

II

(Niet-wetgevingshandelingen)

VERORDENINGEN

UITVOERINGSVERORDENING (EU) 2018/502 VAN DE COMMISSIE

van 28 februari 2018

tot wijziging van Uitvoeringsverordening (EU) 2016/799 tot vaststelling van de eisen voor de constructie, het testen, de installatie, de exploitatie en de reparatie van tachografen en tachograafonderdelen**(Voor de EER relevante tekst)**

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) nr. 165/2014 van het Europees Parlement en de Raad van 4 februari 2014 betreffende tachografen in het wegvervoer ⁽¹⁾, en met name artikel 11 en artikel 12, lid 7,

Overwegende hetgeen volgt:

- (1) Bij Verordening (EU) nr. 165/2014 zijn de slimme tachografen ingevoerd: een tweede generatie digitale tachografen die beschikken over een verbinding met het mondiaal satellitnavigatiesysteem (GNSS), een communicatiesysteem voor vroegtijdige detectie op afstand en een facultatieve interface met intelligente vervoerssystemen.
- (2) De technische eisen voor de constructie, het testen, de installatie, de exploitatie en de reparatie van tachografen en tachograafonderdelen zijn uiteengezet in Verordening (EU) 2016/799 van de Commissie ⁽²⁾.
- (3) Overeenkomstig de artikelen 8, 9 en 10 van Verordening (EU) nr. 165/2014 moeten tachografen die worden geïnstalleerd in voertuigen die op of na 15 juni 2019 voor het eerst worden ingeschreven, slimme tachografen zijn. Uitvoeringsverordening (EU) 2016/799 moet daarom zodanig worden gewijzigd dat de technische bepalingen ervan met ingang van die datum van toepassing zijn.
- (4) Teneinde te voldoen aan artikel 8 van Verordening (EU) nr. 165/2014, waarin is bepaald dat de positie van het voertuig om de drie uur cumulatieve rijtijd moet worden geregistreerd, moet Uitvoeringsverordening (EU) 2016/799 zodanig worden gewijzigd dat informatie over de positie van het voertuig om de drie uur kan worden opgeslagen aan de hand van een meeteenheid die niet kan worden gereset en die, om verwarring met „ononderbroken rijtijd” te voorkomen, een meeteenheid met een verschillende functie is.
- (5) De voertuigunit mag bestaan uit één unit of uit meerdere units die zich op verschillende plaatsen in het voertuig bevinden. Het GNSS en de specifieke voorzieningen voor korteafstandscommunicatie kunnen zich dus binnen of buiten de hoofdbehuizing van de voertuigunit bevinden. Als ze zich erbuiten bevinden, moet het mogelijk zijn een typegoedkeuring af te geven voor beide voorzieningen en de hoofdbehuizing van de voertuigunit als afzonderlijke onderdelen, teneinde het typegoedkeuringsproces voor de slimme tachograaf aan te passen aan de behoeften van de markt.
- (6) De regels inzake de opslag van tijdsoverlappingsen en tijdsafstellingen moeten worden gewijzigd teneinde een onderscheid te maken tussen de automatische tijdsafstellingen die het gevolg zijn van een mogelijke poging tot manipulatie of een storing van de tachograaf en de tijdsafstellingen die het gevolg zijn van andere redenen, zoals onderhoud.
- (7) De gegevensidentificatoren moeten een onderscheid kunnen maken tussen gegevens die zijn gedownload van een slimme tachograaf en gegevens die zijn gedownload van een tachograaf van een vorige generatie.

⁽¹⁾ PB L 60 van 28.2.2014, blz. 1.

⁽²⁾ Uitvoeringsverordening (EU) 2016/799 van de Commissie van 18 maart 2016 tot uitvoering van Verordening (EU) nr. 165/2014 van het Europees Parlement en de Raad tot vaststelling van de eisen voor de constructie, het testen, de installatie, de exploitatie en de reparatie van tachografen en tachograafonderdelen (PB L 139 van 26.5.2016, blz. 1).

- (8) De geldigheidsduur van de bedrijfskaart moet worden verlengd van twee tot vijf jaar, zodat ze overeenstemt met de geldigheidsduur van de bestuurderskaart.
- (9) De beschrijving van bepaalde fouten en voorvallen, de validering van de invoering van plaatsen waar de dagelijkse werkperiode begint en/of eindigt, de instemming van de bestuurder voor het gebruik van de interface met intelligente vervoerssystemen voor wat gegevens betreft die door de voertuigunit via het voertuignetwerk zijn verzonden en andere technische kwesties moeten beter worden gedefinieerd.
- (10) Om te garanderen dat de certificering van de tachograafzegels up-to-date is, moeten ze worden aangepast aan de nieuwe norm inzake de beveiliging van mechanische zegels die voor tachografen worden gebruikt.
- (11) De Verordening heeft betrekking op de constructie, het testen, de installatie en de werking van systemen die ook radioapparatuur bevatten die geregeld is bij Richtlijn 2014/53/EU van het Europees Parlement en de Raad ⁽¹⁾. Deze richtlijn regelt het op de markt brengen en in gebruik nemen van elektronische en elektrische apparatuur die gebruikmaakt van radiogolven voor communicatie en/of radiodeterminatie op horizontaal niveau, waarbij bijzondere aandacht wordt besteed aan elektrische veiligheid, verenigbaarheid met andere systemen, toegang tot het radiospectrum, toegang tot noodhulpdiensten en ze bevat een aantal aanvullende gedelegeerde bepalingen. Om het efficiënte gebruik van het radiospectrum te garanderen, schadelijke radiostoringen te voorkomen, de veiligheid en de elektromagnetische compatibiliteit van de radioapparatuur te garanderen en andere specifieke gedelegeerde eisen mogelijk te maken, laat de onderhavige verordening deze richtlijn onverlet.
- (12) Uitvoeringsverordening (EU) 2016/799 moet derhalve worden gewijzigd.
- (13) De maatregelen van deze verordening zijn in overeenstemming met het advies van het in artikel 42, lid 3, van Verordening (EU) nr. 165/2014 bedoelde comité,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Uitvoeringsverordening (EU) 2016/799 wordt als volgt gewijzigd:

1) Artikel 1 wordt als volgt gewijzigd:

a) de tweede en de derde alinea worden vervangen door:

„2. Bij de constructie, het testen, de installatie, de inspectie, de exploitatie en de reparatie van slimme tachografen en hun onderdelen moeten de in bijlage IC bij deze verordening vastgestelde technische eisen in acht worden genomen.

3. Voor de constructie, het testen, de installatie, de inspectie, de exploitatie en de reparatie van andere tachografen dan slimme tachografen blijven de eisen van bijlage I van Verordening (EU) nr. 165/2014 of bijlage IB bij Verordening (EEG) nr. 3821/85 van de Raad ^(*) van toepassing;

^(*) Verordening (EEG) nr. 3821/85 van de Raad van 20 december 1985 betreffende het controleapparaat in het wegvervoer (PB L 370 van 31.12.1985, blz. 8)."

b) het volgende lid 5 wordt toegevoegd:

„5. Deze verordening doet geen afbreuk aan de toepassing van Richtlijn 2014/53/EU van het Europees Parlement en de Raad ^(*).

^(*) Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG (PB L 153 van 22.5.2014, blz. 62)."

2) Artikel 2 wordt als volgt gewijzigd:

a) definitie 3) wordt vervangen door:

„3) „informatiebrochure”: de volledige papieren of elektronische brochure met alle informatie die door de fabrikant of zijn gemachtigde is meegedeeld aan de typegoedkeuringsinstantie met het oog op de typegoedkeuring van een tachograaf of tachograafonderdeel, met inbegrip van de certificaten als bedoeld in artikel 12, lid 3, van Verordening (EU) nr. 165/2014, de uitvoering van de in bijlage IC bij deze verordening gedefinieerde testen, alsmede schema's, afbeeldingen en andere documenten;”;

⁽¹⁾ Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG (PB L 153 van 22.5.2014, blz. 62).

b) definitie 7) wordt vervangen door:

„7) „slimme tachograaf” of „tachograaf van de tweede generatie”: een digitale tachograaf die voldoet aan de artikelen 8, 9 en 10 van Verordening (EU) nr. 165/2014 en aan bijlage IC bij deze verordening;”;

c) definitie 8) wordt vervangen door:

„8) „tachograafonderdeel”: een van de volgende elementen: de voertuigunit, de bewegingssensor, het registratieblad, het externe GNSS-systeem en het externe systeem voor vroegtijdige detectie op afstand;”;

d) de volgende definitie 10) wordt toegevoegd:

„10) „voertuigunit”: de tachograaf, met uitzondering van de bewegingsopnemer en de kabels waarmee de bewegingsopnemer is aangesloten.

Het kan gaan om één unit of om meerdere units die zich op verschillende plaatsen in het voertuig bevinden, en omvat een verwerkingseenheid, een geheugen, een tijdsmetingsfunctie, twee smartcard-interfaces voor de bestuurder en bijrijder, een printer, een display, connectoren en voorzieningen voor de invoer van de gebruikersgegevens, een GNSS-ontvanger en een systeem voor communicatie op afstand.

De voertuigunit kan uit de volgende onderdelen bestaan, voor zover deze over een typegoedkeuring beschikken:

- voertuigunit, als afzonderlijk onderdeel (met inbegrip van een GNSS-ontvanger en een systeem voor communicatie op afstand),
- hoofdbehuizing van de voertuigunit (met inbegrip van een systeem voor communicatie op afstand), en een externe GNSS-module,
- hoofdbehuizing van de voertuigunit (met inbegrip van een GNSS-ontvanger), en een extern systeem voor communicatie op afstand,
- hoofdbehuizing van de voertuigunit, extern GNSS-systeem, en extern systeem voor communicatie op afstand.

Als de voertuigunit is samengesteld uit meerdere in het voertuig verspreide units, moeten de verwerkingseenheid, het geheugen en de tijdsmetingsfunctie zich in de hoofdbehuizing bevinden.

„voertuigunit (VU)” wordt gebruikt voor voertuigunit” of „hoofdbehuizing van de voertuigunit”.

3) De derde alinea van artikel 6 wordt vervangen door:

„Bijlage IC is evenwel van toepassing met ingang van 15 juni 2019, met uitzondering van aanhangsel 16, dat met ingang van 2 maart 2016 van toepassing is.”.

4) Bijlage IC wordt gewijzigd overeenkomstig bijlage I bij deze verordening.

5) Bijlage II wordt gewijzigd overeenkomstig bijlage II bij deze verordening.

Artikel 2

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 28 februari 2018.

Voor de Commissie
De voorzitter
Jean-Claude JUNCKER

BIJLAGE I

Bijlage IC bij Verordening (EU) 2016/799 wordt als volgt gewijzigd:

1) De inhoudsopgave wordt als volgt gewijzigd:

a) punt 3.12.5 wordt vervangen door:

„3.12.5 Plaatsen en posities waar de dagelijkse werktijd begint, eindigt en/of waar een cumulatieve rijtijd van 3 uur wordt bereikt”;

b) punt 4.5.3.2.16 wordt vervangen door:

„4.5.3.2.16 Plaats en tijdstip cumulatieve rijtijd van drie uur”;

c) punt 4.5.4.2.14 wordt vervangen door:

„4.5.4.2.14 Plaats en tijdstip cumulatieve rijtijd van drie uur”;

d) punt 6.2 wordt vervangen door:

„6.2 Controle van nieuwe of herstelde onderdelen”.

2) Punt 1 wordt als volgt gewijzigd:

a) definitie ll) wordt vervangen door:

„ll) „systeem voor communicatie op afstand” of „systeem voor vroegtijdige detectie”:

de uitrusting van de voertuigunit die wordt gebruikt voor de uitvoering van gerichte wegcontroles;”;

b) definitie tt) wordt vervangen door:

„tt) „tijdsafstelling”:

een afstelling van de lopende tijd; deze afstelling kan automatische gebeuren met geregelde tussenpozen, waarbij de door de GNSS-ontvanger verstrekte tijd als referentie wordt gebruikt, of kan tijdens een kalibrering worden uitgevoerd;”;

c) het eerste streepje van definitie yy) wordt vervangen door:

„— alleen in voertuigen van het type M1 en N1 wordt geïnstalleerd en gebruikt (als gedefinieerd in bijlage II bij Richtlijn 2007/46/EG van het Europees Parlement en de Raad (*), als laatstelijk gewijzigd);”;

d) een nieuwe definitie fff) wordt toegevoegd:

„fff) „cumulatieve rijtijd”:

een waarde die overeenkomt met het totale gecumuleerde aantal minuten dat met een bepaald voertuig is gereden.

De cumulatieve rijtijd is een optelling van alle minuten die als RIJDEN worden beschouwd door de functie bewaken van de rijactiviteiten van het controleapparaat, en wordt alleen gebruikt om het startsein te geven voor de registratie van de positie van het voertuig telkens wanneer een veelvoud van drie uur cumulatieve rijtijd wordt bereikt. De optelling gaat van start op het ogenblik dat het controleapparaat wordt geactiveerd. Ze wordt niet beïnvloed door een andere toestand, zoals „niet verplicht” of „vervoer per veerboot/trein”.

De waarde van de cumulatieve rijtijd is niet bestemd om te worden getoond, geprint of gedownload;”.

3) In punt 2.3 wordt het laatste streepje van punt 13) vervangen door:

„— De normale operationele geldigheidsperiode bedraagt 15 jaar, beginnend op de ingangsdatum van de VU-certificaten; na die periode kunnen ze nog 3 maanden worden gebruikt, maar alleen om gegevens te downloaden.”.

4) In punt 2.4 wordt de eerste alinea vervangen door:

„De systeembeveiliging beoogt het geheugen zodanig te beveiligen dat niet-geautoriseerde toegang tot en manipulatie van de gegevens wordt voorkomen en dat pogingen daartoe worden ontdekt, alsmede ter beveiliging van de integriteit en authenticiteit van de tussen de bewegingssensor en de voertuigunit uitgewisselde gegevens, van de integriteit en authenticiteit van de tussen het controleapparaat en de tachograafkaart uitgewisselde gegevens, van de integriteit en authenticiteit van de tussen de voertuigunit en de eventuele externe GNSS-module uitgewisselde gegevens, van de vertrouwelijkheid, integriteit en authenticiteit van de via vroegtijdige detectie op afstand uitgewisselde gegevens en ter verificatie van gedownloade gegevens.”.

5) In punt 3.2 wordt het tweede streepje van punt 27) vervangen door:

„— de posities waar de cumulatieve rijtijd een veelvoud van drie uur bereikt;”.

6) In punt 3.4 wordt punt 49) vervangen door:

„49) Er wordt van uitgegaan dat de eerste verandering van activiteit naar ONDERBREKING/RUST of BESCHIKBAARHEID die zich binnen 120 seconden na de automatische verandering naar WERK als gevolg van het stoppen van het voertuig voordoet, heeft plaatsgevonden op het moment waarop het voertuig stopt (waardoor de verandering naar WERK eventueel kan worden geannuleerd).”.

7) In punt 3.6.1 wordt punt 59) vervangen door:

„59) Daarna voert de bestuurder de huidige plaats van het voertuig in, die als een tijdelijke invoer wordt beschouwd.

In de volgende omstandigheden wordt de tijdelijke invoer die plaatsvond bij de laatste kaartuitneming gevalideerd (d.w.z. niet meer overschreven):

- invoer van een plaats waar de lopende dagelijkse werkperiode begint tijdens manuele invoer overeenkomstig voorschrift 61);
- de volgende invoer van een plaats waar de lopende dagelijkse werkperiode begint als de kaarthouder tijdens de manuele invoer overeenkomstig voorschrift 61) niet invoert op welke plaats de werkperiode begint of eindigt.

In de volgende omstandigheden wordt de tijdelijke invoer die plaatsvond bij de laatste kaartuitneming overschreven en wordt de nieuwe waarde gevalideerd:

- de volgende invoer van een plaats waar de lopende dagelijkse werkperiode eindigt als de kaarthouder tijdens de manuele invoer overeenkomstig voorschrift 61) niet invoert op welke plaats de werkperiode begint of eindigt”.

8) In punt 3.6.2 worden het vijfde en zesde streepje vervangen door:

- „— een plaats waar een vorige dagelijkse werkperiode is geëindigd, alsook de relevante tijd (waarbij de invoer tijdens de laatste kaartuitneming wordt overschreven en dus gevalideerd),
- een plaats waar de lopende dagelijkse werkperiode begint, alsook de relevante tijd (waarbij dus de tijdelijke invoer die plaatsvond bij de laatste kaartuitneming wordt gevalideerd).”.

9) Punt 3.9.15 wordt vervangen door:

„3.9.15 „Tijdsoverlapping”

86) Dit voorval treedt op wanneer een VU **die zich niet in de kalibreringsmodus bevindt** een afwijking van meer dan 1 minuut detecteert tussen de tijd van de meetfunctie van de voertuigunit en de tijd die door de GNSS-ontvanger wordt doorgestuurd. Dit voorval wordt samen met de interne klokwaarde van de voertuigunit opgeslagen en gaat gepaard met een automatische tijdsafstelling. Nadat een tijdsoverlapping is veroorzaakt, mag de VU de volgende 12 uur geen andere tijdsoverlapping genereren. Er wordt geen tijdsoverlapping gegenereerd wanneer de GNSS-ontvanger gedurende minstens 30 dagen geen geldig GNSS-signaal heeft kunnen detecteren.”.

10) aan punt 3.9.17 wordt het volgende streepje toegevoegd:

„— ITS-interfacefout (indien van toepassing)”.

11) Punt 3.10 wordt als volgt gewijzigd:

i) de tekst boven de tabel in punt 89) wordt vervangen door:

„Het controleapparaat detecteert fouten door middel van zelftests en ingebouwde tests overeenkomstig onderstaande tabel.”;

ii) de volgende rij wordt aan de tabel toegevoegd:

„ITS-interface (optioneel)	Correcte werking”	
----------------------------	-------------------	--

12) Het tweede streepje van punt 3.12 wordt vervangen door:

„— het gemiddeld aantal posities per dag wordt gedefinieerd als ten minste 6 posities bij het begin van de dagelijkse werktijd, 6 posities wanneer de cumulatieve rijtijd van de bestuurder een veelvoud van drie uur bereikt en 6 posities aan het einde van de dagelijkse werktijd, zodat „365 dagen” minstens 6570 posities omvat.”.

13) punt 3.12.5 wordt als volgt gewijzigd:

a) de hoofding en punt 108) worden vervangen door:

„3.12.5 Plaatsen en posities waar de dagelijkse werktijd begint, eindigt en/of waar een cumulatieve rijtijd van 3 uur wordt bereikt

108) Het controleapparaat moet gegevens registreren en in zijn geheugen opslaan met betrekking tot:

- de plaatsen en posities waar de bestuurder en/of rijder hun dagelijkse werktijd aanvangen;
- de posities waar de cumulatieve rijtijd een veelvoud van drie uur bereikt;
- de plaatsen en posities waar de bestuurder en/of de rijder hun dagelijkse werktijd beëindigen.”;

b) het vierde streepje van punt 110) wordt vervangen door:

„— de aard van die gebeurtenis (begin, einde en/of 3 uur cumulatieve rijtijd);”;

c) punt 111) wordt vervangen door:

„111) Het geheugen moet de plaatsen of posities waar de dagelijkse werkperiodes beginnen, eindigen en/of waar een cumulatieve rijtijd van 3 uur wordt bereikt ten minste 365 dagen kunnen bewaren.”

14) In punt 3.12.7 wordt punt 116) vervangen door:

„116) Het controleapparaat moet voor elke seconde van ten minste de laatste 24 uur waarin het voertuig heeft bewogen, de snelheid van het voertuig en de corresponderende datum en het tijdstip registreren en in het geheugen opslaan”.

15) De tabel van punt 3.12.8 wordt als volgt gewijzigd:

a) het volgende punt wordt ingevoegd tussen „Ontbreken van plaatsbepalingsinformatie van de GNSS-ontvanger” en „Fout in de bewegingsgegevens”:

„Fout in de communicatie met de externe GNSS-module	— het langste voorval op elk van de laatste 10 dagen waarop een dergelijk voorval is opgetreden — de 5 langste voorvallen gedurende de afgelopen 365 dagen	— datum en tijdstip van het begin van het voorval, — datum en tijdstip van het einde van het voorval — type, nummer, lidstaat van afgifte en generatie van de bij het begin en/of het einde van het voorval ingevoerde kaart(en) — aantal vergelijkbare voorvallen op die dag.”
---	---	--

b) het punt „Tijdsverlappend” wordt vervangen door:

„Tijdsverlappend	— het ergste voorval voor elk van de laatste 10 dagen waarop een dergelijk voorval heeft plaatsgevonden (d.w.z. het voorval met het grootste verschil tussen de datum en het tijdstip van het controleapparaat en de datum en het tijdstip van het GNSS). — de 5 ergste voorvallen gedurende de afgelopen 365 dagen.	— datum en tijdstip controleapparaat — GNSS-datum en -tijdstip, — type, nummer, lidstaat van afgifte en generatie van de bij het begin en/of het einde van het voorval ingevoerde kaart(en) — aantal vergelijkbare voorvallen op die dag.”
------------------	---	---

16) In punt 3.20 wordt punt 200) vervangen door:

„200) Het controleapparaat kan worden uitgerust met gestandaardiseerde interfaces die ervoor zorgen dat een extern apparaat kan gebruikmaken van de door de tachograaf in operationele of kalibreringsmodus geregistreerde of gegenereerde gegevens.

Aanhangsel 13 bevat specificaties en normen voor een facultatieve ITS-interface. Andere voertuigunitinterfaces zijn eveneens toegestaan indien zij volledig voldoen aan de vereisten van aanhangsel 13 inzake de minimumlijst van gegevens, beveiliging en instemming door de bestuurder.

De instemming door de bestuurder geldt niet voor gegevens die door het controleapparaat naar het voertuignetwerk worden verstuurd. Wanneer de persoonsgegevens die in het voertuignetwerk worden ingevoerd, verder worden verwerkt buiten het voertuignetwerk, is het de verantwoordelijkheid van de voertuigfabrikant om dat proces in overeenstemming te brengen met Verordening (EU) 2016/679 (de „algemene verordening gegevensbescherming”).

De instemming door de bestuurder geldt evenmin voor tachograafgegevens die worden gedownload naar een op afstand aangesloten bedrijf (voorschrift 193), aangezien dit scenario wordt gemonitord door het toegangsrecht van de bedrijfskaart.

De volgende eisen zijn van toepassing voor ITS-gegevens die via die interface worden verstrekt:

- de gegevens zijn een set geselecteerde bestaande data uit de data dictionary van de tachograaf (aanhangsel 1);
- een deel van die geselecteerde gegevens zijn aangeduid als „persoonsgegevens”;
- de subset van „persoonsgegevens” is alleen beschikbaar na de controleerbare bevestiging door de bestuurder dat hij ermee instemt dat zijn persoonsgegevens desgevallend het voertuignetwerk mogen verlaten;
- wanneer de bestuurderskaart is ingebracht, kan de bestuurder op elk moment via het menu zijn instemming geven of intrekken;
- de dataset en -subset worden in een straal rond de cabine van het voertuig verzonden via het draadloos bluetoothprotocol en om de minuut bijgewerkt;
- de verbinding tussen het extern apparaat en de ITS-interface wordt beveiligd door een specifieke willekeurige PIN-code van minstens 4 cijfers, die via het display van elke voertuigunit wordt opgeslagen en kan worden geraadpleegd;
- de ITS-interface mag de correcte werking en beveiliging van de voertuigunit in geen geval verstoren of aantasten.

Bovenop de set van geselecteerde bestaande gegevens, die als minimumlijst geldt, mogen aanvullende gegevens worden doorgestuurd, voor zover het niet om persoonsgegevens gaat.

Het controleapparaat moet de instemmingsstatus van de bestuurder kunnen meedelen aan andere platforms in het voertuignetwerk.

Wanneer het contact van het voertuig AAN staat, worden die gegevens permanent doorgestuurd”.

17) In punt 3.23 wordt punt 211) vervangen door:

„211) De tijdsbepaling van de interne klok van de VU wordt om de 12 uur automatisch bijgewerkt. Wanneer die bijstelling niet mogelijk is omdat er geen GNSS-signaal beschikbaar is, gebeurt de tijdsafstelling zodra de VU toegang krijgt tot een geldige tijdsaanduiding van de GNSS-ontvanger, naargelang het contact al dan niet aan staat. De referentietijd voor de automatische tijdsafstelling van de interne klok van de VU wordt afgeleid van de GNSS-ontvanger.”.

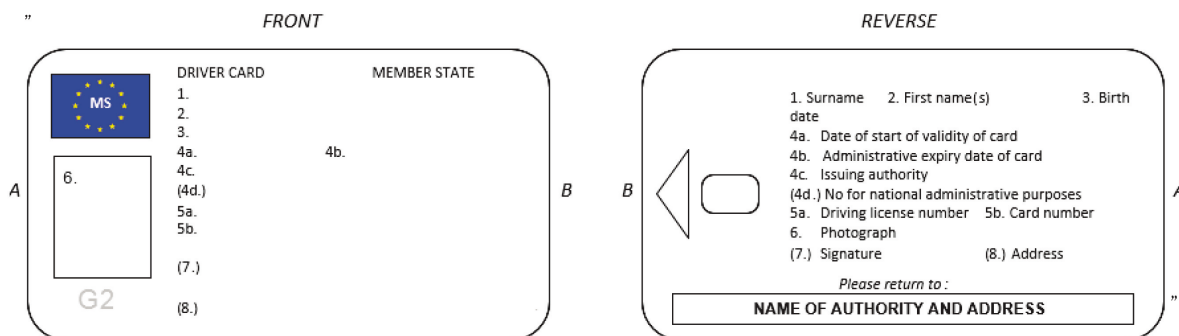
18) In punt 3.26 worden de punten 225) en 226) vervangen door:

„225) Een identificatieplaatje met de volgende gegevens moet op elk afzonderlijk samenstellend deel van het controleapparaat worden aangebracht:

- naam van de fabrikant en zijn adres;
- onderdeelnummer en bouwjaar van het apparaat;
- serienummer;
- typegoedkeuringsmerk.

226) Wanneer er onvoldoende fysieke ruimte is voor alle voornoemde gegevens, moet ten minsten het volgende op het identificatieplaatje zijn vermeld: de naam of het logo van de fabrikant en het onderdeelnummer.”.

19) In punt 4.1 wordt de afbeelding van de voor- en achterkant van de bestuurderskaart vervangen door:



20) In punt 4.5.3.1.8 wordt het eerste streepje van punt 263) vervangen door:

„— kaartfout (indien deze kaart de aanleiding is van de fout)”.

21) In punt 4.5.3.2.8 wordt het eerste streepje van punt (288) vervangen door:

„— kaartfout (indien deze kaart de aanleiding is van de fout)”.

22) punt 4.5.3.2.16 wordt vervangen door:

„4.5.3.2.16 Plaats en tijdstip cumulatieve rijtijd van drie uur

305) Een bestuurderskaart moet de volgende gegevens kunnen bewaren in verband met de positie van het voertuig waar de cumulatieve rijtijd een veelvoud van drie uur bereikt:

- de datum en het tijdstip waarop de cumulatieve rijtijd een veelvoud van drie uur bereikt;
- de positie van het voertuig;
- de GNSS-nauwkeurigheid, de datum en het tijdstip waarop de positie is bepaald;
- de kilometerstand van het voertuig.

306) Een bestuurderskaart moet minstens 252 records kunnen opslaan.”.

23) punt 4.5.4.2.14 wordt vervangen door:

„4.5.4.2.14 Plaats en tijdstip cumulatieve rijtijd van drie uur

353) Een werkplaatskaart moet de volgende gegevens kunnen bewaren in verband met de positie van het voertuig waar de cumulatieve rijtijd een veelvoud van drie uur bereikt:

- de datum en het tijdstip waarop de cumulatieve rijtijd een veelvoud van drie uur bereikt;

- de positie van het voertuig;
- de GNSS-nauwkeurigheid, de datum en het tijdstip waarop de positie is bepaald;
- de kilometerstand van het voertuig.

354) Een werkplaatskaart moet ten minste 18 records kunnen opslaan”.

24) In punt 5.2 wordt punt 396) vervangen door:

„396) Op het plaatje moeten ten minste de volgende gegevens zijn aangebracht:

- naam, adres of handelsnaam van de erkende installateur of werkplaats;
- kenmerkende coëfficiënt van het voertuig in de vorm „w = ... imp/km”;
- constante van het controleapparaat in de vorm „k = ... imp/km”;
- effectieve omtrek van de wielbanden, in de vorm „l = ... mm”;
- bandenmaat;
- de datum waarop de kenmerkende coëfficiënt van het voertuig is vastgesteld en waarop de effectieve omtrek van de wielbanden is gemeten;
- VIN-nummer van het voertuig;
- de aanwezigheid (of afwezigheid) van een externe GNSS-module;
- het serienummer van de externe GNSS-module, indien van toepassing;
- het serienummer van het systeem voor communicatie op afstand, indien van toepassing;
- het serienummer van alle aanwezige verzegelingen;
- het gedeelte van het voertuig waarin de adapter eventueel is geïnstalleerd;
- het gedeelte van het voertuig waarin de bewegingssensor is geïnstalleerd, wanneer deze niet is aangesloten op de versnellingsbak of wanneer geen adapter wordt gebruikt;
- een beschrijving van de kleur van de kabel tussen de adapter en het gedeelte van het voertuig dat impulsen naar de adapter stuurt;
- het serienummer van de ingebouwde bewegingssensor van de adapter.”.

25) Punt 5.3 wordt als volgt gewijzigd:

a) een nieuw punt 398 bis) wordt ingevoegd na punt 398)

„398 bis) de bovengenoemde verzegelingen worden gecertificeerd overeenkomstig norm EN 16882:2016.”;

b) in punt 401) wordt de tweede alinea vervangen door:

„Het unieke identificatienummer wordt als volgt gedefinieerd: MMNNNNNNNN door een niet-verwijderbaar merkteken, waarbij MM een unieke identificatiecode van de fabrikant is (de registratie in de databank wordt beheerd door de EC) en NNNNNNNN een alfanumeriek zegelnummer is binnen het domein van de fabrikant.”;

c) punt 403) wordt vervangen door:

„403) Zegelfabrikanten worden opgenomen in een specifieke databank wanneer zij een zegelmodel krijgen dat gecertificeerd is volgens EN 16882:2016, en maken hun zegelidentificatienummers bekend door middel van een door de Europese Commissie vastgestelde procedure.”;

d) punt 404) wordt vervangen door:

„404) Erkende werkplaatsen en voertuigfabrikanten gebruiken in het kader van Verordening (EU) nr. 165/2014 alleen zegels die gecertificeerd zijn volgens EN 16882:2016 en geproduceerd zijn door in de voornoemde databank opgenomen zegelfabrikanten.”.

26) Punt 6.2 wordt vervangen door:

„6.2 Controle van nieuwe of herstelde onderdelen

407) Iedere afzonderlijke inrichting, zij het nieuw of hersteld, wordt gecontroleerd uit het oogpunt van juiste werking en nauwkeurigheid van de aflezing en registratie, waarbij de in de punten 3.2.1, 3.2.2, 3.2.3 en 3.3 vastgelegde grenswaarden moeten worden gehanteerd”.

27) In punt 6.3 wordt punt 408) vervangen door:

„408) Na plaatsing in een voertuig moeten de volledige installatie en het controleapparaat voldoen aan de bepalingen betreffende de maximumtoleranties zoals vastgelegd in de punten 3.2.1, 3.2.2, 3.2.3 en 3.3. De volledige installatie wordt verzegeld overeenkomstig hoofdstuk 5.3 en omvat een kalibrering.”.

28) Punt 8.1 wordt als volgt gewijzigd:

a) in punt 8.1 wordt de tekst die is ingevoerd vóór punt 425) vervangen door:

„In dit punt wordt onder „controleapparaat” verstaan: „controleapparaat of de componenten daarvan”. Er is geen typegoedkeuring vereist voor de kabels waarmee de bewegingssensor, de externe GNSS-module of het systeem voor communicatie op afstand op de VU worden aangesloten. Het in het controleapparaat gebruikte papier wordt als een onderdeel van het controleapparaat beschouwd.

Elke fabrikant kan een typegoedkeuring vragen van onderdelen van het controleapparaat die om het even welke andere onderdelen van controleapparaten bevatten, op voorwaarde dat elk onderdeel voldoet aan de voorschriften van deze bijlage. Fabrikanten kunnen als alternatief ook een typegoedkeuring voor hun controleapparaten aanvragen.

Zoals beschreven in definitie 10 van artikel 2 van deze verordening, kunnen voertuigunits zijn samengesteld uit diverse onderdelen. Ongeacht uit welke onderdelen de voertuigunit is samengesteld, maken de externe antenne en (indien aanwezig) de antennesplitter die is aangesloten op de GNSS-ontvanger of het systeem voor communicatie op afstand, geen deel uit van de typegoedkeuring van het voertuig.

Desondanks houden fabrikanten die typegoedkeuring voor controleapparaten hebben verkregen een openbaar beschikbare lijst bij van antennes en splitters die compatible zijn met elke voertuigunit, met elke externe GNSS-module en met elk extern systeem voor communicatie op afstand waarvoor typegoedkeuring is verleend.”;

b) punt 427) wordt vervangen door:

„427) De goedkeuringsautoriteiten van de lidstaten geven pas een typegoedkeuringscertificaat af wanneer zij beschikken over:

- een beveiligingscertificaat (indien vereist uit hoofde van deze bijlage),
- een functiecertificaat,
- een interoperabiliteitscertificaat (indien vereist uit hoofde van deze bijlage)

voor het controleapparaat of de tachograafkaart waarvoor de typegoedkeuring wordt aangevraagd.”.

29) Aanhangsel 1 wordt als volgt gewijzigd:

a) de inhoudsopgave wordt als volgt gewijzigd:

i) punt 2.63 wordt vervangen door:

„2.63 Gereserveerd voor toekomstig gebruik”;

ii) punt 2.78 wordt vervangen door:

„2.78 GNSSAccumulatedDriving”;

iii) punt 2.79 wordt vervangen door:

„2.79 GNSSAccumulatedDrivingRecord”;

iv) punt 2.111 wordt vervangen door:

„2.111 NoOfGNSSADRecords”;

v) punt 2.160 wordt vervangen door:

„2.160 Gereserveerd voor toekomstig gebruik”;

vi) punt 2.203 wordt vervangen door:

„2.203 VuGNSSADRecord”;

vii) punt 2.204 wordt vervangen door:

„2.204 VuGNSSADRecordArray”;

viii) punt 2.230 wordt vervangen door:

„2.230 Gereserveerd voor toekomstig gebruik”;

ix) punt 2.231 wordt vervangen door:

„2.231 Gereserveerd voor toekomstig gebruik”;

- b) in punt 2 wordt de volgende tekst ingevoegd vóór punt 2.1:

„Voor kaartgegevens types die worden gebruikt voor toepassingen van de eerste en tweede generatie is het in dit aanhangsel gespecificeerde formaat dat voor toepassingen van de tweede generatie. Het formaat voor toepassingen van de eerste generatie wordt geacht reeds bekend te zijn bij de lezer. Het voorschrift van bijlage IC met betrekking tot dergelijke gegevens types heeft betrekking op toepassingen van zowel de eerste als de tweede generatie.”;

- c) punt 2.19 wordt vervangen door:

„2.19 **CardEventData**

1e generatie:

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de aan de kaarthouder te wijten voorvallen (Bijlage IC, voorschriften 260 en 318).

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

CardEventData is een sequentie, gerangschikt op oplopende waarde van EventFaultType, van cardEventRecords (uitgezonderd records die verband houden met pogingen tot inbreuk op de beveiliging, die in de laatste reeks van de sequentie worden verzameld).

cardEventRecords is een reeks voorvalrecords van een bepaald type voorval (of categorie voor voorvallen met betrekking tot pogingen tot inbreuk op de beveiliging).

2e generatie:

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de aan de kaarthouder te wijten voorvallen (Bijlage IC, voorschriften 285 en 341).

```
CardEventData ::= SEQUENCE SIZE(11) OF {
    cardEventRecords                               SET SIZE(NoOfEventsPerType) OF
                                                    CardEventRecord
}
```

CardEventData is een sequentie, gerangschikt op oplopende waarde van EventFaultType, van cardEventRecords (uitgezonderd records die verband houden met pogingen tot inbreuk op de beveiliging, die in de laatste reeks van de sequentie worden verzameld).

cardEventRecords is een reeks voorvalrecords van een bepaald type voorval (of categorie voor voorvallen met betrekking tot pogingen tot inbreuk op de beveiliging).”;

- d) punt 2.30 wordt vervangen door:

„2.30 **CardRenewalIndex (Vernieuwingsindex van de kaart)**

Vernieuwingsindex van de kaart (definitie i).

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

Waardetoekenning: (zie hoofdstuk 7 van deze bijlage).

„0” Eerste afgifte.

Volgorde van verhoging: „0, ..., 9, A, ..., Z” ”;

- e) in punt 2.61 wordt de tekst na hoofding 2e generatie vervangen door:

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

Als aanvulling op de 1e generatie worden de volgende gegevenselementen gebruikt:

noOfGNSSCDRecords is het aantal GNSS-records van de cumulatieve rijtijd dat op de kaart kan worden opgeslagen.

noOfSpecificConditionRecords is het aantal records van specifieke omstandigheden dat op de kaart kan worden opgeslagen.

noOfCardVehicleUnitRecords is het aantal voertuigrecords dat op de kaart kan worden opgeslagen.”;

- f) punt 2.63 wordt vervangen door:

„2.63 **Gereserveerd voor toekomstig gebruik**”;

- g) in punt 2.67 wordt de tekst onder hoofding 2e generatie vervangen door:

„Er wordt gebruik gemaakt van dezelfde waarden als in de 1e generatie, met de volgende aanvullingen:

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

Opmerking 1: de waarden van de 2e generatie voor het installatieplaatje, de adapter en de externe GNSS-verbinding en de waarden van de 1e generatie voor de VU en de bewegingssensor kunnen, indien van toepassing, in SealRecord worden gebruikt.

Opmerking 2: in het veld CardHolderAuthorisation (CHA) van een certificaat van de 2e generatie wijzen de waarden (1), (2) en (6) op een certificaat van wederzijdse authenticatie voor het desbetreffende type apparatuur. Om het respectieve certificaat voor het opstellen van een digitale handtekening aan te geven, moeten de waarden (17), (18) of (19) worden gebruikt.”;

h) in punt 2.70 wordt de tekst onder hoofding 2e generatie vervangen door:

„2e generatie:

'0x'H	Algemene voorvallen,
'00'H	Geen verdere details,
'01'H	Inbrengen van een ongeldige kaart,
'02'H	Kaartconflict,
'03'H	Tijdsoverlapping,
'04'H	Rijden zonder geschikte kaart,
'05'H	Inbrengen van de kaart tijdens het rijden,
'06'H	Laatste kaartsessie niet correct afgesloten,
'07'H	Snelheidoverschrijding,
'08'H	Onderbreking in de stroomvoorziening,
'09'H	Fout in de bewegingsgegevens,
'0A'H	Tegenstrijdige bewegingsgegevens,
'0B'H	Tijdsconflict (tussen GNSS en de interne klok van de VU),
'0C'H	Fout in de communicatie met het systeem voor communicatie op afstand,
'0D'H	Ontbreken van plaatsbepalingsinformatie van de GNSS-ontvanger,
'0E'H	Fout in de communicatie met de externe GNSS-module,
'0F'H	RFU,
'1x'H	Poging tot inbreuk op de beveiliging van de voertuigunit,
'10'H	Geen verdere details,
'11'H	Authenticatiefout van de bewegingssensor,
'12'H	Authenticatiefout van de tachograafkaart,
'13'H	Niet-geautoriseerde wijziging van de bewegingssensor,
'14'H	Integriteitsfout in de gegevensinvoer op de kaart,
'15'H	Integriteitsfout in de opgeslagen gebruikersgegevens,
'16'H	Overdrachtsfout in de interne gegevens,
'17'H	Niet-geautoriseerde opening van het omhulsel,
'18'H	Hardwaresabotage,
'19'H	GNSS is gemanipuleerd,
'1A'H	Authenticatiefout van de externe GNSS-module,
'1B'H	Certificaat van de externe GNSS-module is vervallen,
'1C'H t.e.m. '1F'H	RFU,
'2x'H	Poging tot inbreuk op de beveiliging van de sensor,
'20'H	Geen verdere details,
'21'H	Authenticatiefout,
'22'H	Integriteitsfout in de opgeslagen gegevens,
'23'H	Overdrachtsfout in de interne gegevens,
'24'H	Niet-geautoriseerde opening van het omhulsel,
'25'H	Hardwaresabotage,
'26'H t.e.m.	RFU,
'2F'H	
'3x'H	Fouten van het controleapparaat,
'30'H	Geen verdere details,
'31'H	Interne fout in de VU,
'32'H	Printerfout,
'33'H	Displayfout,
'34'H	Downloadfout,
'35'H	Sensorfout,
'36'H	Interne GNSS-ontvanger,
'37'H	Externe GNSS-module,
'38'H	Systeem voor communicatie op afstand,
'39'H	ITS-interface,
'3A'H t.e.m. '3F'H	RFU,
'4x'H	
'40'H	Kaartfouten,
'41'H t.e.m.	Geen verdere details,
'4F'H	RFU,
'50'H t.e.m. '7F'H	RFU,
'80'H t.e.m. 'FF'H	Specifiek voor de fabrikant.”;

- i) punt 2.71 wordt vervangen door:

„2.71 **ExtendedSealIdentifier**

2e generatie:

De verlengde zegelidentificatiecode identificeert een zegel op unieke wijze (voorschrift 401 van bijlage IC).

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

manufacturerCode is een code van de zegelfabrikant.

sealIdentifier is een zegelidentificatienummer dat uniek is voor de fabrikant.”;

- j) de punten 2.78 en 2.79 worden vervangen door:

„2.78 **GNSSAccumulatedDriving**

2e generatie:

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de GNSS-positie van het voertuig als de cumulatieve rijtijd een veelvoud van drie uur bereikt (voorschriften 306 en 354 van bijlage IC).

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

gnssADPointerNewestRecord is de index van de laatst gewijzigde GNSS-record van cumulatieve rijtijd.

Waardetoekenning is het cijfer dat correspondeert met de teller van de GNSS-record van cumulatieve rijtijd, beginnend met „0” voor de eerste GNSS-record van cumulatieve rijtijd in de structuur.

gnssAccumulatedDrivingRecords is de reeks records die de datum en tijd bevat waarop de cumulatieve rijtijd een veelvoud van drie uur bereikt en informatie over de positie van het voertuig.

2.79. **GNSSAccumulatedDrivingRecord**

2e generatie:

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de GNSS-positie van het voertuig als de cumulatieve rijtijd een veelvoud van drie uur bereikt (voorschriften 305 en 353 van bijlage IC)

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

timeStamp is de datum en het tijdstip waarop de cumulatieve rijtijd een veelvoud van drie uur bereikt;

gnssPlaceRecord bevat informatie over de positie van het voertuig.

vehicleOdometerValue is de kilometerstand op het ogenblik dat de cumulatieve rijtijd een veelvoud van drie uur bereikt.”;

k) punt 2.86 wordt vervangen door:

„2.86 KeyIdentifier

Een uniek identificatiesymbool van een openbare sleutel dat wordt gebruikt ter verwijzing naar of selectie van de sleutel. Het identificeert tevens de houder van de sleutel.

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

Met de eerste keuze wordt verwezen naar de openbare sleutel van een voertuigunit, een tachograafkaart of een externe GNSS-module.

Met de tweede keuze wordt verwezen naar de openbare sleutel van een voertuigunit (wanneer het serienummer van de voertuigunit op het moment van ontwikkeling van het certificaat nog niet bekend is).

Met de derde keuze wordt verwezen naar de openbare sleutel van een lidstaat.”;

l) punt 2.92 wordt vervangen door:

„2.92 MAC

2e generatie:

Een cryptografische controlesom met een lengte van 8, 12 of 16 bytes die overeenkomt met het in aanhangsel 11 gespecificeerde cijfer

```
MAC ::= CHOICE {
    Mac8      OCTET STRING (SIZE(8)),
    Mac12     OCTET STRING (SIZE(12)),
    Mac16     OCTET STRING (SIZE(16)),
}”;
```

m) punt 2.111 wordt vervangen door:

„2.111 NoOfGNSSADRecords

2e generatie:

Aantal GNSS-records van cumulatieve rijtijd dat op een kaart kan worden opgeslagen.

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

Waardetoekenning: zie aanhangsel 2.”;

n) in punt 2.120 wordt de waardetoekenning „16H” vervangen door:

„' 16' H VuGNSSADRecord ”

o) punt 2.160 wordt vervangen door:

„2.160 Gereserveerd voor toekomstig gebruik”;

p) punt 2.162 wordt vervangen door:

„2.162 **TimeReal**

Code voor een gecombineerd veld voor datum en tijd, waarin de datum en het tijdstip worden uitgedrukt in seconden na 00u.00m.00s. op 1 januari 1970 UTC.

TimeReal {INTEGER:TimeRealRange} ::= INTEGER (0..TimeRealRange)

Waardetoekenning – Octet-uitgericht: aantal seconden sinds middernacht 1 januari 1970 UTC.

De laatst mogelijke datum/tijd is in het jaar 2106.”;

q) punt 2.179 wordt vervangen door:

„2.179 **VuCardRecord**

2e generatie:

In een voertuigunit opgeslagen informatie over een gebruikte tachograafkaart (voorschrift 132 van bijlage IC).

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

cardNumberAndGenerationInformation is het volledige kaartnummer en de generatie van de gebruikte kaart (data type 2.74).

cardExtendedSerialNumber zoals afgelezen uit het bestand EF_ICC onder het stambestand van de kaart.

cardStructureVersion zoals afgelezen uit het bestand EF_Application_Identification onder DF Tachograaf_G2.

cardNumber zoals afgelezen uit het bestand EF_Identification onder DF_Tachograaf_G2.”;

r) de punten 2.203 en 2.204 worden vervangen door:

„2.203 **VuGNSSADRecord**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot de GNSS-positie van het voertuig als de cumulatieve rijtijd een veelvoud van drie uur bereikt (voorschriften 108 en 110 van bijlage IC).

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

timeStamp is de datum en het tijdstip waarop de cumulatieve rijtijd een veelvoud van drie uur bereikt;

cardNumberAndGenDriverSlot identificeert de in de lezer van de bestuurder ingebrachte kaart, inclusief de generatie.

cardNumberAndGenCodriverSlot identificeert de in de lezer van de bijrijder ingebrachte kaart, inclusief de generatie.

gnssPlaceRecord bevat informatie over de positie van het voertuig.

vehicleOdometerValue is de kilometerstand op het ogenblik dat de cumulatieve rijtijd een veelvoud van drie uur bereikt.

2.204. **VuGNSSADRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot de GNSS-positie van het voertuig als de cumulatieve rijtijd een veelvoud van drie uur bereikt (voorschriften 108 en 110 van bijlage IC).

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

recordType geeft de soort record aan (VuGNSSADRecord).

Waardetoekenning: See RecordType.

recordSize is de grootte van VuGNSSADRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks GNSS-records van de cumulatieve rijtijd.”;

s) de punten 2.230 en 2.231 worden vervangen door:

„2.230 Gereserveerd voor toekomstig gebruik.

2.231. Gereserveerd voor toekomstig gebruik”;

t) in punt 2.234 wordt de tekst onder hoofding 2e generatie vervangen door:

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

Als aanvulling op de 1e generatie worden de volgende gegevenselementen gebruikt:

noOfGNSSCDRecords is het aantal GNSS-records van de cumulatieve rijtijd dat op de kaart kan worden opgeslagen.

noOfSpecificConditionRecords is het aantal records van specifieke omstandigheden dat op de kaart kan worden opgeslagen.

noOfCardVehicleUnitRecords is het aantal voertuigrecords dat op de kaart kan worden opgeslagen.”.

30) Aanhangsel 2 wordt als volgt gewijzigd:

a) aan punt 1.1 worden de volgende afkortingen toegevoegd:

„CHA Autorisatie van de certificaathouder

DO Gegevensobject”;

b) punt 3.3 wordt als volgt gewijzigd:

i) punt TCS_24 wordt vervangen door:

„TCS_24 Deze beveiligingsvoorwaarden kunnen op de volgende wijzen aan elkaar worden gekoppeld:

AND: alle beveiligingsvoorwaarden moeten worden nageleefd.

OR: ten minste één beveiligingsvoorwaarde moet worden nageleefd.

De toegangsregels voor het bestandssysteem, dat wil zeggen de SELECT-, READ BINARY- en UPDATE BINARY-commando's, worden gespecificeerd in hoofdstuk 4. De toegangsregels voor de overige commando's worden gespecificeerd in de volgende tabellen. De uitdrukking „niet van toepassing” wordt gebruikt wanneer er geen voorschrift bestaat ter ondersteuning van het commando. In dat geval kan het commando al dan niet worden ondersteund, maar de toegangsvoorwaarde is „niet verplicht”.

ii) in punt TCS_25 wordt de tabel vervangen door:

„Commando	Bestuurderskaart	Werkplaatskaart	Controlekaart	Bedrijfskaart
External Authenticate				
— Voor authenticatie van de eerste generatie	ALW	ALW	ALW	ALW
— Voor authenticatie van de tweede generatie	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Niet van toepassing	Niet van toepassing	Niet van toepassing	Niet van toepassing
PSO: Compute Digital Signature	ALW of SM-MAC-G2	ALW of SM-MAC-G2	Niet van toepassing	Niet van toepassing
PSO: Hash	Niet van toepassing	Niet van toepassing	ALW	Niet van toepassing

Commando	Bestuurderskaart	Werkplaatskaart	Controlekaart	Bedrijfskaart
PERFORM HASH OF FILE	ALW of SM-MAC-G2	ALW of SM-MAC-G2	Niet van toepassing	Niet van toepassing
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Niet van toepassing	Niet van toepassing	ALW	Niet van toepassing
Verify	Niet van toepassing	ALW	Niet van toepassing	Niet van toepassing

iii) in punt TCS_26 wordt de tabel vervangen door:

„Commando	Bestuurderskaart	Werkplaatskaart	Controlekaart	Bedrijfskaart
External Authenticate				
— Voor authenticatie van de eerste generatie	Niet van toepassing	Niet van toepassing	Niet van toepassing	Niet van toepassing
— Voor authenticatie van de tweede generatie	ALW	PWD	ALW	ALW
Internal Authenticate	Niet van toepassing	Niet van toepassing	Niet van toepassing	Niet van toepassing
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Niet van toepassing	ALW	ALW	Niet van toepassing
PSO: Compute Digital Signature	ALW of SM-MAC-G2	ALW of SM-MAC-G2	Niet van toepassing	Niet van toepassing
PSO: Hash	Niet van toepassing	Niet van toepassing	ALW	Niet van toepassing
PERFORM HASH OF FILE	ALW of SM-MAC-G2	ALW of SM-MAC-G2	Niet van toepassing	Niet van toepassing
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Niet van toepassing	Niet van toepassing	ALW	Niet van toepassing
Verify	Niet van toepassing	ALW	Niet van toepassing	Niet van toepassing

iv) in punt TCS_27 wordt de tabel vervangen door:

„Commando	Bestuurderskaart	Werkplaatskaart	Controlekaart	Bedrijfskaart
External Authenticate				
— Voor authenticatie van de eerste generatie	Niet van toepassing	Niet van toepassing	Niet van toepassing	Niet van toepassing
— Voor authenticatie van de tweede generatie	ALW	PWD	ALW	ALW
Internal Authenticate	Niet van toepassing	Niet van toepassing	Niet van toepassing	Niet van toepassing
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Niet van toepassing	Niet van toepassing	Niet van toepassing	Niet van toepassing
PSO: Compute Digital Signature	Niet van toepassing	Niet van toepassing	Niet van toepassing	Niet van toepassing
PSO: Hash	Niet van toepassing	Niet van toepassing	Niet van toepassing	Niet van toepassing
PERFORM HASH OF FILE	Niet van toepassing	Niet van toepassing	Niet van toepassing	Niet van toepassing
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Niet van toepassing	Niet van toepassing	Niet van toepassing	Niet van toepassing
Verify	Niet van toepassing	ALW	Niet van toepassing	Niet van toepassing

c) in punt 3.4 wordt punt TCS_29 vervangen door:

„TCS_29 De statuswoorden SW1 en SW2 worden in een antwoordbericht teruggezonden en geven de verwerkingsstatus van het commando aan.

SW1	SW2	Betekenis
90	00	Normale verwerking
61	XX	Normale verwerking XX = aantal beschikbare antwoordbytes
62	81	Verwerking van waarschuwing. Deel van teruggezonden gegevens kan beschadigd zijn
63	00	Authenticatie mislukt (waarschuwing)
63	CX	Foutieve CHV (pincode). „X” is waarde van teller voor resterende pogingen.

SW1	SW2	Betekenis
64	00	Uitvoeringsfout — Toestand van niet-vluchtig geheugen ongewijzigd. Integriteitsfout
65	00	Uitvoeringsfout — Toestand van niet-vluchtig geheugen gewijzigd
65	81	Uitvoeringsfout — Toestand van niet-vluchtig geheugen gewijzigd. Geheugenfout
66	88	Beveiligingsfout: foutieve cryptografische controlesom (tijdens beveiligde berichtenuitwisseling) of ongeldig certificaat (tijdens certificaatverificatie) of ongeldig cryptogram (tijdens externe authenticatie) of ongeldige handtekening (tijdens handtekeningverificatie)
67	00	Foutieve lengte (ongeldige Lc of Le)
68	83	Laatste commando van de ketting verwacht
69	00	Verboden commando (geen antwoord beschikbaar in T=0)
69	82	Niet voldaan aan beveiligingsstatus
69	83	Authenticatiemethode geblokkeerd
69	85	Niet voldaan aan gebruiksvoorwaarden
69	86	Commando niet toegestaan (geen geldig EF)
69	87	Verwachte gegevensobjecten voor beveiligde berichtenuitwisseling ontbreken
69	88	Onjuiste gegevensobjecten voor beveiligde berichtenuitwisseling
6A	80	Onjuiste parameters in gegevensveld
6A	82	Bestand niet gevonden
6A	86	Foutieve parameters P1-P2
6A	88	Referentiegegevens niet gevonden
6B	00	Onjuiste parameters (offset buiten EF)
6C	XX	Foutieve lengte, SW2 geeft de exacte lengte aan. Er wordt geen gegevensveld teruggezonden
6D	00	Instructiecode niet ondersteund of ongeldig
6E	00	Categorie niet ondersteund
6F	00	— Andere controlefouten

Aanvullende statuswoorden zoals gedefinieerd in ISO/IEC 7816-4 kunnen worden teruggezonden indien hun gedrag niet expliciet wordt genoemd in dit aanhangsel.

Bijvoorbeeld de volgende statuswoorden kunnen facultatief worden teruggezonden:

6881: Logical channel not supported

6882: Secure messaging not supported”;

d) in punt 3.5.1.1 wordt het laatste streepje van punt TCS_38 vervangen door:

„— Indien de geselecteerde toepassing beschadigd is (integriteitsfout vastgesteld in de bestandsattributen), wordt de verwerkingsstatus „6400” of „6500” teruggezonden.”;

e) in punt 3.5.1.2 wordt het laatste streepje van punt TCS_41 vervangen door:

„— Indien het geselecteerde bestand beschadigd is (integriteitsfout vastgesteld in de bestandsattributen), wordt de verwerkingsstatus „6400” of „6500” teruggezonden.”;

f) in punt 3.5.2.1 wordt het zesde streepje van punt TCS_43 vervangen door:

„— Indien binnen de bestandsattributen een integriteitsfout wordt ontdekt, moet de kaart het bestand als beschadigd en verloren beschouwen; de teruggezonden verwerkingsstatus is „6400” of „6500”.”;

g) punt 3.5.2.1.1 wordt als volgt gewijzigd:

i) in punt TCS_45 wordt de tabel vervangen door:

„Byte	Lengte	Waarde	Omschrijving
#1	1	„81h”	T _{PV} : label voor gegevens met ongecodeerde waarde
#2	L	„NNh” of „81 NNh”	L _{PV} : lengte van teruggezonden gegevens (= originele Le) L is 2 bytes indien L _{PV} >127 bytes
#(2+L) - #(1+L+NN)	NN	„XX..XXh”	Ongecodeerde gegevenswaarde
#(2+L+NN)	1	„99h”	Label voor verwerkingsstatus (SW1-SW2) — facultatief voor beveiligde berichtenuitwisseling van de eerste generatie
#(3+L+NN)	1	„02h”	Lengte van verwerkingsstatus — facultatief voor beveiligde berichtenuitwisseling van de eerste generatie
#(4+L+NN) - #(5+L+NN)	2	„XX XXh”	Verwerkingsstatus van het onbeveiligde APDU-antwoord — facultatief voor beveiligde berichtenuitwisseling van de eerste generatie
#(6+L+NN)	1	„8Eh”	TCC: label voor cryptografische controlesom
#(7+L+NN)	1	„XXh”	LCC: lengte van volgende cryptografische controlesom „04h” voor beveiligde berichtenuitwisseling van de eerste generatie (zie aanhangsel 11, deel A) „08h”, „0Ch” of „10h” afhankelijk van de AES-sleutel-lengte voor beveiligde berichtenuitwisseling van de tweede generatie (zie aanhangsel 11, deel B)

Byte	Lengte	Waarde	Omschrijving
$\#(8+L+NN) - \#(7+M+L+NN)$	M	„XX..XXh”	Cryptografische controlesom
SW	2	„XXXXh”	Statuswoorden (SW1, SW2)”

ii) in punt TCS_46 wordt de tabel vervangen door:

„Byte	Lengte	Waarde	Omschrijving
#1	1	„87h”	T _{PI CG} : label voor gecodeerde gegevens (cryptogram)
#2	L	„MMh” of „81 MMh”	L _{PI CG} : lengte van teruggezonden gecodeerde gegevens (afwijkend van de originele Le van het commando wegens padding) L is 2 bytes indien LPI CG > 127 bytes.
$\#(2+L)-\#(1+L+MM)$	MM	„01XX..XXh”	Gecodeerde gegevens: paddingindicator en cryptogram
$\#(2+L+MM)$	1	„99h”	Label voor verwerkingsstatus (SW1-SW2) — facultatief voor beveiligde berichtenuitwisseling van de eerste generatie
$\#(3+L+MM)$	1	„02h”	Lengte van verwerkingsstatus — facultatief voor beveiligde berichtenuitwisseling van de eerste generatie
$\#(4+L+MM) - \#(5+L+MM)$	2	„XX XXh”	Verwerkingsstatus van het onbeveiligde APDU-antwoord — facultatief voor beveiligde berichtenuitwisseling van de eerste generatie
$\#(6+L+MM)$	1	„8Eh”	TCC: label voor cryptografische controlesom
$\#(7+L+MM)$	1	„XXh”	LCC: lengte van volgende cryptografische controlesom „04h” voor beveiligde berichtenuitwisseling van de eerste generatie (zie aanhangsel 11, deel A) „08h”, „0Ch” of „10h” afhankelijk van de AES-sleutel-lengte voor beveiligde berichtenuitwisseling van de tweede generatie (zie aanhangsel 11, deel B)
$\#(8+L+MM)-\#(7+N+L+MM)$	N	„XX..XXh”	Cryptografische controlesom
SW	2	„XXXXh”	Statuswoorden (SW1, SW2)”

h) in punt 3.5.2.2 wordt het zesde streepje van punt TCS_50 vervangen door:

„— Indien binnen de bestandsattributen een integriteitsfout wordt ontdekt, moet de kaart het bestand als beschadigd en verloren beschouwen; de teruggezonden verwerkingsstatus is „6400” of „6500”.”;

i) in punt 3.5.2.3 wordt punt TCS_52 als volgt gewijzigd:

i) de laatste rij van de tabel wordt vervangen door:

„Le	1	„XXh”	Zoals gespecificeerd in ISO/IEC 7816-4”
-----	---	-------	---

ii) de volgende zin wordt toegevoegd:

„Als T=0 gaat de kaart ervan uit dat waarde Le = „00h” wanneer geen beveiligde berichtenuitwisseling wordt toegepast.

Als T = 1 is de teruggezonden verwerkingsstatus „6700” als Le=„01h”.”;

j) in punt 3.5.2.3 wordt het zesde streepje van punt TCS_53 vervangen door:

„— Indien binnen de bestandsattributen een integriteitsfout wordt ontdekt, moet de kaart het bestand als beschadigd en verloren beschouwen; de teruggezonden verwerkingsstatus is „6400” of „6500”.”;

k) in punt 3.5.3.2 wordt het zesde streepje van punt TCS_63 vervangen door:

„— Indien binnen de bestandsattributen een integriteitsfout wordt ontdekt, moet de kaart het bestand als beschadigd en verloren beschouwen; de teruggezonden verwerkingsstatus is „6400” of „6500”.”;

l) in punt 3.5.5 wordt punt TCS_72 vervangen door:

„TCS_72 De door de gebruiker ingevoerde pincode moet in ASCII gecodeerd zijn en rechts door de IFD worden opgevuld met „FFh”-bytes tot een lengte van 8 bytes (zie ook het gegevenstype WorkshopCardPIN in aanhangsel 1).”;

m) in punt 3.5.8 wordt punt TCS_95 vervangen door:

„TCS_95 Indien het INTERNAL AUTHENTICATE-commando succesvol is, wordt de lopende sessiesleutel van de eerste generatie (indien aanwezig) gewist en is die niet langer beschikbaar. Om een nieuwe sessiesleutel van de eerste generatie te krijgen, moet het EXTERNAL AUTHENTICATE-commando succesvol worden uitgevoerd voor het authenticatiemechanisme van de eerste generatie.

Opmerking: Voor sessiesleutels van de tweede generatie, zie aanhangsel 11, punten CSM_193 en CSM_195. Wanneer sessiesleutels van de tweede generatie zijn vastgesteld en de tachograafkaart het ondubbelzinnige commando INTERNAL AUTHENTICATE APDU ontvangt, wordt de sessie voor beveiligde berichtenuitwisseling van de tweede generatie afgebroken en worden de sessiesleutels van generatie 2 vernietigd.”;

n) in punt 3.5.9 wordt punt TCS_97 vervangen door:

„TCS_97 De commandovariant voor de wederzijdse authenticatie van VU-kaarten van de tweede generatie kan worden uitgevoerd in MF, DF Tachograaf en DF Tachograaf_G2 (zie ook TCS_34). Indien dit EXTERNAL AUTHENTICATE-commando van de tweede generatie succesvol is, wordt de lopende sessiesleutel van de eerste generatie (indien aanwezig) gewist en is die niet langer beschikbaar.

Opmerking: Voor sessiesleutels van de tweede generatie, zie aanhangsel 11, punten CSM_193 en CSM_195. Wanneer sessiesleutels van de tweede generatie zijn vastgesteld en de tachograafkaart het ondubbelzinnige commando EXTERNAL AUTHENTICATE APDU ontvangt, wordt de sessie voor beveiligde berichtenuitwisseling van de tweede generatie afgebroken en worden de sessiesleutels van de tweede generatie vernietigd.”;

- o) in punt 3.5.10 wordt de volgende rij toegevoegd aan de tabel in punt TCS_101:

„5 + L + 1	1	„00h”	Zoals gespecificeerd in ISO/IEC 7816-4”
------------	---	-------	---

- p) in punt 3.5.11.2.3 worden de volgende alinea's toegevoegd aan punt TCS_114:

„— Indien de currentAuthenticatedTime van de kaart valt na de datum waarop de geldigheid van geselecteerde openbare sleutel afloopt, wordt de verwerkingsstatus „6A88” teruggezonden.

Opmerking: In het geval van een commando MSE:SET AT for VU Authentication is de genoemde sleutel een openbare sleutel VU_MA. Voor zover beschikbaar in haar geheugen, stelt de kaart de openbare sleutel VU_MA die overeenstemt met de referentie van de certificaathouder (CHR) in het gegevensveld van het commando (de kaart kan openbare sleutels VU_MA identificeren aan de hand van het CHA-veld van het certificaat) in voor gebruik. Een kaart antwoordt alleen met „6A 88” op dit commando wanneer de openbare sleutel VU_Sign niet beschikbaar is of geen enkele openbare sleutel van de voertuigunit beschikbaar is. Zie aanhangsel 11 voor de definitie van het CHA-veld en aanhangsel 1 voor de definitie van het gegevenstype equipmentType.

In het geval een MSE:SET DST-commando dat verwijst naar een EQT (d.w.z. een VU of een kaart) wordt verzonden naar een controlekaart, is de genoemde sleutel volgens CSM_234 altijd een EQT_Sign-sleutel die moet worden gebruikt voor de verificatie van een digitale handtekening. Volgens figuur 13 in aanhangsel 11 slaat de controlekaart altijd de relevante openbare sleutel EQT_Sign op. In sommige gevallen is het mogelijk dat de controlekaart de overeenkomstige openbare sleutel EQT_MA opslaat. De controlekaart stelt altijd de openbare sleutel EQT_Sign in voor gebruik wanneer zij een MSE:SET DST-commando ontvangt.”;

- q) punt 3.5.13 wordt als volgt gewijzigd:

- i) punt TCS_121 wordt vervangen door:

„TCS_121 De tijdelijk opgeslagen hashwaarde wordt verwijderd indien een nieuwe hashwaarde wordt berekend met behulp van het PERFORM HASH of FILE-commando, indien een DF is geselecteerd en indien de tachograafkaart wordt teruggesteld.”;

- ii) punt TCS_123 wordt vervangen door:

„TCS_123 Tachograaftoepassingen van de tweede generatie ondersteunen het SHA-2-algoritme, SHA-256, SHA-384 of SHA-512, gespecificeerd aan de hand van de coderingssuite in aanhangsel 11, deel B, voor de handtekeningssleutel Card_Sign”;

- iii) de tabel in punt TCS_124 wordt vervangen door:

„Byte	Lengte	Waarde	Omschrijving
CLA	1	„80h”	CLA
INS	1	„2Ah”	Voer beveiligingsoperatie uit
P1	1	„90h”	Label: Hash
P2	1	„00h”	Algoritme impliciet bekend Voor tachograaftoepassingen van de eerste generatie: SHA-1 Voor tachograaftoepassingen van de tweede generatie: SHA-2-algoritme (SHA-256, SHA-384 of SHA-512), gedefinieerd aan de hand van de coderingssuite in aanhangsel 11, deel B, voor de handtekeningssleutel Card_Sign”

- r) punt 3.5.14 wordt als volgt gewijzigd:

de tekst onder de hoofding en tot punt TCS_126 wordt vervangen door:

„Dit commando wordt gebruikt om de digitale handtekening van een eerder berekende hashcode te berekenen (zie PERFORM HASH of FILE-commando in punt 3.5.13).

Alleen de bestuurders- en werkplaatskaart zijn vereist om dit commando te ondersteunen in DF Tachograaf en DF Tachograaf_G2.

Op andere soorten tachograafkaarten kan dit commando al dan niet worden geïmplementeerd. In het geval van tachograaftoepassingen van de tweede generatie hebben alleen de bestuurderskaart en de werkplaatskaart een handtekeningssleutel van de tweede generatie; andere kaarten kunnen het commando niet met succes uitvoeren en beëindigen het commando met een geschikte foutcode.

Dit commando kan al dan niet toegankelijk zijn in het stambestand (MF). Als het commando niet toegankelijk is in het MF, eindigt het met een passende foutcode.

Dit commando voldoet aan ISO/IEC 7816-8. Het gebruik van dit commando is beperkt vergeleken met de toepasselijke norm.”;

- s) punt 03.05.15 wordt als volgt gewijzigd:

- i) de tabel in punt TCS_133 wordt vervangen door:

„Byte	Lengte	Waarde	Omschrijving
CLA	1	„00h”	CLA
INS	1	„2Ah”	Voer beveiligingsoperatie uit
P1	1	„00h”	
P2	1	„A8h”	Label: gegevensveld bevat voor verificatie relevante DO's
Lc	1	„XXh”	Lengte Lc van het volgende gegevensveld
#6	1	„9Eh”	Label voor digitale handtekening
# 7 of #7-#8	L	„NNh” of „81 NNh”	Lengte van de digitale handtekening (L is 2 bytes als de digitale handtekening langer is dan 127 bytes): 128 bytes, gecodeerd overeenkomstig deel A van aanhangsel 11 voor tachograaftoepassingen van de eerste generatie. Afhankelijk van de geselecteerde elliptische kromme voor tachograaftoepassingen van de tweede generatie (zie deel B van aanhangsel 11).
#(7+L)-#(6+L+NN)	NN	„XX..XXh”	Inhoud van de digitale handtekening”

- ii) aan punt TCS_134 wordt het volgende streepje toegevoegd:

„— Indien de geselecteerde openbare sleutel (waarmee de digitale handtekening wordt geverifieerd) een CHA.LSB (CertificateHolderAuthorisation.equipmentType) heeft die niet geschikt is voor de verificatie van digitale handtekeningen overeenkomstig aanhangsel 11, wordt de verwerkingsstatus „6985” teruggezonden.”;

t) punt 03.05.16 wordt als volgt gewijzigd:

i) de volgende rij wordt aan de tabel van punt TCS_138 toegevoegd:

„5 + L + 1	1	„00h”	Zoals gespecificeerd in ISO/IEC 7816-4”
------------	---	-------	---

ii) aan punt TCS_139 wordt de volgende alinea toegevoegd:

„— „6985” geeft aan dat de tijdstempel van 4 byte in het gegevensveld van het commando vroeger is dan cardValidityBegin of later dan cardExpiryDate.”;

u) punt 4.2.2 wordt als volgt gewijzigd:

i) in de gegevensstructuur in punt TCS_154 worden de regels van DF Tachograph G2 tot EF CardMA_Certificate en de regels van EF GNSS_Places tot het einde van deze alinea vervangen door:

”

Bestand/gegevenselement	No of Records	Size (bytes)		Default Values
		Min	Max	
DF Tachograph G2		20268	40316	
EF Application Identification		17	17	
└ DriverCardApplicationIdentification		17	17	
└ typeOfTachographCardId		1	1	{00}
└ cardStructureVersion		2	2	{00 00}
└ noOfEventsPerType		1	1	{00}
└ noOfFaultsPerType		1	1	{00}
└ activityStructureLength		2	2	{00 00}
└ noOfCardVehicleRecords		2	2	{00 00}
└ noOfCardPlaceRecords		2	2	{00 00}
└ noOfGNSSADRecords		2	2	{00 00}
└ noOfSpecificConditionRecords		2	2	{00 00}
└ noOfCardVehicleUnitRecords		2	2	{00 00}
EF CardMA_Certificate		204	341	
...				
EF GNSS_Places		4538	6050	
└ GNSSContinuousDriving		4538	6050	
└ gnssADPointerNewestRecord		2	2	{00 00}
└ gnssAccumulatedDrivingRecords		4536	6048	
└ GNSSContinuousDrivingRecord	n ₈	18	18	
└ timeStamp		4	4	{00..00}
└ gnssPlaceRecord		14	14	
└ timeStamp		4	4	{00..00}
└ gnssAccuracy		1	1	{00}
└ geoCoordinates		6	6	{00..00}
└ vehicleOdometerValue		3	3	{00..00}

”

ii) in punt TCS_155 wordt het punt NoOfGNSSCDRecords van de tabel vervangen door:

„n ₈ ”	NoOfGNSSADRecords	252	336”
-------------------	-------------------	-----	------

v) in punt 4.3.1 wordt de tekst die overeenkomt met de afkorting SC4 in punt TCS_156 vervangen door:

„**SC4** Voor het READ BINARY-commando met even instructiebyte (INS):

(SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) OR

(SM-C-MAC-G2 AND SM-R-ENC-MAC-G2)

Voor het READ BINARY-commando met oneven instructiebyte (indien ondersteund): NEV”;

w) punt 4.3.2 wordt als volgt gewijzigd:

i) in de gegevensstructuur in punt TCS_162 worden de regels van DF Tachograph G2 tot EF CardMA_Certificate en de regels van EF Calibration tot extendedSealIdentifier en de regels van EF GNSS_Places tot vehicleOdometerValue vervangen door:

”

Bestand/gegevens­element	Records	Size (bytes)		Values
		Min	Max	
DF Tachograph_G2	1878	49787		
EF Application_Identification	19	19		
└ WorkshopCardApplicationIdentificatio	19	19		
└ typeOfTachographCardId	1	1	{00}	
└ cardStructureVersion	2	2	{00 00}	
└ noOfEventsPerType	1	1	{00}	
└ noOfFaultsPerType	1	1	{00}	
└ activityStructureLength	2	2	{00 00}	
└ noOfCardVehicleRecords	2	2	{00 00}	
└ noOfCardPlaceRecords	2	2	{00 00}	
└ noOfCalibrationRecords	2	2	{00 00}	
└ noOfGNSSADRecords	2	2	{00 00}	
└ noOfSpecificConditionRecords	2	2	{00 00}	
└ noOfCardVehicleUnitRecords	2	2	{00 00}	
EF CardMA_Certificate	204	341		
...				
EF Calibration	15668	45394		
└ WorkshopCardCalibrationData	15668	45394		
└ calibrationTotalNumber	2	2	{00 00}	
└ calibrationPointerNewestRecord	2	2	{00}	
└ calibrationRecords	15664	45390		
└ WorkshopCardCalibrationRecord	n ₅	178	178	
└ calibrationPurpose	1	1	{00}	
└ vehicleIdentificationNumber	17	17	{20..20}	
└ vehicleRegistration				
└ vehicleRegistrationNation	1	1	{00}	
└ vehicleRegistrationNumber	14	14	{00, 20..20}	
└ wVehicleCharacteristicConstant	2	2	{00 00}	
└ kConstantOfRecordingEquipment	2	2	{00 00}	
└ lTyreCircumference	2	2	{00 00}	
└ tyreSize	15	15	{20..20}	
└ authorisedSpeed	1	1	{00}	
└ oldOdometerValue	3	3	{00..00}	
└ newOdometerValue	3	3	{00..00}	
└ oldTimeValue	4	4	{00..00}	
└ newTimeValue	4	4	{00..00}	
└ nextCalibrationDate	4	4	{00..00}	
└ vuPartNumber	16	16	{20..20}	
└ vuSerialNumber	8	8	{00..00}	
└ sensorSerialNumber	8	8	{00..00}	
└ sensorGNSSSerialNumber	8	8	{00..00}	
└ rcmSerialNumber	8	8	{00..00}	
└ vuAbility	1	1	{00}	
└ sealDataCard	56	56		
└ noOfSealRecords	1	1	{00}	
└ SealRecords	55	55		
└ SealRecord	5	11	11	
└ equipmentType	1	1	{00}	
└ extendedSealIdentifier	10	10	{00..00}	

...

EF	GNSS_Places	326	434	
	└ GNSSContinuousDriving	326	434	
	└┐ gnssADPointerNewestRecord	2	2	{00 00}
	└┐ gnssAccumulatedDrivingRecords	324	432	
	└┐┐ GNSSContinuousDrivingRecord	n ₈	18	18
	└┐┐┐ timeStamp	4	4	{00..00}
	└┐┐┐ gnssPlaceRecord	14	14	
	└┐┐┐┐ timeStamp	4	4	{00..00}
	└┐┐┐┐ gnssAccuracy	1	1	{00}
	└┐┐┐┐ geoCoordinates	6	6	{00..00}
	└┐┐┐┐ vehicleOdometerValue	3	3	{00..00}

„

ii) punt NoOfGNSSCDRecords van de tabel in punt TCS_163 wordt vervangen door:

„n ₈	NoOfGNSSADRecords	18	24”
-----------------	-------------------	----	-----

31) in aanhangsel 3 wordt punt 2 als volgt gewijzigd:

- a) de volgende regel wordt ingevoegd na de regel met de pictogrammen „Plaats begin dagelijkse werkperiode” en „Plaats einde dagelijkse werkperiode”:

„ Positie na 3 uur cumulatieve rijtijd”;

- b) de pictogramcombinatie „Tijdafstelling (door werkplaats)” wordt vervangen door:

„ Tijdsconflict of tijdsafstelling (door werkplaats)”;

- c) de volgende pictogramcombinaties worden toegevoegd aan de lijst van voorvallen:

„ Ontbreken van plaatsbepalingsinformatie van de GNSS-ontvanger of fout in de communicatie met de externe GNSS-module;

„ Fout in de communicatie met het systeem voor communicatie op afstand”;

32) Aanhangsel 4 wordt als volgt gewijzigd:

- a) Punt 2 wordt als volgt gewijzigd:

- i) bloknummer 11.4 wordt vervangen door:

„11.4 Invoeren van de plaats waar een dagelijkse werkperiode begint en/of eindigt

pi = pictogram van begin-/eindlocatie, tijd, land, regio
 lengtegraad van de geregistreeerde positie
 breedtegraad van de geregistreeerde positie
 tijdstempel op het ogenblik dat de positie werd bepaald
 Odometer (kilometerteller)

pihh:mm Cou Reg
 lon ±DDD°MM.M'
 lat ± DD°MM.M'
 hh:mm
 x xxx xxx km”

ii) bloknummer 11.5 wordt vervangen door:

„11.5 Posities na 3 uur cumulatieve rijtijd

pi=positie na 3 uur cumulatieve rijtijd

lengtegraad van de geregistreerde

positie

breedtegraad van de geregistreerde positie

tijdstempel op het ogenblik dat de positie werd bepaald

Odometer (kilometerteller)

```

pihh:mm
lon ± DDD°MM.M'
lat ± DD°MM.M '
hh:mm
x xxx xxx km"

```

b) in punt 3.1 wordt positie 11.5 van het formaat van de dagelijkse afdruk vervangen door:

„11.5

Posities na 3 uur cumulatieve rijtijd, in chronologische volgorde”

c) in punt 3.2 wordt het formaat van de dagelijkse afdruk vervangen door:

„1	Datum en tijdstip waarop het document is afgedrukt
2	Soort afdruk
3	Identificatie van de kaarthouder (voor alle in de VU ingebrachte kaarten + GEN)
4	Identificatie van het voertuig (voertuig waarvan de afdruk wordt gemaakt)
5	VU-identificatie (VU waarvan de afdruk wordt gemaakt + GEN)
6	Laatste kalibrering van deze VU
7	Laatste controle van deze tachograaf
9	Begrenzer van de bestuurdersactiviteiten
10	Begrenzer van de lezer voor de bestuurder (lezer 1)
10a	„Niet verplicht”-toestand aan het begin van deze dag
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Activiteiten in chronologische volgorde (lezer voor de bestuurder)
10	Begrenzer van de lezer voor de bijrijder (lezer 2)
10a	„Niet verplicht”-toestand aan het begin van deze dag
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Activiteiten in chronologische volgorde (lezer voor de bijrijder)
11	Dagelijks overzicht begrenzer
11.1	Overzicht van perioden zonder kaart in lezer voor bestuurder
11.4	Ingevoerde plaatsen in chronologische volgorde
11.5	Posities na 3 uur cumulatieve rijtijd, in chronologische volgorde
11.7	Totaal van activiteiten
11.2	Overzicht van perioden zonder kaart in lezer voor bijrijder
11.4	Ingevoerde plaatsen in chronologische volgorde
11.5	Posities na 3 uur cumulatieve rijtijd, in chronologische volgorde

11.8	Totaal van activiteiten
11.3	Overzicht van activiteiten van een bestuurder, beide lezers inbegrepen
11.4	Door deze bestuurder ingevoerde plaatsen, in chronologische volgorde
11.5	Posities na 3 uur cumulatieve rijtijd, in chronologische volgorde
11.9	Totaal van activiteiten voor deze bestuurder
13.1	Begrenzer voorvallen/fouten
13.4	Voorval/fout-records (laatste 5 opgeslagen of lopende voorvallen of fouten in de VU)
22.1	Controleplaats
22.2	Handtekening van de controleur
22.3	Van tijd (ruimte voor een bestuurder zonder een kaart om aan te geven
22.4	Tot tijd welke perioden voor hem relevant zijn)
22.5	Handtekening van de bestuurder"

d) in punt 3.7 wordt punt PRT_014 vervangen door:

„PRT_014 De afdruk van de geschiedenis van ingebrachte kaarten moet in overeenstemming zijn met onderstaande opmaak:

1	Datum en tijdstip waarop het document is afgedrukt
2	Soort afdruk
3	Identificatie van de kaarthouder (voor alle in de VU ingebrachte kaarten)
23	Laatste in de VU ingebrachte kaart
23.1	Ingebrachte kaarten (tot 88 records)
12.3	Begrenzer van fouten"

33) Aanhangsel 7 wordt als volgt gewijzigd:

a) punt 1.1 wordt vervangen door:

„1.1. Toepassingsgebied

Gegevens kunnen naar een ESM worden gedownload:

- uit een voertuigeenheid (VU), door met de VU verbonden intelligente toepassingsgerichte apparatuur (IDE),
- vanaf een tachograafkaart door een met een kaartinterface-inrichting (IFD) uitgeruste IDE;
- vanaf een tachograafkaart via een voertuigunit door een met de VU verbonden IDE.

Om de authenticiteit en integriteit van de overgedragen, op een ESM opgeslagen gegevens te kunnen verifiëren, worden gegevens gedownload met een toegevoegde handtekening overeenkomstig de algemene beveiligingsmechanismen van aanhangsel 11. De identificatie van het bronapparaat (VU of kaart) en de beveiligingscertificaten (lidstaat en apparaat) worden ook gedownload. De controleur van de gegevens moet zelf een betrouwbare Europese openbare sleutel in zijn bezit hebben.

Gegevens die worden gedownload van een VU worden ondertekend overeenkomstig aanhangsel 11 (Algemene beveiligingsmechanismen), deel B (Tachograafsystemen van de tweede generatie), behalve wanneer de controle op de bestuurder wordt uitgevoerd door een controleautoriteit van buiten de EU, waarbij gebruik wordt gemaakt van een controlekaart van de eerste generatie; in dat geval worden de gegevens ondertekend overeenkomstig aanhangsel 11 (Algemene beveiligingsmechanismen), deel A (Tachograafsystemen van de eerste generatie), zoals vereist uit hoofde van punt MIG_015 van aanhangsel 15 (Migratie).

In dit aanhangsel worden dus twee types van gegevensdownload van de VU gespecificeerd:

- gegevensdownloads van VU's van de tweede generatie, met de gegevensstructuur van de tweede generatie, ondertekend overeenkomstig aanhangsel 11 (Algemene beveiligingsmechanismen), deel B,
- gegevensdownloads van VU's van de eerste generatie, met de gegevensstructuur van de eerste generatie, ondertekend overeenkomstig aanhangsel 11 (Algemene beveiligingsmechanismen), deel A.

Naar analogie hiermee bestaan er ook twee soorten gegevensdownload van bestuurderskaarten van de tweede generatie die in een VU worden ingebracht, zoals gespecificeerd in punten 3 en 4 van dit aanhangsel.”;

b) punt 2.2.2 wordt als volgt gewijzigd:

i) de tabel wordt vervangen door:

„Berichtstructuur		Max. 4 bytes Header				Max. 255 bytes Gegevens		1 byte Controlesom
IDE ->	<- VU	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	CS
Start Communication Request		81	EE	F0		81		E0
Positive Response Start Communication		80	F0	EE	03	C1		9B
Start Diagnostic Session Request		80	EE	F0	02	10	81	F1
Positive Response Start Diagnostic		80	F0	EE	02	50	81	31
Link Control Service								
Verify Baud Rate (stage 1)								
9 600 Bd		80	EE	F0	04	87		EC
19 200 Bd		80	EE	F0	04	87		ED
38 400 Bd		80	EE	F0	04	87		EE
57 600 Bd		80	EE	F0	04	87		EF
115 200 Bd		80	EE	F0	04	87		F0
Positive Response Verify Baud Rate		80	F0	EE	02	C7		28
Transition Baud Rate (stage 2)		80	EE	F0	03	87		ED
Request Upload		80	EE	F0	0A	35		99
Positive Response Request Upload		80	F0	EE	03	75		D5
Transfer Data Request								
Overview		80	EE	F0	02	36	01 or 21	97
Activities		80	EE	F0	06	36	02 or 22	CS
Events & Faults		80	EE	F0	02	36	03 or 23	99
Detailed Speed		80	EE	F0	02	36	04 or 24	9A
Technical Data		80	EE	F0	02	36	05 or 25	9B
Card download		80	EE	F0	02	36	06	CS

Berichtstructuur		Max. 4 bytes Header				Max. 255 bytes Gegevens			1 byte Controlesom
IDE ->	<- VU	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	GEGEVENS	CS
Positive Response Transfer Data		80	F0	EE	Len	76	TREP	Data	CS
Request Transfer Exit		80	EE	F0	01	37			96
Positive Response Request Transfer Exit		80	F0	EE	01	77		D6	
Stop Communication Request		80	EE	F0	01	82		E1	
Positive Response Stop Communication		80	F0	EE	01	C2		21	
Acknowledge sub message		80	EE	F0	Len	83		Data	CS
Negative responses									
General reject		80	F0	EE	03	7F	Sid Req	10	CS
Service not supported		80	F0	EE	03	7F	Sid Req	11	CS
Sub function not supported		80	F0	EE	03	7F	Sid Req	12	CS
Incorrect Message Length		80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct or Request sequence error		80	F0	EE	03	7F	Sid Req	22	CS
Request out of range		80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted		80	F0	EE	03	7F	Sid Req	50	CS
Response pending		80	F0	EE	03	7F	Sid Req	78	CS
Data not available		80	F0	EE	03	7F	Sid Req	FA	CS"

ii) de volgende streepjes worden toegevoegd aan de opmerkingen na de tabel:

„— TRTP 21 tot en met 25 worden gebruikt voor gegevensdownloadverzoeken van VU's van de tweede generatie, TRTP 01 tot en met 05 worden gebruikt voor gegevensdownloadverzoeken van VU's van de eerste generatie, die alleen door de VU kunnen worden aanvaard wanneer de bestuurderscontrole wordt uitgevoerd door een controleautoriteit van buiten de EU, waarbij gebruik wordt gemaakt van een controlekaart van de eerste generatie.

— TRTP 11 tot en met 19 en 31 tot en met 39 zijn voorbehouden voor fabrikantsspecifieke downloadverzoeken.”;

c) punt 2.2.2.9 wordt als volgt gewijzigd:

i) punt DDP_011 wordt vervangen door:

„DDP_011 Het Transfer Data Request wordt door de IDE gezonden om de soort over te brengen gegevens mee te delen aan de VU. Een Transfer Request Parameter (TRTP) van één byte geeft de soort overdracht aan.

Er zijn zes soorten gegevensoverdracht. Voor gegevensdownloads uit VU kunnen twee verschillende TRTP-waarden worden gebruikt voor elk type overdracht.

Type gegevensoverdracht	TRTP-waarden voor gegevensdownloads van VU's van de eerste generatie	TRTP-waarden voor gegevensdownloads van VU's van de eerste generatie
Overview	01	21
Activiteiten van een gespecificeerde datum	02	22
Voorvallen en fouten	03	23
Gedetailleerde snelheid	04	24
Technische gegevens	05	25

Type gegevensoverdracht	TRTP-waarde
Card download	06"

ii) punt DDP_054 wordt vervangen door:

„DDP_054 De IDE is verplicht gedurende een overdrachtsessie de overdracht van overzichtsgegevens (TRTP 01 of 21) aan te vragen, omdat alleen dit garandeert dat de VU-certificaten in het gedownloade bestand worden geregistreerd (en verificatie van de digitale handtekening mogelijk maakt).

In het tweede geval (TRTP 02 of 22) bevat het bericht Transfer Data Request de aanwijzing van de te downloaden kalenderdag (TimeReal opmaak).”;

d) in punt 2.2.2.10 wordt punt DDP_055 vervangen door:

„DDP_055 In het eerste geval (TREP 01 of 21) zendt de VU gegevens waarmee de operator van de IDE kan kiezen welke gegevens hij verder wil overdragen. De in dit bericht opgenomen informatie bestaat uit:

- veiligheidscertificaten,
- identificatie van het voertuig,
- huidige datum en tijd van de VU,
- min. en max. opvraagbare datum (VU-gegevens),
- indicatie van in de VU aanwezige kaarten,
- vorige download naar een bedrijf,
- bedrijfsvergrendelingen,
- vorige controles.”;

e) in punt 2.2.2.16 wordt het laatste streepje van punt DDP_018 vervangen door:

„— FA-gegevens niet beschikbaar

Het gegevensobject van een verzoek om gegevensoverdracht is niet beschikbaar in de VU (omdat er bijv. geen kaart is ingebracht, verzoek om download van gegevens van een VU van de eerste generatie buiten het kader van een bestuurderscontrole door een controleautoriteit van buiten de EU).”;

f) punt 2.2.6.1 wordt als volgt gewijzigd:

i) de eerste alinea van punt DDP_029 wordt vervangen door:

„Het gegevensveld van het bericht „Positive Response Transfer Data Overview” moet de onderstaande gegevens in de onderstaande volgorde onder het SID 76 Hex, het TREP 01 of 21 Hex en de passende splitsing en telling van de subberichten verstrekken.”;

ii) de hoofding „Gegevensstructuur 1e generatie” wordt vervangen door:

„Gegevensstructuur 1e generatie (TREP 01 Hex)”;

iii) de hoofding „Gegevensstructuur 2e generatie” wordt vervangen door:

„Gegevensstructuur 2e generatie (TREP 21 Hex)”;

g) punt 2.2.6.2 wordt als volgt gewijzigd:

i) de eerste alinea van punt DDP_030 wordt vervangen door:

„Het gegevensveld van het bericht „Positive Response Transfer Data Activities” moet de onderstaande gegevens in de onderstaande volgorde onder het SID 76 Hex, het TREP 02 of 22 Hex en de passende splitsing en telling van de subberichten verstrekken.”;

ii) de hoofding „Gegevensstructuur 1e generatie” wordt vervangen door:

„Gegevensstructuur 1e generatie (TREP 02 Hex)”;

iii) de hoofding „Gegevensstructuur 2e generatie” wordt vervangen door:

„Gegevensstructuur 2e generatie (TREP 22 Hex)”;

iv) punt VuGNSSCDRecordArray onder hoofding „Gegevensstructuur 2e generatie (TREP 22 Hex)” wordt vervangen door:

„VuGNSSADRecordArray

GNSS-posities van het voertuig wanneer de cumulatieve rijtijd van het voertuig een veelvoud van drie uur bereikt. Indien het segment leeg is, wordt alleen een beginlabel van een reeks met noOfRecords = 0 verzonden.”

h) punt 2.2.6.3 wordt als volgt gewijzigd:

i) de eerste alinea van punt DDP_031 wordt vervangen door:

„Het gegevensveld van het bericht „Positive Response Transfer Data Events and Faults” moet de onderstaande gegevens in de onderstaande volgorde onder het SID 76 Hex, het TREP 03 of 23 Hex en de passende splitsing en telling van de subberichten verstrekken.”;

ii) de hoofding „Gegevensstructuur 1e generatie” wordt vervangen door:

„Gegevensstructuur 1e generatie (TREP 03 Hex)”;

iii) de hoofding „Gegevensstructuur 2e generatie” wordt vervangen door:

„Gegevensstructuur 2e generatie (TREP 23 Hex)”;

iv) het punt VuTimeAdjustmentGNSSRecordArray onder hoofding „Gegevensstructuur 2e generatie (TREP 23 Hex)” wordt geschrapt;

i) punt 2.2.6.4 wordt als volgt gewijzigd:

i) de eerste alinea van punt DDP_032 wordt vervangen door:

„Het gegevensveld van het bericht „Positive Response Transfer Data Detailed Speed” moet de onderstaande gegevens in de onderstaande volgorde onder het SID 76 Hex, het TREP 04 of 24 Hex en de passende splitsing en telling van de subberichten verstrekken.”;

ii) de hoofding „Gegevensstructuur 1e generatie” wordt vervangen door:

„Gegevensstructuur 1e generatie (TREP 04)”;

iii) de hoofding „Gegevensstructuur 2e generatie” wordt vervangen door:

„Gegevensstructuur 2e generatie (TREP 24)”;

j) punt 2.2.6.5 wordt als volgt gewijzigd:

i) de eerste alinea van punt DDP_033 wordt vervangen door:

„Het gegevensveld van het bericht „Positive Response Transfer Data Technical Data” moet de onderstaande gegevens in de onderstaande volgorde onder het SID 76 Hex, het TREP 05 of 25 Hex en de passende splitsing en telling van de subberichten verstrekken:”;

ii) de hoofding „Gegevensstructuur 1e generatie” wordt vervangen door:

„Gegevensstructuur 1e generatie (TREP 05)”;

iii) de hoofding „Gegevensstructuur 2e generatie” wordt vervangen door:

„Gegevensstructuur 2e generatie (TREP 25)”;

k) in punt 3.3 wordt punt DDP_035 vervangen door:

„DDP_035 De download van een tachograafkaart omvat de onderstaande stappen:

- Download van de algemene informatie van de kaart naar de ICC en IC van het EF. Deze informatie is facultatief en wordt niet met een digitale handtekening beveiligd.
- (voor tachograafkaarten van de eerste en tweede generatie) Download EF's in Tachograph DF
- Download het Card_Certificate en CA_Certificate van het EF. Deze informatie wordt niet met een digitale handtekening beveiligd.

Het is verplicht om deze bestanden voor elke sessie te downloaden.

- Download van de andere toepassingsgegevens van de EF's (in Tachograph DF) met uitzondering van EF Card_Download Deze informatie wordt beveiligd met een digitale handtekening, overeenkomstig aanhangsel 11 „Algemene beveiligingsmechanismen”, deel A.
- Het is verplicht om ten minste de Application_Identification en Identification van het EF voor elke sessie te downloaden.
- Bij de download van een bestuurderskaart is het ook verplicht de onderstaande EF's over te brengen:
 - Events_Data,
 - Faults_Data,

- Driver_Activity_Data,
 - Vehicles_Used,
 - Places,
 - Control_Activity_Data,
 - Specific_Conditions,
- (alleen voor tachograafkaarten van de tweede generatie) Download van de EF's in Tachograph_G2 DF DF, behalve wanneer een in een VU ingebrachte bestuurderskaart wordt gedownload tijdens een bestuurderscontrole door een controleautoriteit van buiten de EU, waarbij gebruik wordt gemaakt van een controlekaart van de eerste generatie:
- Download van het CardSignCertificate, CA_Certificate and Link_Certificate (indien aanwezig) van de EF's. Deze informatie wordt niet met een digitale handtekening beveiligd.

Het is verplicht om deze bestanden voor elke sessie te downloaden.

- Download van de andere toepassingsgegevens van de EF's (in Tachograph_G2 DF) met uitzondering van Card_Download van het EF. Deze informatie wordt beveiligd met een digitale handtekening, overeenkomstig aanhangsel 11 „Algemene beveiligings-mechanismen”, deel B.
- Het is verplicht om ten minste de Application_Identification en Identification van het EF voor elke sessie te downloaden.
- Bij de download van een bestuurderskaart is het ook verplicht de onderstaande EF's over te brengen:

- Events_Data,
 - Faults_Data,
 - Driver_Activity_Data,
 - Vehicles_Used,
 - Places,
 - Control_Activity_Data,
 - Specific_Conditions,
 - VehicleUnits_Used,
 - GNSS Places.
- Bij de download van een bestuurderskaart moet de datum van LastCardDownload worden aangepast in Card_Download van het EF, in de Tachograph en, voor zover van toepassing, in de DF's van Tachograph_G2
- Bij de download van een werkplaatskaart moet de kalibreringsteller worden gereset in Card_Download in de Tachograph en, voor zover van toepassing, in de DF's van Tachograph_G2

- Bij de download van een werkplaatskaart mag de `Sensor_Installation_Data` in de `Tachograph` en, voor zover van toepassing, de DF's van `Tachograph_G2` niet worden gedownload.”;

l) in punt 3.3.2 wordt de eerste alinea van punt DDP_037 vervangen door:

„De sequentie voor download van de chipkaart, IC, `Card_Certificate` (of `CardSignCertificate` voor DF `Tachograph_G2`), `CA_Certificate` en `Link_Certificate` (uitsluitend voor DF `Tachograph_G2`) van het EF is als volgt:”;

m) in punt 3.3.3 wordt de tabel vervangen door:

„Kaart	Richting	IDE / IFD	Betekenis/Opmmerkingen
	⇐	Select file	
OK	⇒		
	⇐	Perform Hash of File	— Berekent de hashwaarde van de inhoud van de gegevens van het geselecteerde bestand met het voorgeschreven hashalgoritme overeenkomstig aanhangsel 11, deel A of B. Dit commando is geen ISO-commando.
Bereken Hash of File en sla hashwaarde tijdelijk op			
OK	⇒		
	⇐	Read Binary	Indien het bestand meer gegevens bevat dan het buffergeheugen van de lezer of van de kaart kan bewaren, moet het commando worden herhaald tot het volledige bestand is gelezen.
Bestandsgegevens OK	⇒	Sla ontvangen gegevens in ESM op	Overeenkomstig 3.4 Data storage format
	⇐	PSO: Compute Digital Signature	
Voer beveiligingsoperatie „Bereken digitale handtekening” uit met de tijdelijk opgeslagen hashwaarde			
Handtekening OK	⇒	Koppel gegevens aan de vorige in het ESM opgeslagen gegevens	Overeenkomstig 3.4 Data storage format”

n) in punt 3.4.2 wordt punt DDP_046 vervangen door:

„DDP_046 Een handtekening moet als het volgende TLV-object worden opgeslagen, onmiddellijk na het TLV-object dat de gegevens van het bestand bevat.

Definitie	Betekenis	Lengte
FID (2 Bytes) „00”	Tag voor EF (FID) in de Tachograph of voor gemeenschappelijke informatie van de kaart	3 bytes
FID (2 Bytes) „01”	Label voor handtekening van EF (FID) in de Tachograph	3 bytes
FID (2 Bytes) „02”	Label voor EF (FID) in de Tachograph_G2 DF	3 bytes
FID (2 Bytes) „03”	Label voor handtekening van EF (FID) in de Tachograph_G2 DF	3 bytes
xx xx	Lengte van waardeveld	2 bytes

Voorbeeld van gegevens in een naar een ESM overgedragen bestand:

Label	Lengte	Waarde
00 02 00	00 11	— Gegevens van EF ICC
C1 00 00	00 C2	— Gegevens van EF Card_Certificate
		— ...
05 05 00	0A 2E	Gegevens van EF Vehicles_Used (in de Tachograph DF)
05 05 01	00 80	Handtekening van EF Vehicles_Used (in de Tachograph DF)
05 05 02	0A 2E	Gegevens van EF Vehicles_Used in de Tachograph_G2 DF
05 05 03	xx xx	Handtekening van EF Vehicles_Used in de Tachograph_G2 DF

o) in punt 4 wordt punt DDP_049 vervangen door:

„DDP_049 Bestuurderskaarten van de eerste generatie: de gegevens moeten worden gedownload door gebruik te maken van het downloadprotocol van de eerste generatie, en de gedownloade gegevens moeten hetzelfde formaat hebben als gegevens die zijn gedownload van een voertuigunit van de eerste generatie.

Bestuurderskaarten van de tweede generatie: de VU moet vervolgens overeenkomstig het in punt 3 gedefinieerde kaartdownloadprotocol de hele kaart downloaden, bestand voor bestand, en alle van de kaart ontvangen gegevens in de vereiste TLV-bestandsopmaak (zie 3.4.2) en ingekapseld in een „Positive Response Transfer Data”-bericht naar de IDE zenden.”.

34) In punt 2 van aanhangsel 8 wordt de alinea onder hoofding „Referenties” vervangen door:

„ISO 14230-2: Road Vehicles — Diagnostic Systems — Keyword Protocol 2000 — Part 2: Data Link Layer.

Eerste editie: 1999.”.

35) Aanhangsel 9 wordt als volgt gewijzigd:

a) in de inhoudsopgave wordt punt 6 vervangen door:

„6 TESTS VAN DE EXTERNE APPARATUUR VOOR COMMUNICATIE OP AFSTAND”;

b) het eerste streepje van punt 1.1 wordt vervangen door:

„— een **veiligheidscertificering** volgens de specificaties van de gemeenschappelijke criteria en met een veiligheidsdoelstelling die volledig voldoet aan aanhangsel 10 van deze bijlage,”;

c) in punt 2 wordt tabel van de functietests van de voertuigunit vervangen door:

„Nr.	Test	Omschrijving	Gerelateerde voorschriften
1	Administratieve controle		
1.1	Documentatie	Juistheid van de documentatie	
1.2	Testresultaten van de fabrikant	Resultaten van de tijdens integratie door de fabrikant uitgevoerde test. Papierdemonstraties.	88, 89, 91
2	Visuele inspectie		
2.1	Naleving van de documentatie		
2.2	Identificatie/opschriften		224 t.e.m. 226
2.3	Materiaal		219 t.e.m. 223
2.4	Verzegeling		398, 401 t.e.m. 405
2.5	Externe interfaces		
3	Functietests		
3.1	Aanwezige functies		02, 03, 04, 05, 07, 382
3.2	Werkingsmodi		09 t.e.m. 11*, 134, 135
3.3	Functies en gegevenstoegangsrechten		12* 13*, 382, 383, 386 t.e.m. 389
3.4	Controle op het inbrengen en uitnemen van kaarten		15, 16, 17, 18, 19*, 20*, 134
3.5	Meting van snelheid en afgelegde afstand		21 t.e.m. 31
3.6	Tijdmeting (test uitgevoerd bij 20 °C)		38 t.e.m. 43
3.7	Controle op activiteiten van de bestuurder		44 t.e.m. 53, 134
3.8	Controle op de status van de bestuurders		54, 55, 134
3.9	Handmatige invoer		56 t.e.m. 62
3.10	Beheer van bedrijfsvergrendelingen		63 t.e.m. 68
3.11	Bewaking van controleactiviteiten		69, 70
3.12	Detectie van voorvallen en/of fouten		71 t.e.m. 88, 134

Nr.	Test	Omschrijving	Gerelateerde voorschriften
3.13	Identificatiegegevens van de uitrusting		93*, 94*, 97, 100
3.14	Gegevens over inbrengen en uitnemen van de bestuurderskaart		102* t.e.m. 104*
3.15	Gegevens over activiteiten van de bestuurder		105* t.e.m. 107*
3.16	Plaats- en positiegegevens		108* t.e.m. 112*
3.17	Gegevens over de kilometerstand		113* t.e.m. 115*
3.18	Gedetailleerde snelheidsgegevens		116*
3.19	Gegevens over voorvallen		117*
3.20	Foutgegevens		118*
3.21	Kalibreringsgegevens		119* t.e.m. 121*
3.22	Tijdafstellingsgegevens		124*, 125*
3.23	Gegevens over controleactiviteiten		126*, 127*
3.24	Gegevens over bedrijfsvergrendelingen		128*
3.25	Gegevens over downloadactiviteiten		129*
3.26	Gegevens over specifieke omstandigheden		130*, 131*
3.27	Registreren en opslaan op tachograafkaarten		136, 137, 138*, 139*, 141*, 142, 143 144, 145, 146*, 147*, 148*, 149, 150
3.28	Weergeven		90, 134, 151 t.e.m. 168 PIC_001, DIS_001
3.29	Afdrukken		90, 134, 169 t.e.m. 181, PIC_001, PRT_001 t.e.m. PRT_014
3.30	Waarschuwingssignalen		134, 182 t.e.m. 191, PIC_001
3.31	Doorsturen van gegevens naar externe media		90, 134, 192 t.e.m. 196
3.32	Communicatie op afstand voor gerichte wegcontroles		197 tot en met 199
3.33	Uitvoergegevens naar aanvullende externe apparaten		200, 201
3.34	Kalibrering		202 t.e.m. 206*, 383, 384, 386 t.e.m. 391
3.35	Kalibreringscontrole langs de weg		207 tot en met 209
3.36	Tijdafstelling		210 t.e.m. 212*
3.37	Geen interferentie van aanvullende functies		06, 425

Nr.	Test	Omschrijving	Gerelateerde voorschriften
3.38	Motion sensor interface		02, 122
3.39	Externe GNSS-module		03, 123
3.40	Verifieer of de voertuigunit (VU) de door de VU-fabrikant bepaalde voorvallen en/of fouten detecteert, registreert en opslaat, wanneer een gekoppelde bewegingssensor reageert op een magnetisch veld dat de bewegingsdetectie van het voertuig stoort		217
3.41	Codereeks en gestandaardiseerde domeinparameters		CSM_48, CSM_50
4	Milieutests		
4.1	Temperatuur	Controleer de functionaliteit aan de hand van: ISO 16750-4, punt 5.1.1.2: test bij lage temperatuur in ingeschakelde toestand (72 uur bij -20°C) Deze test berust op IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold. Test overeenkomstig ISO 16750-4: punt 5.1.2.2: test bij hoge temperatuur in ingeschakelde toestand (72 uur bij $+70^{\circ}\text{C}$) Deze test berust op IEC 60068-2-2: Basic environmental testing procedures Deel 2: testen; Tests B: Dry heat Test overeenkomstig ISO 16750-4: punt 5.3.2: snelle temperatuurwisselingen binnen de voorgeschreven overgangsduur (20 wisselingen met een temperatuur variërend van -20°C tot $+70^{\circ}\text{C}$, bij een verblijf gedurende 2 uur bij de laagste en de hoogste temperatuur) Een kleiner aantal tests (zoals gedefinieerd in punt 3 van deze tabel) kan worden uitgevoerd bij de laagste temperatuur, bij de hoogste temperatuur en tijdens de temperatuurwisselingen	213
4.2	Vochtigheid	Controleer de bestandheid van de voertuigunit tegen cyclische vochtigheid (warmteproef) aan de hand van IEC 60068-2-30, test Db, zes cycli van 24 uur, elke temperatuur variërend van $+25^{\circ}\text{C}$ tot $+55^{\circ}\text{C}$ en een relatieve vochtigheid van 97 % bij $+25^{\circ}\text{C}$ en gelijk aan 93 % bij $+55^{\circ}\text{C}$	214
4.3	Vibratie en mechanische schokken	1. Sinusoïdale vibraties Controleer of de voertuigunit bestand is tegen sinusoïdale vibraties met de onderstaande kenmerken: constante verplaatsing tussen 5 en 11 Hz: 10 mm piek constante acceleratie tussen 11 en 300 Hz: 5 g Dit voorschrift wordt gecontroleerd aan de hand van IEC 60068-2-6, test Fc, met een minimale testduur van drie keer 12 uur (12 uur per as) Apparatuur die zich in de aparte bestuurderscabine bevindt, moet volgens ISO 16750-3 niet op sinusoïdale vibraties worden getest	219

Nr.	Test	Omschrijving	Gerelateerde voorschriften
		2. Willekeurige vibraties Test overeenkomstig ISO 16750-3: punt 4.1.2.8: test VIII: bedrijfsvoertuigen met aparte bestuurderscabine Test op willekeurige vibraties, 10...2 000 Hz, effectieve waarde in verticale richting 21,3 m/s², effectieve waarde in lengterichting 11,8 m/s², effectieve waarde in zijwaartse richting 13,1 m/s², drie assen, 32 uur per as, inclusief temperatuurwisseling tussen – 20 °C en + 70 °C Deze test berust op IEC 60068-2-64: Environmental testing - Part 2-64: Tests - Test Fh: Vibration, broadband random and guidance. 3. Schokken Mechanische schok met halve-sinuspuls van 3 g overeenkomstig ISO 16750 De bovengenoemde tests worden op twee verschillende modellen van de te testen apparatuur uitgevoerd	
4.4	Bescherming tegen water en vreemde lichamen	Test overeenkomstig ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (gelijkblijvende parameters); beveiligingsindex ten minste IP 40	220, 221
4.5	Overspanningsbeveiliging	Controleer of de voertuigunit bestand is tegen een stroomvoorziening van: 24V-uitvoeringen: 34 V bij + 40 °C 1 uur 12 V-uitvoeringen: 17 V bij + 40 °C 1 uur (ISO 16750-2)	216
4.6	Beveiliging tegen ompolen	Controleer of de voertuigunit bestand is tegen een omkering in de stroomvoorziening (ISO 16750-2)	216
4.7	Kortsluitbeveiliging	Controleer of de invoer-/uitvoersignalen beveiligd zijn tegen kortsluiting in de stroomvoorziening en tegen aardsluiting (ISO 16750-2)	216
5	EMC-tests		
5.1	Stralingsemissies en gevoeligheid	Overeenkomstig VN/ECE-reglement nr. 10	218
5.2	Elektrostatische ont-ladingen	Overeenkomstig ISO 10605:2008 + technische rectificatie 1:2010 + AMD 1:2014: ± 4 kV contactontlading en ± 8 kV luchtontlading	218

Nr.	Test	Omschrijving	Gerelateerde voorschriften
5.3	Transiënte geleidingsverschijnselen in de stroomvoorziening	Voor 24V-uitvoeringen: overeenkomstig ISO 7637-2 + VN/ECE-reglement nr. 10, herz. 3: puls 1a: $V_s = -450\text{ V}$, $R_i = 50\text{ ohms}$ puls 2 a: $V_s = +37\text{ V}$, $R_i = 2\text{ ohm}$ puls 2b: $V_s = +20\text{ V}$, $R_i = 0,05\text{ ohm}$ puls 3a: $V_s = -150\text{ V}$, $R_i = 50\text{ ohm}$ puls 3b: $V_s = +150\text{ V}$, $R_i = 50\text{ ohm}$ puls 4: $V_s = -16\text{ V}$, $V_a = -12\text{ V}$, $t_6 = 100\text{ ms}$ puls 5: $V_s = +120\text{ V}$, $R_i = 2,2\text{ ohm}$, $t_d = 250\text{ ms}$ Voor 12 V-uitvoeringen: overeenkomstig ISO 7637-1 + VN/ECE-reglement nr. 10, herz. 3: puls 1: $V_s = -75\text{ V}$, $R_i = 10\text{ ohm}$ puls 2 a: $V_s = +37\text{ V}$, $R_i = 2\text{ ohm}$ puls 2b: $V_s = +10\text{ V}$, $R_i = 0,05\text{ ohm}$ puls 3a: $V_s = -112\text{ V}$, $R_i = 50\text{ ohm}$ puls 3b: $V_s = +75\text{ V}$, $R_i = 50\text{ ohm}$ puls 4: $V_s = -6\text{ V}$, $V_a = -5\text{ V}$, $t_6 = 15\text{ ms}$ puls 5: $V_s = +65\text{ V}$, $R_i = 3\text{ ohm}$, $t_d = 100\text{ ms}$ Puls 5 moet alleen worden getest bij voertuigunits die in voertuigen worden geïnstalleerd waarvoor geen externe gewone beveiliging tegen een plotselinge spanningsverlaging geïmplementeerd is Wat betreft de voorstelwaarde voor spanningsverlaging: zie ISO 16750-2, vierde uitgave, punt 4.6.4	218"

d) punt 6 wordt vervangen door:

„6 TEST VAN DE EXTERNE APPARATUUR VOOR COMMUNICATIE OP AFSTAND

Nr.	Test	Omschrijving	Gerelateerde voorschriften
1.	Administratieve controle		
1.1	Documentatie	Juistheid van de documentatie	
2.	Visuele inspectie		
2.1	Naleving van de documentatie		
2.2	Identificatie/opschriften		225, 226
2.3	Materiaal		219 t.e.m. 223
3.	Functietests		
3.1	Communicatie op afstand voor gerichte wegcontroles		4, 197 tot en met 199

Nr.	Test	Omschrijving	Gerelateerde voorschriften
3.2	Registreren en opslaan in het geheugen		91
3.3	Communicatie met de voertuigunit		Aanhangsel 14 DSC_66 tot en met DSC_70, DSC_71 tot en met DSC_76
4.	Milieutests		
4.1	Temperatuur	Controleer de functionaliteit aan de hand van: ISO 16750-4, punt 5.1.1.2: test bij lage temperatuur in ingeschakelde toestand (72 uur bij – 20 °C) Deze test berust op IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold. Test overeenkomstig ISO 16750-4: punt 5.1.2.2: test bij hoge temperatuur in ingeschakelde toestand (72 uur bij + 70 °C) Deze test berust op IEC 60068-2-2: Basic environmental testing procedures Deel 2: testen; Tests B: Dry heat Test overeenkomstig ISO 16750-4: punt 5.3.2: snelle temperatuurwisselingen binnen de voorgeschreven overgangsduur (20 wisselingen met een temperatuur variërend van – 20 °C tot + 70 °C, bij een verblijf gedurende 1 uur bij de laagste en de hoogste temperatuur) Een kleiner aantal tests (zoals gedefinieerd in punt 3 van deze tabel) kan worden uitgevoerd bij de laagste temperatuur, bij de hoogste temperatuur en tijdens de temperatuurwisselingen	213
4.2	Bescherming tegen water en vreemde lichamen	Test overeenkomstig ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (beveiligingsindex ten minste IP 40)	220, 221
5	EMC-tests		
5.1	Stralingsemissies en gevoeligheid	Overeenkomstig VN/ECE-reglement nr. 10	218
5.2	Elektrostatische ontladingen	Overeenkomstig ISO 10605:2008 + technische rectificatie 1:2010 + AMD 1:2014: +/- 4 kV contact-ontlading en +/- 8 kV luchtontlading	218

Nr.	Test	Omschrijving	Gerelateerde voorschriften
5.3	Transiënte geleidingsverschijnselen in de stroomvoorziening	Voor 24V-uitvoeringen: overeenkomstig ISO 7637-2 + VN/ECE-reglement nr. 10, herz. 3: puls 1a: $V_s = -450\text{ V}$, $R_i = 50\text{ ohms}$ puls 2a: $V_s = +37\text{ V}$, $R_i = 2\text{ ohm}$ puls 2b: $V_s = +20\text{ V}$, $R_i = 0,05\text{ ohm}$ puls 3a: $V_s = -150\text{ V}$, $R_i = 50\text{ ohm}$ puls 3b: $V_s = +150\text{ V}$, $R_i = 50\text{ ohm}$ puls 4: $V_s = -16\text{ V}$, $V_a = -12\text{ V}$, $t_6 = 100\text{ ms}$ puls 5: $V_s = +120\text{ V}$, $R_i = 2,2\text{ ohm}$, $t_d = 250\text{ ms}$ Voor 12 V-uitvoeringen: overeenkomstig ISO 7637-1 + VN/ECE-reglement nr. 10, herz. 3: puls 1: $V_s = -75\text{ V}$, $R_i = 10\text{ ohm}$ puls 2a: $V_s = +37\text{ V}$, $R_i = 2\text{ ohm}$ puls 2b: $V_s = +10\text{ V}$, $R_i = 0,05\text{ ohm}$ puls 3a: $V_s = -112\text{ V}$, $R_i = 50\text{ ohm}$ puls 3b: $V_s = +75\text{ V}$, $R_i = 50\text{ ohm}$ puls 4: $V_s = -6\text{ V}$, $V_a = -5\text{ V}$, $t_6 = 15\text{ ms}$ puls 5: $V_s = +65\text{ V}$, $R_i = 3\text{ ohm}$, $t_d = 100\text{ ms}$ Puls 5 moet alleen worden getest bij voertuigunits die in voertuigen worden geïnstalleerd waarvoor geen externe gewone beveiliging tegen een plotselinge spanningsverlaging geïmplementeerd is Wat betreft de voorstelwaarde voor spanningsverlaging: zie ISO 16750-2, vierde uitgave, punt 4.6.4	218"

e) de tabel met betrekking tot interoperabiliteitstests in punt 8 wordt vervangen door:

„Nr.	Test	Omschrijving
8.1 Tests van de interoperabiliteit tussen voertuigunits en tachograafkaarten		
1	Wederzijdse authenticatie	Controleer of de wederzijdse authenticatie tussen de voertuigunit en de tachograafkaart normaal functioneert.
2	Lees-/schrijftests	Voer een typisch functiescenario in de voertuigunit uit. Het scenario moet aan de te testen kaartsoort worden aangepast en schrijfp opdrachten in zoveel mogelijk hoofdbestanden (EF's) op de kaart bevatten. Controleer of alle corresponderende registraties correct zijn ingevoerd door gegevens van de voertuigunit over te brengen. Controleer of alle corresponderende registraties correct zijn ingevoerd door gegevens van de kaart over te brengen. Controleer of alle corresponderende registraties correct kunnen worden gelezen door middel van een dagelijkse afdruk.

„Nr.	Test	Omschrijving
8.2 Tests van de interoperabiliteit tussen voertuigunits en bewegingssensoren		
1	Koppeling	Controleer of de koppelingsprocedure tussen de voertuigunit en de bewegingssensoren foutloos wordt uitgevoerd.
2	Activiteitstests	Voer een typisch activiteitsscenario op de bewegingssensor uit. Het scenario heeft betrekking op een normale activiteit waarbij zoveel mogelijk voorvallen en fouten worden gegenereerd. Controleer of alle corresponderende registraties correct zijn ingevoerd door gegevens van de voertuigunit over te brengen. Controleer of alle corresponderende registraties correct zijn ingevoerd door gegevens van de kaart over te brengen. Controleer of alle corresponderende registraties correct kunnen worden gelezen door middel van een dagelijkse afdruk.
8.3 Interoperabiliteitstests tussen voertuigunits en externe GNSS-modules (indien van toepassing)		
1	Wederzijdse authenticatie	Controleer of de wederzijdse authenticatie (verbindingsofbouw) tussen de voertuigunit en de externe GNSS-module normaal functioneert.
2	Activiteitstests	Voer een typisch activiteitsscenario uit op de externe GNSS-module. Het scenario heeft betrekking op een normale activiteit waarbij zoveel mogelijk voorvallen en fouten worden gegenereerd. Controleer of alle corresponderende registraties correct zijn ingevoerd door gegevens van de voertuigunit over te brengen. Controleer of alle corresponderende registraties correct zijn ingevoerd door gegevens van de kaart over te brengen. Controleer of alle corresponderende registraties correct kunnen worden gelezen door middel van een dagelijkse afdruk.”

36) Aanhangsel 11 wordt als volgt gewijzigd:

a) in punt 8.2.3 wordt punt CSM_49 vervangen door:

„CSM_49 Voertuigunits, tachograafkaarten en externe GNSS-modules ondersteunen de in [SHS] gespecificeerde algoritmen SHA-256, SHA-384 en SHA-512”;

b) in punt 9.1.2 wordt de eerste alinea van punt CSM_58 vervangen door:

„CSM_58 Telkens wanneer de ERCA een nieuw Europees basissleutelpaar genereert, maakt zij een verbindingscertificaat voor de nieuwe Europese openbare sleutel en ondertekent die met de vorige Europese particuliere sleutel. Het verbindingscertificaat is 17 jaar en 3 maand geldig. Dit wordt eveneens verduidelijkt in Figuur 1 onder 9.1.7.”;

c) in punt 9.1.4 wordt punt CSM_72 vervangen door:

„CSM_72 Voor elke voertuigunit worden twee unieke ECC-sleutelparen gegenereerd, aangeduid als VU_MA en VU_Sign. Deze taak wordt uitgevoerd door de VU-fabrikanten. De partij die een VU-sleutelpaar genereert, verzendt de openbare sleutel naar haar MSCA om het desbetreffende, door de MSCA ondertekende VU-certificaat te verkrijgen. De particuliere sleutel wordt uitsluitend door de voertuigunit gebruikt.”;

d) punt 9.1.5 wordt als volgt gewijzigd:

i) punt CSM_83 wordt vervangen door:

„CSM_83 Voor elke tachograafkaart wordt een uniek ECC-sleutelpaar gegenereerd, aangeduid als Card_MA. Daarnaast wordt voor elke bestuurders- en werkplaatskaart een tweede uniek ECC-sleutelpaar gegenereerd, aangeduid als Card_Sign. Deze taak kan worden uitgevoerd door kaartfabrikanten of -personalisatoren. De partij die een sleutelpaar voor een kaart genereert, verzendt de openbare sleutel naar haar MSCA om het desbetreffende, door de MSCA ondertekende kaartcertificaat te verkrijgen. De particuliere sleutel wordt uitsluitend door de tachograafkaart gebruikt.”;

ii) punt CSM_88 wordt vervangen door:

„CSM_88 Het certificaat Card_MA heeft de volgende geldigheidsduur:

— voor bestuurderskaarten: 5 jaar;

— voor bedrijfskaarten: 5 jaar;

— voor controlekaarten: 2 jaar;

— voor werkplaatskaarten: 1 jaar”;

iii) aan punt CSM_91 wordt de volgende tekst toegevoegd:

„— Bovendien uitsluitend voor controlekaarten, bedrijfskaarten en werkplaatskaarten, en alleen als deze kaarten zijn afgegeven tijdens de eerste drie maanden van de geldigheidsduur van een nieuw EUR-certificaat: het EUR-certificaat dat twee generaties ouder is, indien aanwezig.

Opmerking bij het laatste streepje: In de eerste drie maanden van het ERCA(3)-certificaat (zie figuur 1) moeten de genoemde kaarten bijvoorbeeld het ERCA(1)-certificaat bevatten om te garanderen dat deze kaarten kunnen worden gebruikt om gegevens te downloaden van ERCA(1)-voertuigunits waarvan de normale levensduur van 15 jaar plus de periode van 3 maanden voor het downloaden van gegevens gedurende deze maanden verstrijkt; zie het laatste streepje van voorschrift 13 van bijlage IC.”;

e) punt 9.1.6 wordt als volgt gewijzigd:

i) punt CSM_93 wordt vervangen door:

„CSM_93 Voor elke externe GNSS-module wordt een uniek ECC-sleutelpaar gegenereerd, aangeduid als EGF_MA. Deze taak wordt uitgevoerd door de fabrikanten van externe GNSS-modules. De partij die een EGF_MA-sleutelpaar voor een kaart genereert, verzendt de openbare sleutel naar haar MSCA om het desbetreffende, door de MSCA ondertekende EGF_MA-certificaat te verkrijgen. De particuliere sleutel wordt uitsluitend door de externe GNSS-module gebruikt.”;

ii) punt CSM_95 wordt vervangen door:

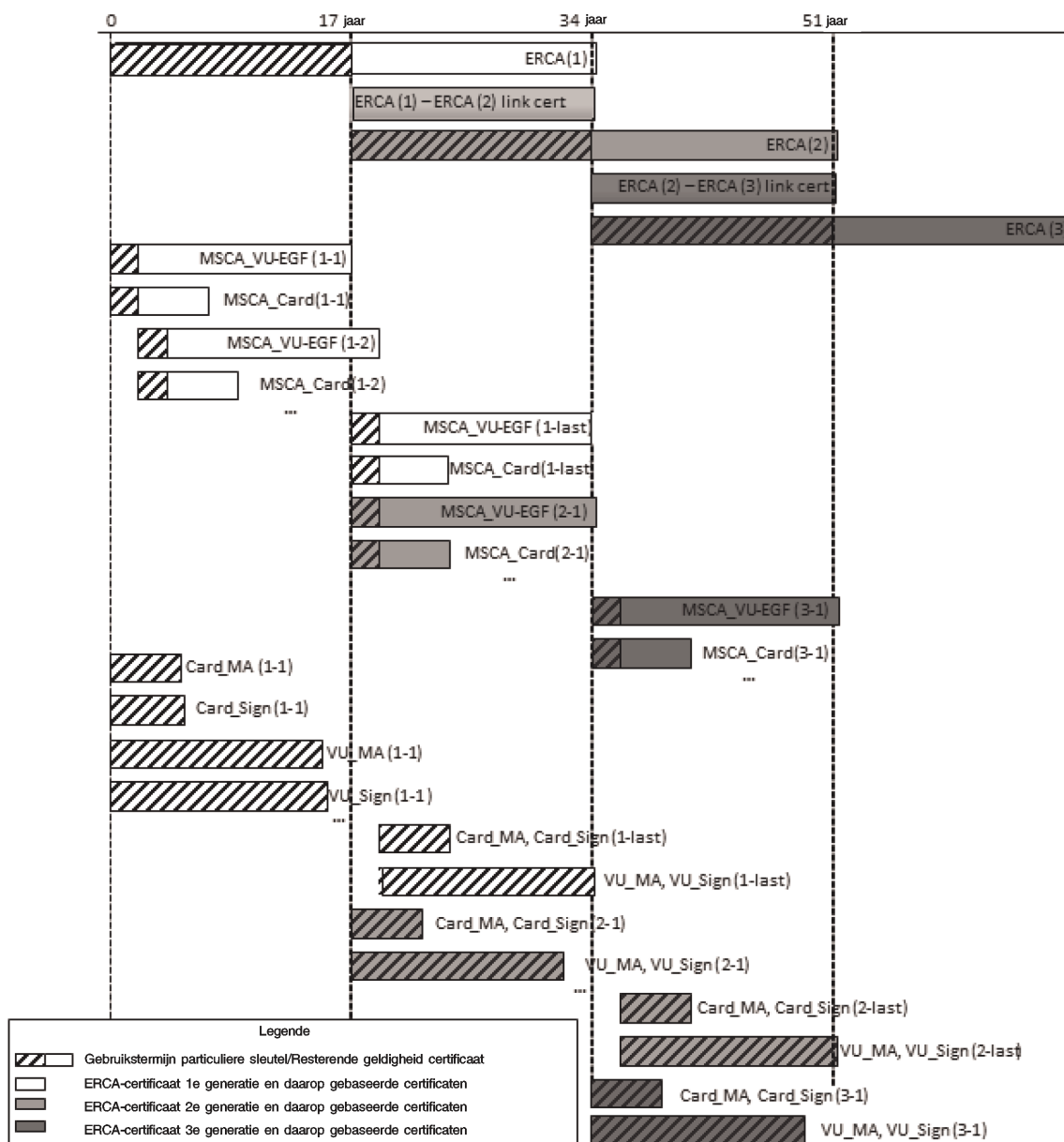
„CSM_95 De externe GNSS-module gebruikt het sleutelpaar EGF_MA, bestaande uit de particuliere sleutel EGF_MA.SK en de openbare sleutel EGF_MA.PK, uitsluitend met het oog op de wederzijdse authenticatie en sleutelovereenstemming tijdens de sessie met voertuigunits, zoals gespecificeerd in punt 11.4 van dit aanhangsel.”;

f) punt 9.1.7 wordt als volgt gewijzigd:

i) figuur 1 wordt vervangen door:

„Figuur 1

Afgifte- en gebruikstermijnen voor de verschillende generaties ERCA-basiscertificaten, ERCA-verbindingscertificaten, MSCA-certificaten en apparaatcertificaten



ii) punt 6 van de opmerkingen bij figuur 1 wordt vervangen door:

„6 Om ruimte te besparen, wordt het verschil in geldigheidsduur tussen de certificaten Card_MA en Card_Sign alleen voor de eerste generatie aangegeven.”;

g) punt 9.2.1.1 wordt als volgt gewijzigd:

i) het eerste streepje van punt CSM_106 wordt vervangen door:

„— Voor 128-bits hoofdsleutels van de bewegingssensor: CV = 'B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5D 83'";

ii) de eerste alinea van punt CSM_107 wordt vervangen door:

„Elke fabrikant van bewegingssensoren genereert voor elke bewegingssensor een aselechte en unieke koppelingssleutel K_p , en verzendt elke koppelingssleutel naar zijn MSCA. De MSCA codeert elke koppelingssleutel afzonderlijk met de hoofdsleutel van de bewegingssensor K_M en zendt de gecodeerde sleutel terug naar de fabrikant van bewegingssensoren. Voor elke gecodeerde sleutel deelt de MSCA het versienummer van de bijbehorende sleutel K_M mee aan de fabrikant van bewegingssensoren.”;

iii) punt CSM_108 wordt vervangen door:

„CSM_108 Elke fabrikant van bewegingssensoren genereert een uniek serienummer voor elke bewegingssensor en verzendt alle serienummers naar zijn MSCA. De MSCA codeert elk serienummer afzonderlijk met de identificatiesleutel K_{ID} en zendt het gecodeerde serienummer terug naar de fabrikant van bewegingssensoren. Voor elk gecodeerd serienummer deelt de MSCA het versienummer van de bijbehorende sleutel K_{ID} mee aan de fabrikant van bewegingssensoren.”;

h) punt 9.2.2.1 wordt als volgt gewijzigd:

i) punt CSM_123 wordt vervangen door:

„CSM_123 De VU-fabrikant genereert voor elke voertuigunit een uniek VU-serienummer en verzendt dit naar de MSCA met het verzoek twee VU-specifieke DSRC-sleutels te krijgen. Het VU-serienummer heeft het gegevenstype VuSerialNumber.

Opmerking:

— Dit VU-serienummer is identiek aan het element vuSerialNumber element van VuIdentification (zie aanhangsel 1) en aan de referentie van de certificaathouder op de certificaten van de voertuigunit.

— Het is mogelijk dat het VU-serienummer niet bekend is op het ogenblik dat een fabrikant van voertuigunits de VU-specifieke DSRC-sleutels aanvraagt. In dat geval verstuurt de VU-fabrikant in plaats daarvan de unieke identifier van de certificaataanvraag die hij heeft gebruikt voor het aanvragen van de certificaten van de VU; zie CSM_153. Deze identifier van de certificaataanvraag moet bijgevolg gelijk zijn aan de referentie van de certificaathouder in de certificaten van de VU.”;

ii) in punt CSM_124 wordt het info-voorschrift in stap 2 vervangen door:

„info = VU-serienummer of identifier van de certificaataanvraag, zoals gespecificeerd in CSM_123”;

iii) punt CSM_128 wordt vervangen door:

„CSM_128 De MSCA houdt registraties bij van alle door haar gegenereerde VU-specifieke DSRC-sleutels, van het bijbehorende versienummer en van het VU-serienummer of de identifier van de certificaataanvraag die voor het afleiden van deze sleutels werden gebruikt”;

i) in punt 9.3.1 wordt de eerste alinea van punt CSM_135 vervangen door:

„De kenmerkende coderingsregels (DER) overeenkomstig [ISO 8825-1] worden toegepast om de gegevensobjecten in certificaten te coderen. Tabel 4 bevat de volledige codering van het certificaat, met inbegrip van alle tags en lengtebytes.”;

j) in punt 9.3.2.3 wordt punt CSM_141 vervangen door:

„CSM_141 De autorisatie van de certificaathouder (CHA) dient om het certificaatype te identificeren. De CHA bestaat uit de zes meest significante bytes van de toepassingsidentificator (AID) van de tachograaf, samengevoegd met het type apparatuur, dat aangeeft voor welk type van apparatuur het certificaat bedoeld is. In het geval van een certificaat van een voertuigunit, een bestuurderskaart of een werkplaatskaart, wordt het type apparatuur ook gebruikt om een onderscheid te maken tussen een certificaat voor wederzijdse authenticatie en een certificaat voor het opstellen van digitale handtekeningen (zie punt 9.1 en aanhangsel 1, gegevenstype EquipmentType).”;

k) in punt 9.3.2.5 wordt de volgende alinea toegevoegd aan punt CSM_146:

„Opmerking: voor een kaartcertificaat is de waarde van de CHR gelijk aan de waarde van het cardExtendedSerialNumber in EF_ICC; zie aanhangsel 2. voor een EGF-certificaat is de waarde van de CHR gelijk aan de waarde van het sensorGNSSSerialNumber in EF_ICC; zie aanhangsel 14. Voor een VU-certificaat is de waarde van de CHR gelijk aan het vuSerialNumber element van Vulidentification (zie aanhangsel 1), tenzij de fabrikant het fabrikantspecifieke serienummer niet kent op het ogenblik dat het certificaat wordt aangevraagd.”;

l) in punt 9.3.2.6 wordt punt CSM_148 vervangen door:

„CSM_148 Dit veld bevat de begindatum en -tijd van de geldigheidsduur van het certificaat.”;

m) punt 9.3.3 wordt als volgt gewijzigd:

i) de eerste alinea van punt CSM_151 wordt vervangen door:

„Wanneer een MSCA een certificaat aanvraagt, stuurt zij de volgende gegevens naar de ERCA:”;

ii) punt CSM_153 wordt vervangen door:

„CSM_153 De apparatuurfabrikant verstuurt in een certificaataanvraag de volgende gegevens naar de MSCA zodat die de referentie van de certificaathouder van het nieuwe apparatuurcertificaat kan aanmaken:

— voor zover bekend (zie CSM_154), een fabrikantspecifiek serienummer voor de apparatuur, het model van de apparatuur en de maand van fabricage; zo niet, een unieke identificator van de certificaataanvraag;

— de maand en het jaar van fabricage of van de certificaataanvraag.

De fabrikant zorgt ervoor dat deze gegevens juist zijn en dat het door de MSCA teruggezonden certificaat wordt ingebracht in de apparatuur waarvoor dit bedoeld is.”;

n) punt 10.2.1 wordt als volgt gewijzigd:

i) in punt CSM_157 wordt de tekst die voorafgaat aan de opmerkingen bij figuur 4 vervangen door:

„Voertuigunits verifiëren de certificaatketen van een tachograafkaart volgens het stroomschema in Figuur 4. Voor elk certificaat dat de VU van de kaart leest, gaat hij na of het veld Certificate Holder Authorisation (CHA) correct is:

— In het veld CHA van het kaartcertificaat moet een kaartcertificaat voor wederzijdse authenticatie zijn vermeld (zie aanhangsel 1, gegevenstype EquipmentType).

— In de CHA van het certificaat Card.CA moet een MSCA vermeld zijn.

— In de CHA van het certificaat Card.Link moet een ERCA vermeld zijn.”;

ii) aan punt CSM_159 wordt de volgende zin toegevoegd:

„Een nieuw verbindingscertificaat dat door een kaart wordt gepresenteerd, moet verplicht in de VU worden opgeslagen; de opslag van alle andere types certificaten is facultatief.”;

o) punt 10.2.2 wordt als volgt gewijzigd:

i) in punt CSM_161 wordt de tekst die voorafgaat aan figuur 5 vervangen door:

„Tachograafkaarten verifiëren de certificaatketen van een voertuigunit (VU) volgens het stroomschema in Figuur 5. Voor elk certificaat dat door de VU wordt gepresenteerd, gaat de kaart na of het veld Certificate Holder Authorisation (CHA) correct is:

— In de CHA van het certificaat VU.Link moet een ERCA vermeld zijn.

— In de CHA van het certificaat VU.CA moet een MSCA vermeld zijn.

— In het veld CHA van het VU-certificaat moet een VU-certificaat voor wederzijdse authenticatie zijn vermeld (zie aanhangsel 1, gegevenstype EquipmentType).”;

ii) punt CSM_165 wordt vervangen door:

„CSM_165 In het MSE:Set AT-commando succesvol is, stelt de kaart de opgegeven sleutel VU.PK in voor later gebruik bij VU-authenticatie, en wordt de sleutel Comp(VU.PKeph) tijdelijk opgeslagen. Indien twee of meer MSE:Set AT-commando's met succes worden verzonden vóór de sleutelovereenstemming tijdens de sessie, slaat de kaart alleen de laatste ontvangen sleutel Comp(VU.PKeph) op. De kaart zal Comp(VU.PKeph) resetten na een succesvol commando GENERAL AUTHENTICATE.”;

p) punt 10.3 wordt als volgt gewijzigd:

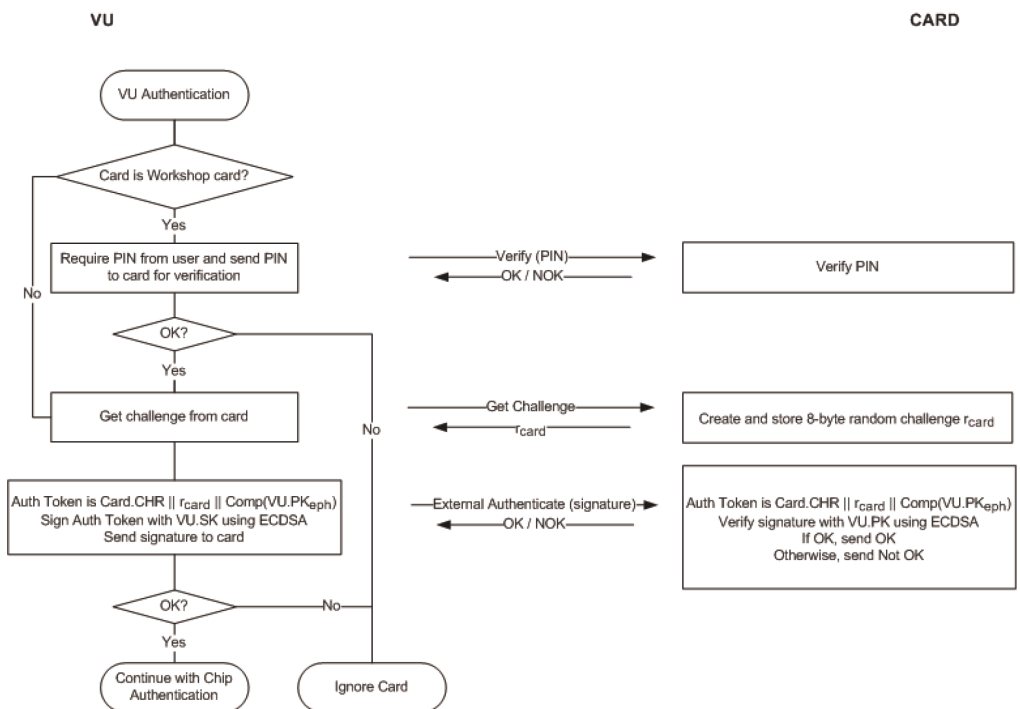
i) de eerste alinea van punt CSM_170 wordt vervangen door:

„Naast de door de kaart afgegeven identiteit vermeldt de VU in de handtekening de in het kaartcertificaat vermelde referentie van de certificaathouder.”;

ii) in punt CSM_171 wordt figuur 6 vervangen door:

„Figuur 6

Stroomschema van de VU-authenticatie



iii) punt CSM_174 wordt vervangen door:

„CSM_174 Op het ogenblik dat de kaart de handtekening van de VU ontvangt in een EXTERNAL AUTHENTICATE-commando:

- berekent de kaart het authenticatietoken door samenvoeging van Card.CHR, de door de kaart afgegeven identiteit rcard en de identicator van de tijdelijke openbare sleutel van de VU Comp(VU.PKeph) ;
- verifieert de kaart de handtekening van de VU met behulp van het ECDSA-algoritme, met behulp van het hashalgoritme dat gerelateerd is aan de grootte van het sleutelpaar VU_MA van de VU, zoals gespecificeerd in CSM_50, in combinatie met de sleutel VU.PK en het berekende authenticatietoken.”;

q) in punt 10.4 wordt punt CSM_176 als volgt gewijzigd:

i) alinea 2 wordt vervangen door:

„2 De VU verzendt het openbare punt VU.PKeph van zijn tijdelijke sleutelpaar naar de kaart. Zoals gespecificeerd in [TR-03111], wordt het openbare punt omgezet in een bytereeks (octet string). Het niet-gecomprimeerde coderingsformaat wordt gebruikt. Zoals uiteengezet in CSM_164, heeft de VU dit tijdelijke sleutelpaar gegenereerd alvorens de certificaatketen op VU-niveau te verifiëren. De VU verzendt de identicator van de tijdelijke openbare sleutel Comp(VU.PKeph) naar de kaart, en de kaart slaat deze op.”;

ii) alinea 6 wordt vervangen door:

„6 Met behulp van K_{MAC} berekent de kaart een authenticatietoken voor de identicator van de tijdelijke openbare punt van de VU: $T_{PICC} = \text{CMAC}(K_{MAC}, \text{VU.PKeph})$. Het openbare punt is in het formaat dat door de VU wordt gebruikt (zie tweede streepje hierboven). De kaart verzendt N_{PICC} en T_{PICC} naar de voertuigunit.”;

r) in punt 10.5.2 wordt punt CSM_191 vervangen door:

„CSM_191 Elk te coderen gegevensobject wordt opgevuld overeenkomstig [ISO 7816-4] met behulp van de paddingindicator „01”. Om de MAC te berekenen, worden gegevensobjecten in de APDU opgevuld overeenkomstig [ISO 7816-4].

Opmerking: de opvulling (padding) voor beveiligde berichtenuitwisseling wordt altijd uitgevoerd door de SM-laag, niet door het CMAC- of CBC-algoritme.

Samenvatting en voorbeelden

Afhankelijk van het desbetreffende onbeveiligde commando heeft een APDU-commando waarop beveiligde berichtenuitwisseling is toegepast, de volgende structuur („DO” staat voor gegevensobject):

Geval 1: CLA INS P1 P2 || Lc' || DO '8E' || Le

Geval 2: CLA INS P1 P2 || Lc' || DO '97' || DO'8E' || Le

Geval 3 (even instructiebyte INS): CLA INS P1 P2 || Lc' || DO '81' || DO'8E' || Le

Geval 3 (oneven instructiebyte INS): CLA INS P1 P2 || Lc' || DO 'B3' || DO'8E' || Le

Geval 4 (even instructiebyte INS): CLA INS P1 P2 || Lc' || DO '81' || DO'97' || DO'8E' || Le

Geval 4 (oneven instructiebyte INS): CLA INS P1 P2 || Lc' || DO 'B3' || DO'97' || DO'8E' || Le

waarbij de lengtebyte Le = '00' of '00 00' naargelang velden met korte lengte of met uitgebreide lengte worden gebruikt; zie [ISO 7816-4].

Afhankelijk van het desbetreffende onbeveiligde antwoord heeft een APDU-antwoord waarop beveiligde berichtenuitwisseling is toegepast, de volgende structuur:

Geval 1 of 3: DO '99' || DO '8E' || SW1SW2

Geval 2 of 4 (even instructiebyte INS) zonder codering: DO '81' || DO '99' || DO '8E' || SW1SW2

Geval 2 of 4 (even instructiebyte INS) met codering: DO '87' || DO '99' || DO '8E' || SW1SW2

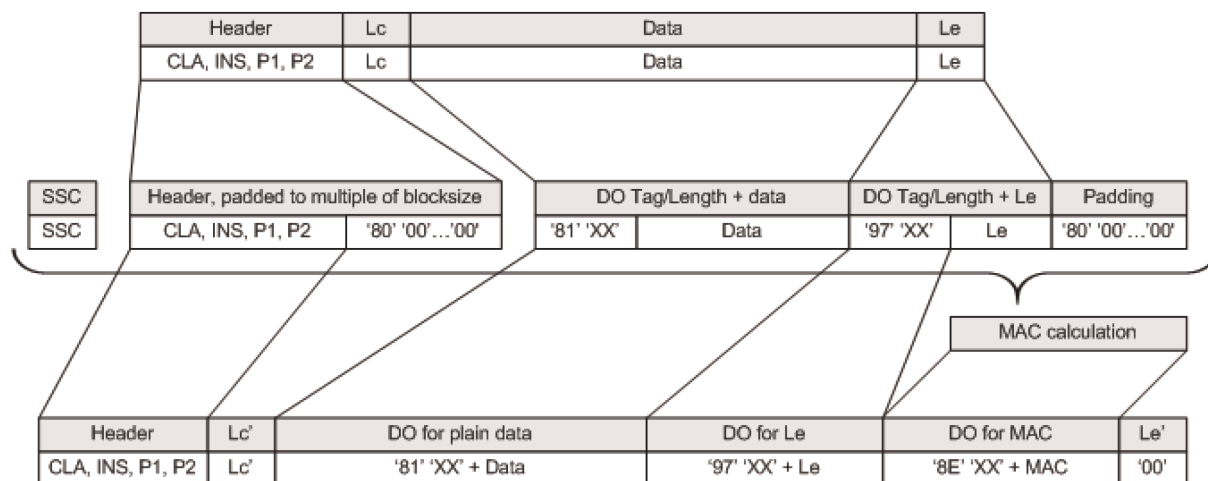
Geval 2 of 4 (oneven instructiebyte INS) zonder codering: DO 'B3' || DO '99' || DO '8E' || SW1SW2

Opmerking: geval 2 of 4 (oneven instructiebyte INS) met codering wordt nooit gebruikt bij de communicatie tussen een VU en een kaart.

Hieronder staan drie voorbeelden van APDU-transformaties voor commando's met een even instructiecode (INS). Figuur 8 toont een geauthenticeerd APDU-commando in geval 4, Figuur 9 toont een geauthenticeerd APDU-antwoord in geval 1/geval 3, en Figuur 10 toont een gecodeerd en geauthenticeerd APDU-antwoord in geval 2/geval 4.

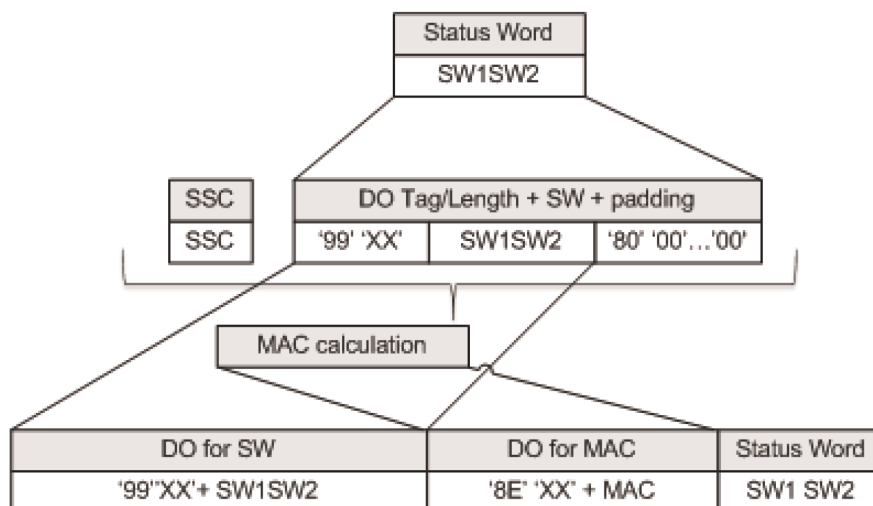
Figuur 8

Transformatie van een geauthenticeerd APDU-commando in geval 4

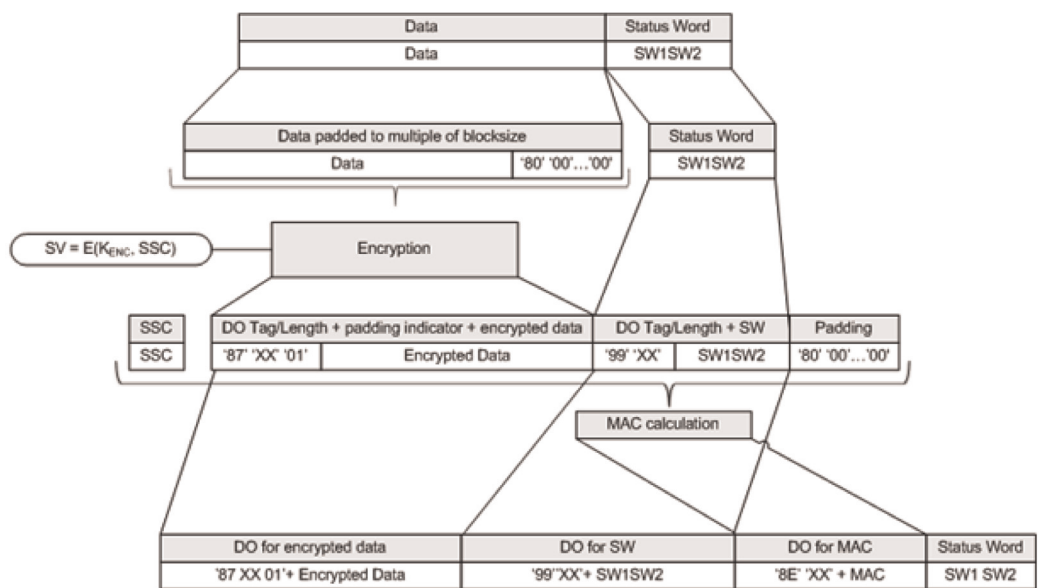


Figuur 9

Transformatie van een geauthenticeerd APDU-antwoord in geval 1/geval 3



Figuur 10

Transformatie van een gecodeerd en geauthenticeerd APDU-antwoord in geval 2/geval 4

s) in punt 10.5.3 wordt punt CSM_193 vervangen door:

„CSM_193 De tachograafkaart breekt een actieve SM-sessie enkel en alleen af indien een van de volgende omstandigheden zich voordoet:

- de kaart ontvangt een ongecodeerd APDU-commando;
- de kaart stelt een SM-fout in een APDU-commando vast:
- een verwacht SM-gegevensobject ontbreekt, de gegevensobjecten staan niet in de juiste volgorde, of er is een onbekend gegevensobject aanwezig;
- een SM-gegevensobject is onjuist, bijvoorbeeld onjuiste MAC-waarde of onjuiste TLV-structuur;
- onderbreking van de stroomvoorziening of kaartterugstelling (reset);
- de VU start de VU-authenticatieprocedure,
- het maximaal aantal commando's en bijbehorende antwoorden van de huidige sessie is bereikt. Dit maximaal aantal wordt voor de kaart vastgelegd door de fabrikant, rekening houdend met de beveiligingseisen van de gebruikte hardware, en bedraagt 240 SM-commando's en bijbehorende antwoorden per sessie”;

t) punt 11.3.2 wordt als volgt gewijzigd:

i) de eerste alinea van punt CSM_208 wordt vervangen door:

„Tijdens de koppeling met een VU gaat de externe GNSS-module te werk volgens het stroomschema in Figuur 5 (zie punt 10.2.2) om de certificaatketen op VU-niveau te verifiëren”;

ii) punt CSM_210 wordt vervangen door:

„CSM_210 Na verificatie van het certificaat VU_MA slaat de externe GNSS-module dit certificaat op voor gebruik tijdens normaal bedrijf; zie punt 11.3.3.”;

u) in punt 11.3.3 wordt de eerste alinea van punt CSM_211 vervangen door:

„Tijdens normaal bedrijf gaan de voertuigunit en externe GNSS-module te werk volgens het stroomschema in Figuur 11 om de temporele geldigheid te verifiëren van het opgeslagen EGF_MA-certificaat en om de openbare sleutel VU_MA in te stellen met het oog op de VU-authenticatie op een later tijdstip. Er vindt geen verdere wederzijdse verificatie van de certificaatketens plaats tijdens normaal bedrijf.”;

v) in punt 12.3 wordt tabel 6 vervangen door:

„Tabel 6

Aantal ongecodeerde en gecodeerde gegevensbytes per instructie overeenkomstig [ISO 16844-3]

Instructie	Type	Gegevensbeschrijving	Aantal ongecodeerde gegevensbytes overeenkomstig [ISO 16844-3]	Aantal ongecodeerde gegevensbytes bij gebruik van AES-sleutels	Aantal gecodeerde gegevensbytes bij gebruik van AES-sleutels met bitlengte		
					128	192	256
10	Verzoek	Authenticatiegegevens + bestandsnummer	8	8	16	16	16
11	Antwoord	Authenticatiegegevens + bestandsinhoud	16 of 32, afhankelijk van bestand	16 of 32, afhankelijk van bestand	32 / 48	32 / 48	32 / 48
41	Verzoek	Serienummer bewegingssensor	8	8	16	16	16
41	Antwoord	Koppelingssleutel	16	16 / 24 / 32	16	32	32
42	Verzoek	Sessiesleutel	16	16 / 24 / 32	16	32	32
43	Verzoek	Koppelingsinformatie	24	24	32	32	32
50	Antwoord	Koppelingsinformatie	24	24	32	32	32
70	Verzoek	Authenticatiegegevens	8	8	16	16	16
80	Antwoord	Tellerwaarde bewegingssensor + authenticatiegegevens	8	8	16	16	16”

w) in punt 13.1 wordt het voorschrift inzake het serienummer van de VU in punt CSM_224 vervangen door:

„**Serienummer van de VU** het serienummer van de VU of de identicator van de certificaataanvraag (gevenstype VuSerialNumber of CertificateRequestID) – zie CSM_123”;

x) in punt 13.3 wordt het tweede streepje van punt CSM_228 vervangen door:

„2 De controlekaart gebruikt de opgegeven DSRC-hoofdsleutel in combinatie met het VU-serienummer of de identifier van de certificataanvraag in de DSRC-beveiligingsgegevens om de VU-specifieke DSRC-sleutels $K_{VU_{DSRC_ENC}}$ en $K_{VU_{DSRC_MAC}}$ af te leiden, zoals gespecificeerd in CSM_124.”;

y) punt 14.3 wordt als volgt gewijzigd:

i) in punt CSM_234 wordt de tekst die voorafgaat aan de opmerkingen bij figuur 13 vervangen door:

„De IDE kan de handtekening van gedownloade gegevens zelf verifiëren of kan daartoe gebruikmaken van een controlekaart. Bij gebruik van een controlekaart verloopt de handtekeningverificatie zoals aangegeven in figuur 13. Om de temporele geldigheid van een door de IDE aangeboden certificaat te verifiëren, gebruikt de controlekaart zijn interne klok, zoals gespecificeerd in CSM_167. De controlekaart actualiseert de lopende tijd indien de ingangsdatum van een authentiek „geldige tijdbron”-certificaat recenter is dan de tijdaanduiding van de kaart. De kaart accepteert uitsluitend de volgende certificaten als geldige tijdbron:

- ERCA-verbindingscertificaten van de tweede generatie;
- MSCA-certificaten van de tweede generatie;
- VU_Sign of Card_Sign van de tweede generatie die zijn afgegeven door het land dat ook het kaartcertificaat van de controlekaart heeft afgegeven.

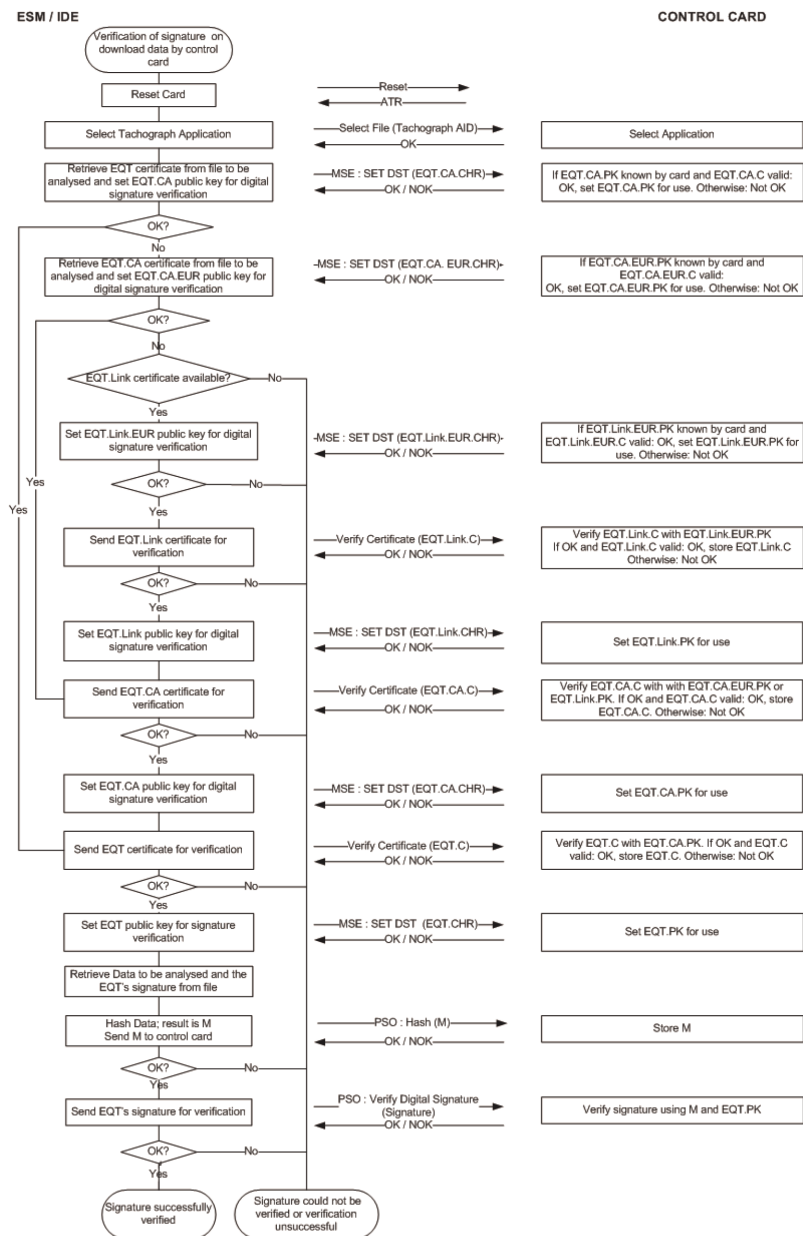
Indien de IDE de handtekeningverificatie zelf uitvoert, verifieert de IDE de authenticiteit en geldigheid van alle certificaten in de certificaatketen van het gegevensbestand, alsook de handtekening van de gegevens volgens het in [DSS] vastgestelde handtekeningschema. In beide gevallen moet voor elk certificaat dat van het gegevensbestand wordt gelezen, worden nagegaan of het veld Certificate Holder Authorisation (CHA) correct is:

- In het veld CHA van het EQT-certificaat moet een VU-certificaat of kaartcertificaat (al naargelang van toepassing) zijn vermeld voor ondertekening (zie aanhangsel 1, gegevenstype EquipmentType).
- In de CHA van het certificaat EQT.CA moet een MSCA vermeld zijn.
- In de CHA van het certificaat EQT.Link moet een ERCA vermeld zijn.”;

ii) figuur 13 wordt vervangen door:

„Figuur 13

Stroomschema ter verificatie van de handtekening van een gedownload gegevensbestand



37) Aanhangsel 12 wordt als volgt gewijzigd:

a) punt 3 wordt als volgt gewijzigd:

i) in punt GNS_4 wordt de tweede alinea na figuur 2 vervangen door:

„De positienauwkeurigheid (resolutie) is gebaseerd op de hierboven beschreven notatie van de RMC-zin. De eerste twee cijfers van de velden 3 en 5 stellen de graden voor. De resterende cijfers stellen de minuten voor met drie cijfers achter de komma. De resolutie bedraagt bijgevolg één duizendste van een minuut of één zestigduizendste van een graad (aangezien een minuut één zestigste van een graad is).”;

ii) punt GNS_5 wordt vervangen door:

„GNS_5 Zoals toegelicht in aanhangsel 1 voor het type GeoCoordinates, slaat de voertuigunit de positie-informatie voor de breedte- en lengtegraad op in de VU-database met een resolutie van één tiende van een minuut of één zeshonderdste van een graad.

Met behulp van het GSA-commando (GPS DOP en actieve satellieten) kan de VU de beschikbaarheid en nauwkeurigheid van het signaal bepalen en registreren. Met name de HDOP-waarde wordt gebruikt als aanwijzing voor de mate van nauwkeurigheid van de geregistreerde locatiegegevens (zie punt 4.2.2). De VU slaat de verzwakking van horizontale nauwkeurigheid (HDOP) op, berekend als minimum van de HDOP-waarden die voor de beschikbare GNSS-systemen werden verzameld.

In de GNSS Id is de overeenkomstige NMEA Id voor elke GNSS-constellatie en elk satellietaugmentatiesysteem (SBAS) vermeld.

Figuur 3

Opbouw van de GSA-zin

1234	1415161718
↓ ↓ ↓ ↓	↓ ↓ ↓ ↓ ↓

\$<GNSS Id.>GSA,a,a,x,x,x,x,x,x,x,x,x,x,x,x,x,x,x,x*hh

- 1) Selection mode
- 2) Mode
- 3) ID of 1st satellite used for fix
- 4) ID of 2nd satellite used for fix
- ...
- 14) ID of 12th satellite used for fix
- 15) PDOP
- 16) HDOP
- 17) VDOP
- 18) Controlesom "

iii) punt GNS_6 wordt vervangen door:

„GNS_6 De GSA-zin wordt opgeslagen onder recordnummer „02” tot en met „06”.”;

b) punt 4.2.1 wordt als volgt gewijzigd:

i) punt GNS_16 wordt vervangen door:

„GNS_16 Velden met uitgebreide lengte worden niet ondersteund in het communicatieprotocol.”;

ii) punt GNS_18 wordt vervangen door:

„GNS_18 Wat betreft de functies 1) verzameling en verspreiding van GNSS-gegevens en 2) verzameling van configuratiegegevens van de externe GNSS-module en 3) beheerprotocol, simuleert de beveiligde GNSS-transceiver een smartcard met een bestandssysteemarchitectuur bestaande uit een stambestand (MF — Master File), een toepassingsgericht bestand (DF — Dedicated File) waarvan de toepassingsidentificatie is gespecificeerd in aanhangsel 1, punt 6.2 („FF 44 54 45 47 4D”) en drie hoofdbestanden (EF's — Elementary Files) die certificaten bevatten en één hoofdbestand (EF.EGF) waarvan de identificatie gelijk is aan „2F2F”, zoals beschreven in Tabel 1.”;

iii) punt GNS_20 wordt vervangen door:

„GNS_20 De beveiligde GNSS-transceiver slaat de gegevens op in een geheugen en kan ten minste 20 miljoen lees-/schrijfcycli uitvoeren. Afgezien daarvan worden het interne ontwerp en de uitvoering van de beveiligde GNSS-transceiver overgelaten aan de fabrikanten.

De recordnummers en gegevens worden toegewezen zoals aangegeven in Tabel 1. Er zijn vijf GSA-zinnen voor de GNSS-systemen en het satellietaugmentatiesysteem (SBAS).”;

c) in punt 4.2.2 wordt de vijfde alinea van punt GNS_23 vervangen door:

„5 De verwerkingseenheid van de VU controleert de ontvangen gegevens door de informatie (bijvoorbeeld lengtegraad, breedtegraad, tijd) te lezen in de NMEA RMC-zin. Indien de positie geldig is, staat deze informatie in de NMEA RMC-zin. Is de positie ongeldig, dan zijn er nog geen locatiegegevens beschikbaar en is het niet mogelijk de voertuigpositie op basis daarvan te registreren. Indien de positie geldig is, leest de verwerkingseenheid van de VU ook de HDOP-waarden in de NMEA GSA-zinnen en wordt de minimumwaarde voor de beschikbare satellietssystemen berekend (voor zover positiebepaling mogelijk is).”;

d) In punt 4.4.1 wordt punt GNS_28 vervangen door:

„GNS_28 Indien de VU gedurende ten minste twintig aaneengesloten minuten er niet in slaagt te communiceren met de gekoppelde externe GNSS-module, genereert en registreert de VU een voorval van het type EventFaultType met de enum-waarde „0E”H Communication error with the external GNSS facility (Communicatiefout externe GNSS-module) en waarvan de tijdaanduiding is ingesteld op de huidige tijd. Het voorval wordt uitsluitend gegenereerd indien aan de volgende twee voorwaarden is voldaan: a) de slimme tachograaf staat niet in kalibreringsmodus en b) het voertuig is aan het rijden. In dit geval is sprake van een communicatiefout indien de beveiligde VU-transceiver geen antwoordbericht ontvangt op een verzoekbericht, zoals omschreven in 4.2.”;

e) in punt 4.4.2 wordt punt GNS_29 vervangen door:

„GNS_29 Indien de fysieke integriteit is aangetast, wist de externe GNSS-module het volledige geheugen samen met al het cryptografisch materiaal. Zoals omschreven in GNS_25 en GNS_26, detecteert de VU manipulatie indien de antwoordstatus „6690” is. De VU genereert dan een voorval van het type EventFaultType met de enum-waarde „19”H Tamper detection of GNSS (Manipulatie GNSS gedetecteerd). Als alternatief is het ook mogelijk dat de GNSS-module op geen enkele externe aanvraag meer antwoordt.”;

f) in punt 4.4.3 wordt punt GNS_30 vervangen door:

„GNS_30 Indien gedurende ten minste drie aaneengesloten uren geen gegevens van de GNSS-ontvanger worden ontvangen, genereert de beveiligde GNSS-transceiver een antwoordbericht op het Read Record-commando waarvan het recordnummer gelijk is aan „01” en met een gegevensveld van 12 bytes, allemaal ingesteld op „0xFF”. Bij ontvangst van het antwoordbericht waarvan het gegevensveld deze waarde heeft, genereert en registreert de VU een voorval van het type EventFaultType met de enum-waarde „0D”H Absence of position information from GNSS receiver (ontbreken van plaatsbepalingsinformatie van de GNSS-ontvanger). De tijdaanduiding van dit voorval is uitsluitend gelijk aan de huidige tijd indien aan de volgende twee voorwaarden is voldaan: a) de slimme tachograaf staat niet in kalibreringsmodus en b) het voertuig is aan het rijden.”;

- g) in punt 4.4.4 wordt de tekst van punt GNS_31 tot figuur 4 vervangen door:

„Indien de VU vaststelt dat het voor de wederzijdse authenticatie gebruikte certificaat van de externe GNSS-module niet langer geldig is, genereert en registreert de VU een controleapparaatvoorval van het type EventFaultType met de enum-waarde *'1BH External GNSS facility certificate expired'* (Geldigheidsduur certificaat externe GNSS-module verstreken) en waarvan de tijdaanduiding gelijk is aan de huidige tijd. De VU blijft gebruikmaken van de ontvangen GNSS-positiegegevens.”;

- h) in punt 5.2.1 wordt punt GNS_34 vervangen door:

„GNS_34 Indien gedurende ten minste drie aaneengesloten uren geen gegevens van de GNSS-ontvanger worden ontvangen, genereert en registreert de VU een voorval van het type EventFaultType met de enum-waarde *'0DTH Absence of position information from GNSS receiver'* (ontbreken van plaatsbepalingsinformatie van de GNSS-ontvanger). De tijdaanduiding van dit voorval is uitsluitend gelijk aan de huidige tijd indien aan de volgende twee voorwaarden is voldaan: a) de slimme tachograaf staat niet in kalibreringsmodus en b) het voertuig is aan het rijden.”;

- i) punt 6 wordt vervangen door:

„6 TEGENSTRIJDIGE GNSS-TIJDGEGEVENS

Indien een verschil van meer dan één minuut wordt vastgesteld tussen de door de tijdmetersfunctie van de VU vastgestelde tijd en de tijdaanduiding afkomstig van de GNSS-ontvanger, registreert de VU een voorval van het type EventFaultType met de enum-waarde *'0BTH Time conflict (GNSS versus VU internal clock)* (Tegenstrijdige tijdgegevens tussen GNSS en interne klok VU). Nadat een voorval van tegenstrijdige tijdgegevens werd gestart, voert de VU de eerstvolgende twaalf uren geen controle op tijdverschillen uit. Er wordt geen tijdsoverlappending gegenereerd indien de GNSS-ontvanger de jongste 30 dagen geen geldig GNSS-signaal heeft kunnen detecteren.”.

- 38) Aanhangsel 13 wordt als volgt gewijzigd:

- a) in punt 2 wordt de vierde alinea vervangen door:

„Voor alle duidelijkheid: dit aanhangsel bevat geen specificaties met betrekking tot:

- de verzameling van *de gegevens* met het oog op de werking en het beheer in de VU (deze wordt elders in *de verordening* gespecificeerd of hangt af van het productontwerp);
- de aanbiedingsvorm van de verzamelde gegevens aan de toepassing op het externe apparaat;
- de bepalingen inzake gegevensbeveiliging die verder gaan dan hetgeen waarin Bluetooth® voorziet (zoals codering) met betrekking tot de inhoud van *de gegevens* (die elders in *de verordening* worden gespecificeerd [aanhangsel 11 „Algemene beveiligingsmechanismen”]);
- de door de ITS-interface gebruikte Bluetooth®-protocollen.”;

- b) punt 4.2, derde alinea, komt als volgt te luiden:

„Wanneer een extern apparaat voor het eerst binnen het bereik van de VU komt, kan de Bluetooth®-koppelingsprocedure worden gestart (zie ook bijlage 2). Beide apparaten wisselen hun adressen, namen en profielen uit en delen een gemeenschappelijke geheime sleutel, waardoor ze nadien automatisch verbinding met elkaar kunnen maken. Na deze stap wordt het externe apparaat vertrouwd en kan dit verzoeken initiëren om gegevens van de tachograaf te downloaden. Het is niet de bedoeling coderingsmechanismen in te voeren die verder gaan dan hetgeen waarin Bluetooth® voorziet. Indien aanvullende beveiligingsmechanismen noodzakelijk zijn, worden die ingevoerd overeenkomstig aanhangsel 11 Algemene beveiligingsmechanismen.”;

- c) punt 4.3 wordt als volgt gewijzigd:

- i) de eerste alinea wordt vervangen door:

„Om veiligheidsredenen vereist de VU een systeem voor pincodeverificatie dat losstaat van de Bluetooth-koppelingsprocedure. Elke VU kan voor authenticatiedoeleinden pincodes genereren die ten minste uit vier cijfers bestaan. Een extern apparaat dat aan de VU wordt gekoppeld, kan pas gegevens ontvangen nadat een juiste pincode is opgegeven.”;

ii) de derde alinea na tabel 1 wordt vervangen door:

„De PUC-code kan niet worden gewijzigd, ook al biedt de fabrikant de mogelijkheid om de pincode rechtstreeks te wijzigen via de VU. Om de pincode in voorkomend geval te wijzigen, moet de huidige pincode rechtstreeks in de VU worden ingevoerd.”;

d) in punt 4.4 wordt de tweede alinea na de titel „Gegevensveld” vervangen door:

„Indien de te verwerken gegevens te groot zijn voor de beschikbare ruimte van één bericht, wordt het bericht opgesplitst in meerdere subberichten. Elk subbericht bevat dezelfde header en SID, maar heeft ook een teller van 2 bytes, te weten de teller van het huidige subberichtnummer (CC — Counter Current) en de teller van het maximumaantal subberichten (CM — Counter Max), om het subberichtnummer aan te geven. Met het oog op foutencontrole en voortijdige beëindiging van de overdracht bevestigt de ontvanger elk subbericht. De ontvanger kan het subbericht accepteren, vragen om het opnieuw te zenden, de verzender verzoeken om opnieuw te beginnen of de overdracht voortijdig beëindigen.”;

e) bijlage 1 wordt als volgt gewijzigd:

i) de titel wordt vervangen door:

„1) LIJST VAN VIA DE ITS-INTERFACE BESCHIKBARE GEGEVENS”;

ii) het volgende punt wordt ingevoegd in de tabel van punt 3, na het punt „Ontbreken van plaatsbepalingsinformatie van de GNSS-ontvanger”:

„Fout in de communicatie met de externe GNSS-module	— het langste voorval op elk van de laatste 10 dagen waarop een dergelijk voorval is opgetreden — de 5 langste voorvallen gedurende de afgelopen 365 dagen	— datum en tijdstip van het begin van het voorval — datum en tijdstip van het einde van het voorval — type, nummer, lidstaat van afgifte en generatie van de bij het begin en/of het einde van het voorval ingevoerde kaart(en) — aantal vergelijkbare voorvallen op die dag.”
---	---	---

iii) in punt 5 wordt het volgende streepje toegevoegd:

„— ITS-interfacefout (indien van toepassing)”;

f) de ASN.1-specificaties in bijlage 3 worden als volgt gewijzigd:

i) de volgende lijnen 206a tot en met 206e worden ingevoegd na lijn 206:

```

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

```

ii) lijnen 262, 263 en 264 worden vervangen door:

```

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

```

iii) lijn 275 wordt vervangen door:

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

iv) lijnen 288, 263 en 310 worden vervangen door:

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

v) lijnen 362 en 363 worden vervangen door:

```
„362 driver1MaximumDailyDrivingTime BIT STRING (SIZE(4)),
363 driver2MaximumDailyDrivingTime BIT STRING (SIZE(4)),”;
```

vi) de volgende lijnen 410a en 410b worden ingevoegd na lijn 410:

```
„410a comErrorWithExternalGNSSFacility
410b CommunicationErrorWithTheExternalGNSSFacility,”;
```

vii) de volgende lijnen 539a tot en met 539j worden ingevoegd na lijn 539:

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

39) Aanhangsel 14 wordt als volgt gewijzigd:

a) punt 5.5 van de inhoudsopgave wordt vervangen door:

„5.5 Naleving van Richtlijn (EU) 2015/719490”;

b) punt 2, derde alinea, komt als volgt te luiden:

„In dit geval is de voor *de communicatie* beschikbare tijd beperkt omdat gerichte gegevens over korte afstand moeten worden uitgewisseld. Voorts kunnen de bevoegde controleautoriteiten dezelfde communicatiemiddelen voor tachograafcontrole op afstand (RTM) ook voor andere toepassingen inzetten (bijvoorbeeld ter bepaling van de maximaal toegestane afmetingen en gewichten van zware vrachtoertuigen als bedoeld in Richtlijn (EU) 2015/719). Dit kan, naar keuze van de bevoegde controleautoriteiten, geschieden in de vorm van aparte of opeenvolgende verrichtingen.”;

c) punt 5.1 wordt als volgt gewijzigd:

i) in punt DSC_19 wordt het twaalfde streepje vervangen door:

„— De antenne van de DSRC-VU wordt aangebracht op een plaats waar zij zorgt voor optimale DSRC-communicatie tussen het voertuig en de antenne langs de weg, waarbij de lezer op een afstand van 15 m vóór het voertuig en een hoogte van 2 m wordt geïnstalleerd, gericht op het horizontale en verticale middenpunt van de voorruit. Voor lichte voertuigen (bestelwagens e.d.) kan de antenne aan de bovenzijde van de voorruit worden gemonteerd. Voor alle andere voertuigen wordt de DSRC-antenne in de nabijheid van de onderzijde of de bovenzijde van de voorruit geïnstalleerd.”;

ii) de eerste alinea van punt DSC_22 wordt vervangen door:

„De vormfactor van de antenne is niet nader bepaald; de beslissing daarover wordt in de commerciële sfeer genomen mits de geïnstalleerde DSRC-VU voldoet aan de in punt 5 hierna vastgestelde conformiteitsvoorschriften. De antenne wordt geplaatst volgens het bepaalde in DSC_19 en biedt op efficiënte wijze ondersteuning aan de in punten 4.1.2 en 4.1.3 toegelichte praktijkgevallen.”;

d) in punt 5.4.3 wordt volgorde 7 vervangen door:

„7 REDCR > DSRC-VU Sends GET.request for data of other Attribute (if appropriate)”

e) in punt 5.4.4 wordt de definitie van de ASN.1-module in DSC_40 als volgt gewijzigd:

i) de eerste lijn van de volgorde voor `TachographPayload` wordt vervangen door:

„tp15638VehicleRegistrationPlate LPN - Vehicle Registration Plate as per EN 15509¹”

ii) de volgende voetnoot 1 wordt toegevoegd:

„1 als een LPN een `AlphabetIndicator LatinAlphabetNo2` of `latinCyrillicAlphabet` bevat, worden de speciale karakters opnieuw in kaart gebracht bij het systeem voor ondervraging op afstand volgens speciale regels, overeenkomstig bijlage E van ISO/DIS 14 906,2”;

iii) het superscript 2 wordt geschrapt uit de lijn waarop het tijdstempel van de huidige record is gedefinieerd;

iv) de definitie van de ASN.1-module voor `RtmTransferAck` wordt vervangen door:

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

```

f) in punt 5.4.5 wordt punt RTM12 van tabel 14.3 vervangen door:

„RTM12 Sensor Fault	De VU genereert een integerwaarde voor het gegevenselement RTM12. De VU wijst aan de variabele sensorFault de volgende waarde toe: — 1 indien tijdens de laatste tien dagen een voorval van het type „35”H (Fout in de sensor) is geregistreerd. — 2 indien tijdens de laatste tien dagen een voorval van het type fout in de GNSS-ontvanger (interne fout of externe fout met enum-waarden „36”H of „37”H) is geregistreerd. — 3 indien tijdens de laatste tien dagen een voorval van het type „0E”H (communicatiefout met de externe GNSS-module) is geregistreerd. — 4 indien tijdens de laatste tien dagen fouten in zowel de sensor als de GNSS-ontvanger zijn geregistreerd. — 5 indien tijdens de laatste tien dagen zowel fouten in de sensor als communicatiefouten met de externe GNSS-module zijn geregistreerd. — 6 indien tijdens de laatste tien dagen zowel fouten in de GNSS-ontvanger als communicatiefouten met de externe GNSS-module zijn geregistreerd. — 7 indien tijdens de laatste tien dagen alle drie de fouten in de sensor zijn geregistreerd. Indien er tijdens de laatste tien dagen geen voorvallen zijn geregistreerd, wordt aan de variabele de waarde 0 toegekend.	–fout in de sensor één byte volgens de verklarende woordenlijst van de gegevens	sensorFault INTEGER (0..255),;
--------------------------------	--	--	---

g) in punt 5.4.6 wordt punt DSC_43 vervangen door:

DSC_43 „Voor elke uitwisseling via DSRC-interfaces worden de gegevens gecodeerd op basis van PER (Packed Encoding Rules) UNALIGNED, behalve TachographPayload en OwsPayload; die worden gecodeerd op basis van OER (Octet Encoding Rules), zoals gedefinieerd in ISO/IEC 8825-7, Rec. ITU-T X.696.”;

h) in de vierde kolom van tabel 14.9 van punt 5.4.7 wordt de cel met Rtm-ContextMark; vervangen door:

„Object Identifier of the supported standard, part, and version. Bijvoorbeeld: ISO (1) Standard (0) TARV (15638) part9 (9) Version1 (1).

Eerste byte is 06H, zijnde de object-ID. Tweede byte is 06H, zijnde de lengte ervan. De volgende 6 bytes bevatten het voorbeeld van de object-ID.”;

i) de punten 5.5 en 5.5.1 worden vervangen door:

„5.5 Naleving van Richtlijn (EU) 2015/719

5.5.1. Overview

DSC_59 Ter ondersteuning van Richtlijn (EU) 2015/719 met betrekking tot de maximaal toegestane afmetingen en gewichten voor zware vrachtoertuigen wordt voor het downloaden van OWS-gegevens via de 5,8 GHz DSRC-interface hetzelfde transactieprotocol gebruikt als voor de RTM-gegevens (zie 5.4.1). Het enige verschil is dat de objectidentificatie van de TARV-norm verwijst naar deel 20 van de norm ISO 15638 (TARV) met betrekking tot WOB/OWS.”;

j) in punt 5.6.1 wordt het bepaalde onder a) in punt DSC_68 vervangen door:

„a) De verbinding tussen de VU en de DSRC-VU die zich niet in de VU bevindt, moet berusten op een open industriestandaard zodat verschillende fabrikanten in aanmerking komen voor de levering van de VU en de DSRC-VU, met inbegrip van de diverse uitvoeringsvormen daarvan. De VU wordt verbonden met de DSRC-VU door middel van”;

k) in punt 5.7.1 wordt punt DSC_77 vervangen door:

„DSC_77 De gegevens worden in beveiligde vorm beschikbaar gesteld aan de DSRC-VU door de VUSM. De VUSM controleert of de gegevens juist zijn geregistreerd in de DSRC-VU. Eventuele fouten in de gegevensoverdracht van de VU naar het geheugen van de DSRC-VU worden geregistreerd en gemeld op basis van een voorval van het type EventFaultType met de enum-waarde „OCH „Communicatiefout met het systeem voor communicatie op afstand”, samen met de tijdaanduiding.”.

40) Aanhangsel 15 wordt als volgt gewijzigd:

a) de eerste alinea van punt 2.2 wordt vervangen door:

„Er wordt van uitgegaan dat tachograafkaarten van de eerste generatie interoperabel zijn met voertuigunits van de eerste generatie, overeenkomstig bijlage IB bij Verordening (EEG° nr. 3821/85), en dat tachograafkaarten van de tweede generatie interoperabel zijn met voertuigunits van de tweede generatie, overeenkomstig bijlage IC bij deze verordening. Voorts zijn ook de onderstaande voorschriften van toepassing.”;

b) in punt 2.4.1 wordt punt MIG_11 als volgt gewijzigd:

i) het eerste streepje wordt vervangen door:

„— de IC en ICC (facultatief) van niet-ondertekende EF's”;

ii) het derde streepje wordt vervangen door:

„— de andere gegevensbestanden van de EF's (in DF Tachograph) die worden gevraagd door de eerste generatie van het downloadprotocol. Deze informatie wordt beveiligd met een digitale handtekening, volgens de beveiligingsmechanismen van de eerste generatie.

Een dergelijke download omvat geen gegevensbestanden van EF's die alleen aanwezig zijn in bestuurders- (en werkplaats-)kaarten van de tweede generatie (gegevensbestanden van EF's in DF Tachograph_G2).”;

c) in punt 2.4.3 worden de punten MIG_014 en MIG_015 vervangen door:

„MIG_014 Buiten het kader van de controle van bestuurders door controle-autoriteiten van buiten de EU, wordt voor het downloaden van gegevens van een voertuigunit van de tweede generatie gebruikgemaakt van de beveiligingsmechanismen van de tweede generatie en van het in aanhangsel 7 van deze bijlage gespecificeerde downloadprotocol.

MIG_015 Om controle-autoriteiten van buiten de EU de mogelijkheid te geven om bestuurders te controleren, kan het ook mogelijk zijn om gegevens van voertuigunits van de tweede generatie te downloaden met de beveiligingsmechanismen. De gedownloade gegevens hebben dan hetzelfde formaat als gegevens die zijn gedownload uit een voertuigunit van de eerste generatie. Deze mogelijkheid kan worden geselecteerd via commando's in het menu.”.

BIJLAGE II

Bijlage II bij Verordening (EU) 2016/799 wordt als volgt gewijzigd:

1) in hoofdstuk I, onder b), wordt punt 1 vervangen door:

„b) een goedkeuringsnummer, dat overeenstemt met het nummer op het goedkeuringscertificaat dat is opgesteld voor het model van het controleapparaat of van het registratieblad of van de tachograafkaart, en aangebracht in een willekeurige stand in de nabijheid van die rechthoek.”;

2) in hoofdstuk III wordt punt 5 vervangen door:

„5 Ter goedkeuring aangeboden op”;

3) In hoofdstuk IV wordt punt 5 vervangen door:

„5 Ter goedkeuring aangeboden op”.
