'authentification																			x	
UIA_302 Contrôles de PIN																			x	
ACT_301 Données d'identification																				
ACT_302 Date de personnalisation																				
RLB_301 Intégrité du logiciel												x		x						
RLB_302 Essais automatiques												x		x						
RLB_303 Essais en fabrication					x	x						x		x						
RLB_304 Analyse logicielle					x		x	x				x		x						
RLB_305 Entrée logicielle					x	x		x				x		x						
RLB_306 Alimentation									x	x		x		x						
RLB_307 Réinitialisation												x		x						
DEX_301 Importation de données sécurisées											x									x
DEX_302 Importation de données sécurisées											x									x

▼M1

	Menaces											Objectifs de sécurité informatique								
	T.CLON*	T.DIS_ES2	M.T_ES	M.T_CMD	T.MOD_SOFT*	T.MOD_LOAD	T.MOD_EXE	T.MOD_SHARE	M.Données_Identification	M.Données_Activité	M.Échange_Données	O.TAMPER_ES	O.CLON*	O.OPERATE*	O.FLAW*	O.DIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	O.Accès_Données	O.Communication_Sécurisée
DEX_303 Exportation de données sécurisées vers l'UEV											x									x
DEX_304 Preuve d'origine											x									x
DEX_305 Preuve d'origine											x									x
DEX_306 Exportation de données sécurisées vers des supports de mémoire externes											x									x
CSP_301 Génération de clés												x								x
CSP_302 Distribution de clés												x								x

▼**M1**

Appendice 11

MÉCANISMES DE SÉCURITÉ COMMUNS

TABLE DES MATIÈRES

▼**M1**

1. GÉNÉRALITÉS

Le présent appendice indique les mécanismes de sécurité garantissant:

— l'authentification mutuelle entre les UEV et les cartes tachygraphiques, y compris la concordance des clés de session;

— la confidentialité, l'intégrité et l'authentification des données transférées entre les UEV et les cartes tachygraphiques;

— l'intégrité et l'authentification des données téléchargées à partir des UEV sur des supports de mémoire externes;

— l'intégrité et l'authentification des données téléchargées à partir des cartes tachygraphiques sur des supports de mémoire externes.

1.1. **Références**

Le présent appendice fait référence aux documents suivants:

SHA-1	National Institute of Standards and Technology (NIST). FIPS Publication 180-1: Secure Hash Standard. Avril 1995
PKCS1	RSA Laboratories. PKCS # 1: RSA Encryption Standard. Version 2.0. Octobre 1998
TDES	National Institute of Standards and Technology (NIST). FIPS Publication 46-3: Data Encryption Standard. Projet de norme 1999
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998
ISO/CEI 7816-4	IT — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 4: commandes intersectorielles pour les échanges. Première édition: 1995 + Amendement 1: 1997
ISO/CEI 7816-6	IT — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 6: éléments de données intersectorielles. Première édition: 1996 + Cor 1: 1998
ISO/CEI 7816-8	IT — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 8: commandes intersectorielles de sécurité. Première édition: 1999
ISO/CEI 9796-2	IT — Techniques de sécurité — Schémas de signature numérique rétablissant le message — Partie 2: mécanismes utilisant une fonction de hachage. Première édition: 1997
ISO/CEI 9798-3	IT — Techniques de sécurité — Mécanismes d'authentification d'entité — Partie 3: authentification d'entité utilisant un algorithme à clé publique. Seconde édition: 1998
ISO 16844-3	Véhicules routiers — Systèmes tachygraphes — Partie 3: Interface de détection de mouvements

1.2. **Notations et abréviations**

Les notations et abréviations qui suivent apparaissent dans le présent appendice:

(K_a, K_b, K_c)	Faisceau de clés destiné au triple algorithme d'encryptage des données
CA	Organisme de certification
CAR	Références de l'organisme de certification
CC	Total de contrôle cryptographique
CG	Cryptogramme
CH	En-tête de commande
CHA	Autorisation d'un détenteur de certificat
CHR	Références d'un détenteur de certificat
D()	Décryptage avec DES (Data Encryption Standard)
DE	Élément de données
DO	Objet de données
d	Clé privée — Exposant privé RSA
e	Clé publique — Exposant public RSA
E()	Encryptage avec DES
EQT	Équipement
Hash()	Valeur de hachage, en tant que sortie de *Hash*
Hash	Fonction Hash

▼**M1**

KID	Identificateur de clé
Km	Clé TDES. Clé maîtresse définie dans ISO 16844-3.
Km_{VU}	Clé TDES insérée dans les unités embarqués sur le véhicule.
Km_{WC}	Clé TDES insérée dans les cartes d'ateliers
m	Représentant de message, nombre entier compris entre 0 et *n*−1
n	Clés RSA, modulo
PB	Octets de remplissage
PI	Octet indicateur de remplissage (employé dans les cryptogrammes destinés aux instructions DO de confidentialité)
PV	Valeur ordinaire
s	Représentant de signature, nombre entier compris entre 0 et *n*−1
SSC	Compteur de séquences d'émission
SM	Messagerie sécurisée
TCBC	Mode d'exploitation par chaînage de blocs de données chiffrées TDEA
TDEA	Triple algorithme d'encryptage des données
TLV	Longueur des marqueurs
VU	Unité sur véhicule
X.C	Certificat de l'utilisateur X, émis par un organisme de certification
X.CA	Organisme de certification de l'utilisateur X
$X.CA.PK_oX.C$	Opération de dévoilement d'un certificat pour en extraire une clé publique. Il s'agit d'un opérateur infixe dont l'opérande de gauche correspond à la clé publique d'un organisme de certification et l'opérande de droite au certificat émis par ce même organisme. Nous obtenons en résultat la clé publique de l'utilisateur X, dont le certificat est l'opérande de droite
X.PK	Clé publique RSA d'un utilisateur X
X.PK[I]	Encryptage RSA de certaines informations I, à l'aide de la clé publique de l'utilisateur X
X.SK	Clé privée RSA d'un utilisateur X
X.SK[I]	Encryptage RSA de certaines informations I, à l'aide de la clé privée de l'utilisateur X
′xx′	Valeur hexadécimale
||	Opérateur de concaténation.

2. SYSTÈMES ET ALGORITHMES CRYPTOGRAPHIQUES

2.1. **Systèmes cryptographiques**

Les unités sur véhicule et les cartes tachygraphiques auront recours à un système cryptographique classique à clé publique RSA pour assurer les mécanismes de sécurité suivants:

— Authentification mutuelle entre unités sur véhicule et cartes tachygraphiques

— Acheminement des clés triples de session DES (Data Encryption Standard) entre unités sur véhicule et cartes tachygraphiques

— Signature numérique des données téléchargées sur des supports externes à partir d'unités sur véhicule ou de cartes tachygraphiques.

Les unités sur véhicule et les cartes tachygraphiques auront recours à un système cryptographique symétrique DES triple pour assurer un mécanisme garantissant l'intégrité des données lors des échanges de données utilisateur entre les unités sur véhicule et les cartes tachygraphiques et pour assurer, le cas échéant, la confidentialité des échanges de données entre les unités sur véhicule et les cartes tachygraphiques.

▼M1

2.2. **Algorithmes cryptographiques**

2.2.1. ***Algorithme RSA***

L'algorithme RSA est parfaitement défini par les relations suivantes:

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

Pour une description plus détaillée de la fonction RSA, reportez-vous au document de référence PKCS1.

L'exposant public, e, pour les calculs de RSA sera différent de 2 dans toutes les clés générées avec RSA.

2.2.2. ***Algorithme de hachage***

Les mécanismes de signature numérique auront recours à l'algorithme de hachage SHA-1 tel qu'il est défini dans le document de référence SHA-1.

2.2.3. ***Algorithme d'encryptage des données***

Des algorithmes DES seront utilisés en mode chaînage de blocs de données chiffrées.

3. CLÉS ET CERTIFICATS

3.1. **Génération et distribution de clés**

3.1.1. ***Génération et distribution de clés RSA***

Des clés RSA seront générées à trois niveaux hiérarchiques fonctionnels:

— Niveau européen

— Niveau État membre

— Niveau équipement.

Au niveau européen, une seule paire de clés européenne (EUR.SK et EUR.PK) sera générée. La clé privée européenne permettra d'homologuer les clés publiques des États membres. Des enregistrements de l'ensemble des clés certifiées seront sauvegardés. Ces tâches seront exécutées par un organisme de certification européen, placé sous l'autorité et la responsabilité de la Commission européenne.

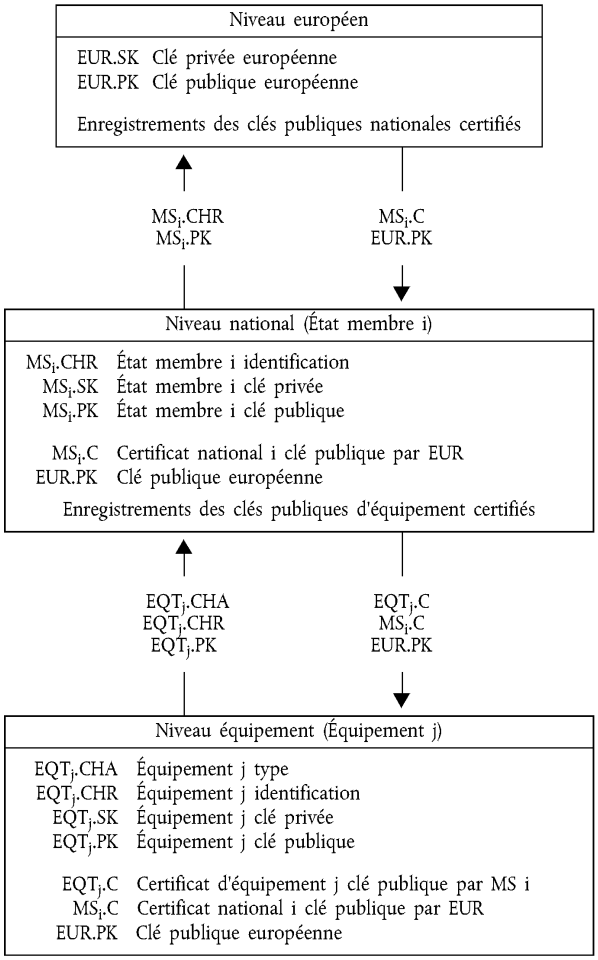
Au niveau État membre, une paire de clés par État membre (MS.SK et MS.PK) sera générée. Les clés publiques des États membres seront homologuées par l'organisme de certification européen. La clé privée de l'État membre permettra d'homologuer les clés publiques à introduire dans l'équipement (unité embarquée sur le véhicule ou carte tachygraphique). Des enregistrements de l'ensemble des clés publiques certifiées seront sauvegardés avec les données d'identification de l'équipement auquel elles sont destinées. Ces tâches seront exécutées par un organisme de certification national. Tout État membre est habilité à changer régulièrement de paire de clés.

Au niveau équipement, une seule paire de clés (EQT.SK et EQT.PK) sera générée et introduite dans chaque équipement. Les clés publiques d'équipement seront homologuées par un organisme de certification national. Ces tâches seront exécutées par les fabricants d'équipements, personnalisateurs d'équipement ou autorités compétentes à l'échelon national. Cette paire de clés sera utilisée par les services d'authentification, de signature numérique et d'encryptage

La confidentialité des clés privées doit être préservée durant leur génération, leur acheminement (éventuel) et leur archivage.

Le schéma fonctionnel qui suit représente une synthèse du cheminement des données caractérisant ce processus:

▼**M1**



3.1.2. ***Clés de contrôle RSA***

Aux fins d'essai des équipements (essais d'interopérabilité inclus), l'organisme de certification européen générera une paire de clés de contrôle européenne distincte et deux paires de clés de contrôle nationales au moins, dont les clés publiques seront homologuées conjointement avec la clé de contrôle privée européenne. Les fabricants introduiront, dans les équipements en cours de certification de type, des clés de test certifiées par l'une des clés de test nationales.

3.1.3. ***Clés du détecteur de mouvement***

La confidentialité des trois clés TDES décrites ci-après est protégée de manière appropriée au cours de la génération, du transport (le cas échéant) et du stockage.

Afin de permettre l'utilisation d'appareils de contrôles conformes à la norme ISO 16844, l'autorité de certification européenne et les autorités de certification de l'État membre veilleront également aux aspects suivants:

L'autorité de certification européenne génère les clés Km_{VU} et Km_{WC} deux clés triple DES uniques et indépendantes, ainsi que la clé Km selon la formule:

$$Km = Km_{VU} \text{ XOR } Km_{WC}$$

L'autorité de certification européenne transmet ces clés, selon les procédures sécurisées appropriées, aux autorités de certification des États membres qui en font la demande.

▼**M1**

Les autorités de certification des États membres:

— utilisent la clé Km pour crypter les données du détecteur de mouvement demandées par les fabricants des détecteurs de mouvement (les données à crypter avec la clé Km sont définies dans ISO 16844-3),

— transmettent la clé Km_{VU} aux fabricants d'unités embarquées sur le véhicule, selon les procédures sécurisées appropriées, afin qu'elles soient insérées dans les UEV,

— veillent à ce que la clé Km_{WC} soit insérée dans toutes les cartes d'atelier (SensorInstallationSecData dans le fichier élémentaire *Sensor_Installation_Data*) lors de la personnalisation de la carte.

3.1.4. ***Génération et distribution de clés de session T-DES***

Lors de leur processus d'authentification mutuelle, les unités sur véhicule et les cartes tachygraphiques généreront et échangeront les données nécessaires à l'élaboration d'une clé de session T-DES commune. La confidentialité de cet échange de données sera préservée par un mécanisme d'encryptage RSA.

Cette clé sera utilisée lors de toutes les opérations ultérieures, faisant appel à la messagerie sécurisée. Sa validité expirera à la fin de la session (retrait ou réinitialisation de la carte) et/ou après 240 usages (définition d'un usage de la clé: l'envoi d'une commande recourant à la messagerie sécurisée vers la carte appropriée et la réponse associée à cet envoi).

3.2. **Clés**

Les clés RSA auront (quel qu'en soit le niveau) les longueurs suivantes: modules *n* 1024 bits, exposant public *e* 64 bits maximum, exposant privé *d* 1024 bits.

Les clés T-DES prendront la forme (K_a, K_b, K_a), où K_a et K_b sont des clés indépendantes de 64 bits de long. Aucun bit de détection d'erreur de parité ne sera mis à 1.

3.3. **Certificats**

Les certificats associés aux clés publiques RSA seront du type «non self-descriptive» et «card verifiable» (Réf.: ISO/CEI 7816-8)

3.3.1. ***Contenu des certificats***

Les certificats associés aux clés publiques RSA comportent les données qui suivent dans l'ordre suivant:

Données	Format	Octets	Observations
CPI	ENTIER	1	Identificateur de profil du certificat (′01′ pour cette version)
CAR	CHAÎNE	8	Référence de l'organisme de certification
CHA	CHAÎNE OCTALE	7	Autorisation du détenteur de certificat
EOV	Temps réel	4	Expiration du certificat. Optionnel, ′FF′ complété par des octets de remplissage en cas d'inutilisation
CHR	CHAÎNE OCTALE	8	Référence du détenteur de certificat
n	CHAÎNE OCTALE	128	Clé publique (module)
e	CHAÎNE OCTALE	8	Clé publique (exposant public)
		164	

Remarques:

1. «L'Identificateur de profil du certificat» (CPI) détermine la structure précise d'un certificat d'authentification. Il fait office d'identificateur interne d'équipement au sein d'une liste en-tête appropriée qui décrit la concaténation des éléments d'information que comporte le certificat.

▼**M1**

La liste en-tête associée au contenu de ce certificat se présente comme suit:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Balise de liste en-tête étendue	Longueur de la liste en-tête	Balise CPI	Longueur CPI	Balise CAR	Longueur CAR	Balise CHA	Longueur CHA	Balise EOV	Longueur EOV	Balise CHR	Longueur CHR	Balise de clé publique (Construite)	Longueur des DO ultérieurs	Module	Longueur du module	Exposant public	Longueur de l'exposant public

2. Les «Références de l'organisme de certification» (CAR) permettent d'identifier l'OH émetteur du certificat de telle manière que l'élément d'information puisse faire simultanément office d'identificateur de clé d'autorité renvoyant à la clé publique de l'organisme de certification (pour plus d'informations concernant le codage, reportez-vous à l'Identificateur de clé ci-après).

3. «L'Autorisation du détenteur de certificat» (CHA) permet d'identifier les droits du détenteur de certificat. Elle se compose de l'ID d'application du tachygraphe et du type d'équipement auquel est destiné le certificat considéré (en fonction de l'élément d'information *EquipmentType*, «00» pour un État membre).

4. Les «Références du détenteur de certificat» (CHR) permettent d'identifier exclusivement le détenteur de certificat de telle manière que l'élément d'information puisse faire simultanément office d'identificateur de clé de sujet renvoyant à la clé publique du détenteur de certificat.

5. Les identificateurs de clé identifient uniquement les détenteurs de certificat ou les organismes de certification. Ils sont codés comme suit:

5.1. Équipement (UEV ou carte):

Données	Numéro de série de l'équipement	Date	Type	Fabricant
Longueur	4 octets	2 octets	1 octet	1 octet
Valeur	Entier	Codage DCB mm jj	Caractéristiques de fabrication	Code du fabricant

S'il s'agit d'une UEV, le fabricant est susceptible, lors de la demande de certificats, de connaître ou non les données d'identification de l'équipement au sein duquel les clés seront introduites.

Dans le premier cas de figure, le fabricant enverra les données d'identification de l'équipement accompagnées de la clé publique à l'organisme de certification national compétent. Le certificat contiendra alors les données d'identification de l'équipement concerné. Le fabricant devra veiller à ce que les clés et le certificat appropriés soient introduits dans l'équipement voulu. L'Identificateur de clé se présente sous la forme indiquée ci-avant.

Dans le second cas de figure, le fabricant doit identifier individuellement chaque demande de certificat et envoyer les données d'identification correspondantes accompagnées de la clé publique à l'organisme de certification national compétent. Le certificat contiendra alors les données d'identification de la demande de certificat concernée. Le fabricant doit communiquer en retour à l'organisme de certification national compétent les données d'affectation des clés à l'équipement concerné (c.-à-d., les données d'identification de la demande de certificat et d'identification de l'équipement visé) après leur installation sur cet équipement. L'Identificateur de clé se présente sous la forme indiquée ci-après:

▼**M1**

Données	Numéro de série de la demande de certificat	Date	Type	Fabricant
Longueur	4 octets	2 octets	1 octet	1 octet
Valeur	Codage DCB	Codage DCB mm jj	'FF'	Code du fabricant

5.2. Organisme de certification:

Données	Identification de l'organisme	Numéro de série de la clé	Informations complémentaires	Identificateur
Longueur	4 octets	1 octet	2 octets	1 octet
Valeur	1 octet code numérique nation 3 octets code alphanumérique nation	Entier	Codage supplémentaire (propre à l'OH) 'FF FF' en cas de non utilisation	'01'

Le numéro de série d'une clé permet de faire la distinction entre les différentes clés d'un État membre, en cas de changement de clé.

6. Les vérificateurs de certificat sauront implicitement que la clé publique certifiée est une clé RSA propre à l'authentification, à la vérification et à l'encryptage de signatures numériques aux fins de confidentialité (le certificat ne contient aucun Identificateur d'objet permettant de le préciser).

3.3.2. ***Certificats émis***

Le certificat émis se présente comme une signature numérique assortie d'une récupération partielle du contenu du certificat en conformité avec la norme ISO/CEI 9796-2, les «Références de l'organisme de certification» clôturant le certificat.

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, Hash(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

Contenu du certificat

$$= Cc = \underset{106 \text{ octets}}{C_r} \,||\, \underset{58 \text{ octets}}{C_n}$$

Remarques:

1. Ce certificat comporte 194 octets.

2. Les CAR, masquées par la signature, s'ajoutent également à cette dernière, afin que la clé publique de l'organisme de certification puisse être sélectionnée pour procéder à la vérification du certificat.

3. Le vérificateur du certificat connaîtra implicitement l'algorithme employé par l'organisme de certification pour signer le certificat.

▼**M1**

4. La liste en-tête associée à ce certificat émis se présente comme suit:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Balise de certificat CV (construite)	Longueur des DO ultérieurs	Balise de la signature	Longueur de la signature	Balise du reste	Longueur du reste	Balise CAR	Longueur CAR

3.3.3. ***Vérification et dévoilement des certificats***

La vérification et le dévoilement des certificats consistent à vérifier la signature conformément à la norme ISO/CEI 9796-2, à extraire le contenu du certificat et la clé publique qu'il contient: X.PK = X.CA.PK$_o$X.C, set à vérifier la validité du certificat.

Cette procédure comporte les opérations suivantes:

Vérification de la signature et extraction du contenu:

— À partir de X.C, extraire la Sign., C_n' et CAR′:

$$X.C = \underset{128\ \text{octets}}{\text{Sign}} \;||\; \underset{58\ \text{octets}}{C_n'} \;||\; \underset{8\ \text{octets}}{\text{CAR}'}$$

À partir de CAR′ sélectionner la clé publique de l'organisme de certification approprié (dans l'éventualité où cette opération n'aurait pas été exécutée par d'autres moyens).

— Ouvrir Sign. avec la clé publique de l'OH: Sr′ = X.CA.PK [Sign],

— S'assurer que le Sr′ commence par ′6A′ et prend fin avec ′BC′

— Calculer Cr′ et H′ à partir de:

$$Sr' = \text{'6A'} \;||\; \underset{106\ \text{octets}}{C_r'} \;||\; \underset{20\ \text{octets}}{H'} \;||\; \text{'BC'}$$

Récupérer le contenu du certificat C′ = C_r' || C_n',

— Vérifier le *Hachage* (C′) = H′

Si les vérifications sont concluantes, le certificat est un original et son contenu est C′.

Vérifier la validité. À partir de C′:

— Contrôler, le cas échéant, la date d'expiration

Extraire et mémoriser la clé publique, l'identificateur de clé, l'autorisation du détenteur de certificat et la date d'expiration du certificat à partir du certificat C′:

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MÉCANISME D'AUTHENTIFICATION MUTUELLE

L'authentification mutuelle entre cartes et UEV repose sur le principe suivant:

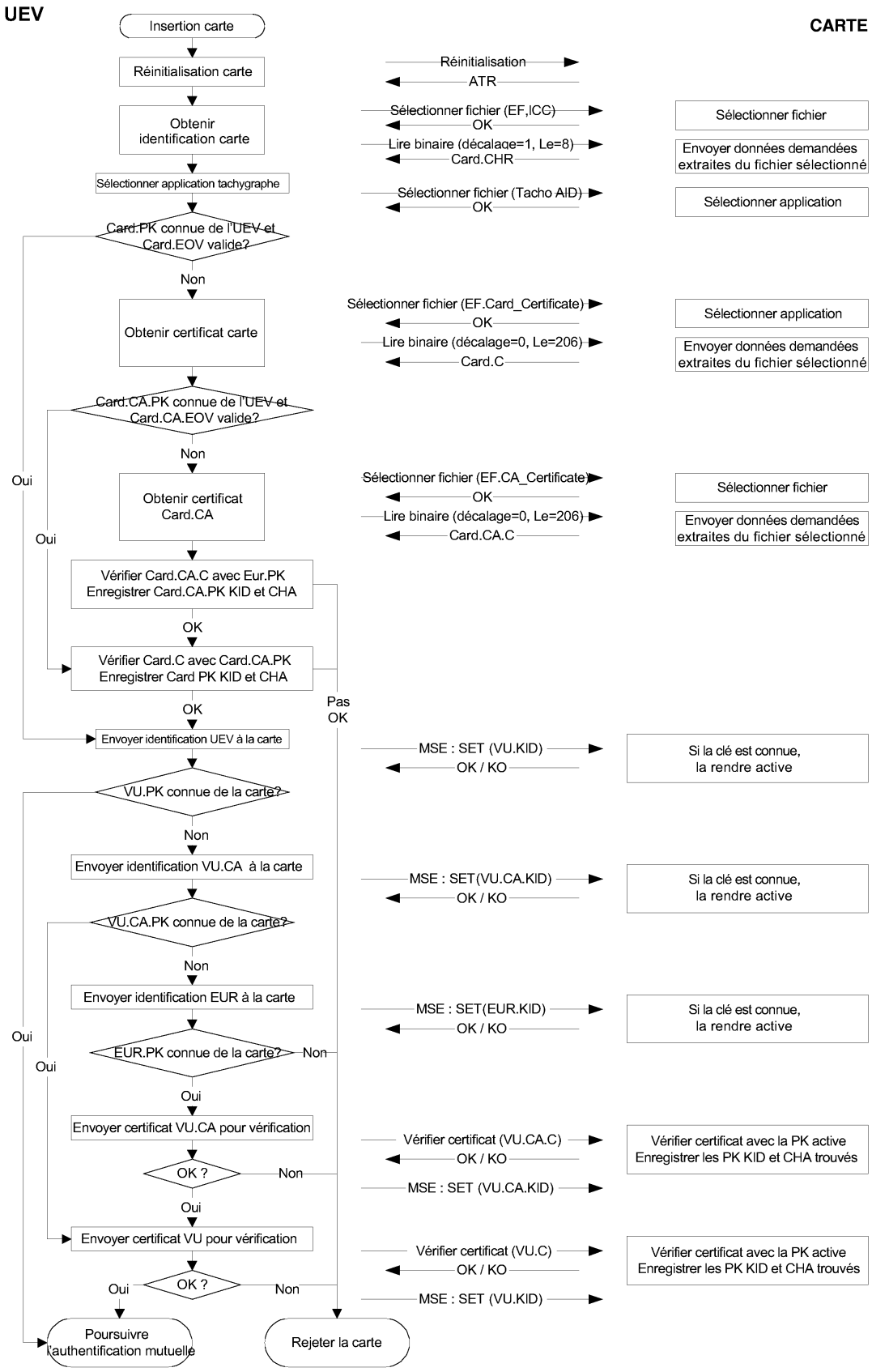
Chacune des parties doit démontrer à l'autre qu'elle possède une paire de clés valides, la clé publique qui aura permis leur homologation par l'organisme de certification national compétent étant elle-même homologuée par l'organisme de certification européen.

Cette démonstration consiste à signer avec la clé privée un nombre aléatoire envoyé par l'autre partie, laquelle doit récupérer, lors de la vérification de cette signature, le nombre aléatoire préalablement envoyé.

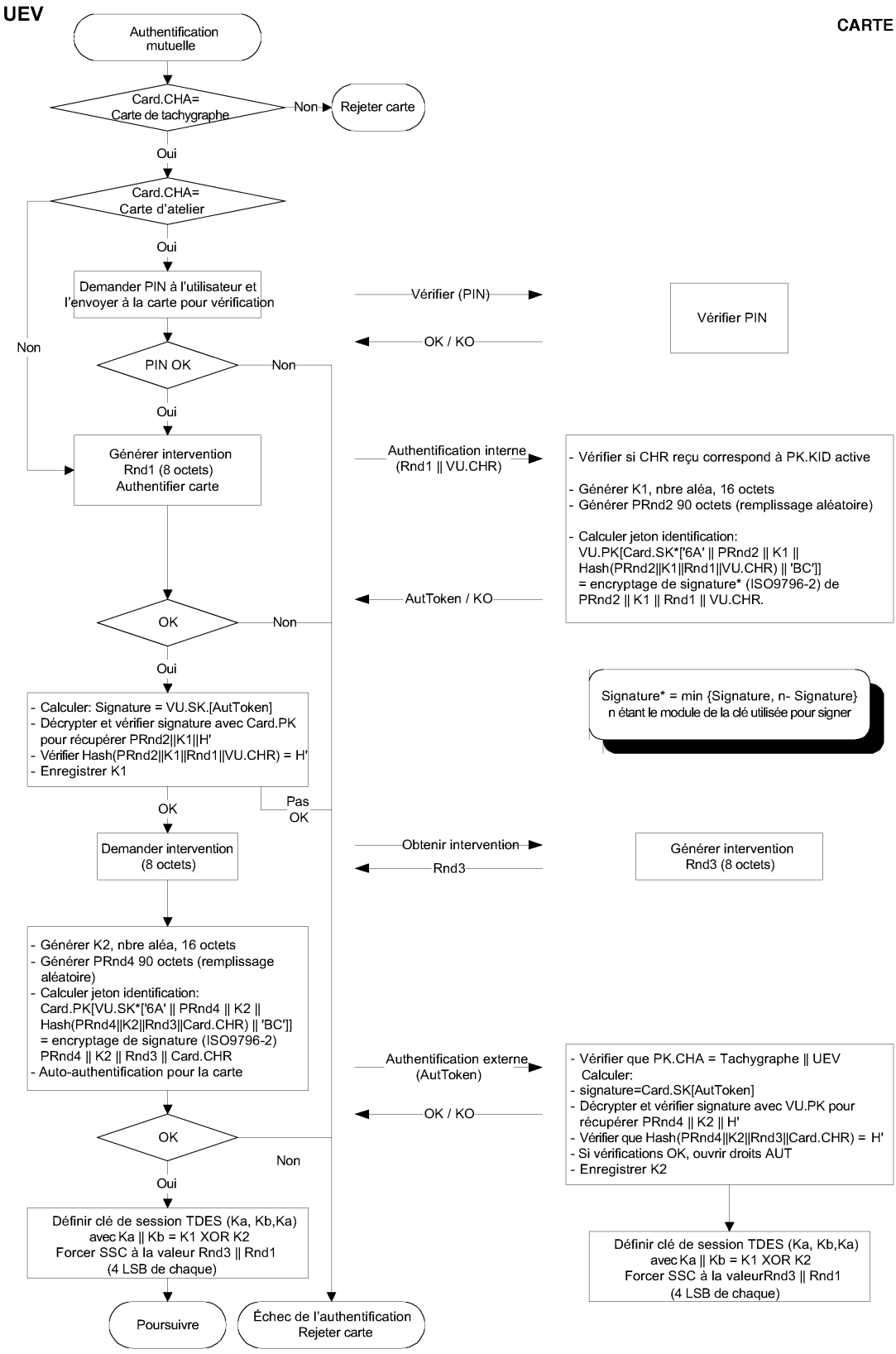
L'UEV concernée déclenche le mécanisme d'authentification dès l'insertion de la carte. La procédure commence par l'échange des certificats et le dévoilement des clés publiques ; elle prend fin avec la définition d'une clé de session.

▼**M1**

Le protocole ci-après sera utilisé [les flèches indiquent les commandes et données échangées (voir Appendice 2)]:



▼M1



5. CONFIDENTIALITÉ, INTÉGRITÉ ET MÉCANISMES D'AUTHENTIFICATION DES DONNÉES TRANSFÉRÉES ENTRE LES UEV ET LES CARTES

5.1. **Messagerie sécurisée**

L'intégrité des transferts de données entre les UEV et les cartes sera préservée par un dispositif de messagerie sécurisée, en conformité avec les normes de référence ISO/CEI 7816-4 et ISO/CEI 7816-8.

▼**M1**

Si la protection de données s'impose pendant leur transfert, le système adjoindra un objet données du type total de contrôle cryptographique aux objets données transmis dans la commande ou la réponse. Le récepteur procédera à une vérification du total de contrôle cryptographique.

Le total de contrôle cryptographique des données transmises dans une commande intégrera l'en-tête de cette commande ainsi que la totalité des objets données envoyés (= > CLA = ′0C′, et tous les objets données seront encapsulés dans des balises au sein desquelles b1=1).

Les octets d'état/information transmis en réponse seront protégés par un total de contrôle cryptographique si cette réponse ne comporte aucun champ de données.

Les totaux de contrôle cryptographiques mesureront 4 octets de long.

Par conséquent, en cas de recours à la messagerie sécurisée, les commandes et réponses présentent la structure suivante:

Les instructions DO utilisées représentent un jeu partiel des DO de messagerie sécurisée décrites dans les dispositions de la norme ISO/CEI 7816-4:

Balise	Mnémonique	Signification
′81′	T_{PV}	Valeur simple non codée en BER-TLV (à protéger par CC)
′97′	T_{LE}	Valeur de Le dans la commande non sécurisée (à protéger par CC)
′99′	T_{SW}	Infos d'état (à protéger par CC)
′8E′	T_{CC}	Total de contrôle cryptographique
′87′	$T_{PI\ CG}$	Octet indicateur de remplissage || Cryptogramme (valeur simple non codée en BER-TLV)

Étant donné une paire de réponses à une commande non sécurisée:

En-tête de commande (CH)	Corps de la commande
CLA INS P1 P2	[champ L_c] [champ de données] [champ L_e]
Quatre octets	Octets L, indiquant B_1 à B_L

Corps de la réponse	En-queue de réponse
[champ de données]	SW1 SW2
Octets de données L_r	Deux octets

La paire correspondante de réponses à une commande sécurisée se présente comme suit:

Commande sécurisée:

En-tête de commande (CH)	Corps de la commande										
CLA INS P1 P2	[nouveau champ L_c]	[nouveau champ de données]									[nouveau champ L_e]
′OC′	Longueur du nouveau champ de données	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	′00′
		′81′	L_c	Champ de données	′97′	′01′	L_e	′8E′	′04′	CC	

▼**M1**

Données à intégrer dans le total de contrôle = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = octets de remplissage (80 .. 00) en conformité avec les normes ISO-CEI 7816-4 et ISO 9797 méthode 2.

Les PV et LE des instructions DO ne sont présents que si la commande non sécurisée comporte un certain nombre de données correspondantes.

Réponse sécurisée:

1. Cas où le champ de données de la réponse n'est pas vide et ne nécessite aucune protection aux fins de confidentialité:

Corps de la réponse						En queue de réponse
[nouveau champ de données]						Nouveau SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
′81′	L_r	Champ de données	′8E′	′04′	CC	

Données à intégrer dans le total de contrôle = T_{PV} || L_{PV} || PV || PB

2. Cas où le champ de données de la réponse n'est pas vide mais nécessite une protection garantissant sa confidentialité:

Corps de la réponse						En queue de réponse
[nouveau champ de données]						Nouveau SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
′87′		PI || CG	′8E′	′04′	CC	

Données à acheminer par CG: données non codées en BER-TLV et octets de remplissage.

Données à intégrer dans le total de contrôle = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Cas où le champ de données de la réponse est vide:

Corps de la réponse						En queue de réponse
[nouveau champ de données]						Nouveau SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
′99′	′02′	Nouveau SW1 SW2	′8E′	′04′	CC	

Données à intégrer dans le total de contrôle = T_{SW} || L_{SW} || SW || PB

5.2. **Traitement des erreurs de messagerie sécurisée**

Si la carte tachygraphique reconnaît une erreur MS lors de l'interprétation d'une commande, les octets d'état doivent être renvoyés sans MS. Conformément à la norme ISO/CEI 7816-4, les octets d'état suivants sont définis pour indiquer la manifestation d'erreurs de MS:

′66 88′: Échec de la vérification du total de contrôle cryptographique

′69 87′: Absence d'objets données MS prévus

▼**M1**

′69 88′: Objets données MS incorrects.

Si la carte tachygraphique renvoie des octets d'état sans instructions DO MS ou avec une DO MS erronée, l'UEV doit mettre fin à la session en cours.

5.3. **Algorithme de calcul des totaux de contrôle cryptographiques**

La constitution des totaux de contrôle cryptographiques se fait à l'aide des contrôles d'accès au support (MAC) détaillés, en conformité avec la norme ANSI X9.19 du cryptage DES:

— Phase initiale: le bloc de contrôle y0 est E(Ka, SSC).

— Phase séquentielle: les blocs de contrôle y1, …, yn se calculent à l'aide de Ka.

— Phase finale: le total de contrôle cryptographique se calcule à partir du dernier bloc de contrôle yn en procédant comme suit: E[Ka, D(Kb, yn)],

Où l'abréviation E() signifie encryptage avec DES et l'abréviation D() décryptage avec DES.

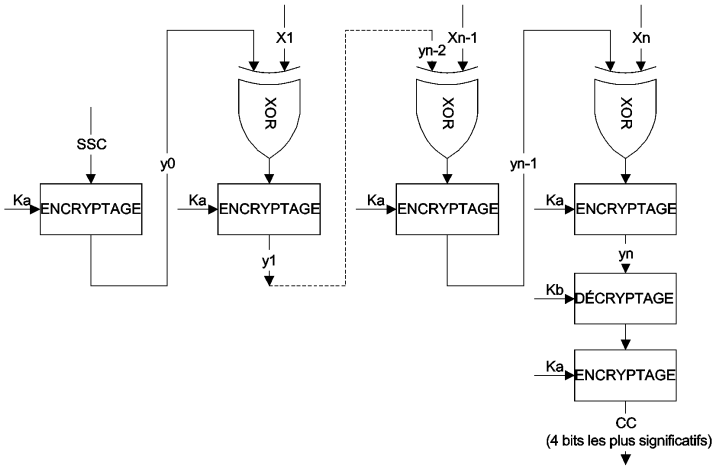
Les quatre octets les plus significatifs du total de contrôle cryptographique sont transférés.

Le compteur de séquences à l'émission (SSC) sera lancé pendant la procédure d'acceptation des clés:

SSC initial: Rnd3 (4 octets les moins significatifs) || Rnd1 (4 octets les moins significatifs).

Le compteur de séquences à l'émission sera incrémenté d'une unité avant le calcul de chaque MAC (en d'autres termes, le SSC associé à la première commande correspond au SSC initial + 1, tandis que le SSC associé à la première réponse correspond au SSC initial + 2).

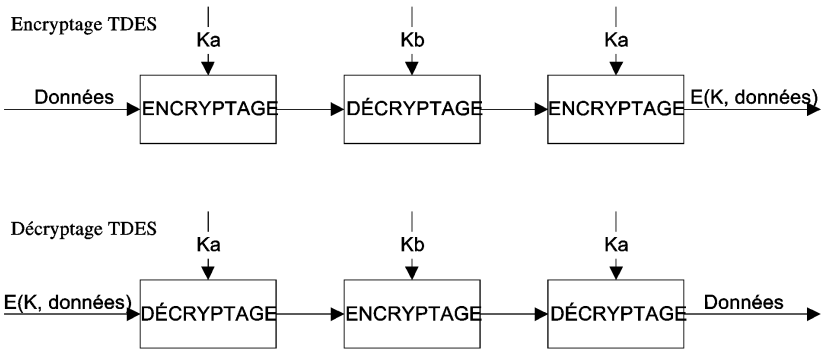
La figure ci-après illustre le calcul du MAC détaillé:



5.4. **Algorithme de calcul des cryptogrammes destinés aux instructions DO de confidentialité**

Ces cryptogrammes se calculent à l'aide du TDEA en mode d'exploitation TCBC, en conformité avec les TDES et TDES-OP de référence et avec le vecteur nul comme bloc de valeur initial.

La figure qui suit illustre l'application des clés en TDES:



▼**M1**

6. MÉCANISMES DE SIGNATURE NUMÉRIQUE DES TÉLÉCHARGEMENTS DE DONNÉES

L'équipement spécialisé intelligent (IDE) enregistre au sein d'un fichier de données physiques les données transmises à partir d'un équipement (UEV ou carte) donné, pendant une session de téléchargement. Ce fichier doit contenir les certificats MS_i.C et EQT.C. Le fichier contient les signatures numériques associées de blocs de données conformément aux indications fournies dans l'appendice 7 (Protocoles de téléchargement des données).

Les signatures numériques des données téléchargées reposeront sur l'utilisation d'un schéma de signature numérique avec appendice permettant, le cas échéant, de lire des données téléchargées sans aucun décryptage.

6.1. **Génération de signatures**

La génération de signatures de données par l'équipement respectera le schéma de signature avec appendice, défini dans le document de référence PKCS1 avec la fonction de hachage SHA-1:

Signature = EQT.SK[′00′ || ′01′ || *PS* || ′00′ || DER[SHA-1(donnéesData)]

PS = Chaîne d'octets de remplissage de valeur ′FF′ dont la longueur équivaut à 128.

DER(SHA-1(*M*)) correspond à l'encodage de l'ID de l'algorithme pour la fonction de hachage et la valeur de hachage, dans une valeur ASN.1 de type *DigestInfo* (règles d'encodage distinctes):

′30′||′21′||′30′||′09′||′06′||′05′||′2B′||′0E′||′03′||′02′||′1A′||′05′||′00′||′04′||′14′|| valeur de hachage.

6.2. **Vérification de signatures**

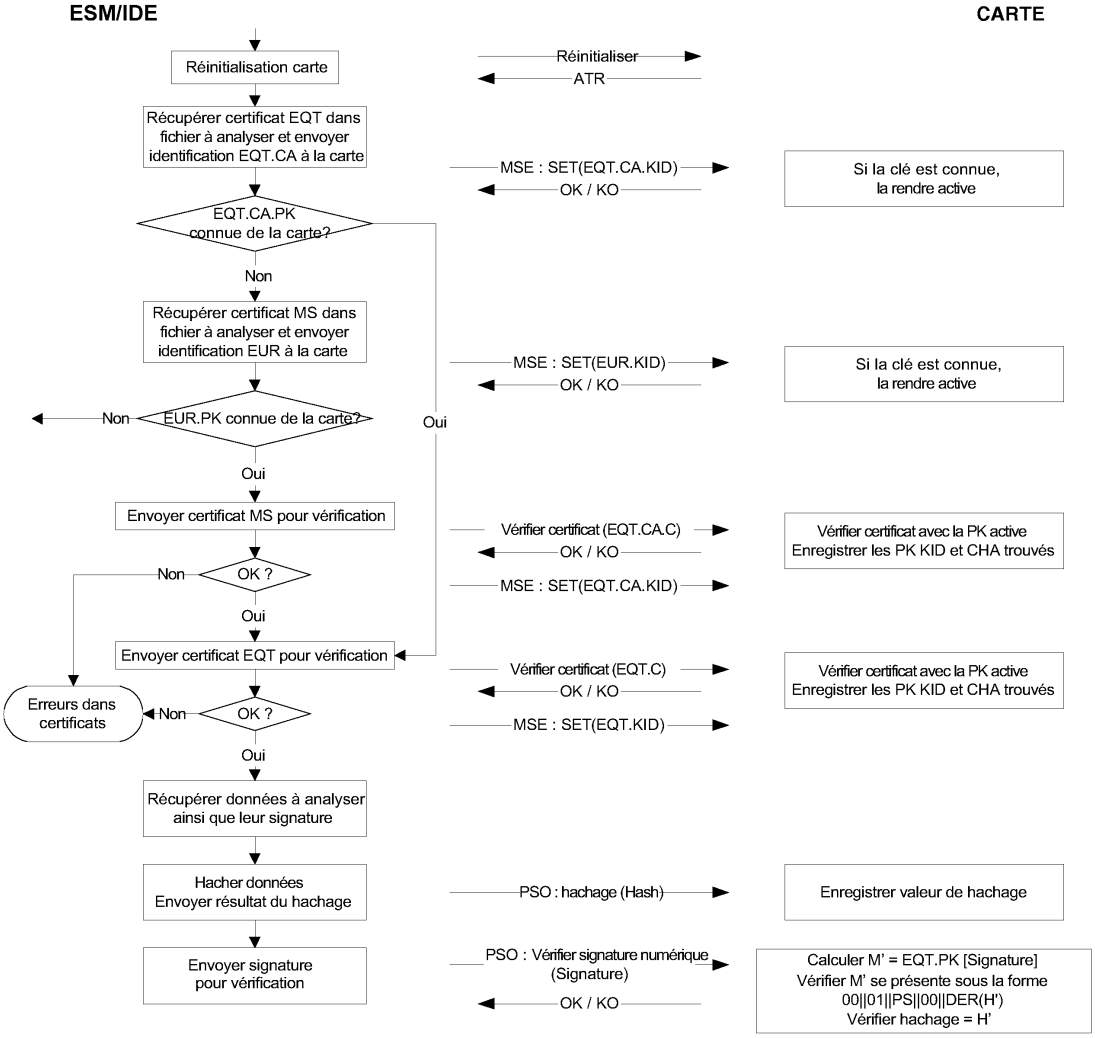
La vérification de signatures de données, à laquelle sont soumises les données téléchargées, respectera le schéma de signature avec appendice, défini dans le document de référence PKCS1 avec la fonction de hachage SHA-1.

Le vérificateur doit connaître (et approuver) la clé publique européenne EUR.PK.

Le tableau qui suit illustre le protocole qu'un équipement IDE doté d'une carte de contrôle est susceptible de respecter pour vérifier l'intégrité des données téléchargées et enregistrées sur l'ESM (support de mémoire externe). La carte de contrôle permet de procéder au décryptage des signatures numériques. Dans le cas présent, cette fonction n'est pas nécessairement implémentée au sein de l'IDE.

L'équipement qui a participé au téléchargement et à la signature des données à analyser est désigné par l'abréviation EQT.»

▼**M1**


ESM/IDE
CARTE
Réinitialisation carte
Réinitialiser
ATR
Récupérer certificat EQT dans fichier à analyser et envoyer identification EQT.CA à la carte
MSE : SET(EQT.CA.KID)
OK / KO
Si la clé est connue, la rendre active
EQT.CA.PK connue de la carte?
Non
Oui
Récupérer certificat MS dans fichier à analyser et envoyer identification EUR à la carte
MSE : SET(EUR.KID)
OK / KO
Si la clé est connue, la rendre active
EUR.PK connue de la carte?
Non
Oui
Envoyer certificat MS pour vérification
Vérifier certificat (EQT.CA.C)
OK / KO
Vérifier certificat avec la PK active
Enregistrer les PK KID et CHA trouvés
OK ?
Non
MSE : SET(EQT.CA.KID)
Oui
Envoyer certificat EQT pour vérification
Vérifier certificat (EQT.C)
OK / KO
Vérifier certificat avec la PK active
Enregistrer les PK KID et CHA trouvés
Erreurs dans certificats
OK ?
Non
MSE : SET(EQT.KID)
Oui
Récupérer données à analyser ainsi que leur signature
Hacher données
Envoyer résultat du hachage
PSO : hachage (Hash)
Enregistrer valeur de hachage
Envoyer signature pour vérification
PSO : Vérifier signature numérique (Signature)
OK / KO
Calculer M' = EQT.PK [Signature]
Vérifier M' se présente sous la forme 00||01||PS||00||DER(H')
Vérifier hachage = H'