II

(Niet-wetgevingshandelingen)

VERORDENINGEN

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

(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 is een tweede generatie digitale tachografen ingevoerd, de zogenaamde slimme tachografen, die beschikken over een verbinding met het mondiaal satellietnavigatiesysteem (GNSS), een communicatiesysteem voor vroegtijdige detectie op afstand en een interface met intelligente vervoerssystemen (ITS). Er moeten specificaties worden vastgesteld voor de technische eisen voor de constructie van slimme tachografen.

(2) De op grond van artikel 9, lid 4, van Verordening (EU) nr. 165/2014 ingevoerde vroegtijdige detectie op afstand moet de gegevens van de digitale tachograaf en de informatie over de gewichten en het gewicht per as van de volledige voertuigcombinatie (trekker en aanhanger of oplegger) overeenkomstig Richtlijn 96/53/EG van het Europees Parlement en de Raad ([2]) doorsturen naar de ambtenaar die wegcontroles uitvoert. Dit moet de controle-instanties in staat stellen voertuigen effectief en snel te controleren, terwijl er minder elektronische apparaten in de stuurcabine vereist zijn.

(3) Overeenkomstig Richtlijn 96/53/EG moet het systeem voor vroegtijdige detectie op afstand gebruikmaken van de CEN DSRC-normen ([3]), als bedoeld in die richtlijn in de frequentieband 5 795-5 805 MHz. Aangezien die frequentieband ook voor elektronische tolheffing wordt gebruikt en teneinde interferenties tussen tolheffings- en controletoepassingen te vermijden, mogen controleambtenaren het systeem voor vroegtijdige detectie op afstand niet op een tolplein gebruiken.

(4) De invoering van de slimme tachograaf moet gepaard gaan met de invoering van nieuwe veiligheidsmechanismen om het beveiligingsniveau van de digitale tachograaf op peil te houden en bestaande beveiligingslacunes weg te werken. Een van die lacunes is het ontbreken van een vervaldatum voor digitale certificaten. Om te voldoen aan de beste praktijken op het gebied van beveiliging moet het gebruik van digitale certificaten zonder vervaldatum worden vermeden. Een voertuigunit moet normaal gezien 15 jaar kunnen worden gebruikt, met ingang van de afgiftedatum van de digitale certificaten voor de unit. Na afloop van de geldigheidstermijn moeten voertuigunits worden vervangen.

([1]) PB L 60 van 28.2.2014, blz. 1.
([2]) Richtlijn 96/53/EG van de Raad van 25 juli 1996 houdende vaststelling, voor bepaalde aan het verkeer binnen de Gemeenschap deelnemende wegvoertuigen, van de in het nationale en het internationale verkeer maximaal toegestane afmetingen, en van de in het internationale verkeer maximaal toegestane gewichten (PB L 235 van 17.9.1996, blz. 59).
([3]) Specifieke normen voor korteafstandscommunicatie van het Europees Comité voor normalisatie (CEN) EN 12253, EN 12795, EN 12834, EN 13372 en ISO 14906.

(5) Het aanbieden van beveiligde en betrouwbare plaatsbepalingsinformatie is essentieel voor het doelmatig gebruik van slimme tachografen. Derhalve moet worden gewaarborgd dat de tachografen compatibel zijn met de via het Galileo-programma op grond van Verordening (EU) nr. 1285/2013 van het Europees Parlement en de Raad ([1]) aangeboden diensten met toegevoegde waarde om de beveiliging van de slimme tachograaf te verbeteren.

(6) Overeenkomstig artikel 8, lid 1, artikel 9, lid 1, en artikel 10, leden 1 en 2, van Verordening (EU) nr. 165/2014 moeten de bij die verordening ingevoerde beveiligingsmechanismen 36 maanden na de inwerkingtreding van de vereiste uitvoeringsbesluiten in werking treden teneinde de fabrikanten de tijd te geven om de nieuwe generatie slimme tachografen te ontwikkelen en hun typegoedkeuringscertificaten aan te vragen bij de bevoegde instanties.

(7) Overeenkomstig Verordening (EU) nr. 165/2014 moeten voertuigen die ten minste 36 maanden na de inwerkingtreding van die verordening voor het eerst in een lidstaat worden ingeschreven, uitgerust zijn met een slimme tachograaf die aan de eisen van deze verordening van de Commissie voldoet. In ieder geval moeten alle voertuigen die in een andere lidstaat dan de lidstaat van inschrijving worden ingezet, 15 jaar na de inwerkingtreding van die eisen met een conforme slimme tachograaf zijn uitgerust.

(8) Op grond van Verordening (EG) nr. 68/2009 ([2]) mocht gedurende een overgangsperiode tot en met 31 december 2013 een adapter worden gebruikt om een tachograaf te kunnen gebruiken in voertuigen van de categorieën M1 en N1. Gezien de technische problemen bij het zoeken naar een alternatief voor het gebruik van de adapter, zijn de deskundigen van de voertuig- en tachograaffabrikanten, samen met de Commissie, tot de conclusie gekomen dat een alternatieve oplossing voor de adapter voor de sector zou leiden tot hoge kosten die niet in verhouding staan tot de omvang van de markt. Derhalve moet het gebruik van de adapter in voertuigen van de types M1 en N1 voor onbeperkte duur worden toegestaan.

(9) 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

Onderwerp en werkingssfeer

1. Bij deze verordening worden de regels vastgesteld die noodzakelijk zijn voor de uniforme toepassing van de volgende aspecten betreffende tachografen:

a) registratie van de positie van het voertuig op bepaalde momenten tijdens de dagelijkse werktijd van de bestuurder;

b) vroegtijdige detectie op afstand van eventueel manipulatie of misbruik van slimme tachografen;

c) interface met intelligente vervoerssystemen;

d) de administratieve en technische eisen voor de typegoedkeuringsprocedure voor tachografen, met inbegrip van de beveiligingsmechanismen.

2. Bij de constructie, het testen, de installatie, de inspectie, het gebruik en de reparatie van slimme tachografen en hun onderdelen moeten de in de bijlage vastgestelde technische eisen in acht worden genomen.

3. Voor de constructie, het testen, de installatie, de inspectie, het gebruik en de reparatie van andere tachografen dan slimme tachografen blijven de eisen van bijlage 1 of bijlage 1B bij Verordening (EEG) nr. 3821/85 van de Raad ([3]) van toepassing.

([1]) Verordening (EU) nr. 1285/2013 van het Europees Parlement en de Raad van 11 december 2013 betreffende de uitvoering en exploitatie van de Europese satellietnavigatiesystemen en tot intrekking van Verordening (EG) nr. 876/2002 van de Raad en Verordening (EG) nr. 683/2008 van het Europees Parlement en de Raad (PB L 347 van 20.12.2013, blz. 1).

([2]) Verordening (EG) nr. 68/2009 van de Commissie van 23 januari 2009 betreffende de negende aanpassing aan de vooruitgang van de techniek van Verordening (EEG) nr. 3821/85 van de Raad betreffende het controleapparaat in het wegvervoer (PB L 21 van 24.1.2009, blz. 3).

([3]) 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).

4. Overeenkomstig artikel 10 quinquies van Richtlijn 96/53/EG moet het systeem voor de vroegtijdige detectie op afstand de gewichtsgegevens die door de interne weegapparatuur van het voertuig worden gegenereerd, doorsturen met het oog op de vroegtijdige detectie van fraude.

Artikel 2

Definities

Voor de toepassing van deze verordening gelden de definities van artikel 2 van Verordening (EU) nr. 165/2014.

Bovendien wordt verstaan onder:

1) „digitale tachograaf" of „tachograaf van de eerste generatie": een andere digitale tachograaf dan een slimme tachograaf;

2) „extern GNSS-systeem": het systeem dat de GNSS-ontvanger bevat wanneer de voertuigunit uit meer dan één unit bestaat, alsmede de andere onderdelen die nodig zijn voor de bescherming van de naar de rest van de voertuigunit doorgestuurde plaatsbepalingsgegevens;

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 1C bij deze verordening gedefinieerde testen, alsmede schema's, afbeeldingen en andere documenten;

4) „informatiepakket": de papieren of elektronische informatiebrochure, vergezeld van de andere tijdens de uitoefening van haar functies door de typegoedkeuringsinstantie aan de informatiebrochure toegevoegde documenten, waaronder het na afloop van de typegoedkeuringsprocedure afgegeven EG-typegoedkeuringscertificaat van de tachograaf of het tachograafonderdeel;

5) „index bij het informatiepakket": het document met een lijst van de genummerde inhoud van het informatiepakket en een overzicht van alle relevante delen van dat pakket. In het opzet van dit document wordt een onderscheid gemaakt tussen de verschillende stappen van de EG-typegoedkeuringsprocedure, met vermelding van de data waarop het pakket eventueel is herzien of bijgewerkt;

6) „systeem voor vroegtijdige detectie op afstand": de apparatuur van de voertuigunit die voor de uitvoering van wegcontroles wordt gebruikt;

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 1C bij deze verordening;

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

9) „typegoedkeuringsinstantie": de instantie van een lidstaat die bevoegd is voor de typegoedkeuring van tachografen of tachograafonderdelen, de goedkeuringsprocedure, de afgifte en desgevallend intrekking van typegoedkeuringscertificaten, die optreedt als aanspreekpunt voor de typegoedkeuringsinstanties van andere lidstaten en die erop toeziet dat fabrikanten hun verplichtingen op grond van deze verordening nakomen.

Artikel 3

Locatiegebaseerde diensten

1. De fabrikanten zorgen ervoor dat slimme tachografen compatibel zijn met de plaatsbepalingsdiensten die worden aangeboden door Galileo en de European Geostationary Navigation Overlay Service (Egnos).

2. Boven op de in de eerste alinea genoemde diensten mogen fabrikanten ook de compatibiliteit met andere satellietnavigatiesystemen waarborgen.

Artikel 4

Procedure voor de typegoedkeuring van tachografen en tachograafonderdelen

1. Een fabrikant of zijn gemachtigde dient een aanvraag voor de typegoedkeuring van een tachograaf, tachograafonderdeel of groep onderdelen in bij de door elke lidstaat aangewezen typegoedkeuringsinstanties. Deze aanvraag omvat een informatiebrochure met informatie over alle onderdelen, waaronder desgevallend de typegoedkeuringscertificaten van andere onderdelen die deel uitmaken van de volledige tachograaf, alsmede alle andere relevante documenten.

2. Een lidstaat verleent een typegoedkeuring voor een tachograaf, tachograafonderdeel of groep onderdelen die, naargelang het geval, voldoet aan de administratieve en technische eisen als bedoeld in artikel 1, lid 2 of 3. In dat geval verleent de typegoedkeuringsinstantie de aanvrager een typegoedkeuringscertificaat dat overeenstemt met het model in bijlage II bij deze verordening.

3. De typegoedkeuringsinstantie kan de fabrikant of zijn gemachtigde om aanvullende informatie verzoeken.

4. De fabrikant of zijn gemachtigde stelt voldoende tachografen of tachograafonderdelen ter beschikking van de typegoedkeuringsinstanties en de met de afgifte van de in artikel 12, lid 3, van Verordening (EU) nr. 165/2014 bedoelde certificaten belaste instanties om de typegoedkeuringsprocedure correct te kunnen uitvoeren.

5. Een fabrikant of zijn gemachtigde die een typegoedkeuring van bepaalde tachograafonderdelen of groepen onderdelen aanvraagt, zorgt ervoor dat de typegoedkeuringsinstanties kunnen beschikken over de andere reeds goedgekeurde tachograafonderdelen, alsmede over alle andere onderdelen die nodig zijn om een volledige tachograaf samen te stellen, zodat de instanties de nodige tests kunnen uitvoeren.

Artikel 5

Wijzigingen van typegoedkeuringen

1. De fabrikant of zijn gemachtigde stelt de typegoedkeuringsinstantie die de oorspronkelijke typegoedkeuring heeft verleend, onverwijld in kennis van alle wijzigingen aan de software of hardware van de tachograaf of de aard van de in het informatiepakket vermelde materialen waaruit de tachograaf is vervaardigd, en dient een verzoek tot wijziging van de typegoedkeuring in.

2. De typegoedkeuringsinstanties kunnen een bestaande typegoedkeuring herzien of verlengen, dan wel een nieuwe afgeven in het licht van de aard en kenmerken van de wijzigingen.

Een typegoedkeuring wordt „herzien" wanneer de typegoedkeuringsinstantie van oordeel is dat de wijzigingen aan de software of hardware van de tachograaf of aan de aard van de materialen waaruit deze is vervaardigd, minimaal zijn. In dergelijke gevallen stelt de typegoedkeuringsinstantie herziene documenten van het informatiepakket op met vermelding van de aard van de wijzigingen en van de datum waarop ze zijn goedgekeurd. Om aan deze eis te voldoen, volstaat een geconsolideerde bijgewerkte versie van het informatiepakket met een nauwkeurige beschrijving van de aangebrachte wijzigingen.

Een typegoedkeuring wordt „verlengd" wanneer de typegoedkeuringsinstantie van oordeel is dat de wijzigingen aan de software of hardware van de tachograaf of aan de aard van de materialen waaruit deze is vervaardigd, significant zijn. In dergelijke gevallen kan zij eisen dat nieuwe testen worden uitgevoerd en stelt zij de fabrikant of zijn gemachtigde daarvan in kennis. Indien deze testen naar wens verlopen, geeft de typegoedkeuringsinstantie een herzien typegoedkeuringscertificaat af, met een nummer dat naar de toegestane verlenging verwijst. De typegoedkeuringsinstantie vermeldt de reden voor de verlenging en de datum van afgifte.

3. In de index van het informatiepakket wordt de datum van de jongste verlenging of herziening van de typegoedkeuring vermeld, dan wel de datum van de jongste geconsolideerde of bijgewerkte versie van de typegoedkeuring.

4. Een nieuwe typegoedkeuring is noodzakelijk wanneer op basis van de gevraagde aanpassingen van de goedgekeurde tachograaf of tachograafonderdelen een nieuw beveiligings- of interoperabiliteitscertificaat moet worden afgegeven.

Artikel 6

Inwerkingtreding

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

Zij is van toepassing met ingang van 2 maart 2016.

De bijlagen zijn evenwel van toepassing met ingang van 2 maart 2019, met uitzondering van aanhangsel 16, dat met ingang van 2 maart 2016 van toepassing is.

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

Gedaan te Brussel, 18 maart 2016.

Voor de Commissie

De voorzitter

Jean-Claude JUNCKER

BIJLAGE I C

Constructie-, test-, installatie- en controlevoorschriften

INLEIDING 12

1 DEFINITIES 13

2 ALGEMENE KENMERKEN EN FUNCTIES VAN HET CONTROLEAPPARAAT 19

2.1 Algemene kenmerken 19

2.2 Functies 20

2.3 Werkingsmodi 21

2.4 Beveiliging 22

3 CONSTRUCTIE EN FUNCTIONELE EISEN VOOR CONTROLEAPPARATEN 22

3.1 Controle op het inbrengen en uitnemen van kaarten 22

3.2 Meting van snelheid, positie en afstand 23

3.2.1 Meting van de afgelegde afstand 23

3.2.2 Meting van de snelheid 23

3.2.3 Bepalen van de positie 24

3.3 Tijdmeting 24

3.4 Controle op activiteiten van bestuurders 24

3.5 Controle op de status van bestuurders 25

3.6 Invoer door bestuurders 25

3.6.1 Invoer van begin- en eindpunt van de dagelijkse werkperiode 25

3.6.2 Manuele invoer van bestuurdersactiviteiten en toestemming van de bestuurder voor de ITS-interface ... 25

3.6.3 Invoer van specifieke omstandigheden 27

3.7 Beheer van bedrijfsvergrendelingen 27

3.8 Bewaken van controleactiviteiten 28

3.9 Opsporing van voorvallen en/of fouten 28

3.9.1 „Inbrengen van een ongeldige kaart” 28

3.9.2 „Kaartconflict” 28

3.9.3 „Tijdsoverlapping” 28

3.9.4 „Rijden zonder geschikte kaart” 29

3.9.5 „Inbrengen van de kaart tijdens het rijden” 29

3.9.6 „Laatste kaartsessie niet correct afgesloten” 29

3.9.7 „Snelheidsoverschrijding” 29

3.9.8 „Onderbreking van de stroomvoorziening” 29

3.9.9 „Communicatiefout met het systeem voor communicatie op afstand” 29

3.9.10 „Ontbreken van plaatsbepalingsinformatie van de GNSS-ontvanger” 29

3.9.11	„Fout in communicatie met de externe GNSS-module”	30
3.9.12	„Fout in de bewegingsgegevens”	30
3.9.13	„Tegenstrijdige bewegingsgegevens”	30
3.9.14	„Poging tot inbreuk op de beveiliging”	30
3.9.15	„Tijdsoverlapping”	30
3.9.16	„Kaartfout”	30
3.9.17	„Controleapparaatfout”	30
3.10	Ingebouwde tests en zelftests	31
3.11	Lezen van het geheugen	31
3.12	Registratie en opslag in het geheugen	31
3.12.1	Identificatiegegevens van de uitrusting	32
3.12.1.1	Identificatiegegevens van de voertuigunit	32
3.12.1.2	Identificatiegegevens van de bewegingssensor	32
3.12.1.3	Identificatiegegevens GNSS-systemen	33
3.12.2	Sleutels en certificaten	33
3.12.3	Gegevens over het inbrengen en uitnemen van de bestuurders- of werkplaatskaart	33
3.12.4	Gegevens over activiteiten van de bestuurder	34
3.12.5	Plaatsen en posities waar de dagelijkse werktijd begint, eindigt en/of waar een ononderbroken rijtijd van 3 uur wordt bereikt	34
3.12.6	Gegevens over de kilometerstand	35
3.12.7	Gedetailleerde snelheidsgegevens	35
3.12.8	Gegevens over voorvallen	35
3.12.9	Gegevens over fouten	37
3.12.10	Kalibreringsgegevens	38
3.12.11	Tijdafstellingsgegevens	39
3.12.12	Gegevens over controleactiviteiten	39
3.12.13	Gegevens over bedrijfsvergrendelingen	39
3.12.14	Gegevens over overdrachtactiviteiten	39
3.12.15	Gegevens over specifieke omstandigheden	40
3.12.16	Gegevens tachograafkaart	40
3.13	Lezen van de tachograafkaart	40
3.14	Registratie en opslag op een tachograafkaart	40
3.14.1	Registreren en opslaan op tachograafkaarten van de eerste generatie	40
3.14.2	Registreren en opslaan op tachograafkaarten van de tweede generatie	41
3.15	Weergave	41
3.15.1	Standaarddisplay	42

3.15.2	Waarschuwingsdisplay	43
3.15.3	Toegang tot het menu	43
3.15.4	Overige displays	43
3.16	Afdrukken	43
3.17	Waarschuwingen	44
3.18	Downloaden van gegevens met externe media	45
3.19	Communicatie op afstand met het oog op gerichte wegcontroles	45
3.20	Doorsturen van gegevens naar aanvullende externe apparaten	46
3.21	Kalibrering	47
3.22	Kalibreringscontrole langs de weg	47
3.23	Tijdafstelling	48
3.24	Prestatiekenmerken	48
3.25	Materialen	48
3.26	Opschriften	49
4	FUNCTIONELE EN CONSTRUCTIE-EISEN VOOR TACHOGRAAFKAARTEN	49
4.1	Zichtbare gegevens	49
4.2	Beveiliging	52
4.3	Normen	53
4.4	Milieu- en elektrotechnische specificaties	53
4.5	Opslag van gegevens	53
4.5.1	Hoofdbestanden voor identificatie en kaartbeheer	54
4.5.2	IC-kaartidentificatie	54
4.5.2.1	Chipidentificatie	54
4.5.2.2	DIR (alleen aanwezig in tachograafkaarten van de tweede generatie)	54
4.5.2.3	ATR-informatie (voorwaardelijk, alleen aanwezig in tachograafkaarten van de tweede generatie)	54
4.5.2.4	Uitgebreide informatie (voorwaardelijk, alleen aanwezig in tachograafkaarten van de tweede generatie)	55
4.5.3	Bestuurderskaart	55
4.5.3.1	Tachograaftoepassingen (toegankelijk voor voertuigunits van de eerste en tweede generatie)	55
4.5.3.1.1	Toepassingsidentificatie	55
4.5.3.1.2	Sleutels en certificaten	55
4.5.3.1.3	Identificatie van de kaart	55
4.5.3.1.4	Identificatie van de kaarthouder	55
4.5.3.1.5	Kaartgegevens downloaden	55
4.5.3.1.6	Informatie over het rijbewijs	55
4.5.3.1.7	Gegevens over voorvallen	56

4.5.3.1.8 Gegevens over fouten 56
4.5.3.1.9 Gegevens over de activiteiten van de bestuurder 57
4.5.3.1.10 Gegevens over de gebruikte voertuigen 57
4.5.3.1.11 Plaatsen waar dagelijkse werkperioden beginnen en/of eindigen 58
4.5.3.1.12 Gegevens over kaartsessies 58
4.5.3.1.13 Gegevens over controleactiviteiten 58
4.5.3.1.14 Gegevens over specifieke omstandigheden 58
4.5.3.2 Toepassing tachograaf van de 2de generatie (niet toegankelijk voor voertuigunits van de eerste generatie) 59
4.5.3.2.1 Toepassingsidentificatie 59
4.5.3.2.2 Sleutels en certificaten 59
4.5.3.2.3 Identificatie van de kaart 59
4.5.3.2.4 Identificatie van de kaarthouder 59
4.5.3.2.5 Kaartgegevens downloaden 59
4.5.3.2.6 Informatie over het rijbewijs 59
4.5.3.2.7 Gegevens over voorvallen 59
4.5.3.2.8 Gegevens over fouten 60
4.5.3.2.9 Gegevens over de activiteiten van de bestuurder 61
4.5.3.2.10 Gegevens over de gebruikte voertuigen 61
4.5.3.2.11 Plaatsen en posities waar de dagelijkse werkperioden beginnen en/of eindigen 62
4.5.3.2.12 Gegevens over kaartsessies 62
4.5.3.2.13 Gegevens over controleactiviteiten 62
4.5.3.2.14 Gegevens over specifieke omstandigheden 63
4.5.3.2.15 Gegevens over de gebruikte voertuigunits 63
4.5.3.2.16 Plaats en tijdstip ononderbroken rijtijd van drie uur 63
4.5.4 Werkplaatskaart 63
4.5.4.1 Tachograaftoepassingen (toegankelijk voor voertuigunits van de eerste en tweede generatie) 63
4.5.4.1.1 Toepassingsidentificatie 63
4.5.4.1.2 Sleutels en certificaten 63
4.5.4.1.3 Identificatie van de kaart 64
4.5.4.1.4 Identificatie van de kaarthouder 64
4.5.4.1.5 Kaartgegevens downloaden 64
4.5.4.1.6 Gegevens over kalibrering en tijdafstelling 64

4.5.4.1.7 Gegevens over voorvallen en fouten 65
4.5.4.1.8 Gegevens over de activiteiten van de bestuurder 65
4.5.4.1.9 Gegevens over de gebruikte voertuigen 65
4.5.4.1.10 Gegevens over het begin en einde van dagelijkse werkperioden 65
4.5.4.1.11 Gegevens over kaartsessies 65
4.5.4.1.12 Gegevens over controleactiviteiten 65
4.5.4.1.13 Gegevens over specifieke omstandigheden 65
4.5.4.2 Toepassing tachograaf van de tweede generatie (niet toegankelijk voor voertuigunits van de eerste generatie) 65
4.5.4.2.1 Toepassingsidentificatie 65
4.5.4.2.2 Sleutels en certificaten 66
4.5.4.2.3 Identificatie van de kaart 66
4.5.4.2.4 Identificatie van de kaarthouder 66
4.5.4.2.5 Kaartgegevens downloaden 66
4.5.4.2.6 Gegevens over kalibrering en tijdafstelling 66
4.5.4.2.7 Gegevens over voorvallen en fouten 67
4.5.4.2.8 Gegevens over de activiteiten van de bestuurder 67
4.5.4.2.9 Gegevens over de gebruikte voertuigen 67
4.5.4.2.10 Gegevens over het begin en einde van dagelijkse werkperioden 67
4.5.4.2.11 Gegevens over kaartsessies 67
4.5.4.2.12 Gegevens over controleactiviteiten 67
4.5.4.2.13 Gegevens over de gebruikte voertuigunits 67
4.5.4.2.14 Plaats en tijdstip ononderbroken rijtijd van drie uur 68
4.5.4.2.15 Gegevens over specifieke omstandigheden 68
4.5.5 Controlekaart 68
4.5.5.1 Tachograaftoepassingen (toegankelijk voor voertuigunits van de eerste en tweede generatie) 68
4.5.5.1.1 Toepassingsidentificatie 68
4.5.5.1.2 Sleutels en certificaten 68
4.5.5.1.3 Identificatie van de kaart 68
4.5.5.1.4 Identificatie van de kaarthouder 68
4.5.5.1.5 Gegevens over controleactiviteiten 69
4.5.5.2 Tachograaftoepassingen van de tweede generatie (niet toegankelijk voor voertuigunits van de eerste generatie) 69
4.5.5.2.1 Toepassingsidentificatie 69
4.5.5.2.2 Sleutels en certificaten 69

4.5.5.2.3	Identificatie van de kaart	69
4.5.5.2.4	Identificatie van de kaarthouder	69
4.5.5.2.5	Gegevens over controleactiviteiten	70
4.5.6	Bedrijfskaart	70
4.5.6.1	Tachograaftoepassingen (toegankelijk voor voertuigunits van de eerste en tweede generatie)	70
4.5.6.1.1	Toepassingsidentificatie	70
4.5.6.1.2	Sleutels en certificaten	70
4.5.6.1.3	Identificatie van de kaart	70
4.5.6.1.4	Identificatie van de kaarthouder	70
4.5.6.1.5	Gegevens over bedrijfsactiviteiten	70
4.5.6.2	Tachograaftoepassingen van de tweede generatie (niet toegankelijk voor voertuigunits van de eerste generatie)	71
4.5.6.2.1	Toepassingsidentificatie	71
4.5.6.2.2	Sleutels en certificaten	71
4.5.6.2.3	Identificatie van de kaart	71
4.5.6.2.4	Identificatie van de kaarthouder	71
4.5.6.2.5	Gegevens over bedrijfsactiviteiten	71
5	INSTALLATIE VAN HET CONTROLEAPPARAAT	72
5.1	Installatie	72
5.2	Installatieplaatje	73
5.3	Verzegeling	74
6	CONTROLES, INSPECTIES EN HERSTELLINGEN	74
6.1	Erkenning van installateurs, werkplaatsen en voertuigfabrikanten	74
6.2	Controle van nieuwe of herstelde inrichtingen	75
6.3	Installatie-inspectie	75
6.4	Periodieke controles	75
6.5	Meting van afwijkingen	76
6.6	Reparaties	76
7	AFGIFTE VAN KAARTEN	76
8	TYPEGOEDKEURING VAN CONTROLEAPPARATEN EN TACHOGRAAFKAARTEN	77
8.1	Algemeen	77
8.2	Veiligheidscertificaat	78
8.3	Functiecertificaat	78
8.4	Interoperabiliteitscertificaat	78
8.5	Typegoedkeuringscertificaat	79
8.6	Bijzondere procedure: eerste interoperabiliteitscertificaten voor controleapparaten en tachograafkaarten van de 2de generatie	80

INLEIDING

Digitale tachografen van de eerste generatie worden sinds 1 mei 2006 gebruikt. Zij mogen tot einde levensduur worden gebruikt voor binnenlands vervoer. Voor internationaal vervoer daarentegen, moeten alle voertuigen uiterlijk 15 jaar na de vankrachtwording van deze verordening van de Commissie uitgerust zijn met een slimme tachograaf van de tweede generatie als beschreven in deze verordening.

In deze bijlagen worden de eisen beschreven voor controleapparaten en tachograafkaarten van de tweede generatie. Vanaf de introductiedatum wordt controleapparatuur van de tweede generatie geïnstalleerd in voertuigen die voor het eerst worden ingeschreven, en worden tachograafkaarten van de tweede generatie afgegeven.

Om een vlotte introductie van de tachograaf van de tweede generatie te waarborgen:

— wordt er bij het ontwerp van de tachograafkaarten van de tweede generatie voor gezorgd dat ze ook in voertuigunits van de eerste generatie kunnen worden gebruikt;

— zal het niet verplicht zijn geldige kaarten van de eerste generatie op de introductiedatum te vervangen.

Hierdoor kunnen bestuurders hun unieke kaart behouden en deze in beide systemen gebruiken.

Controleapparaten van de tweede generatie worden echter alleen gekalibreerd met behulp van werkplaatskaarten van de tweede generatie.

In deze bijlage zijn alle eisen opgenomen in verband met de interoperabiliteit tussen de tachografen van de eerste en tweede generatie.

In aanhangsel 15 is nauwkeurig beschreven hoe het naast elkaar bestaan van de twee systemen moet worden beheerd.

Lijst van aanhangsels

Aanhangsel 1: DATA DICTIONARY

Aanhangsel 2: SPECIFICATIE VAN TACHOGRAAFKAARTEN

Aanhangsel 3: PICTOGRAMMEN

Aanhangsel 4: AFDRUKKEN

Aanhangsel 5: DISPLAY

Aanhangsel 6: FRONTCONNECTOR VOOR KALIBRERING EN DOWNLOADEN

Aanhangsel 7: PROTOCOL VOOR GEGEVENSOVERDRACHT

Aanhangsel 8: KALIBRERINGSPROTOCOL

Aanhangsel 9: TYPEGOEDKEURING EN LIJST VAN MINIMAAL VEREISTE TESTS

Aanhangsel 10: BEVEILIGINGSVOORSCHRIFTEN

Aanhangsel 11: ALGEMENE BEVEILIGINGSMECHANISMEN

Aanhangsel 12: PLAATSBEPALING OP BASIS VAN WERELDWIJD SATELLIETNAVIGATIESYSTEEM (GNSS)

Aanhangsel 13: ITS-INTERFACE

Aanhangsel 14: FUNCTIE VOOR COMMUNICATIE OP AFSTAND

Aanhangsel 15: MIGRATIE: DE COËXISTENTIE VAN VERSCHILLENDE GENERATIES APPARATUUR BEHEREN

Aanhangsel 16: ADAPTER VOOR VOERTUIGEN VAN DE CATEGORIE M1 EN N1

1 DEFINITIES

In deze bijlage wordt verstaan onder:

a) „activering”:

de fase waarin de tachograaf volledig operationeel wordt en alle functies, inclusief de veiligheidsfuncties, uitvoert, met gebruikmaking van een werkplaatskaart;

b) „authenticatie”:

een functie om een opgegeven identiteit vast te stellen en te verifiëren;

c) „authenticiteit”:

de eigenschap dat informatie afkomstig is van een persoon wiens identiteit kan worden geverifieerd;

d) „ingebouwd testsysteem (BIT)”:

tests die op verzoek worden uitgevoerd en door de bestuurder of een externe inrichting worden gestart;

e) „kalenderdag”:

een dag van 00.00 uur tot en met 24.00 uur. Alle kalenderdagen worden uitgedrukt in UTC-tijd (gecoördineerde universele tijd);

f) „kalibrering” van een digitale tachograaf:

het bijwerken of bevestigen van voertuigparameters die in het geheugen opgeslagen zijn. Voertuigparameters zijn onder andere voertuigidentificatie (VIN (voertuigidentificatienummer), kentekennummer en de lidstaat van registratie) en voertuigkenmerken (w, k, l, bandenmaat, snelheidsbegrenzer (indien van toepassing), actuele UTC-tijd, actuele kilometerstand). Bij de kalibrering van een controleapparaat worden het type en de identificatiecodes van alle aanwezige verzegelingen die relevant zijn voor de typekeuring, opgeslagen in het geheugen.

Het bijwerken of bevestigen van alleen de UTC-tijd wordt beschouwd als een tijdafstelling en niet als een kalibrering, op voorwaarde dat er geen tegenspraak is met voorschrift 409.

Voor het kalibreren van een controleapparaat is een werkplaatskaart nodig;

g) „kaartnummer”:

een nummer van 16 alfanumerieke tekens dat een tachograafkaart binnen een lidstaat op unieke wijze identificeert. Het kaartnummer omvat een opeenvolgende index van de kaart (indien van toepassing), een vervangingsindex van de kaart en een vernieuwingsindex van de kaart.

Een kaart wordt dus op unieke wijze door de code van de lidstaat van afgifte en het kaartnummer geïdentificeerd;

h) „opeenvolgende index van de kaart”:

het 14e teken van een kaartnummer, dat wordt gebruikt om de verschillende kaarten te onderscheiden die zijn afgegeven aan een bedrijf, werkplaats of controle-instantie die meerdere tachograafkaarten mag bezitten. Het bedrijf, de werkplaats of de controle-instantie wordt op unieke wijze door de eerste 13 tekens van het kaartnummer geïdentificeerd;

i) „vernieuwingsindex van de kaart”:

het 16e alfanumerieke teken van een kaartnummer, dat bij elke vernieuwing van een tachograafkaart verhoogd wordt;

j) „vervangingsindex van de kaart”:

het 15e alfanumerieke teken van een kaartnummer, dat bij elke vervanging van een tachograafkaart verhoogd wordt;

k) „kenmerkende coëfficiënt van het voertuig":

het getal dat de waarde aangeeft van het uitgangssignaal dat door het onderdeel van het voertuig (secundaire as van de versnellingsbak of as) dat in verbinding staat met het controleapparaat, wordt verstuurd wanneer het voertuig een afstand van één kilometer heeft afgelegd, gemeten onder normale testomstandigheden als gedefinieerd in voorschrift nr. 414. De kenmerkende coëfficiënt wordt uitgedrukt in impulsen per kilometer (w = … imp/km);

l) „bedrijfskaart":

een tachograafkaart die door de autoriteiten van een lidstaat is afgegeven aan een vervoersonderneming welke met tachografen uitgeruste voertuigen moet gebruiken, die de vervoersonderneming identificeert en waarmee de in de tachografen opgeslagen gegevens, die door de vervoersonderneming zijn versleuteld, kunnen worden weergegeven, gedownload en afgedrukt;

m) „constante van het controleapparaat":

het getal dat de waarde aangeeft van het ingangssignaal dat nodig is ter aanwijzing en registratie van een afgelegde afstand van één kilometer; deze constante moet in impulsen per kilometer (k = … imp/km) worden uitgedrukt;

n) de „rijtijd" wordt in het controleapparaat berekend als ([1]):

de op dat moment cumulatieve rijtijd van een individuele bestuurder afzonderlijk sinds het verstrijken van zijn laatste BESCHIKBAARHEID, RUSTPAUZE of ONBEKENDE ([2]) periode van 45 minuten of meer (deze periode kan worden opgedeeld overeenkomstig Verordening (EG) nr. 561/2006 van het Europees Parlement en de Raad ([3])). De betreffende berekeningen houden, indien nodig, rekening met eerdere op de bestuurderskaart opgeslagen activiteiten. Wanneer de bestuurder zijn kaart niet heeft ingebracht, zijn de betreffende berekeningen gebaseerd op de geheugenrecords voor de lopende periode waarin geen kaart ingebracht was, en met betrekking tot de relevante lezer;

o) „controlekaart":

een door de autoriteiten van een lidstaat aan een nationale bevoegde controle-instantie afgegeven tachograafkaart die de controle-instanties en, eventueel, de controleambtenaar identificeert en die toegang verschaft tot de in het geheugen, op de bestuurderskaart en, eventueel, op de werkplaatskaart opgeslagen gegevens om deze te lezen, af te drukken en/of te downloaden.

Deze kaart dient ook toegang te verschaffen tot de functie voor kalibreringscontroles langs de weg en de gegevens op het leestoestel voor berichten voor vroegtijdige detectie op afstand;

p) „cumulatieve rusttijd" wordt in het controleapparaat berekend als ([1]):

de cumulatieve onderbreking van de rijtijd wordt berekend als de op dat moment verzamelde BESCHIKBAARHEIDS-, RUSTPAUZE- of ONBEKENDE ([2]) perioden van 15 minuten of meer van elke bestuurder afzonderlijk sinds zijn laatste BESCHIKBAARHEIDS-, RUSTPAUZE- of ONBEKENDE ([2]) periode van 45 minuten of meer (deze periode kan worden opgedeeld overeenkomstig Verordening (EG) nr. 561/2006).

De betreffende berekeningen houden, indien nodig, rekening met eerdere op de bestuurderskaart opgeslagen activiteiten. Bij de berekening wordt geen rekening gehouden met onbekende periodes van negatieve duur (begin van een onbekende periode > einde van een onbekende periode) ten gevolge van tijdsoverlapping tussen twee verschillende controleapparaten.

Wanneer de bestuurder zijn kaart niet heeft ingebracht, zijn de betreffende berekeningen gebaseerd op de geheugenrecords voor de lopende periode waarin geen kaart was ingebracht, en voor de relevante lezer;

([1]) Door deze berekeningswijze van de rijtijd en de cumulatieve rusttijd kan het controleapparaat de rijtijdwaarschuwing berekenen. Hiermee wordt niet vooruitgelopen op de wettelijke interpretatie van deze tijden. Alternatieve manieren voor het berekenen van de rijtijd en de cumulatieve rusttijd kunnen worden gebruikt ter vervanging van deze definities, indien deze voorbijgestreefd zijn door andere bijgewerkte wetgeving.

([2]) ONBEKENDE periodes komen overeen met periodes waarin de bestuurderskaart niet in het controleapparaat ingebracht was en activiteiten van de bestuurder niet manueel zijn ingevoerd.

([3]) Verordening (EG) nr. 561/2006 van het Europees Parlement en de Raad van 15 maart 2006 tot harmonisatie van bepaalde voorschriften van sociale aard voor het wegvervoer, tot wijziging van Verordeningen (EEG) nr. 3821/85 en (EG) nr. 2135/98 van de Raad en tot intrekking van Verordening (EEG) nr. 3820/85 van de Raad (PB L 102 van 11.4.2006, blz. 1).

q) „geheugen”:

een elektronisch geheugenmedium dat is ingebouwd in het controleapparaat;

r) „digitale handtekening”:

gegevens toegevoegd aan, of een cryptografische transformatie van, een gegevensblok waarmee de ontvanger van die gegevens de authenticiteit en integriteit van de gegevens kan verifiëren;

s) „downloaden”:

het kopiëren, samen met een digitale handtekening, van (een gedeelte van) de gegevensbestanden die in het geheugen van de voertuigunit of in het geheugen van de tachograafkaart zijn geregistreerd, op voorwaarde dat dit proces geen opgeslagen gegevens wijzigt of vernietigt.

Fabrikanten van slimme tachografen voor voertuigen en fabrikanten van apparatuur die is ontworpen en bedoeld om gegevens te downloaden, moeten alle maatregelen nemen die redelijkerwijs haalbaar zijn om ervoor te zorgen dat die gegevens met minimale vertraging door vervoersondernemingen of bestuurders kunnen worden gedownload.

Het downloaden van gedetailleerde snelheidsgegevens is niet per definitie nodig om te voldoen aan Verordening (EG) nr. 561/2006, maar kan worden gebruikt voor andere doeleinden, zoals het onderzoeken van ongevallen;

t) „bestuurderskaart”:

een door de autoriteiten van een lidstaat aan elke bestuurder afzonderlijk afgegeven tachograafkaart die de bestuurder identificeert en de activiteiten van de bestuurder registreert;

u) „effectieve omtrek van de wielen”:

gemiddelde afstand, afgelegd door elk van de wielen die het voertuig aandrijven, (aandrijfwielen) bij een volledige omwenteling. Het meten van deze afstanden moet gebeuren onder normale testomstandigheden als gedefinieerd in voorschrift nr. 414 en wordt als volgt uitgedrukt: „l = … mm”. Voertuigfabrikanten kunnen het meten van deze afstanden vervangen door een theoretische berekening waarbij wordt uitgegaan van de verdeling van het gewicht over de assen van een ongeladen voertuig in normale rijklare toestand ([1]). De methode voor die theoretische berekening moet worden goedgekeurd door de bevoegde instantie van de lidstaat en dat moet gebeuren voor de tachograaf in werking wordt gesteld;

v) „voorval”:

een door de slimme tachograaf gedetecteerd abnormaal functioneren dat mogelijk het gevolg is van een poging tot fraude;

w) „externe GNSS-module”:

wanneer een voertuigunit uit verschillende onderdelen bestaat, de voorziening met de GNSS-ontvanger en de andere onderdelen die nodig zijn om de overdracht van positiegegevens naar de rest van de voertuigunit te beveiligen;

x) „fout”:

een door de slimme tachograaf ontdekt abnormaal functioneren dat mogelijk het gevolg is van een slechte werking van of storing in het apparaat;

y) „GNSS-ontvanger”:

een elektronisch apparaat dat signalen van een of meer mondiale satellietnavigatiesystemen (in het Engels: GNSS) ontvangt en digitaal verwerkt om de positie-, snelheids- en tijdsinformatie te verstrekken;

z) „installatie”:

de installatie van de tachograaf in een voertuig;

([1]) Verordening (EU) nr. 1230/2012 van de Commissie van 12 december 2012 tot uitvoering van Verordening (EG) nr. 661/2009 van het Europees Parlement en de Raad wat de typegoedkeuringsvoorschriften voor massa's en afmetingen van motorvoertuigen en aanhangwagens daarvan betreft en tot wijziging van Richtlijn 2007/46/EG van het Europees Parlement en de Raad (PB L 353 van 21.12.2012, blz. 31), als laatstelijk gewijzigd.

aa) „interoperabiliteit":

het vermogen van systemen en van de daaraan ten grondslag liggende bedrijfsprocessen om onderling gegevens uit te wisselen en informatie te delen;

bb) „interface":

een voorziening tussen systemen die de communicatiemiddelen verschaft waardoor deze systemen aan elkaar kunnen worden gekoppeld en onderling kunnen communiceren;

cc) „positie":

geografische coördinaten van een voertuig op een bepaald tijdstip;

dd) „bewegingssensor":

deel van de tachograaf dat een signaal geeft betreffende de snelheid van het voertuig en/of de afgelegde afstand;

ee) „ongeldige kaart":

een kaart die ongeldig is of waarvan de eerste authenticatie mislukt is, of waarvan de geldigheidstermijn nog niet begonnen is of reeds verstreken is;

ff) „open norm":

een norm vastgelegd in een normspecificatiedocument, gratis of tegen geringe kosten verkrijgbaar, die gratis of voor een gering bedrag gekopieerd, verspreid en gebruikt mag worden;

gg) „niet verplicht":

gevallen waarin het gebruik van het controleapparaat volgens de bepalingen van Verordening (EG) nr. 561/2006 niet vereist is;

hh) „snelheidsoverschrijding":

overschrijding van de toegestane maximumsnelheid van het voertuig, omschreven als een periode van meer dan 60 seconden waarin de gemeten snelheid van het voertuig hoger ligt dan de maximumsnelheid waarop de snelheidsbegrenzer is afgesteld, zoals vastgelegd in Richtlijn 92/6/EEG van de Raad [1], als laatstelijk gewijzigd;

ii) „periodieke controle":

een reeks verrichtingen die wordt uitgevoerd om te controleren of de tachograaf goed werkt en of de instellingen overeenkomen met de voertuigparameters en of er geen manipulatieapparatuur aan de tachograaf is bevestigd;

jj) „printer":

deel van het controleapparaat dat opgeslagen gegevens afdrukt;

kk) „vroegtijdige detectie op afstand":

tijdens gerichte wegcontroles de communicatie tussen het systeem voor vroegtijdige detectie op afstand en het leestoestel voor berichten voor vroegtijdige detectie op afstand om op afstand mogelijke gevallen van manipulatie van of fraude met controleapparaten te kunnen detecteren;

ll) „systeem voor communicatie op afstand":

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

[1] Richtlijn 92/6/EEG van de Raad van 10 februari 1992 betreffende de installatie en het gebruik, in de Gemeenschap, van snelheidsbegrenzers in bepaalde categorieën motorvoertuigen (PB L 57 van 2.3.1992, blz. 27).

mm) „leestoestel voor berichten voor de vroegtijdige detectie op afstand":

het systeem dat door controleambtenaren voor gerichte wegcontroles wordt gebruikt;

nn) „vernieuwing":

afgifte van een nieuwe tachograafkaart wanneer een bestaande kaart verlopen of defect is en teruggestuurd is naar de autoriteit van afgifte. Vernieuwing geeft altijd de zekerheid dat er geen twee geldige kaarten tegelijk in omloop zijn;

oo) „reparatie":

reparatie van een bewegingssensor, een voertuigunit of een kabel waarvoor de stroomvoorziening moet worden losgekoppeld, de tachograaf moet worden losgekoppeld van andere onderdelen of de bewegingssensor of voertuigunit moet worden geopend;

pp) „vervanging van de kaart":

afgifte van een tachograafkaart ter vervanging van een bestaande kaart, die als verloren, gestolen of defect gemeld is en die niet teruggestuurd is naar de autoriteit van afgifte. Bij vervanging bestaat altijd het risico dat er twee geldige kaarten in omloop zijn;

qq) „veiligheidscertificering":

proces ter certificering, door een gemeenschappelijke certificeringsinstantie, dat het onderzochte controleapparaat (of een onderdeel daarvan) of de tachograafkaart voldoet aan de in de toepasselijke beveiligingsprofielen gedefinieerde veiligheidseisen;

rr) „zelftest":

tests die het controleapparaat periodiek en automatisch uitvoert om fouten te ontdekken;

ss) „tijdmeting":

een permanente digitale registratie van de gecoördineerde universele datum en tijdstip (UTC);

tt) „tijdafstelling":

een automatische afstelling van de lopende tijd met geregelde tussenpozen en binnen een maximale tolerantie van één minuut of een afstelling tijdens een kalibrering;

uu) „bandenmaat":

de omschrijving van de afmetingen van de banden (externe aandrijfwielen) overeenkomstig Richtlijn 92/23/EEG van de Raad ([1]), als laatstelijk gewijzigd;

vv) „voertuigidentificatie":

nummers die het voertuig identificeren: het kentekennummer van het voertuig met een indicatie van de lidstaat van registratie en het voertuigidentificatienummer (VIN) ([2]);

ww) voor de berekening in het controleapparaat betekent „week":

het tijdvak tussen maandag 00.00 uur UTC-tijd en zondag 24.00 uur UTC-tijd;

([1]) Richtlijn 92/23/EEG van de Raad van 31 maart 1992 betreffende banden voor motorvoertuigen en aanhangwagens daarvan alsmede betreffende de montage ervan (PB L 129 van 14.5.1992, blz. 95).

([2]) Richtlijn 76/114/EEG van de Raad van 18 december 1975 betreffende de onderlinge aanpassing van de wetgevingen der Lid-Staten inzake de voorgeschreven platen en gegevens, en de plaats en wijze waarop zij op motorvoertuigen en aanhangwagens daarvan moeten worden aangebracht (PB L 24 van 30.1.1976, blz. 1).

xx) „werkplaatskaart":

een tachograafkaart, afgegeven door de autoriteiten van een lidstaat aan door die lidstaat erkende aangewezen personeelsleden van een fabrikant van tachografen, installateur, voertuigfabrikant of werkplaats, die de kaarthouder identificeert en waarmee tachografen kunnen worden getest, gekalibreerd en geactiveerd en/of waarmee gegevens kunnen worden gedownload;

yy) „adapter":

een apparaat dat een signaal afgeeft dat permanent representatief is voor de snelheid van het voertuig en/of de afgelegde afstand, dat verschilt van het signaal dat voor de onafhankelijke bewegingsdetectie wordt gebruikt en dat:

— 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 ([1]), als laatstelijk gewijzigd) en dat na 1 mei 2006 in bedrijf is gesteld;

— geïnstalleerd is wanneer het mechanisch niet mogelijk is een ander bestaand type bewegingssensor te installeren dat verenigbaar is met de bepalingen van deze bijlage en de aanhangsels 1 tot en met 15 daarvan;

— geïnstalleerd is tussen de voertuigunit en de plaats waar de snelheids-/afstandsimpulsen worden voortgebracht door geïntegreerde sensoren of alternatieve interfaces;

— gezien vanuit het standpunt van een voertuigunit, hetzelfde gedrag vertoont als dat van een bewegingssensor die voldoet aan de voorschriften van deze bijlagen en van aanhangsels 1 t.e. m. 16 en die wordt aangesloten op de voertuigunit.

Door in de bovenvermelde voertuigen een dergelijke adapter te gebruiken, kan een voertuigunit worden gebruikt en geïnstalleerd die aan alle voorschriften van deze bijlage voldoet.

Voor die voertuigen bestaat de slimme tachograaf uit kabels, een adapter en een voertuigunit;

zz) „integriteit van gegevens":

de nauwkeurigheid en coherentie van opgeslagen gegevens, aangetoond door het ontbreken van wijzigingen van de gegevens tussen twee updates van een gegevensbestand. Integriteit betekent dat de gegevens een exacte kopie zijn van de originele versie, d.w.z. dat ze niet beschadigd zijn tijdens het schrijven op en aflezen van een tachograafkaart of specifieke apparatuur, of tijdens de overdracht via een communicatiekanaal;

aaa) „gegevensprivacy":

de algemene technische maatregelen die worden genomen voor de correcte toepassing van de beginselen die zijn vastgesteld bij Richtlijn 95/46/EG van het Europees Parlement en de Raad ([2]) en bij Richtlijn 2002/58/EG van het Europees Parlement en de Raad ([3]);

bbb) „slimme tachograaf":

het controleapparaat, de tachograafkaart en alle uitrusting waarmee tijdens de constructie, de installatie, het gebruik, het testen en de controle, directe of indirecte interactie bestaat, zoals kaarten, leestoestellen voor berichten voor vroegtijdige detectie op afstand en andere apparatuur voor het downloaden van gegevens, de analyse van gegevens, kalibrering, het genereren, beheren en invoeren van beveiligingselementen enz.;

ccc) „datum van invoering":

36 maanden na de inwerkingtreding van de gedetailleerde bepalingen als bedoeld in artikel 11 van Verordening (EU) nr. 165/2014 van het Europees Parlement en de Raad ([4]).

([1]) Richtlijn 2007/46/EG van het Europees Parlement en de Raad van 5 september 2007 tot vaststelling van een kader voor de goedkeuring van motorvoertuigen en aanhangwagens daarvan en van systemen, onderdelen en technische eenheden die voor dergelijke voertuigen zijn bestemd (Kaderrichtlijn) (PB L 263 van 9.10.2007, blz. 1).

([2]) Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB L 281 van 23.11.1995, blz. 31).

([3]) Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37).

([4]) Verordening (EU) nr. 165/2014 van het Europees Parlement en van de Raad van 4 februari 2014 betreffende tachografen in het wegvervoer, tot intrekking van Verordening (EEG) nr. 3821/85 van de Raad betreffende het controleapparaat in het wegvervoer en tot wijziging van Verordening (EG) nr. 561/2006 van het Europees Parlement en de Raad tot harmonisatie van bepaalde voorschriften van sociale aard voor het wegvervoer (PB L 60 van 28.2.2014, blz. 1).

Dit is de datum waarna voertuigen die voor het eerst zijn ingeschreven:

— *worden uitgerust met een tachograaf die verbonden is met een plaatsbepalingsdienst op basis van satellietnavigatie;*

— *tijdens het rijden gegevens kunnen doorsturen naar de controle-instanties met het oog op gerichte wegcontroles;*

— *en kunnen worden uitgerust met gestandaardiseerde interfaces die ervoor zorgen dat een extern apparaat gebruik kan maken van de door tachografen voor operationeel gebruik geregistreerde of gegenereerde gegevens;*

ddd) „beveiligingsprofiel":

een document dat wordt gebruik als onderdeel van het certificeringsproces op basis van gemeenschappelijke criteria, met toepassingsonafhankelijke beveiligingseisen op het gebied van informatieborging;

eee) „GNSS-nauwkeurigheid":

in het kader van de registratie van de positie met de tachograaf met behulp van de GNSS-module: de HDOP (horizontal dilution of precision) berekend als het minimum van de via de beschikbare GNSS-module verzamelde HDOP-waarden.

2 ALGEMENE KENMERKEN EN FUNCTIES VAN HET CONTROLEAPPARAAT

2.1 **Algemene kenmerken**

Het controleapparaat moet gegevens betreffende de activiteiten van de bestuurder kunnen registreren, opslaan, weergeven, afdrukken en uitvoeren.

Alle met een controleapparaat uitgeruste voertuigen die aan de bepalingen van deze bijlage voldoen, moeten voorzien zijn van een snelheidsdisplay en een kilometerteller. Deze functies kunnen in het controleapparaat worden opgenomen.

01) Het controleapparaat bestaat uit kabels, een bewegingssensor en een voertuigunit.

02) De interface tussen de bewegingssensoren en de voertuigunits moet voldoen aan de eisen van aanhangsel 11.

03) De voertuigunit wordt overeenkomstig de specificaties in aanhangsel 12 aangesloten op een GNSS-systeem.

04) De voertuigunit communiceert met leestoestellen voor berichten voor vroegtijdige detectie op afstand overeenkomstig de specificaties in aanhangsel 14.

05) De voertuigunit kan een ITS-interface omvatten, als gespecificeerd in aanhangsel 13.

Het controleapparaat mag door middel van een extra interface en/of de optionele ITS-interface op andere systemen worden aangesloten.

06) Elke integratie of verbinding van een al of niet goedgekeurde functie, inrichting of inrichtingen, in c. q. met het controleapparaat, mag de juiste en veilige werking van het controleapparaat niet schaden of kunnen schaden en mag niet in strijd zijn met de bepalingen van deze verordening.

Gebruikers van controleapparaten identificeren zich door middel van een tachograafkaart.

07) Het controleapparaat geeft selectieve toegangsrechten tot gegevens en functies overeenkomstig het type en/of de identiteit van de gebruiker.

Het controleapparaat registreert gegevens en slaat deze op in het geheugen, in het systeem voor communicatie op afstand en op de tachograafkaart.

Dit gebeurt met inachtneming van Richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens [1], Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie [2] en artikel 7 van Verordening (EU) nr. 165/2014.

2.2 **Functies**

08) Het controleapparaat moet onderstaande functies kunnen uitvoeren:

— bewaken van het invoeren en uitnemen van de kaart,

— meten van de snelheid, afstand en positie,

— opnemen van de tijd,

— bewaken van de activiteiten van de bestuurder,

— bewaken van de status van de bestuurders,

— manuele invoer door de bestuurders:

  — invoer van gegevens over het begin- en/of eindpunt van de dagelijkse werkperiode,

  — manuele invoer van de activiteiten van de bestuurder,

  — invoer van specifieke omstandigheden,

— beheer van bedrijfsvergrendelingen,

— bewaken van controleactiviteiten,

— detecteren van voorvallen en/of fouten,

— ingebouwde tests en zelftests.

— lezen van het geheugen,

— registreren en opslaan in het geheugen,

— lezen van de tachograafkaart,

— registreren en opslaan op de tachograafkaart,

— weergeven op scherm,

— afdrukken,

— waarschuwen,

— gegevens downloaden met externe media,

— communicatie op afstand met het oog op gerichte wegcontroles,

— gegevensoutput naar aanvullende systemen,

— kalibrering,

— kalibreringscontrole langs de weg,

— tijdafstelling.

[1] PB L 281 van 23.11.1995, blz. 31.
[2] PB L 201 van 31.7.2002, blz. 37.

2.3 **Werkingsmodi**

09) Het controleapparaat heeft vier werkingsmodi:

— operationele modus,

— controlemodus,

— kalibreringsmodus,

— bedrijfsmodus.

10) Het controleapparaat wisselt naar de volgende werkingsmodus overeenkomstig de geldige tachograafkaart die in de kaartinterface ingebracht is. De generatie van de tachograafkaart is niet relevant om de werkingsmodus te bepalen, voor zover het om een geldige kaart gaat. Een werkplaatskaart van de eerste generatie wordt als ongeldig beschouwd wanneer ze in een voertuigunit van de tweede generatie wordt ingevoerd.

Werkingsmodus		Kaartlezer bestuurder				
		Geen kaart	Bestuurderskaart	Controlekaart	Werkplaatskaart	Bedrijfskaart
Kaartlezer bijrijder	Geen kaart	Operationeel	Operationeel	Controle	Kalibrering	Bedrijfsmodus
	Bestuurderskaart	Operationeel	Operationeel	Controle	Kalibrering	Bedrijfsmodus
	Controlekaart	Controle	Controle	Controle (*)	Operationeel	Operationeel
	Werkplaatskaart	Kalibrering	Kalibrering	Operationeel	Kalibrering (*)	Operationeel
	Bedrijfskaart	Bedrijfsmodus	Bedrijfsmodus	Operationeel	Operationeel	Bedrijfsmodus (*)

(*) in deze gevallen gebruikt het controleapparaat alleen de in lezer van de bestuurder ingevoerde tachograafkaart.

11) Het controleapparaat negeert ongeldige ingebrachte kaarten. Het blijft echter mogelijk om gegevens op ongeldige kaarten weer te geven, af te drukken of te downloaden.

12) Alle in 2.2 genoemde functies werken in iedere werkingsmodus met de onderstaande uitzonderingen:

— de kalibreringsfunctie is alleen toegankelijk in de kalibreringsmodus,

— de kalibreringscontrole langs de weg is alleen toegankelijk in de controlemodus,

— de beheersfunctie van bedrijfsvergrendelingen is alleen toegankelijk in de bedrijfsmodus,

— het bewaken van controleactiviteiten werkt alleen in de controlemodus,

— de downloadfunctie is niet beschikbaar in de operationele modus (behalve zoals bepaald in voorschrift 193), en behalve bij het downloaden van een bestuurderskaart wanneer er geen ander type kaart in de voertuigunit is ingevoerd.

13) Het controleapparaat kan gegevens uitvoeren naar een display, printer of externe interfaces met de onderstaande uitzonderingen:

— in de operationele modus: persoonsidentificatie (naam en voornaam(namen)) die niet overeenkomt met een ingebrachte tachograafkaart, wordt niet getoond en een kaartnummer dat niet overeenkomt met een ingebrachte tachograafkaart wordt slechts gedeeltelijk getoond (alle oneven tekens — gelezen van links naar rechts — worden niet getoond);

— in bedrijfsmodus: gegevens over de bestuurder (voorschriften 102, 105 en 108) kunnen alleen worden uitgevoerd tijdens perioden waarvoor geen vergrendeling aanwezig is of die niet door een ander bedrijf zijn vergrendeld (zoals geïdentificeerd door de eerste 13 cijfers van het bedrijfskaartnummer),

— wanneer geen kaart in het controleapparaat ingebracht is: kunnen gegevens over de bestuurder alleen worden uitgevoerd voor de huidige en de 8 voorafgaande kalenderdagen,

— persoonsgegevens van de VU worden slechts via de ITS-interface van de VU doorgegeven na controle van de instemming door de bestuurder waarop de gegevens betrekking hebben;

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

2.4 **Beveiliging**

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 het controleapparaat en de 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.

14) Om de veiligheid van het systeem te waarborgen, moeten de volgende onderdelen voldoen aan de veiligheidseisen die zijn vastgelegd in de beveiligingsprofielen overeenkomstig de eisen van aanhangsel 10.

— voertuigunit;

— tachograafkaart;

— bewegingssensor,

— externe GNSS-module (dit profiel is alleen vereist en van toepassing voor de externe GNSS-variant).

3 CONSTRUCTIE EN FUNCTIONELE EISEN VOOR CONTROLEAPPARATEN

3.1 **Controle op het inbrengen en uitnemen van kaarten**

15) Het controleapparaat bewaakt de kaartinterfaces om het inbrengen en uitnemen van kaarten te detecteren.

16) Bij het inbrengen van de kaart moet het controleapparaat bepalen of de ingebrachte kaart geldig is. Indien dit het geval is, wordt het kaarttype en de generatie van de kaart geïdentificeerd.

Wanneer er voordien reeds een kaart met hetzelfde kaartnummer en een hogere vernieuwingsindex in het controleapparaat is ingevoerd, wordt de kaart ongeldig verklaard.

Wanneer er voordien reeds een kaart met hetzelfde kaartnummer en dezelfde vernieuwingsindex, maar een hogere vervangingsindex in het controleapparaat is ingevoerd, wordt de kaart ongeldig verklaard.

17) Nadat een werkplaats de mogelijkheid om tachograafkaarten van de eerste generatie te gebruiken heeft opgeheven overeenkomstig aanhangsel 15 (voorschrift MIG003) worden tachograafkaarten van de eerste generatie door het controleapparaat als ongeldig beschouwd.

18) Werkplaatskaarten van de eerste generatie die in controleapparaten van de tweede generatie worden ingevoerd, worden als ongeldig beschouwd.

19) Het controleapparaat wordt zodanig geconstrueerd dat de tachograafkaart bij juiste invoer in de kaartinterface vergrendeld wordt.

20) De tachograafkaart kan alleen worden uitgenomen wanneer het voertuig stilstaat en nadat de relevante gegevens op de kaart zijn opgeslagen. Het uitnemen van de kaart vereist een doelgerichte handeling van de gebruiker.

3.2 **Meting van snelheid, positie en afstand**

21) De bewegingssensor (desgevallend geïntegreerd in de adapter) is de belangrijkste bron voor de meting van de snelheid en afstand.

22) Aan de hand van de door de bewegingssensor uitgestuurde pulsen, meet deze functie continu de kilometerstand die overeenkomt met de totale door het voertuig afgelegde afstand en kan ze deze weergeven.

23) Aan de hand van de door de bewegingssensor uitgestuurde pulsen, meet deze functie continu de snelheid van het voertuig en kan ze deze weergeven.

24) De snelheidsmeter geeft ook aan of het voertuig rijdt of stilstaat. Het voertuig rijdt wanneer de functie gedurende ten minste 5 seconden meer dan 1 imp/s van de bewegingssensor waarneemt. Als dit niet het geval is, wordt aangenomen dat het voertuig stilstaat.

25) Inrichtingen die snelheid (tachometer) en totale afgelegde afstand (kilometerteller) zichtbaar maken en geïnstalleerd zijn in een voertuig dat uitgerust is met een controleapparaat dat voldoet aan de bepalingen van deze verordening, moeten voldoen aan de in deze bijlage vastgestelde eisen betreffende de maximumtoleranties (zie 3.2.1 en 3.2.2).

26) Om manipulatie van bewegingsgegevens te detecteren, moet informatie van de bewegingssensor worden bevestigd door informatie over beweging van het voertuig die afkomstig is van de GNSS-ontvanger of andere facultatieve van de bewegingssensor onafhankelijke bronnen.

27) Deze functie meet de positie van het voertuig met het oog op de automatische registratie van:

— de posities waar de bestuurder en/of de bijrijder hun dagelijkse werktijd aanvatten;

— de posities waar de rijtijd van de bestuurder een veelvoud van drie uur bereikt;

— de posities waar de bestuurder en/of de bijrijder hun dagelijkse werktijd beëindigen.

3.2.1 *Meting van de afgelegde afstand*

28) De afgelegde afstand kan worden gemeten:

— hetzij bij vooruitrijden en achteruitrijden,

— hetzij uitsluitend bij vooruitrijden.

29) Het controleapparaat moet afstanden van 0 tot 9 999 999,9 km meten.

30) De gemeten afstand moet binnen de onderstaande toleranties liggen (afstanden van ten minste 1 000 m):

— ± 1 % voor installatie,

— ± 2 % bij installatie en periodieke controle,

— ± 4 % in gebruik.

31) De resolutie van de gemeten afstand bedraagt ten minste 0,1 km.

3.2.2 *Meting van de snelheid*

32) Het controleapparaat moet snelheden van 0 tot 220 km/h meten.

33) Om een maximumtolerantie op de getoonde snelheid van ± 6 km/h tijdens gebruik te garanderen en rekening houdend met:

— een tolerantie van ± 2 km/h voor invoervariaties (bandenvariaties, …),

— een tolerantie van ± 1 km/h voor metingen gedurende de installatie of periodieke controles,

moet het controleapparaat bij snelheden tussen 20 en 180 km/h en bij kenmerkende coëfficiënten van het voertuig tussen 4 000 en 25 000 imp/km de snelheid meten met een tolerantie van ± 1 km/h (bij constante snelheid).

Aantekening: De resolutie van de gegevensopslag geeft een extra tolerantie van ± 0,5 km/h aan de door het controleapparaat opgeslagen snelheid.

34) De snelheid moet binnen de normale toleranties correct worden gemeten binnen 2 seconden na het einde van een versnelling wanneer de versnelling maximaal 2 m/s^2 bedraagt.

35) De resolutie van de gemeten snelheid bedraagt ten minste 1 km/h.

3.2.3 *Bepalen van de positie*

36) Het controleapparaat meet de absolute positie van het voertuig aan de hand van de GNSS-ontvanger.

37) De absolute positie wordt gemeten in geografische coördinaten van de lengte- en breedtegraad in graden en minuten met een resolutie van 1/10 minuut.

3.3 **Tijdmeting**

38) De tijdmetingsfunctie moet permanent operationeel zijn en de UTC-datum en UTC-tijd digitaal leveren.

39) De UTC-datum en UTC-tijd worden gebruikt voor datering van gegevens in het controleapparaat (registraties, gegevensuitwisseling) en voor alle in aanhangsel 4, „Afdrukken" gespecificeerde afdrukken.

40) Om de plaatselijke tijd zichtbaar te maken, moet de op het display getoonde tijd in stappen van een half uur kunnen worden gewijzigd. Andere instellingen dan negatieve of positieve veelvouden van een half uur zijn niet toegestaan.

41) Bij gebrek aan elke vorm van tijdafstelling, mogen afwijkingen niet meer dan ± 2 seconden per dag bedragen onder typegoedkeuringsvoorwaarden.

42) De resolutie van de gemeten tijd bedraagt ten minste 1 seconde.

43) De tijdmeting mag niet worden beïnvloed door een externe stroomonderbreking van minder dan 12 maanden onder typegoedkeuringsvoorwaarden.

3.4 **Controle op activiteiten van bestuurders**

44) Deze functie moet voortdurend en afzonderlijk de activiteiten van een bestuurder en een bijrijder controleren.

45) Activiteiten van de bestuurder zijn RIJDEN, WERKEN, BESCHIKBAARHEID of RUSTPAUZE.

46) De bestuurder en/of de bijrijder kunnen WERKEN, BESCHIKBAARHEID of RUSTPAUZE manueel selecteren.

47) Wanneer het voertuig rijdt, wordt RIJDEN automatisch geselecteerd voor de bestuurder en BESCHIKBAARHEID voor de bijrijder.

48) Wanneer het voertuig stopt, wordt WERKEN automatisch geselecteerd voor de bestuurder.

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

50) Deze functie moet veranderingen van activiteiten naar de registratiefuncties uitvoeren met een resolutie van één minuut.

51) Wanneer binnen de onmiddellijk voorafgaande en de onmiddellijk volgende kalenderminuut de activiteit RIJDEN is geregistreerd, wordt de hele minuut beschouwd als RIJDEN.

52) Wanneer een kalenderminuut niet wordt beschouwd als RIJDEN overeenkomstig het voorgaande voorschrift 051, dan wordt de hele minuut gerekend als de langste ononderbroken activiteit binnen de minuut (of de laatste van een aantal even lange activiteiten).

53) Deze functie moet ook voortdurend de rijtijd en de cumulatieve rusttijd van de bestuurder controleren.

3.5 **Controle op de status van bestuurders**

54) Deze functie moet voortdurend en automatisch de status van bestuurders controleren.

55) De status TEAM wordt geselecteerd wanneer twee geldige bestuurderskaarten in het apparaat worden ingebracht, in alle andere gevallen wordt de status ALLEEN geselecteerd.

3.6 **Invoer door bestuurders**

3.6.1 *Invoer van begin- en eindpunt van de dagelijkse werkperiode*

56) Met deze functie kan het begin- en eindpunt van de dagelijkse werkperiode van een bestuurder en/of een bijrijder worden ingevoerd.

57) Plaatsen worden gedefinieerd als het land en — voorzover relevant — de regio, die manueel worden ingevoerd of bevestigd.

58) Bij het uitnemen van een bestuurderskaart moet het controleapparaat de bestuurder (bijrijder) vragen een „plaats waar de dagelijkse werkperiode eindigt" in te voeren.

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

60) Het moet mogelijk zijn plaatsen waar de dagelijkse werkperiode begint en/of eindigt, in te voeren via commando's in de menu's. Indien meer dan één dergelijke invoer gebeurt binnen één kalenderminuut, mogen slechts de laatst ingevoerde beginplaats en de laatst ingevoerde eindplaats binnen die tijdspanne geregistreerd blijven.

3.6.2 *Manuele invoer van bestuurdersactiviteiten en toestemming van de bestuurder voor de ITS-interface*

61) Manuele invoer van activiteiten is uitsluitend toegestaan bij het inbrengen van een bestuurderskaart of werkplaatskaart. Bij het manueel invoeren van activiteiten worden de plaatselijke tijd- en datumwaarden van de tijdszone (UTC offset) gebruikt die op dat moment voor de voertuigunit zijn ingesteld.

Bij het inbrengen van een bestuurders- of werkplaatskaart wordt de kaarthouder herinnerd aan:

— de datum en de tijd dat de kaart voor het laatst is uitgenomen;

— en facultatief: de voor de voertuigunit ingestelde plaatselijke tijd.

Bij de invoer van een bestuurders- of werkplaatskaart die voor de voertuigunit nog niet bekend is, wordt de kaarthouder gevraagd te bevestigen dat hij ermee instemt dat zijn persoonlijke tachograafgegevens via de optionele ITS-interface worden doorgegeven.

Wanneer de bestuurderskaart (resp. werkplaatskaart) is ingegeven, kan de bestuurder (resp. werkplaats) op elk moment via het menu zijn of haar instemming geven of intrekken.

Activiteiten kunnen worden ingevoerd met de volgende beperkingen:

— Activiteiten zijn WERKEN, BESCHIKBAARHEID of RUSTPAUZE.

— De begin- en eindtijden van elke activiteit liggen enkel binnen de laatste periode tussen het uitnemen en inbrengen van de kaart.

— Activiteiten mogen elkaar niet in tijd overlappen.

Zo nodig is manuele invoer mogelijk wanneer een nog niet eerder gebruikte bestuurderskaart (of werkplaatskaart) voor het eerst wordt ingebracht.

De procedure voor manuele invoer van activiteiten bestaat uit evenveel opeenvolgende stappen als nodig voor het instellen van het type en de begin- en eindtijd van elke activiteit. Voor elk willekeurig deel van de laatste periode tussen het invoeren en uitnemen van de kaart kan de kaarthouder ervoor kiezen geen enkele activiteit op te geven.

Tijdens de met het inbrengen van een kaart verbonden manuele invoer kan de kaarthouder, indien van toepassing, het volgende invoeren:

— een plaats waar een vorige dagelijkse werkperiode is geëindigd, alsook de relevante tijd (waarbij de invoer tijdens de laatste kaartuitneming wordt overschreven);

— een plaats waar de lopende dagelijkse werkperiode begint, samen met de relevante tijd.

Wanneer de kaarthouder tijdens de met het inbrengen van een kaart verbonden manuele invoer niet invoert op welke plaats de werkperiode begint of eindigt, wordt er vanuit gegaan dat die plaats niet is gewijzigd na de laatste keer dat de kaart is uitgenomen. De volgende invoer van een plaats waar de vorige dagelijkse werkperiode eindigt, overschrijft in dat geval de tijdelijke invoer bij de laatste kaartuitneming.

Wanneer een plaats is ingevoerd, wordt deze geregistreerd op de relevante tachograafkaart.

De manuele invoer wordt onderbroken indien:

— de kaart wordt uitgenomen; of

— het voertuig in beweging is en de kaart zich in de lezer van de bestuurder bevindt.

Extra onderbrekingen zijn toegestaan, bv. een time-out na een zekere periode van inactiviteit van de gebruiker. Indien de manuele invoer wordt onderbroken, valideert het controleapparaat elke volledige invoer van plaats en activiteit (met ondubbelzinnige vermelding van plaats en tijd, of type activiteit, begintijd en eindtijd).

Indien een tweede bestuurders- of werkplaatskaart wordt ingebracht terwijl nog manueel wordt ingevoerd voor een eerder ingebrachte kaart, mag deze manuele invoer worden voltooid voordat de manuele invoer voor de tweede kaart begint.

De kaarthouder kan manueel activiteiten invoeren overeenkomstig de volgende minimumprocedure:

— Voer activiteiten manueel in, in chronologische volgorde, voor de laatste periode tussen het uitnemen en inbrengen van de kaart.

— De begintijd van de eerste activiteit is het tijdstip waarop de kaart wordt uitgenomen. Voor elke volgende invoer wordt de begintijd vooraf ingesteld als onmiddellijk volgend op de eindtijd van de voorafgaande invoer. Voor elke activiteit wordt het type activiteit en de eindtijd geselecteerd.

De procedure eindigt wanneer de eindtijd van een manueel ingevoerde activiteit gelijk is aan het tijdstip waarop de kaart is ingebracht. Het controleapparaat kan vervolgens facultatief de kaarthouder een manueel ingevoerde activiteit laten wijzigen, totdat wordt gevalideerd door een specifiek commando te selecteren. Daarna kunnen dergelijke wijzigingen niet meer worden aangebracht.

3.6.3 *Invoer van specifieke omstandigheden*

62) De bestuurder kan de twee onderstaande specifieke omstandigheden in real-time in het controleapparaat invoeren:

— „NIET VERPLICHT” (begin, einde);

— „VERVOER PER FERRY/TREIN” (begin, einde).

„VERVOER PER FERRY/TREIN” is niet toegestaan wanneer een „NIET VERPLICHT”-omstandigheid geopend is.

Een geopende „NIET VERPLICHT”-omstandigheid moet door het controleapparaat automatisch worden gesloten wanneer een bestuurderskaart wordt ingebracht of uitgenomen.

Een geopende „NIET VERPLICHT”-omstandigheid onderdrukt de volgende voorvallen en waarschuwingssignalen:

— rijden zonder geschikte kaart

— waarschuwingssignalen in verband met de rijtijd.

De vlag begin VERVOER PER FERRY/TREIN moet zichtbaar zijn voor de bestuurder de motor op de trein of ferry stillegt.

Een openstaande VERVOER PER FERRY/TREIN moet aflopen in de volgende gevallen:

— wanneer de bestuurder het VERVOER PER FERRY/TREIN manueel beëindigt;

— wanneer de bestuurder zijn kaart uitneemt;

Een openstaande VERVOER PER FERRY/TREIN wordt beëindigd wanneer deze op grond van Verordening (EG) nr. 561/2006 niet langer geldig is.

3.7 **Beheer van bedrijfsvergrendelingen**

63) Deze functie beheert de vergrendelingen die een bedrijf aanbrengt om ervoor te zorgen dat het alleen zelf toegang heeft tot de gegevens in de bedrijfsmodus.

64) Bedrijfsvergrendelingen bestaan uit een begindatum/-tijd (lock-in) en een einddatum/-tijd (lock-out) in combinatie met de identiteit van het bedrijf zoals aangegeven door het bedrijfskaartnummer (bij lock-in).

65) Vergrendelingen kunnen alleen in real-time worden „in-” of „uitgeschakeld”.

66) Het uitschakelen van de vergrendeling is alleen mogelijk voor het bedrijf waarvan de vergrendeling is „ingeschakeld” (zoals geïdentificeerd door de eerste 13 cijfers van het bedrijfskaartnummer), of,

67) het uitschakelen van de vergrendeling gebeurt automatisch wanneer een ander bedrijf de vergrendeling inschakelt.

68) Indien een bedrijf de vergrendeling inschakelt en de vorige vergrendeling voor hetzelfde bedrijf was, dan wordt aangenomen dat de vorige vergrendeling niet is „uitgeschakeld" en nog steeds is „ingeschakeld".

3.8 **Bewaken van controleactiviteiten**

69) Deze functie moet controle uitoefenen op het WEERGEVEN, AFDRUKKEN, DOWNLOADEN van VU en kaarten en de KALIBERINGSCONTROLE LANGS DE WEG, die in de controlemodus uitgevoerd worden.

70) Deze functie moet ook controle uitoefenen op de SNELHEIDSOVERSCHRIJDING in de controlemodus. Controle van snelheidsoverschrijding wordt geacht te hebben plaatsgevonden wanneer, in de controlemodus, de afdruk „snelheidsoverschrijding" naar de printer of het display is gezonden, of wanneer gegevens over „voorvallen en fouten" uit het VU-geheugen zijn gedownload.

3.9 **Opsporing van voorvallen en/of fouten**

71) Deze functie detecteert de onderstaande voorvallen en/of fouten:

3.9.1 *„Inbrengen van een ongeldige kaart"*

72) Dit voorval treedt op bij het inbrengen van een ongeldige kaart, het inbrengen van een reeds vervangen bestuurderskaart en/of wanneer de ingebrachte kaart vervalt.

3.9.2 *„Kaartconflict"*

73) Dit voorval treedt op bij een van de combinaties van geldige kaarten die in de onderstaande tabel met een X gemerkt zijn:

Kaartconflict		Kaartlezer bestuurder				
		Geen kaart	Bestuurderskaart	Controlekaart	Werkplaatskaart	Bedrijfskaart
Kaartlezer bijrijder	Geen kaart					
	Bestuurderskaart				X	
	Controlekaart			X	X	X
	Werkplaatskaart		X	X	X	X
	Bedrijfskaart			X	X	X

3.9.3 *„Tijdsoverlapping"*

74) Dit voorval treedt op wanneer de datum/het tijdstip waarop de bestuurderskaart de laatste keer is uitgenomen, later is dan de actuele datum/tijd van het controleapparaat waarin de kaart wordt ingebracht.

3.9.4 *„Rijden zonder geschikte kaart"*

75) Dit voorval treedt op bij combinaties van geldige tachograafkaarten die in de onderstaande tabel met een X zijn aangemerkt, wanneer de activiteit van de bestuurder verandert in RIJDEN, of wanneer de werkingsmodus tijdens het RIJDEN verandert:

Rijden zonder geschikte kaart		Kaartlezer bestuurder				
		Geen (of ongeldige) kaart	Bestuurderskaart	Controlekaart	Werkplaatskaart	Bedrijfskaart
Kaartlezer bijrijder	Geen (of ongeldige) kaart	X		X		X
	Bestuurderskaart	X		X	X	X
	Controlekaart	X	X	X	X	X
	Werkplaatskaart	X	X	X		X
	Bedrijfskaart	X	X	X	X	X

3.9.5 *„Inbrengen van de kaart tijdens het rijden"*

76) Dit voorval treedt op wanneer een tachograafkaart tijdens het RIJDEN in een lezer wordt ingebracht.

3.9.6 *„Laatste kaartsessie niet correct afgesloten"*

77) Dit voorval treedt op wanneer het controleapparaat bij kaartinvoer ontdekt dat, niettegenstaande de bepalingen van punt 3.1, de voorafgaande kaartsessie niet correct is afgesloten (de kaart is uitgenomen voordat alle relevante gegevens op de kaart opgeslagen zijn). Dit mag uitsluitend voorkomen bij bestuurders- en werkplaatskaarten.

3.9.7 *„Snelheidsoverschrijding"*

78) Dit voorval treedt op bij elke snelheidsoverschrijding.

3.9.8 *„Onderbreking van de stroomvoorziening"*

79) Dit voorval treedt op bij een onderbreking van ten minste 200 milliseconden in de stroomvoorziening van de bewegingssensor en/of de voertuigunit, echter niet in de kalibrerings- of controlemodus. De drempel van de onderbreking wordt door de fabrikant bepaald. De spanningsval door het starten van de motor van het voertuig mag dit voorval niet veroorzaken.

3.9.9 *„Communicatiefout met het systeem voor communicatie op afstand"*

80) Dit voorval treedt, **behalve in de kalibreringsmodus**, op wanneer het systeem voor communicatie op afstand na meer dan drie pogingen niet bevestigt dat het de door de voertuigunit vanop afstand doorgestuurde gegevens heeft ontvangen.

3.9.10 *„Ontbreken van plaatsbepalingsinformatie van de GNSS-ontvanger"*

81) Dit voorval treedt, **behalve in kalibreringsmodus**, op bij het ontbreken van plaatsbepalingsinformatie van de (interne of externe) GNSS-ontvanger gedurende meer dan 3 uren cumulatieve rijtijd.

3.9.11 *„Fout in communicatie met de externe GNSS-module"*

82) Dit voorval treedt, **behalve in kalibreringsmodus**, op bij het ontbreken van communicatie tussen de externe GNSS-module en het voertuig gedurende meer dan 20 opeenvolgende minuten terwijl het voertuig aan het rijden is.

3.9.12 *„Fout in de bewegingsgegevens"*

83) Dit voorval treedt, **behalve in de kalibreringsmodus**, op bij een onderbreking in de normale gegevensstroom tussen de bewegingssensor en de voertuigunit en/of bij een fout in de integriteit of authenticatie van de gegevens tijdens de gegevensuitwisseling tussen de bewegingssensor en de voertuigunit.

3.9.13 *„Tegenstrijdige bewegingsgegevens"*

84) Dit voorval treedt, **behalve in de kalibreringsmodus**, op wanneer de op basis van de bewegingssensor berekende bewegingsinformatie verschilt van de bewegingsinformatie die is berekend op basis van informatie van de interne GNSS-ontvanger of de externe GNSS-module, en eventuele andere facultatieve bronnen, als gespecificeerd in aanhangsel 12. Dit voorval treedt niet op tijdens vervoer per ferry of trein, een „NIET VERPLICHT"-omstandigheid, of wanneer er geen plaatsbepalingsinformatie van de GNSS-ontvanger beschikbaar is.

3.9.14. *„Poging tot inbreuk op de beveiliging"*

85) Dit voorval treedt op bij elk ander voorval dat de beveiliging van de bewegingssensor en/of de voertuigunit en/of de externe GNSS-module als vereist bij aanhangsel 10 aantast, echter niet in de kalibreringsmodus.

3.9.15 *„Tijdsoverlapping"*

86) Dit voorval treedt op wanneer de VU 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 indien de GNSS-ontvanger de jongste 30 dagen geen geldig GNSS-signaal heeft kunnen detecteren. Wanneer de automatische plaatsbepalingsinformatie van de GNSS-ontvanger opnieuw beschikbaar is, vindt een automatische tijdsafstelling plaats.

3.9.16 *„Kaartfout"*

87) Deze fout wordt veroorzaakt wanneer tijdens de werking een storing in de tachograafkaart optreedt.

3.9.17. *„Controleapparaatfout"*

88) Deze fout wordt veroorzaakt door de onderstaande storingen, echter niet in de kalibreringsmodus:

— Interne fout in de VU

— Printerfout

— Displayfout

— Downloadfout

— Sensorfout

— Fout met GNSS-ontvanger of externe GNSS-module

— Fout in systeem voor communicatie op afstand

3.10 **Ingebouwde tests en zelftests**

89) Het controleapparaat moet zelf fouten detecteren door middel van zelftests en ingebouwde tests overeenkomstig onderstaande tabel:

Onderdelen ter test	Zelftest	Ingebouwde test
Software		Integriteit
Geheugen	Toegang	Toegang, gegevensintegriteit
Kaartinterfaces	Toegang	Toegang
Toetsenbord		Manuele controle
Printer	(afhankelijk van de fabrikant)	Afdruk
Display		Visuele controle
Downloaden (alleen uitgevoerd tijdens het downloaden)	Correcte werking	
Sensor	Correcte werking	Correcte werking
Systeem voor communicatie op afstand	Correcte werking	Correcte werking
GNSS-module	Correcte werking	Correcte werking

3.11 **Lezen van het geheugen**

90) Het controleapparaat moet alle gegevens die in zijn geheugen opgeslagen zijn kunnen lezen.

3.12 **Registratie en opslag in het geheugen**

Voor de toepassing van dit punt

— wordt „365 dagen" gedefinieerd als 365 kalenderdagen van gemiddelde activiteit van de bestuurder in een voertuig. De gemiddelde activiteit per dag in een voertuig wordt gedefinieerd als ten minste 6 bestuurders of bijrijders, 6 cycli van kaartinvoer en -uitname en 256 wijzigingen in de activiteiten. „365 dagen" omvat derhalve ten minste 2 190 bestuurders (bijrijders), 2 190 cycli van kaartinvoer en kaartuitname en 93 440 wijzigingen van activiteiten;

— 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 6 570 posities omvat;

— wordt de tijd geregistreerd met een resolutie van 1 minuut, tenzij anders gespecificeerd;

— worden kilometerstanden geregistreerd met een resolutie van 1 kilometer;

— wordt de snelheid geregistreerd met een resolutie van 1 km/h;

— posities (lengte en breedte) worden geregistreerd in graden en minuten, met een resolutie van 1/10 minuut, met de daaraan gekoppelde GNSS-nauwkeurigheid en acquisitietijd.

91) De in het geheugen opgeslagen gegevens mogen niet worden beïnvloed door een externe stroomonderbreking van minder dan 12 maanden onder typegoedkeuringsvoorwaarden. Gegevens die zijn opgeslagen in het extern systeem voor communicatie op afstand, als gedefinieerd in aanhangsel 14, mogen niet worden aangetast door een stroomonderbreking van minder dan 28 dagen.

92) Het controleapparaat moet in zijn geheugen impliciet of expliciet de volgende gegevens registreren en opslaan:

3.12.1 *Identificatiegegevens van de uitrusting*

3.12.1.1 Identificatiegegevens van de voertuigunit

93) Het controleapparaat moet in zijn geheugen de volgende identificatiegegevens van de voertuigunit opslaan:

— naam van de fabrikant

— adres van de fabrikant

— onderdeelnummer

— serienummer

— generatie voertuigunit

— mogelijkheid tachograafkaarten van de eerste generatie te gebruiken

— nummer van de softwareversie

— installatiedatum van de softwareversie

— bouwjaar

— goedkeuringsnummer

94) Identificatiegegevens van de voertuigunit worden door de fabrikant van de voertuigunit definitief geregistreerd en opgeslagen, met uitzondering van gegevens in verband met de software en het goedkeuringsnummer, die in geval van een software-upgrade gewijzigd kunnen worden, en compatibiliteit met tachograafkaarten van de eerste generatie.

3.12.1.2 Identificatiegegevens van de bewegingssensor

95) De bewegingssensor moet in zijn geheugen de volgende identificatiegegevens opslaan:

— naam van de fabrikant,

— serienummer,

— goedkeuringsnummer,

— identificatie van ingebouwde veiligheidscomponent (bijv. onderdeelnummer van de interne chip/verwerkingseenheid),

— identificatie van het besturingssysteem (bv. nummer van de softwareversie).

96) De identificatiegegevens van de bewegingssensor worden door de fabrikant van de bewegingssensor definitief in de bewegingssensor geregistreerd en opgeslagen.

97) De voertuigunit moet voor de 20 recentste verbindingen met bewegingssensoren (indien op één kalenderdag meerdere verbindingen tot stand worden gebracht, worden alleen de eerste en laatste van de dag opgeslagen) de volgende gegevens kunnen registeren en in zijn geheugen opslaan:

De volgende gegevens moeten bij elke verbinding worden geregistreerd:

— identificatiegegevens van de bewegingssensor:

— serienummer

— goedkeuringsnummer,

— verbindingsgegevens van de bewegingssensor:

— datum verbinding.

3.12.1.3 Identificatiegegevens GNSS-systemen

98) De externe GNSS-module moet in haar geheugen de volgende identificatiegegevens opslaan:

— naam van de fabrikant,

— serienummer,

— goedkeuringsnummer,

— identificatie van ingebouwde veiligheidscomponent (bijv. onderdeelnummer van de interne chip/verwerkingseenheid),

— identificatie van het besturingssysteem (bv. nummer van de softwareversie).

99) De identificatiegegevens worden door de fabrikant van de externe GNSS-module definitief in de externe GNSS-module geregistreerd en opgeslagen.

100) De voertuigunit moet voor de 20 recentste koppelingen met externe GNSS-systemen (indien op één kalenderdag meerdere koppelingen tot stand worden gebracht, worden alleen de eerste en laatste van de dag opgeslagen) de volgende gegevens kunnen registreren en opslaan in zijn geheugen:

De volgende gegevens moeten bij elke koppeling worden geregistreerd:

— identificatiegegevens van de externe GNSS-module:

— serienummer,

— goedkeuringsnummer,

— koppelingsgegevens van de externe GNSS-module:

— eerste koppelingsdatum.

3.12.2 *Sleutels en certificaten*

101) Het controleapparaat moet een aantal cryptografische sleutels en certificaten kunnen opslaan overeenkomstig de specificaties in aanhangsel 11, delen A en B.

3.12.3 *Gegevens over het inbrengen en uitnemen van de bestuurders- of werkplaatskaart*

102) Telkens een bestuurders- of werkplaatskaart in het apparaat wordt ingebracht of uitgenomen, moet het controleapparaat in zijn geheugen de volgende gegevens registreren en opslaan:

— de naam en voornaam (of namen) van de kaarthouder zoals opgeslagen op de kaart;

— het kaartnummer, de lidstaat van afgifte en de vervaldatum zoals opgeslagen op de kaart;

— de generatie van de kaart;

— datum en tijdstip van inbrengen;

— de kilometerstand bij kaartinvoer;

— de lezer waarin de kaart wordt ingebracht;

— datum en tijdstip van uitnemen;

— de kilometerstand bij het uitnemen van de kaart;

— de volgende informatie over het vorige door de bestuurder gebruikte voertuig zoals opgeslagen op de kaart:

— kentekennummer en registrerende lidstaat;

— de generatie voertuigunit (indien beschikbaar);

— datum en tijdstip waarop de kaart wordt uitgenomen;

— een teken dat aangeeft of de kaarthouder bij de kaartinvoer manueel activiteiten heeft ingevoerd.

103) Het geheugen moet deze gegevens ten minste 365 dagen bewaren.

104) Wanneer de opslagcapaciteit volledig is gebruikt, worden de oudste gegevens overschreven door de meest recente.

3.12.4 *Gegevens over activiteiten van de bestuurder*

105) Bij elke wijziging in de activiteiten van de bestuurder en/of de bijrijder, bij elke wijziging in de status van de bestuurder(s) en telkens wanneer een bestuurders- of werkplaatskaart wordt ingebracht of uitgenomen, worden de volgende gegevens door het controleapparaat geregistreerd en opgeslagen:

— de status van de bestuurder(s) (ALLEEN/ALS TEAM);

— de kaartlezer (BESTUURDER, BIJRIJDER);

— de status van de kaart in de betreffende kaartlezer (INGEBRACHT, NIET INGEBRACHT);

— de activiteiten (RIJDEN, BESCHIKBAARHEID, WERKEN, ONDERBREKING/RUST);

— de datum en het tijdstip van de wijziging.

INGEBRACHT betekent dat een geldige bestuurders- of werkplaatskaart in de lezer ingebracht is. NIET INGEBRACHT betekent het tegenovergestelde, d.w.z. er is geen geldige bestuurders- of werkplaatskaart in de lezer ingebracht (er is bv. wel een bedrijfskaart ingebracht of er is geen kaart ingebracht).

Gegevens over activiteiten die door een bestuurder manueel worden ingevoerd, worden niet in het geheugen geregistreerd.

106) Het geheugen moet de gegevens over de activiteiten van de bestuurder ten minste 365 dagen kunnen bewaren.

107) Wanneer de opslagcapaciteit volledig is gebruikt, worden de oudste gegevens overschreven door de meest recente.

3.12.5 *Plaatsen en posities waar de dagelijkse werktijd begint, eindigt en/of waar een ononderbroken 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 de bijrijder hun dagelijkse werktijd aanvatten;

— de posities waar de ononderbroken rijtijd van de bestuurder een veelvoud van drie uur bereikt;

— de plaatsen en posities waar de bestuurder en/of de bijrijder hun dagelijkse werktijd beëindigen.

109) Wanneer de positie van het voertuig op die momenten niet via de GNSS-ontvanger kan worden bepaald, gebruikt het controleapparaat de recentste beschikbare positie en de daaraan gekoppelde datum en tijd.

110) Samen met elke plaats en positie moet het controleapparaat gegevens registreren en in zijn geheugen opslaan met betrekking tot:

— het bestuurderskaartnummer en de lidstaat van afgifte;

— de generatie van de kaart;

— de datum en het tijdstip van de ingevoerde gebeurtenis;

— de aard van die gebeurtenis (begin, eind en/of 3 uur ononderbroken rijtijd);

— desgevallend de gerelateerde GNSS-nauwkeurigheid, datum- en tijd;

— de kilometerstand van het voertuig.

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

112) Wanneer de opslagcapaciteit volledig is gebruikt, worden de oudste gegevens overschreven door de meest recente.

3.12.6 *Gegevens over de kilometerstand*

113) Het controleapparaat moet elke kalenderdag om middernacht de kilometerstand van het voertuig en de bijbehorende datum in zijn geheugen registreren.

114) Het geheugen moet deze kilometerstanden ten minste 365 kalenderdagen kunnen opslaan.

115) Wanneer de opslagcapaciteit volledig is gebruikt, worden de oudste gegevens overschreven door de meest recente.

3.12.7 *Gedetailleerde snelheidsgegevens*

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

3.12.8 *Gegevens over voorvallen*

Voor de toepassing van dit punt wordt de tijd geregistreerd met een resolutie van 1 seconde.

117) Het controleapparaat moet in zijn geheugen de volgende gegevens voor elk gedetecteerd voorval volgens de onderstaande opslagvoorschriften registreren en opslaan:

Voorval	Opslagvoorschriften	Te registreren gegevens per voorval
Inbrengen van een ongeldige kaart	— de 10 meest recente voorvallen	— datum en tijdstip van het voorval — type, nummer, lidstaat van afgifte en generatie van de kaart die het voorval genereert — aantal vergelijkbare voorvallen op die dag
Kaartconflict	— de 10 meest recente voorvallen	— 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 twee kaarten die een conflict opleveren
Rijden zonder geschikte kaart	— het langste voorval voor elk van de laatste 10 dagen waarop een dergelijk voorval heeft plaatsgevonden — de 5 langste voorvallen gedurende de laatste 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; — aantal vergelijkbare voorvallen op die dag

Voorval	Opslagvoorschriften	Te registreren gegevens per voorval
Inbrengen van kaart tijdens het rijden	— het laatste voorval op elk van de laatste 10 dagen waarop een dergelijk voorval plaatshad	— datum en tijdstip van het voorval — type, nummer, lidstaat van afgifte en generatie van de kaart — aantal vergelijkbare voorvallen op die dag
Laatste kaartsessie niet correct afgesloten	— de 10 meest recente voorvallen	— datum en tijdstip van kaartinvoer — type, nummer, lidstaat van afgifte en generatie van de kaart — laatste sessiegegevens zoals af te lezen van de kaart: — datum en tijdstip van kaartinvoer — kentekennummer, lidstaat van inschrijving en generatie voertuigunit
Snelheidsoverschrijding (1)	— het ernstigste voorval op elk van de laatste 10 dagen waarop een dergelijk voorval plaatshad (d.w.z. het voorval met de hoogste gemiddelde snelheid) — de 5 ernstigste voorvallen gedurende de afgelopen 365 dagen — het eerste voorval dat is opgetreden na de laatste kalibrering	— datum en tijdstip van het begin van het voorval — datum en tijdstip van het einde van het voorval — tijdens het voorval gemeten maximumsnelheid — tijdens het voorval gemeten rekenkundige maximumsnelheid — type, nummer, lidstaat van afgifte en generatie van de bestuurderskaart (indien van toepassing) — aantal vergelijkbare voorvallen op die dag
Onderbreking stroomvoorziening (2)	— het langste voorval voor elk van de laatste 10 dagen waarop een dergelijk voorval heeft plaatsgevonden — de 5 langste voorvallen gedurende de laatste 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 — aantal vergelijkbare voorvallen op die dag
Fout in de communicatie met het systeem voor communicatie op afstand	— het langste voorval voor elk van de laatste 10 dagen waarop een dergelijk voorval heeft plaatsgevonden — de 5 langste voorvallen gedurende de laatste 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 — aantal vergelijkbare voorvallen op die dag
Ontbreken van plaatsbepalingsinformatie van de GNSS-ontvanger	— het langste voorval voor elk van de laatste 10 dagen waarop een dergelijk voorval heeft plaatsgevonden — de 5 langste voorvallen gedurende de laatste 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 — aantal vergelijkbare voorvallen op die dag

Voorval	Opslagvoorschriften	Te registreren gegevens per voorval
Fout in de bewegingsgegevens	— het langste voorval voor elk van de laatste 10 dagen waarop een dergelijk voorval heeft plaatsgevonden — de 5 langste voorvallen gedurende de laatste 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 — aantal vergelijkbare voorvallen op die dag
Tegenstrijdige bewegingsgegevens,	— het langste voorval voor elk van de laatste 10 dagen waarop een dergelijk voorval heeft plaatsgevonden, — de 5 langste voorvallen gedurende de laatste 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; — aantal vergelijkbare voorvallen op die dag
Poging tot inbreuk in de beveiliging	— de 10 meest recente voorvallen per soort voorval	— datum en tijdstip van het begin van het voorval — datum en tijdstip van het einde van het voorval (indien relevant) — type, nummer, lidstaat van afgifte en generatie van de bij het begin en/of het einde van het voorval ingevoerde kaart; — soort voorval
Tijdsoverlapping	— het langste voorval voor elk van de laatste 10 dagen waarop een dergelijk voorval heeft plaatsgevonden, — de 5 langste voorvallen gedurende de laatste 365 dagen.	— datum en tijdstip controleapparaat — GNSS-datum en -tijd, — type, nummer, lidstaat van afgifte en generatie van de bij het begin en/of het einde van het voorval ingevoerde kaart; — aantal vergelijkbare voorvallen op die dag

(1) Het controleapparaat moet ook gegevens registreren en in zijn geheugen opslaan met betrekking tot:

— datum en tijdstip laatste controle op SNELHEIDSOVERSCHRIJDING,

— datum en tijdstip eerste snelheidsoverschrijding na die controle op SNELHEIDSOVERSCHRIJDING.

— het aantal snelheidsoverschrijdingen na de laatste CONTROLE OP DE SNELHEIDSOVERSCHRIJDING.

(2) Deze gegevens mogen alleen worden opgeslagen bij een herstel van de stroomvoorziening, tijden kunnen bekend zijn met een nauwkeurigheid tot één minuut.

3.12.9 *Gegevens over fouten*

Voor de toepassing van dit punt wordt de tijd geregistreerd met een resolutie van 1 seconde.

118) Het controleapparaat moet de volgende gegevens voor elke gedetecteerde fout registreren en in zijn geheugen opslaan volgens de onderstaande opslagvoorschriften:

Fout	Opslagvoorschriften	Te registreren gegevens per fout
Kaartfout	— de 10 meest recente bestuurderskaartfouten	— datum en tijdstip begin van de fout — datum en tijdstip einde van de fout — type, nummer, lidstaat van afgifte en generatie van de kaart
Fouten controleapparaat	— de 10 meest recente fouten van iedere soort — de eerste fout na de recentste kalibrering	— datum en tijdstip begin van de fout — datum en tijdstip einde van de fout — soort fout — type, nummer, lidstaat van afgifte en generatie van de bij het begin en/of het einde van het voorval ingevoerde kaart

3.12.10 *Kalibreringsgegevens*

119) Het controleapparaat registreert en bewaart in zijn geheugen gegevens met betrekking tot:

— bekende kalibreringsparameters op het moment van activering;

— de eerste kalibrering na activering;

— de eerste kalibrering in het huidige voertuig (geïdentificeerd door zijn VIN);

— de 20 meest recente kalibreringen (wanneer een aantal kalibreringen op dezelfde kalenderdag plaatsvinden, worden alleen de eerste en laatste kalibrering van de dag opgeslagen).

120) De volgende gegevens moeten bij elke kalibrering worden geregistreerd:

— doel van de kalibrering (activering, eerste installatie, installatie, periodieke controle);

— naam en adres van de werkplaats;

— werkplaatskaartnummer, de lidstaat die de kaart afgeeft en de vervaldatum van de kaart;

— voertuigidentificatie;

— geactualiseerde en bevestigde parameters: w, k, l, bandenmaat, instelling van de snelheidsbegrenzer, kilometerstand (oude en nieuwe waarden), datum en tijdstip (oude en nieuwe waarden);

— types en identificatienummers van alle aanwezige verzegelingen.

121) Bovendien moet het controleapparaat in zijn geheugen de mogelijkheid opslaan en bewaren om tachograafkaarten van de eerste generatie te gebruiken (al dan niet nog geactiveerd).

122) De bewegingssensor moet de volgende installatiegegevens van de bewegingssensor registreren en in zijn geheugen opslaan:

— eerste verbinding met een VU (datum, tijd, goedkeuringsnummer en serienummer van de VU);

— laatste verbinding met een VU (datum, tijd, goedkeuringsnummer en serienummer van de VU).

123) De externe GNSS-module moet de volgende installatiegegevens van de externe GNSS-module opslaan en in zijn geheugen opslaan:

— eerste koppeling aan een VU (datum, tijd, goedkeuringsnummer en serienummer van de VU);

— laatste koppeling aan een VU (datum, tijd, goedkeuringsnummer en serienummer van de VU).

3.12.11 *Tijdafstellingsgegevens*

124) Het controleapparaat registreert en bewaart in zijn geheugen alle gegevens met betrekking tot tijdafstellingen die in de kalibreringsmodus worden uitgevoerd buiten het bestek van een normale kalibrering (def. f):

— de meest recente tijdafstelling;

— de 5 grootste tijdafstellingen;

125) Voor elke tijdafstelling worden de volgende gegevens geregistreerd:

— datum en tijd, oude waarde;

— datum en tijd, nieuwe waarde;

— naam en adres van de werkplaats;

— werkplaatskaartnummer, de lidstaat die de kaart afgeeft, de generatie van de kaart en haar vervaldatum;

3.12.12 *Gegevens over controleactiviteiten*

126) Het controleapparaat moet de volgende gegevens met betrekking tot de 20 meest recente controleactiviteiten registreren en in zijn geheugen opslaan:

— datum en tijdstip van de controle;

— werkplaatskaartnummer, de lidstaat die de kaart afgeeft, en de vervaldatum en generatie van de kaart;

— aard van de controle (weergeven en/of afdrukken en/of VU-gegevens downloaden en/of kaartgegevens downloaden en/of kalibreringscontrole langs de weg).

127) Bij het downloaden worden de gegevens van de oudste en van de meest recent gedownloade dagen ook geregistreerd.

3.12.13 *Gegevens over bedrijfsvergrendelingen*

128) Het controleapparaat moet de volgende gegevens met betrekking tot de 255 recentste bedrijfsvergrendelingen registreren en in zijn geheugen opslaan:

— datum en tijdstip van vergrendeling;

— datum en tijdstip van ontgrendeling;

— bedrijfskaartnummer, de lidstaat die de kaart afgeeft, en de vervaldatum en generatie van de kaart;

— naam en adres van het bedrijf.

Gegevens die eerder zijn vergrendeld met een vergrendeling die uit het geheugen is verwijderd omwille van de bovengenoemde beperking, moeten worden behandeld als niet-vergrendeld.

3.12.14 *Gegevens over overdrachtactiviteiten*

129) Het controleapparaat moet de volgende gegevens met betrekking tot de laatste geheugenoverdracht naar externe media tijdens de bedrijfs- en kalibreringsmodus registreren en in zijn geheugen opslaan:

— datum en tijdstip van de overdracht;

— bedrijfs- of werkplaatskaartnummer, de lidstaat die de kaart afgeeft, en de vervaldatum en generatie van de kaart;

— naam van het bedrijf of de werkplaats.

3.12.15 *Gegevens over specifieke omstandigheden*

130) Het controleapparaat moet de volgende gegevens met betrekking tot specifieke omstandigheden in zijn geheugen registreren:

— datum en tijdstip van de invoer;

— aard van de specifieke omstandigheid.

131) Het geheugen moet gegevens over specifieke omstandigheden ten minste 365 dagen kunnen bewaren (in de veronderstelling dat gemiddeld 1 omstandigheid per dag wordt geopend en gesloten). Wanneer de opslagcapaciteit volledig is gebruikt, worden de oudste gegevens overschreven door de meest recente.

3.12.16 *Gegevens tachograafkaart*

132) Het controleapparaat moet de volgende gegevens kunnen bewaren in verband met de verschillende tachograafkaarten die in de VU zijn gebruikt:

— het nummer en serienummer van de tachograafkaart;

— de fabrikant van de tachograafkaart;

— het type tachograafkaart;

— de versie van de tachograafkaart;

133) Het controleapparaat moet ten minste 88 records kunnen opslaan.

3.13 **Lezen van de tachograafkaart**

134) Het controleapparaat moet op tachograafkaarten van de eerste en tweede generatie de noodzakelijke gegevens kunnen lezen van om:

— de kaartsoort, de kaarthouder, het eerder gebruikte voertuig, datum en tijdstip van de laatste kaartuitneming en de op dat moment geselecteerde activiteit te identificeren;

— om te controleren of de laatste kaartsessie correct is afgesloten;

— de rijtijd van de bestuurder, de cumulatieve rustperiode en de cumulatieve rijtijden gedurende de voorafgaande en de lopende week te berekenen;

— gevraagde afdrukken met betrekking tot op de bestuurderskaart geregistreerde gegevens te leveren;

— een bestuurderskaart naar externe media over te brengen.

Dit voorschrift geldt alleen voor tachografen van de eerste generatie indien het gebruik daarvan niet door een werkplaats is opgeheven.

135) In het geval van een leesfout moet het controleapparaat dezelfde leesopdracht maximaal drie keer opnieuw uitvoeren. Wanneer de kaart nog steeds niet kan worden gelezen, moet ze defect en ongeldig worden verklaard.

3.14 **Registratie en opslag op een tachograafkaart**

3.14.1 *Registreren en opslaan op tachograafkaarten van de eerste generatie*

136) Indien het gebruik van tachograafkaarten van de eerste generatie niet door een werkplaats is opgeheven, moet het controleapparaat de gegevens op exact dezelfde manier als controleapparaten van de eerste generatie opslaan en bewaren.

137) Het controleapparaat moet de „gegevens van de kaartsessie" onmiddellijk na de kaartinvoer op de bestuurderskaart of werkplaatskaart zetten.

138) Het controleapparaat moet de gegevens die op een geldige bestuurderskaart, bedrijfskaart, werkplaatskaart en/of controlekaart zijn opgeslagen, bijwerken met behulp van alle noodzakelijke gegevens die verband houden met de periode waarin de kaart ingebracht is, en met alle noodzakelijke gegevens betreffende de kaarthouder. In hoofdstuk 4 is gespecificeerd welke gegevens op die kaarten moeten worden opgeslagen.

139) Het controleapparaat moet de op een geldige bestuurderskaart of werkplaatskaart opgeslagen gegevens over de activiteiten van de bestuurder en plaatsen (zoals gespecificeerd in de punten 4.5.3.1.9 en 4.5.3.1.11) bijwerken; gegevens over activiteiten en plaatsen worden manueel door de kaarthouder ingevoerd.

140) Alle voorvallen die niet zijn gedefinieerd voor controleapparaten van de eerste generatie worden niet op de bestuurders- en werkplaatskaarten opgeslagen.

141) Het bijwerken van gegevens op de tachograafkaart moet zodanig gebeuren dat, indien noodzakelijk en rekening houdend met de opslagcapaciteit de oudste gegevens door de nieuwe worden overschreven.

142) In het geval van een schrijffout moet het controleapparaat dezelfde schrijfopdracht maximaal drie keer opnieuw uitvoeren. Wanneer de fout blijft optreden, moet de kaart defect en ongeldig worden verklaard.

143) Voordat een bestuurderskaart uitgenomen wordt en nadat alle relevante gegevens op de kaart zijn opgeslagen, moet het controleapparaat de „gegevens van de kaartsessie" terugplaatsen.

3.14.2 *Registreren en opslaan op tachograafkaarten van de tweede generatie*

144) Tachograafkaarten van de tweede generatie bevatten 2 verschillende kaarttoepassingen: de eerste is volledig identiek aan de TACHO-toepassing van de eerste generatie tachograafkaarten, de tweede toepassing, „TACHO_G2", is beschreven in hoofdstuk 4 en aanhangsel 2.

145) Het controleapparaat moet de „gegevens van de kaartsessie" onmiddellijk na de kaartinvoer op de bestuurderskaart of werkplaatskaart zetten.

146) Het controleapparaat moet de gegevens die zijn opgeslagen in toepassingen van de tweede generatie op een geldige bestuurderskaart, bedrijfskaart, werkplaatskaart en/of controlekaart, bijwerken met behulp van alle noodzakelijke gegevens die verband houden met de periode waarin de kaart ingebracht is, en met alle noodzakelijke gegevens betreffende de kaarthouder. In hoofdstuk 4 is gespecificeerd welke gegevens op die kaarten moeten worden opgeslagen.

147) Het controleapparaat moet de op een geldige bestuurderskaart of werkplaatskaart opgeslagen gegevens over de plaatsen van activiteiten van de bestuurder, alsmede de positiegegevens (zoals gespecificeerd in de punten 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 en 4.5.3.2.11) bijwerken; gegevens over activiteiten en plaatsen worden manueel door de kaarthouder ingevoerd.

148) Het bijwerken van gegevens op de tachograafkaart moet zodanig gebeuren dat, indien noodzakelijk en rekening houdend met de opslagcapaciteit van de kaart, de oudste gegevens door de nieuwe worden overschreven.

149) In het geval van een schrijffout moet het controleapparaat dezelfde schrijfopdracht maximaal drie keer opnieuw uitvoeren. Wanneer de fout blijft optreden, moet de kaart defect en ongeldig worden verklaard.

150) Voordat een bestuurderskaart uitgenomen wordt en nadat alle relevante gegevens op de twee kaarttoepassingen van de kaart zijn opgeslagen, moet het controleapparaat de „gegevens van de kaartsessie" terugplaatsen.

3.15 **Weergave**

151) Het display moet ten minste 20 tekens bevatten.

152) De minimale tekengrootte moet 5 mm hoog en 3,5 mm breed zijn.

153) Het display ondersteunt de tekens die zijn gespecificeerd in aanhangsel 1, hoofdstuk 4 „Tekensets". Het display kan vereenvoudigde tekens gebruiken (bijv. letters met een accent kunnen zonder accent worden getoond, of kleine letters kunnen als hoofdletters worden getoond).

154) Het display moet voorzien zijn van een voldoende sterke, niet verblindende verlichting.

155) Aanwijzingen moeten aan de buitenzijde van het controleapparaat zichtbaar zijn.

156) Het controleapparaat moet het volgende kunnen weergeven:

— standaardgegevens;

— gegevens met betrekking tot waarschuwingssignalen;

— gegevens met betrekking tot de toegang tot het menu;

— andere door de gebruiker opgevraagde gegevens.

Aanvullende informatie mag door het controleapparaat worden weergegeven indien deze duidelijk te onderscheiden is van de hierboven vermelde vereiste informatie.

157) Het display van het controleapparaat moet de in aanhangsel 3 vermelde pictogrammen of pictogramcombinaties gebruiken. Extra pictogrammen of pictogramcombinaties mogen ook op het display worden weergegeven wanneer ze duidelijk te onderscheiden zijn van de voornoemde pictogrammen of pictogramcombinaties.

158) Wanneer het voertuig aan het rijden is, moet het display altijd ingeschakeld zijn.

159) Het controleapparaat kan over een manuele of automatische voorziening beschikken om het display uit te schakelen wanneer het voertuig stilstaat.

Het formaat van het display is gespecificeerd in aanhangsel 5.

3.15.1 *Standaarddisplay*

160) Wanneer geen andere informatie getoond hoeft te worden, geeft het controleapparaat standaard de volgende informatie weer:

— de plaatselijke tijd (de uitkomst van UTC-tijd + instelling door de bestuurder);

— de werkingsmodus;

— de lopende activiteiten van de bestuurder en de lopende activiteiten van de bijrijder;

— informatie met betrekking tot de bestuurder:

— indien zijn lopende activiteit RIJDEN is: zijn lopende rijtijd en zijn lopende cumulatieve rusttijd;

— indien zijn lopende activiteit niet RIJDEN is: de lopende duur van zijn activiteit (sinds deze geselecteerd werd) en zijn lopende cumulatieve rusttijd.

161) De gegevens met betrekking tot elke bestuurder moeten duidelijk en ondubbelzinnig worden weergegeven. Wanneer de informatie met betrekking tot de bestuurder en de bijrijder niet tegelijkertijd kan worden getoond, geeft het controleapparaat standaard de informatie weer met betrekking tot de bestuurder en kan de gebruiker de informatie met betrekking tot de bijrijder zichtbaar maken.

162) Als het display niet breed genoeg is om standaard de werkingsmodus weer te geven, moet het controleapparaat kort de nieuwe werkingsmodus weergeven wanneer deze wijzigt.

163) Het controleapparaat moet bij kaartinvoer kort de naam van de kaarthouder weergeven.

164) Wanneer een „NIET VERPLICHT" of „FERRY/TREIN"-omstandigheid wordt geopend, moet het standaarddisplay door middel van het relevante pictogram weergeven dat die specifieke omstandigheid geopend is (daarbij wordt aanvaard dat de lopende activiteit van de bestuurder niet tegelijkertijd wordt getoond).

3.15.2 *Waarschuwingsdisplay*

165) Het controleapparaat moet waarschuwingssignalen voornamelijk weergeven door middel van de pictogrammen van aanhangsel 3, die waar nodig worden aangevuld met extra numerieke informatie. Een letterlijke beschrijving van de waarschuwing kan in de voorkeurstaal van de bestuurder worden toegevoegd.

3.15.3 *Toegang tot het menu*

166) Het controleapparaat moet de benodigde opdrachten door middel van een geschikte menustructuur leveren.

3.15.4 *Overige displays*

167) Er kan voor een selectieve weergave worden geopteerd:

— de UTC-datum en UTC-tijd, en offset van plaatselijke tijd;

— de inhoud van de zes afgedrukte documenten in hetzelfde formaat als de afdrukken zelf;

— de ononderbroken rijtijd en cumulatieve rusttijd van de bestuurder;

— de ononderbroken rijtijd en cumulatieve rusttijd van de bijrijder;

— de cumulatieve rijtijd van de bestuurder van de voorbije en de lopende week;

— de cumulatieve rijtijd van de bijrijder van de voorbije en de lopende week;

facultatief:

— de lopende duur van activiteit van de bijrijder (sinds die geselecteerd werd);

— de cumulatieve rijtijd van de bestuurder van de lopende week;

— de cumulatieve rijtijd van de bijrijder voor de lopende dagelijkse werkperiode;

— de cumulatieve rijtijd van de bestuurder voor de lopende dagelijkse werkperiode.

168) De inhoud van de afdrukken moet sequentieel, regel voor regel, worden weergegeven. Indien de breedte van het display minder dan 24 tekens telt, moet de gebruiker de volledige informatie op een geschikte manier (een aantal regels, scrollen, …) aangeboden krijgen.

Afgedrukte regels voor handgeschreven informatie kunnen op het display worden weggelaten.

3.16 **Afdrukken**

169) Het controleapparaat moet informatie uit zijn geheugen en/of van de tachograafkaart overeenkomstig de zeven onderstaande documenten afdrukken:

— dagelijkse afdruk van de activiteiten van de bestuurder op de kaart;

— dagelijkse afdruk van de activiteiten van de bestuurder in de VU;

— afdruk van voorvallen en fouten op de kaart;

— afdruk van voorvallen en fouten in de VU;

— afdruk van technische gegevens;

— afdruk van snelheidsoverschrijdingen;

— tachograafkaartgegevens voor een bepaalde VU (zie punt 3.12.16).

De gedetailleerde vorm en inhoud van deze afdrukken zijn gespecificeerd in aanhangsel 4.

Aan het einde van de afdruk kunnen aanvullende gegevens worden verstrekt.

Het controleapparaat mag extra afdrukken leveren, indien deze duidelijk te onderscheiden zijn van de zeven voornoemde documenten.

170) De „dagelijkse afdruk van de activiteiten van de bestuurder op de kaart" en de „afdruk van voorvallen en fouten op de kaart" zijn alleen beschikbaar wanneer een bestuurderskaart of een werkplaatskaart in het controleapparaat ingebracht is. Het controleapparaat werkt de opgeslagen gegevens op de betrokken kaart bij voordat met afdrukken wordt begonnen.

171) Om de „dagelijkse afdruk van de activiteiten van de bestuurder op de kaart" of de „afdruk van voorvallen en fouten op de kaart" te leveren moet het controleapparaat:

— automatisch de bestuurderskaart of de werkplaatskaart selecteren indien een van deze kaarten ingebracht is, dan wel

— een opdracht geven om de bronkaart te selecteren of om de kaart in de kaartlezer van de bestuurder te selecteren indien twee kaarten in het controleapparaat zijn ingebracht.

172) De printer moet 24 tekens per regel afdrukken.

173) De minimale tekengrootte moet 2,1 mm hoog en 1,5 mm breed zijn.

174) De printer ondersteunt de tekens zoals gespecificeerd in aanhangsel 1, hoofdstuk 4 „Tekensets".

175) De printers zijn zo ontworpen dat zij de bedoelde afdrukken kunnen maken met een dusdanige afdrukscherpte dat leesfouten worden vermeden.

176) Afmetingen en gegevens moeten bij normale luchtvochtigheid (10-90 %) en temperatuur behouden blijven.

177) Het door het controleapparaat gebruikte typegekeurde printpapier moet over het relevante typegoedkeuringsmerk beschikken. Daarnaast moet op het papier vermeld staan voor welk(e) type(s) controleapparatuur dit papier geschikt is.

178) De afdrukken moeten onder normale opslagomstandigheden voor wat betreft lichtsterkte, vochtigheid en temperatuur, gedurende ten minste twee jaar duidelijk leesbaar en identificeerbaar blijven.

179) Afdrukken moeten ten minste voldoen aan de in aanhangsel 9 gedefinieerde testspecificaties.

180) Bovendien moeten op deze documenten geschreven aantekeningen, zoals de handtekening van de bestuurder, kunnen worden aangebracht.

181) Op „paper out" voorvallen tijdens het afdrukken reageert het controleapparaat door, zodra het papier is bijgevuld, het afdrukken vanaf het begin te hernemen of door te gaan met het afdrukken en een ondubbelzinnige referentie naar het reeds afgedrukte gedeelte te geven.

3.17 **Waarschuwingen**

182) Het controleapparaat moet de bestuurder waarschuwen als een voorval en/of fout wordt gedetecteerd.

183) Een waarschuwing met betrekking tot een onderbreking in de stroomvoorziening mag worden uitgesteld totdat de stroomvoorziening is hersteld.

184) Het controleapparaat moet de bestuurder 15 minuten van tevoren waarschuwen bij een naderende overschrijding van de maximale rijtijd, en op het tijdstip van overschrijding zelf.

185) Waarschuwingen moeten visueel worden gegeven. Daarnaast kunnen akoestische waarschuwingssignalen worden gegeven.

186) De visuele waarschuwingssignalen moeten voor de gebruiker duidelijk herkenbaar zijn, ze moeten in het gezichtsveld van de bestuurder liggen en zowel overdag als 's nachts duidelijk leesbaar zijn.

187) Visuele waarschuwingssignalen kunnen in het controleapparaat ingebouwd zijn en/of zich buiten het controleapparaat bevinden.

188) In dat geval is een „T"-teken aangebracht.

189) De waarschuwingssignalen moeten ten minste 30 seconden duren, tenzij de bestuurder deze bevestigt door op een of meer specifieke toetsen van het controleapparaat te drukken. Deze eerste bevestiging mag de getoonde reden van de waarschuwing zoals bedoeld in de volgende alinea niet uitwissen.

190) De reden van de waarschuwing moet op het controleapparaat worden getoond en zichtbaar blijven totdat de bestuurder deze bevestigt door op een specifieke toets van het controleapparaat te drukken of een opdracht te geven.

191) Aanvullende waarschuwingssignalen kunnen worden ingebouwd, mits de bestuurder hierdoor niet in verwarring wordt gebracht met betrekking tot de reeds gedefinieerde waarschuwingssignalen.

3.18 **Downloaden van gegevens met externe media**

192) Het controleapparaat moet op verzoek vanuit zijn geheugen of vanaf een bestuurderskaart via de kalibrerings-/downloadverbinding gegevens naar externe opslagmedia kunnen doorsturen. Het controleapparaat werkt de opgeslagen gegevens op de betrokken kaart bij voordat met het downloaden van gegevens wordt begonnen.

193) Verder is er een optie waardoor het controleapparaat in elke werkingsmodus gegevens via een willekeurig ander middel naar een door dit kanaal geauthenticeerd bedrijf kan doorsturen. In dit geval zijn de gegevenstoegangsrechten in de bedrijfsmodus van toepassing op de gegevensoverdracht.

194) Opgeslagen gegevens worden door het downloaden niet gewijzigd of verwijderd.

195) De elektrotechnische interface van de kalibrerings-/downloadverbinding is gespecificeerd in aanhangsel 6.

196) Downloadprotocollen zijn gespecificeerd in aanhangsel 7.

3.19 **Communicatie op afstand met het oog op gerichte wegcontroles**

197) Wanneer de motor aan staat, bewaart de voertuigunit in het systeem voor communicatie op afstand om de 60 seconden de recentste gegevens die nodig zijn voor gerichte wegcontroles. Die gegevens worden versleuteld en ondertekend overeenkomstig de aanhangsels 11 en 14.

198) Gegevens die op afstand moeten worden gecontroleerd, kunnen via een draadloze verbinding worden gelezen door de in aanhangsel 14 gespecificeerde apparatuur.

199) De gegevens die nodig zijn voor gerichte wegcontroles hebben betrekking op:

— de recentste inbreuk op de beveiliging;

— de langste stroomstoring;

— fout in de sensor;

— fout in de bewegingsgegevens;

— tegenstrijdige bewegingsgegevens;

— rijden zonder geldige kaart;

— invoeren van een kaart tijdens het rijden;

— tijdafstellingsgegevens;

— kalibreringsgegevens, waaronder de datums van de laatste twee bewaarde kalibreringsrecords;

— het voertuigkenteken;

— de door de tachograaf geregistreerde snelheid.

3.20 **Doorsturen van gegevens naar aanvullende externe apparaten**

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

Aanhangsel 13 bevat specificaties en normen voor een facultatieve ITS-interface. Andere vergelijkbare interfaces 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 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 kunnen 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 informeert andere apparaten over de instemming van de bestuurder.

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

201) Om de achterwaartse compatibiliteit te waarborgen mogen tachografen ook worden voorzien van de in bijlage 1B van Verordening (EEG) nr. 3821/85, als laatstelijk gewijzigd, gespecificeerde seriële verbinding. Voor de verzending van persoonsgegevens is steeds de instemming van de bestuurder vereist.

3.21 **Kalibrering**

202) De kalibreringsfunctie moet:

— de bewegingssensor automatisch aan de VU koppelen;

— de externe GNSS-module desgevallend automatisch koppelen aan de VU;

— de constante van het controleapparaat (k) digitaal aanpassen aan de kenmerkende coëfficiënt van het voertuig (w);

— de huidige tijd aanpassen binnen de geldigheidsperiode van de ingebrachte werkplaatskaart;

— de lopende kilometerstand bijstellen;

— de in het geheugen opgeslagen identificatiegegevens van de bewegingssensor bijwerken;

— de in het geheugen opgeslagen identificatiegegevens van de externe GNSS-module bijwerken;

— types en identificatienummers van alle aanwezige verzegelingen bijwerken;

— andere parameters van het controleapparaat bijwerken of bevestigen: VIN van het voertuig, w, l, bandenmaat en instelling van de snelheidsbegrenzer, indien van toepassing.

203) Indien de voorwaarden van aanhangsel 15 zijn vervuld, moet de kalibreringsfunctie het bovendien mogelijk maken het gebruik van tachograafkaarten van de eerste generatie in het controleapparaat op te heffen.

204) Het verbinden van de bewegingssensor met de VU omvat ten minste:

— het bijwerken van installatiegegevens van de bewegingssensor die door de bewegingssensor worden bewaard (indien nodig);

— het kopiëren van essentiële identificatiegegevens van de bewegingssensor naar het geheugen van de VU.

205) Het koppelen van de externe GNSS-module aan de VU omvat ten minste:

— het bijwerken van de installatiegegevens van de externe GNSS-module die in dat systeem zijn opgeslagen (indien nodig);

— het kopiëren van de vereiste identificatiegegevens van de externe GNSS-module naar het geheugen van de VU, met inbegrip van het serienummer van de externe GNSS-module.

Na de koppeling wordt de GNSS-positie-informatie geverifieerd.

206) De kalibreringsfunctie kan via de kalibrerings-/downloadverbinding essentiële gegevens invoeren in overeenstemming met het in aanhangsel 8 gedefinieerde kalibreringsprotocol. Met de kalibreringsfunctie kunnen ook op andere manieren essentiële gegevens worden ingevoerd.

3.22 **Kalibreringscontrole langs de weg**

207) Via de functie voor kalibreringscontroles langs de weg moet het mogelijk zijn de serienummers van de op het moment van het verzoek aan de VU gekoppelde bewegingssensor (al dat niet geïntegreerd in de adapter) en van de externe GNSS-module (indien aanwezig) op te vragen.

208) De nummers moeten op het display van de voertuigunit minstens kunnen worden gelezen via commando's in de menu's.

209) Met de functie kalibreringscontrole langs de weg moet de I/O-modus van de in aanhangsel 6 gespecificeerde I/O-signaallijn voor kalibrering via de K-lijninterface kunnen worden geselecteerd. Dat gebeurt via de EDU/Adjustment/Sessie als gespecificeerd in aanhangsel 8, deel 7 „Controle van testpulsen — invoer-/uitvoercontrole functionele unit".

3.23 **Tijdafstelling**

210) Met de tijdafstellingsfunctie kan de lopende tijd worden bijgesteld. De tijdafstelling gebeurt op basis van twee tijdsregistratiebronnen in het controleapparaat: 1) de interne klok van de VU, 2) de GNSS-ontvanger.

211) De tijdsbepaling van de interne klok van de VU wordt met intervallen van maximum 12 uur automatisch bijgewerkt. Wanneer die termijn verstreken is en er geen GNSS-signaal beschikbaar is, gebeurt de tijdafstelling 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 tijdafstelling van de interne klok van de VU wordt afgeleid van de GNSS-ontvanger. Er treedt een tijdsconflict op wanneer de huidige tijd meer dan één (1) minuut afwijkt van de tijdsinformatie die de GNSS-ontvanger verstrekt.

212) In de kalibreringsmodus kan de tijdafstellingsfunctie voor de bijwerking van de huidige tijd worden geactiveerd.

3.24 **Prestatiekenmerken**

213) De voertuigunit moet volledig operationeel zijn bij temperaturen van – 20 °C tot 70 °C, de externe GNSS-module bij temperaturen van – 20 °C tot 70 °C, en de bewegingssensor bij temperaturen van – 40 °C tot 135 °C. De gegevens in het geheugen worden bewaard tot een temperatuur van – 40 °C.

214) De tachograaf moet correct functioneren binnen het vochtigheidsbereik van 10 % tot 90 %.

215) De in slimme tachografen gebruikte zegels moeten bestand zijn tegen dezelfde omstandigheden als die welke gelden voor de onderdelen waarop ze zijn aangebracht.

216) Het controleapparaat moet worden beveiligd tegen overspanning, polariteitsomkering en kortsluiting.

217) De bewegingssensoren moeten:

— reageren op een magnetisch veld dat de detectie van beweging van het voertuig stoort. In dat geval wordt door de voertuigunit een fout in de sensor (voorschrift 88) geregistreerd en opgeslagen, ofwel

— een aftastelement bevatten dat beschermd is tegen, of ongevoelig is voor, een magnetisch veld.

218) Het controleapparaat en de externe GNSS-module moeten voldoen aan het internationaal Reglement VN-ECE R10 en beveiligd zijn tegen elektrostatische ontladingen en stootspanning.

3.25 **Materialen**

219) Alle onderdelen van het controleapparaat moeten uitgevoerd zijn in materiaal van voldoende stabiliteit en mechanische sterkte en met onveranderlijke elektrische en magnetische eigenschappen.

220) Alle inwendige delen van het apparaat moeten bij normale gebruiksomstandigheden beschermd zijn tegen vocht en stof.

221) De voertuigunit en de externe GNSS-module moeten voldoen aan beschermingsklasse IP 40 en de bewegingssensor moet voldoen aan beschermingsklasse IP 64, volgens IEC-norm IEC 60529:1989, m.i.v. A1:1999 en A2:2013.

222) Het ergonomisch ontwerp van het controleapparaat moet voldoen aan de toepasselijke technische specificaties.

223) Het controleapparaat moet worden beschermd tegen onopzettelijke beschadiging.

3.26 **Opschriften**

224) Indien het controleapparaat de kilometerstand en snelheid van het voertuig weergeeft, moeten onderstaande aanduidingen op het display voorkomen:

— bij het getal voor de afstandsaanduiding, de voor het meten van de afstand gebruikte eenheid, weergegeven door het symbool „km";

— bij het getal voor de snelheidsaanduiding, de aanduiding „km/h".

Het controleapparaat kan ook de snelheid in mijl per uur weergeven, in dat geval wordt voor de snelheidsaanduiding het symbool „mph" gebruikt. Het controleapparaat kan ook de afstand in mijl per uur weergeven, in welk geval voor de afstand het symbool „mi" gebruikt wordt.

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

— naam en adres van de fabrikant van het apparaat;

— onderdeelnummer en bouwjaar van het apparaat;

— serienummer van het apparaat;

— goedkeuringsmerk van het type apparaat.

226) Wanneer er onvoldoende fysieke ruimte is voor alle voornoemde gegevens, moeten op het identificatieplaatje ten minste voorkomen: de naam of het logo van de fabrikant en het onderdeelnummer van het apparaat.

4 FUNCTIONELE EN CONSTRUCTIE-EISEN VOOR TACHOGRAAFKAARTEN

4.1 **Zichtbare gegevens**

De voorzijde bevat:

227) de woorden „Bestuurderskaart", „Controlekaart", „Werkplaatskaart" dan wel „Bedrijfskaart", in hoofdletters, gedrukt in de officiële taal/talen van de lidstaat die de kaart afgeeft;

228) de naam van de lidstaat die de kaart afgeeft (facultatief);

229) het kenteken van de lidstaat die de kaart afgeeft, negatief afgedrukt in een door twaalf gele sterren omringde blauwe rechthoek. De kentekens zijn:

B	België	LV	Letland
BG	Bulgarije	L	Luxemburg
CZ	Tsjechië	LT	Litouwen
CY	Cyprus	M	Malta
DK	Denemarken	NL	Nederland

D EST	Duitsland Estland	A PL	Oostenrijk Polen
GR	Griekenland	P RO SK SLO	Portugal Roemenië Slowakije Slovenië
E	Spanje	FIN	Finland
F HR H	Frankrijk Kroatië Hongarije	S	Zweden
IRL	Ierland	UK	Verenigd Koninkrijk
I	Italië		

230) de gegevens die specifiek zijn voor de afgegeven kaart, met de volgende nummers:

	Bestuurderskaart	Controlekaart	Bedrijfs- of Werkplaatskaart
1.	Naam bestuurder	Naam controle-instantie	Naam bedrijf of werkplaats
2.	Voorna(a)men van de bestuurder	Naam controleur (indien van toepassing)	Naam kaarthouder (indien van toepassing)
3.	Geboortedatum van de bestuurder	Voorna(a)men controleur (indien van toepassing)	Voorna(a)m(en) kaarthouder (indien van toepassing)
4.a	Datum van afgifte van de kaart		
4.b	Vervaldatum van de kaart		
4.c	Naam van de bevoegde instantie die het rijbewijs afgeeft (mag op achterzijde worden afgedrukt)		
4.d	Een ander nummer dan dat in rubriek 5, dat nuttig is voor de administratie van de kaart (facultatief)		
5. a	Nummer van het rijbewijs (op het moment van afgifte van de bestuurderskaart)	—	—
5. b	Kaartnummer		
6.	Foto bestuurder	Foto controleur (facultatief)	Foto installateur (facultatief)

	Bestuurderskaart	Controlekaart	Bedrijfs- of Werkplaatskaart
7.	Handtekening houder (facultatief)		
8.	Woon- of verblijfplaats of postadres van de houder (facultatief)	Postadres controle-instantie	Postadres bedrijf of werkplaats

231) datums worden geschreven in het formaat „dd/mm/jjjj" of „dd.mm.jjjj" (dag, maand, jaar).

De achterkant bevat:

232) een toelichting bij de genummerde rubrieken op kant 1 van de kaart;

233) Zo nodig, en met de uitdrukkelijke schriftelijke instemming van de houder, kunnen gegevens die geen verband houden met de administratie van de kaart in deze ruimte worden opgenomen; de toevoeging van deze vermeldingen heeft geen gevolgen voor het gebruik van het model als tachograafkaart.

234) Tachograafkaarten moeten worden gedrukt met de volgende achtergrondkleuren:

— bestuurderskaart: wit,

— controlekaart: blauw,

— werkplaatskaart: rood,

— bedrijfskaart: geel.

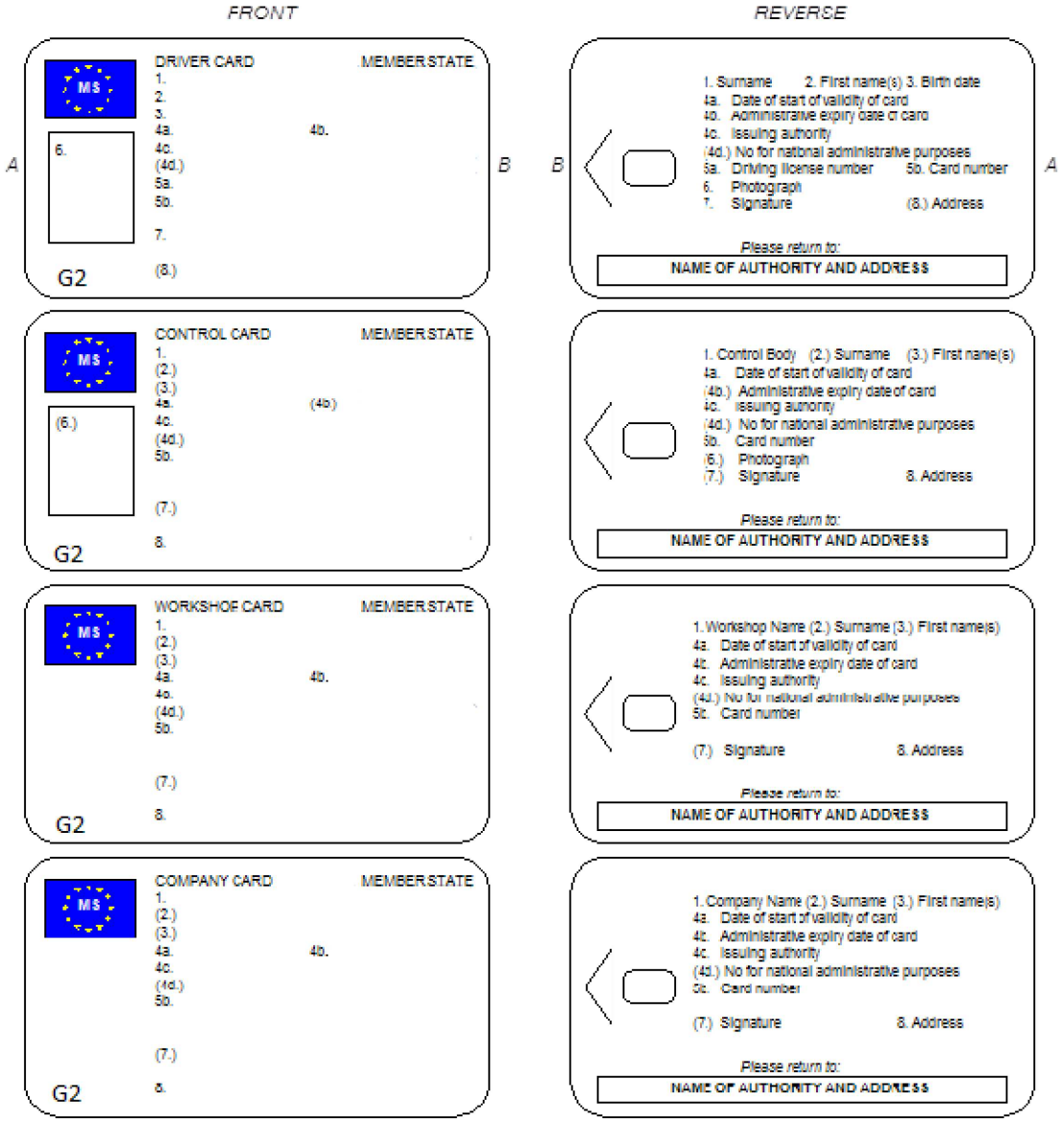
235) Tachograafkaarten moeten ten minste de volgende eigenschappen hebben om de kaart te beschermen tegen vervalsing en misbruik:

— een beveiligd achtergrondontwerp met fijne guillochepatronen en regenboogdruk,

— bij de foto moeten het beveiligd achtergrondontwerp en de foto elkaar overlappen,

— ten minste één tweekleurige microzeefdrukregel.

COMMUNITY MODEL TACHOGRAPH CARDS



236) Na overleg met de Commissie kunnen lidstaten kleuren of aanduidingen, zoals nationale symbolen of beveiligingstekens, toevoegen, onverminderd de andere bepalingen van deze bijlage.

237) Tijdelijke kaarten als bedoeld in artikel 26, lid 4, van Verordening (EU) nr. 165/2014 moeten voldoen aan de bepalingen in deze bijlage.

4.2 **Beveiliging**

De beveiliging van het systeem beoogt het beschermen van de integriteit en authenticiteit van de tussen de kaarten en het controleapparaat uitgewisselde gegevens, het beschermen van de integriteit en authenticiteit van de gegevens die van de kaarten worden gedownload, het beletten van bepaalde schrijfopdrachten op de kaarten door andere apparaten dan controleapparaten, het coderen van bepaalde gegevens, het uitsluiten van mogelijke vervalsing van op de kaarten opgeslagen gegevens, alsmede het voorkomen van manipulaties en het detecteren van pogingen daartoe.

238) Teneinde het systeem te beveiligen, moeten tachograafkaarten voldoen aan de in de aanhangsels 10 en 11 vastgestelde beveiligingseisen.

239) Tachograafkaarten moeten door andere apparatuur, zoals computers, kunnen worden gelezen.

4.3 **Normen**

240) Tachograafkaarten moeten voldoen aan de volgende normen:

— ISO/IEC 7810 Identificatiekaarten — Fysieke kenmerken

— ISO/IEC 7816 Identificatiekaarten — Kaarten met geïntegreerde schakeling(en)

— Deel 1: Fysieke kenmerken,

— Deel 2: Afmetingen en plaats van de contacten (ISO/IEC 7816-2:2007),

— Deel 3: Elektrische eigenschappen van de contacten, transmissieprotocollen (ISO/IEC 7816-3:2006),

— Deel 4: Inhoud van de communicatie, datastructuur van de chipkaart, veiligheidsarchitectuur en toegangsmechanismen (ISO/IEC 7816-4:2013 + Cor 1:2014),

— Deel 6: Interindustriële data-uitwisselingselementen (ISO/IEC 7816-6:2004 + Cor 1:2006),

— Deel 8: Veiligheidsrelevante commando's (ISO/IEC 7816-8:2004).

— Tachograafkaarten worden getest overeenkomstig ISO/IEC 10373-3:2010 Identificatiekaarten — Testmethodes — deel 3: Kaarten met geïntegreerde schakeling(en) met contacten en gerelateerde interfaces.

4.4 **Milieu- en elektrotechnische specificaties**

241) De tachograafkaart moet onder alle klimatologische omstandigheden die zich normaliter op het grondgebied van de Gemeenschap voordoen, en ten minste binnen het temperatuurbereik van – 25 °C tot + 70 °C met incidentele pieken tot + 85 °C naar behoren kunnen functioneren; „incidenteel" betekent niet meer dan 4 uur per keer en niet meer dan 100 keer tijdens de levensduur van de kaart.

242) Tachograafkaarten moeten binnen het vochtigheidsbereik van 10 % tot 90 % naar behoren kunnen functioneren.

243) Tachograafkaarten moeten vijf jaar lang naar behoren kunnen functioneren indien de vastgestelde milieu- en elektrotechnische grenswaarden niet overschreden worden.

244) Tijdens de werking moeten tachograafkaarten voldoen aan de ECE-norm R10 inzake elektromagnetische compatibiliteit en moeten de kaarten beveiligd zijn tegen elektrostatische ontladingen.

4.5 **Opslag van gegevens**

Voor de toepassing van dit punt

— wordt de tijd geregistreerd met een resolutie van 1 minuut, tenzij anders gespecificeerd;

— worden kilometerstanden geregistreerd met een resolutie van 1 kilometer;

— wordt de snelheid geregistreerd met een resolutie van 1 km/h;

— worden posities (lengte en breedte) geregistreerd in graden en minuten, met een resolutie van 1/10 minuut.

De functies, opdrachten en logische structuren van de tachograafkaart die voldoen aan de gegevensopslageisen, zijn gespecificeerd in aanhangsel 2.

Tenzij anders bepaald, worden gegevens op tachograafkaarten op dusdanige wijze opgeslagen dat de oudste gegevens door nieuwe worden overschreven wanneer de beschikbare geheugenruimte voor bepaalde records op is.

245) Dit punt specificeert de minimale opslagcapaciteit voor de verschillende gegevensbestanden. Tachograafkaarten moeten de effectieve opslagcapaciteit van deze gegevensbestanden aan het controleapparaat meedelen.

246) De opslag van aanvullende gegevens op tachograafkaarten, in verband met eventuele andere toepassingen waarvoor de kaart als drager fungeert, gebeurt met inachtneming van Richtlijn 95/46/EG, Richtlijn 2002/58/EG en artikel 7 van Verordening (EU) nr. 165/2014.

247) Elk stambestand (master file, MF) van een tachograafkaart bevat tot vijf hoofdbestanden (elementary files, EF) voor het beheer van de kaart en de identificatie van de toepassing en chip, en twee toepassingsgerichte bestanden (dedicated files, DF):

— DF tachograaf bevat de toepassing die toegankelijk is voor voertuigunits van de eerste generatie en staat ook op de eerste generatie tachograafkaarten;

— DF tachograaf_G2 bevat de toepassing die alleen toegankelijk is voor voertuigunits van de tweede generatie en staat alleen op tachograafkaarten van de tweede generatie.

De volledige structuur van de tachograafkaarten is gespecificeerd in aanhangsel 2.

4.5.1 *Hoofdbestanden voor identificatie en kaartbeheer*

4.5.2 *IC-kaartidentificatie*

248) Tachograafkaarten moeten de volgende smartcard-identificatiegegevens kunnen opslaan:

— klokstop;

— serienummer van de kaart (inclusief productiereferenties);

— typegoedkeuringsnummer van de kaart;

— persoonlijke identificatie van de kaart (ID);

— embedder ID;

— IC-identificatiesymbool;

4.5.2.1 Chipidentificatie

249) Tachograafkaarten moeten de volgende identificatiegegevens van het Integrated Circuit (IC) kunnen opslaan:

— IC-serienummer,

— IC-productiereferenties.

4.5.2.2 DIR (alleen aanwezig in tachograafkaarten van de tweede generatie)

250) Tachograafkaarten moeten de in aanhangsel 2 gespecificeerde toepassingsidentificatiegegevensobjecten kunnen opslaan.

4.5.2.3 ATR-informatie (voorwaardelijk, alleen aanwezig in tachograafkaarten van de tweede generatie)

251) Tachograafkaarten moeten de volgende uitgebreide informatiegegevensobjecten kunnen opslaan:

— wanneer de tachograafkaart uitgebreide velden ondersteunt, het in aanhangsel 2 gespecificeerde uitgebreide informatiegegevensobject.

4.5.2.4 Uitgebreide informatie (voorwaardelijk, alleen aanwezig in tachograafkaarten van de tweede generatie)

252) Tachograafkaarten moeten de volgende uitgebreide informatiegegevensobjecten kunnen opslaan:

— wanneer de tachograafkaart uitgebreide velden ondersteunt, de in aanhangsel 2 gespecificeerde uitgebreide informatiegegevensobjecten.

4.5.3 *Bestuurderskaart*

4.5.3.1 Tachograaftoepassingen (toegankelijk voor voertuigunits van de eerste en tweede generatie)

4.5.3.1.1 Toepassingsidentificatie

253) Een bestuurderskaart moet de volgende toepassingsidentificatiegegevens kunnen opslaan:

— toepassingsidentificatie van de tachograaf;

— type tachograafkaartidentificatie.

4.5.3.1.2 Sleutels en certificaten

254) Een bestuurderskaart moet een aantal cryptografische sleutels en certificaten kunnen opslaan overeenkomstig de specificaties in aanhangsel 11, deel A.

4.5.3.1.3 Identificatie van de kaart

255) Een bestuurderskaart moet de volgende kaartidentificatiegegevens kunnen opslaan:

— kaartnummer;

— lidstaat van afgifte, instantie van afgifte, datum van afgifte;

— datum van afgifte en vervaldatum van de kaart.

4.5.3.1.4 Identificatie van de kaarthouder

256) Een bestuurderskaart moet de volgende identificatiegegevens van de kaarthouder kunnen opslaan:

— naam van de houder;

— voorna(a)m(en) van de houder;

— geboortedatum;

— voorkeurstaal.

4.5.3.1.5 Kaartgegevens downloaden

257) Een bestuurderskaart moet de volgende gegevens inzake downloads opslaan:

— datum en tijdstip van het downloaden van de laatste kaart (voor andere doeleinden dan controle).

258) Een bestuurderskaart moet één van deze records kunnen bewaren.

4.5.3.1.6 Informatie over het rijbewijs

259) Een bestuurderskaart moet de volgende rijbewijsgegevens kunnen opslaan:

— lidstaat van afgifte, autoriteit van afgifte;

— rijbewijsnummer (op het moment van afgifte van de kaart).

4.5.3.1.7 Gegevens over voorvallen

Voor de toepassing van dit punt wordt de tijd geregistreerd met een resolutie van 1 seconde.

260) Een bestuurderskaart moet gegevens kunnen opslaan over de volgende voorvallen die door het controleapparaat gedetecteerd zijn terwijl de kaart was ingebracht:

— tijdsoverlapping (indien deze kaart het voorval heeft veroorzaakt);

— kaartinvoer tijdens het rijden (indien het voorval betrekking heeft op deze kaart);

— laatste kaartsessie niet correct afgesloten (indien het voorval betrekking heeft op deze kaart);

— onderbreking in de stroomvoorziening;

— fout in de bewegingsgegevens;

— pogingen tot inbreuk in de beveiliging:

261) Een bestuurderskaart moet de volgende gegevens over deze voorvallen kunnen opslaan:

— code van het voorval;

— datum en tijdstip van het begin van het voorval (of van de kaartinvoer indien het voorval op dat moment plaatsvond);

— datum en tijdstip van het einde van het voorval (of van de kaartinvoer indien het voorval op dat moment plaatsvond);

— kentekennummer en lidstaat van registratie van het voertuig waarin het voorval plaatsvond.

Aantekening: in het geval van „tijdsoverlapping”:

— moeten de datum en het tijdstip van het begin van het voorval overeenkomen met de datum en het tijdstip waarop de kaart uit het vorige voertuig is uitgenomen;

— moeten de datum en het tijdstip van het einde van het voorval overeenkomen met de datum en het tijdstip van kaartinvoer in het huidige voertuig;

— moeten de voertuiggegevens overeenkomen met die van het voertuig dat het voorval heeft veroorzaakt.

Aantekening: in het geval van „laatste kaartsessie niet correct afgesloten”:

— moeten de datum en het tijdstip van het begin van het voorval overeenkomen met de datum en het tijdstip van kaartinvoer van de sessie die niet correct afgesloten is;

— moeten de datum en het tijdstip van het einde van het voorval overeenkomen met de datum en het tijdstip van kaartinvoer van de sessie tijdens welke het voorval ontdekt werd (lopende sessie);

— moeten de voertuiggegevens overeenkomen met het voertuig waarin de sessie niet correct werd afgesloten.

262) Een bestuurderskaart moet gegevens over de 6 meest recente voorvallen van elke soort (d.w.z. 36 voorvallen) kunnen opslaan.

4.5.3.1.8 Gegevens over fouten

Voor de toepassing van dit punt wordt de tijd geregistreerd met een resolutie van 1 seconde.

263) Een bestuurderskaart moet gegevens kunnen opslaan met betrekking tot de volgende fouten die het controleapparaat heeft gedetecteerd terwijl de kaart was ingebracht:

— kaartfout (indien die kaart aanleiding is voor het voorval);

— fout in controleapparaat.

264) Een bestuurderskaart moet de volgende gegevens over deze fouten kunnen opslaan:

— foutcode;

— datum en tijdstip van het begin van de fout (of van de kaartinvoer indien de fout reeds eerder is begonnen);

— datum en tijdstip van het einde van de fout (of van de kaartuitneming indien de fout daarna blijft voortduren);

— kentekennummer en lidstaat van registratie van het voertuig waarin de fout optrad.

265) Een bestuurderskaart moet gegevens over de twaalf meest recente fouten van elke soort (d.w.z. 24 fouten) kunnen opslaan.

4.5.3.1.9 Gegevens over de activiteiten van de bestuurder

266) Een bestuurderskaart moet de volgende gegevens kunnen opslaan voor elke kalenderdag waarop de kaart wordt gebruikt of waarvoor de bestuurder manueel activiteiten heeft ingevoerd:

— de datum;

— een dagelijkse aanwezigheidsteller (met één verhoogd voor elk van de betrokken kalenderdagen);

— de totale afstand die de bestuurder gedurende deze dag heeft afgelegd;

— de bestuurdersstatus om 00.00 uur;

— wanneer de bestuurder zijn activiteiten wijzigt en/of wanneer de status van de bestuurder verandert en/of wanneer hij zijn kaart heeft ingevoerd of uitgenomen:

— de status van de bestuurder (ALLEEN/TEAM);

— de lezer (BESTUURDER, BIJRIJDER);

— de status van de kaart (INGEVOERD, NIET INGEVOERD);

— de activiteiten (RIJDEN, BESCHIKBAARHEID, WERKEN, ONDERBREKING/RUST);

— het tijdstip van de wijziging.

267) Het geheugen van de bestuurderskaart moet de gegevens over de activiteiten van de bestuurder ten minste 28 dagen bewaren (een bestuurder wijzigt zijn activiteiten gemiddeld 93 keer per dag).

268) De in de voorschriften 261, 264 en 266 genoemde gegevens moeten zodanig worden opgeslagen dat de activiteiten in de volgorde van optreden kunnen worden opgezocht, zelfs in het geval van tijdsoverlapping.

4.5.3.1.10 Gegevens over de gebruikte voertuigen

269) Een bestuurderskaart moet voor elke kalenderdag waarop de kaart wordt gebruikt, en voor elke gebruiksperiode van een bepaald voertuig op die dag (deze periode omvat de opeenvolgende cycli van inbrengen en uitnemen van de betrokken kaart in het voertuig) de volgende gegevens kunnen opslaan:

— datum en tijdstip van het eerste gebruik van het voertuig (d.w.z. de eerste kaartinvoer voor deze gebruiksperiode van het voertuig, of 00.00 uur wanneer de gebruiksperiode op dat moment voortduurt);

— kilometerstand van het voertuig op dat moment;

— datum en tijdstip van het laatste gebruik van het voertuig (d.w.z. de laatste kaartuitneming voor deze gebruiksperiode van het voertuig of 23.59 uur wanneer de gebruiksperiode op dat moment voortduurt);

— kilometerstand van het voertuig op dat moment;

— kentekennummer en lidstaat waar het voertuig geregistreerd is.

270) Een bestuurderskaart moet ten minste 84 gebruiksrecords kunnen opslaan.

4.5.3.1.11 Plaatsen waar dagelijkse werkperioden beginnen en/of eindigen

271) Een bestuurderskaart moet de volgende door de bestuurder ingevoerde gegevens betreffende de plaatsen waar dagelijkse werkperioden beginnen en/of eindigen, kunnen opslaan:

— datum en tijdstip van de invoer (of datum/tijd van de invoer indien deze manueel gebeurt);

— het type invoer (begin of einde, omstandigheid van invoer);

— het ingevoerde land en de ingevoerde regio;

— de kilometerstand van het voertuig.

272) Het geheugen van de bestuurderskaart moet ten minste 42 paar records kunnen bewaren.

4.5.3.1.12 Gegevens over kaartsessies

273) Een bestuurderskaart moet gegevens opslaan met betrekking tot het voertuig waarin de lopende sessie geopend is:

— datum en tijdstip waarop de sessie werd geopend (d.w.z. kaartinvoer), met een resolutie van één seconde;

— kentekennummer en lidstaat van registratie.

4.5.3.1.13 Gegevens over controleactiviteiten

274) Een bestuurderskaart moet de volgende gegevens met betrekking tot controleactiviteiten opslaan:

— datum en tijdstip van de controle;

— controlekaartnummer en lidstaat die de kaart heeft afgegeven;

— soort controle (weergeven en/of printen en/of downloaden van VU en/of kaart (zie opmerking));

— gedownloade periode, in het geval van downloaden;

— kentekennummer en lidstaat van registratie van het voertuig waarin de controle plaatsvond.

Aantekening: het downloaden van de kaart wordt uitsluitend geregistreerd wanneer dat via een controleapparaat gebeurt.

275) Een bestuurderskaart moet één van deze records kunnen bewaren.

4.5.3.1.14 Gegevens over specifieke omstandigheden

276) Een bestuurderskaart moet de volgende gegevens met betrekking tot specifieke omstandigheden kunnen opslaan, die ingevoerd werden terwijl de kaart werd ingevoerd (ongeacht het slot):

— datum en tijdstip van de invoer;

— aard van de specifieke omstandigheid.

277) Een bestuurderskaart moet minstens 56 records kunnen opslaan.

4.5.3.2 Toepassing tachograaf van de 2de generatie (niet toegankelijk voor voertuigunits van de eerste generatie)

4.5.3.2.1 Toepassingsidentificatie

278) Een bestuurderskaart moet de volgende toepassingsidentificatiegegevens kunnen opslaan:

— toepassingsidentificatie van de tachograaf;

— type tachograafkaartidentificatie.

4.5.3.2.2 Sleutels en certificaten

279) Een bestuurderskaart moet een aantal cryptografische sleutels en certificaten kunnen opslaan overeenkomstig de specificaties in aanhangsel 11, deel B.

4.5.3.2.3 Identificatie van de kaart

280) Een bestuurderskaart moet de volgende kaartidentificatiegegevens kunnen bewaren:

— kaartnummer;

— lidstaat van afgifte, instantie van afgifte, datum van afgifte;

— datum van afgifte en vervaldatum van de kaart.

4.5.3.2.4 Identificatie van de kaarthouder

281) Een bestuurderskaart moet de volgende identificatiegegevens van de kaarthouder kunnen opslaan:

— naam van de houder;

— voorna(a)m(en) van de houder;

— geboortedatum;

— voorkeurstaal.

4.5.3.2.5 Kaartgegevens downloaden

282) Een bestuurderskaart moet de volgende gegevens inzake downloads opslaan:

— datum en tijdstip van het downloaden van de laatste kaart (voor andere doeleinden dan controle).

283) Een bestuurderskaart moet één van deze records kunnen bewaren.

4.5.3.2.6 Informatie over het rijbewijs

284) Een bestuurderskaart moet de volgende rijbewijsgegevens kunnen opslaan:

— lidstaat van afgifte, autoriteit van afgifte,

— rijbewijsnummer (op het moment van afgifte van de kaart).

4.5.3.2.7 Gegevens over voorvallen

Voor de toepassing van dit punt wordt de tijd geregistreerd met een resolutie van 1 seconde.

285) Een bestuurderskaart moet gegevens kunnen opslaan over de volgende voorvallen, die door het controleapparaat gedetecteerd zijn terwijl de kaart was ingebracht:

— tijdsoverlapping (indien deze kaart het voorval heeft veroorzaakt);

— kaartinvoer tijdens het rijden (indien deze kaart aanleiding is voor het voorval);

— laatste kaartsessie niet correct afgesloten (indien deze kaart aanleiding is voor het voorval);

— onderbreking in de stroomvoorziening;

— fout in de communicatie met het systeem voor communicatie op afstand

— ontbreken van positie-informatie van de GNSS-ontvanger;

— fout in communicatie met de externe GNSS-module;

— fout in de bewegingsgegevens,

— tegenstrijdige bewegingsgegevens,

— pogingen tot inbreuk op de beveiliging:

— tijdsoverlapping.

286) Een bestuurderskaart moet de volgende gegevens over deze voorvallen kunnen opslaan:

— code van het voorval;

— datum en tijdstip van het begin van het voorval (of van de kaartinvoer indien het voorval op dat moment plaatsvond);

— datum en tijdstip van het einde van het voorval (of van de kaartinvoer indien het voorval op dat moment plaatsvond);

— kentekennummer en lidstaat van registratie van het voertuig waarin het voorval plaatsvond.

Aantekening: in het geval van „tijdsoverlapping”:

— moeten de datum en het tijdstip van het begin van het voorval overeenkomen met de datum en het tijdstip waarop de kaart uit het vorige voertuig is uitgenomen;

— moeten de datum en het tijdstip van het einde van het voorval overeenkomen met de datum en het tijdstip van kaartinvoer in het huidige voertuig;

— moeten de voertuiggegevens overeenkomen met die van het voertuig dat het voorval heeft veroorzaakt.

Aantekening: in het geval van „laatste kaartsessie niet correct afgesloten”:

— moeten de datum en het tijdstip van het begin van het voorval overeenkomen met de datum en het tijdstip van kaartinvoer van de sessie die niet correct afgesloten is;

— moeten de datum en het tijdstip van het einde van het voorval overeenkomen met de datum en het tijdstip van kaartinvoer van de sessie tijdens welke het voorval ontdekt werd (lopende sessie);

— moeten de voertuiggegevens overeenkomen met het voertuig waarin de sessie niet correct werd afgesloten.

287) Een bestuurderskaart moet gegevens over de 6 meest recente voorvallen van elke soort (d.w.z. 66 voorvallen) kunnen opslaan.

4.5.3.2.8 Gegevens over fouten

Voor de toepassing van dit punt wordt de tijd geregistreerd met een resolutie van 1 seconde.

288) Een bestuurderskaart moet gegevens kunnen opslaan met betrekking tot de volgende fouten, die het controleapparaat heeft gedetecteerd terwijl de kaart was ingebracht:

— kaartfout (indien deze kaart aanleiding is voor het voorval);

— fout in controleapparaat.

289) Een bestuurderskaart moet de volgende gegevens over deze fouten kunnen opslaan:

— foutcode;

— datum en tijdstip van het begin van de fout (of van de kaartinvoer indien de fout reeds eerder was begonnen);

— datum en tijdstip van het einde van de fout (of van de kaartuitneming indien de fout daarna bleef voortduren);

— kentekennummer en lidstaat van registratie van het voertuig waarin de fout optrad.

290) Een bestuurderskaart moet gegevens over de twaalf meest recente fouten van elke soort (d.w.z. 24 fouten) kunnen opslaan.

4.5.3.2.9 Gegevens over de activiteiten van de bestuurder

291) Een bestuurderskaart moet voor elke kalenderdag waarop de kaart wordt gebruikt of waarvoor de bestuurder manueel activiteiten heeft ingevoerd, de volgende gegevens kunnen opslaan:

— de datum;

— een dagelijkse aanwezigheidsteller (met één verhoogd voor elk van de betrokken kalenderdagen);

— de totale afstand die de bestuurder gedurende deze dag heeft afgelegd;

— de bestuurdersstatus om 00.00 uur;

— wanneer de bestuurder zijn activiteiten wijzigt en/of wanneer de status van de bestuurder verandert en/of wanneer hij zijn kaart heeft ingevoerd of uitgenomen:

— de status van de bestuurder (ALLEEN/TEAM);

— het slot (BESTUURDER, BIJRIJDER);

— de status van de kaart (INGEVOERD, NIET INGEVOERD);

— de activiteiten (RIJDEN, BESCHIKBAARHEID, WERKEN, ONDERBREKING/RUST);

— het tijdstip van de wijziging.

292) Het geheugen van de bestuurderskaart moet de gegevens over de activiteiten van de bestuurder ten minste 28 dagen bewaren (een bestuurder wijzigt zijn activiteiten gemiddeld 93 keer per dag).

293) De in de voorschriften 286, 289 en 291 genoemde gegevens moeten zodanig worden opgeslagen dat de activiteiten in de volgorde van optreden kunnen worden opgezocht, zelfs in het geval van tijdsoverlapping.

4.5.3.2.10 Gegevens over de gebruikte voertuigen

294) Een bestuurderskaart moet voor elke kalenderdag waarop de kaart wordt gebruikt, en voor elke gebruiksperiode van een bepaald voertuig op die dag (deze periode omvat de opeenvolgende cycli van inbrengen en uitnemen van de betrokken kaart in het voertuig) de volgende gegevens kunnen opslaan:

— datum en tijdstip van het eerste gebruik van het voertuig (d.w.z. de eerste kaartinvoer voor deze gebruiksperiode van het voertuig, of 00.00 uur wanneer de gebruiksperiode op dat moment voortduurt);

— kilometerstand van het voertuig bij eerste gebruik;

— datum en tijdstip van het laatste gebruik van het voertuig, (d.w.z. de laatste kaartuitneming voor deze gebruiksperiode van het voertuig, of 23.59 uur wanneer de gebruiksperiode op dat moment voortduurt);

— kilometerstand van het voertuig bij laatste gebruik;

— kentekennummer en lidstaat waar het voertuig geregistreerd is;

— VIN van het voertuig.

295) Een bestuurderskaart moet minstens 84 records kunnen bewaren.

4.5.3.2.11 Plaatsen en posities waar de dagelijkse werkperioden beginnen en/of eindigen

296) Een bestuurderskaart moet de volgende door de bestuurder ingevoerde gegevens betreffende de plaatsen waar dagelijkse werkperioden beginnen en/of eindigen, kunnen opslaan:

— de datum en tijdstip van de invoer (of de datum/tijd van de invoer indien deze manueel gebeurt);

— het type invoer (begin of einde, omstandigheid van invoer);

— het ingevoerde land en de ingevoerde regio;

— de kilometerstand van het voertuig;

— de positie van het voertuig;

— de GNSS-nauwkeurigheid, datum en tijdstip waarop de positie is bepaald.

297) Het geheugen van de bestuurderskaart moet ten minste 84 paar records kunnen bewaren.

4.5.3.2.12 Gegevens over kaartsessies

298) Een bestuurderskaart moet gegevens opslaan met betrekking tot het voertuig waarin de lopende sessie geopend is:

— datum en tijdstip waarop de sessie geopend werd (d.w.z. kaartinvoer), met een resolutie van 1 seconde;

— kentekennummer en lidstaat van registratie.

4.5.3.2.13 Gegevens over controleactiviteiten

299) Een bestuurderskaart moet de volgende gegevens met betrekking tot controleactiviteiten opslaan:

— datum en tijdstip van de controle;

— controlekaartnummer en lidstaat die de kaart heeft afgegeven;

— soort controle (weergeven en/of printen en/of downloaden van VU en/of kaart (zie opmerking));

— gedownloade periode, in het geval van downloaden;

— kentekennummer en lidstaat van registratie van het voertuig waarin de controle plaatsvond.

Aantekening: de beveiligingseisen impliceren dat het downloaden van de kaart uitsluitend geregistreerd wordt wanneer dat via een controleapparaat gebeurt.

300) Een bestuurderskaart moet één van deze records kunnen bewaren.

4.5.3.2.14 Gegevens over specifieke omstandigheden

301) Met betrekking tot specifieke omstandigheden moeten de volgende gegevens die werden ingevoerd terwijl de kaart werd ingevoerd (ongeacht het slot), kunnen worden bewaard op de bestuurderskaart:

— datum en tijdstip van de invoer;

— aard van de specifieke omstandigheid.

302) Een bestuurderskaart moet minstens 56 records kunnen opslaan.

4.5.3.2.15 Gegevens over de gebruikte voertuigunits

303) Een bestuurderskaart moet de volgende gegevens kunnen bewaren in verband met de verschillende voertuigunits waarin ze is gebruikt:

— de datum en het tijdstip waarop het gebruik in de voertuigunit begint (eerste invoer in de VU voor de periode);

— de fabrikant van de voertuigunit;

— het type voertuigunit;

— het nummer van de softwareversie van de VU.

304) Een bestuurderskaart moet minstens 84 records kunnen opslaan.

4.5.3.2.16 Plaats en tijdstip ononderbroken rijtijd van drie uur

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

— de datum en het tijdstip waarop de ononderbroken rijtijd van de bestuurder een veelvoud van drie uur bereikt;

— de positie van het voertuig;

— de GNSS-nauwkeurigheid, datum en tijdstip waarop de positie is bepaald.

306) Een bestuurderskaart moet minstens 252 records kunnen opslaan.

4.5.4 *Werkplaatskaart*

4.5.4.1 Tachograaftoepassingen (toegankelijk voor voertuigunits van de eerste en tweede generatie)

4.5.4.1.1 Toepassingsidentificatie

307) Een werkplaatskaart moet de volgende toepassingsidentificatiegegevens kunnen opslaan:

— toepassingsidentificatie van de tachograaf;

— type tachograafkaartidentificatie.

4.5.4.1.2 Sleutels en certificaten

308) Een werkplaatskaart moet een aantal cryptografische sleutels en certificaten kunnen opslaan overeenkomstig de specificaties in aanhangsel 11, deel A.

309) Een werkplaatskaart moet een Personal Identification Number (pincode) kunnen opslaan.

4.5.4.1.3 Identificatie van de kaart

310) Een werkplaatskaart moet de volgende kaartidentificatiegegevens kunnen opslaan:

— kaartnummer;

— lidstaat van afgifte, instantie van afgifte, datum van afgifte;

— datum van afgifte van en vervaldatum van de kaart.

4.5.4.1.4 Identificatie van de kaarthouder

311) Een werkplaatskaart moet de volgende identificatiegegevens van de kaarthouder kunnen opslaan:

— naam van de werkplaats;

— adres van de werkplaats;

— naam van de houder;

— voorna(a)m(en) van de houder;

— voorkeurstaal.

4.5.4.1.5 Kaartgegevens downloaden

312) Een werkplaatskaart moet de gegevens over het downloaden van de kaart op dezelfde manier kunnen opslaan als een bestuurderskaart.

4.5.4.1.6 Gegevens over kalibrering en tijdafstelling

313) Een werkplaatskaart moet records kunnen opslaan van kalibreringen en/of tijdafstellingen die worden uitgevoerd terwijl de kaart zich in een controleapparaat bevindt.

314) Elke kalibreringsrecord moet de volgende gegevens kunnen bevatten:

— doel van de kalibrering (activering, eerste installatie, installatie, periodieke controle);

— identificatie van het voertuig

— bijgewerkte of bevestigde parameters (w, k, l, bandenmaat, instelling van de snelheidsbegrenzer, kilometerstand (nieuwe en oude waarde), datum en tijdstip (nieuwe en oude waarde));

— identificatienummer van het controleapparaat (onderdeelnummer en serienummer van de VU, serienummer van de bewegingssensor).

315) Een werkplaatskaart moet ten minste 88 records kunnen opslaan.

316) Een werkplaatskaart moet een teller bevatten die het totale aantal kalibreringen aangeeft dat met de kaart is uitgevoerd.

317) Een werkplaatskaart moet een teller bevatten die het aantal kalibreringen sinds de laatste download aangeeft.

4.5.4.1.7 Gegevens over voorvallen en fouten

318) Een werkplaatskaart moet records over voorvallen en fouten op dezelfde manier kunnen opslaan als een bestuurderskaart.

319) Een werkplaatskaart moet gegevens over de drie meest recente voorvallen van elke soort (d.w.z. 18 voorvallen) en de zes meest recente fouten van elke soort (d.w.z. 12 fouten) kunnen opslaan.

4.5.4.1.8 Gegevens over de activiteiten van de bestuurder

320) Een werkplaatskaart moet de gegevens over de activiteiten van de bestuurder op dezelfde manier kunnen opslaan als een bestuurderskaart.

321) Een werkplaatskaart moet de gegevens over de activiteiten van de bestuurder ten minste gedurende 1 dag met gemiddelde activiteiten van de bestuurder bewaren.

4.5.4.1.9 Gegevens over de gebruikte voertuigen

322) Een werkplaatskaart moet records over de gebruikte voertuigen op dezelfde manier kunnen opslaan als een bestuurderskaart.

323) Een werkplaatskaart moet ten minste 4 records kunnen opslaan.

4.5.4.1.10 Gegevens over het begin en einde van dagelijkse werkperioden

324) Een werkplaatskaart moet records over het begin en einde van dagelijkse werkperioden op dezelfde manier kunnen opslaan als een bestuurderskaart.

325) Een werkplaatskaart moet ten minste 3 paren van dergelijke records kunnen bewaren.

4.5.4.1.11 Gegevens over kaartsessies

326) Een werkplaatskaart moet gegevens over het downloaden van de kaart op dezelfde manier kunnen opslaan als een bestuurderskaart.

4.5.4.1.12 Gegevens over controleactiviteiten

327) Een werkplaatskaart moet de gegevens over controleactiviteiten op dezelfde manier kunnen opslaan als een bestuurderskaart.

4.5.4.1.13 Gegevens over specifieke omstandigheden

328) Een werkplaatskaart moet gegevens over specifieke omstandigheden op dezelfde manier kunnen opslaan als een bestuurderskaart.

329) Een werkplaatskaart moet ten minste 2 records kunnen opslaan.

4.5.4.2 Toepassing tachograaf van de tweede generatie (niet toegankelijk voor voertuigunits van de eerste generatie)

4.5.4.2.1 Toepassingsidentificatie

330) Een werkplaatskaart moet de volgende toepassingsidentificatiegegevens kunnen opslaan:

— toepassingsidentificatie van de tachograaf;

— type tachograafkaartidentificatie.

4.5.4.2.2 Sleutels en certificaten

331) Een werkplaatskaart moet een aantal cryptografische sleutels en certificaten kunnen opslaan overeenkomstig de specificaties in aanhangsel 11, deel B.

332) Een werkplaatskaart moet een Personal Identification Number (pincode) kunnen opslaan.

4.5.4.2.3 Identificatie van de kaart

333) Een werkplaatskaart moet de volgende kaartidentificatiegegevens kunnen opslaan:

— kaartnummer;

— lidstaat van afgifte, instantie van afgifte, datum van afgifte;

— datum van afgifte en vervaldatum van de kaart.

4.5.4.2.4 Identificatie van de kaarthouder

334) Een werkplaatskaart moet de volgende identificatiegegevens van de kaarthouder kunnen opslaan:

— naam van de werkplaats;

— adres van de werkplaats;

— naam van de houder;

— voorna(a)m(en) van de houder;

— voorkeurstaal.

4.5.4.2.5 Kaartgegevens downloaden

335) Een werkplaatskaart moet de gegevens over het downloaden van de kaart op dezelfde manier kunnen opslaan als een bestuurderskaart.

4.5.4.2.6 Gegevens over kalibrering en tijdafstelling

336) Een werkplaatskaart moet records kunnen opslaan van kalibreringen en/of tijdafstellingen die worden uitgevoerd terwijl de kaart zich in een controleapparaat bevindt.

337) Elke kalibreringsrecord moet de volgende gegevens kunnen bevatten:

— doel van de kalibrering (activering, eerste installatie, installatie, periodieke controle);

— voertuigidentificatie;

— bijgewerkte of bevestigde parameters (w, k, l, bandenmaat, instelling van de snelheidsbegrenzer, kilometerstand (nieuwe en oude waarde), datum en tijdstip (nieuwe en oude waarde);

— identificatie van het controleapparaat (onderdeel- en serienummer VU, serienummer bewegingssensor, serienummer systeem voor communicatie op afstand en, indien van toepassing, serienummer externe GNSS-module);

— types en identificatienummers van alle aanwezige verzegelingen;

— mogelijkheid van de VU om tachograafkaarten van de eerste generatie te gebruiken (geactiveerd of niet).

338) Een werkplaatskaart moet ten minste 88 records kunnen opslaan.

339) Een werkplaatskaart moet een teller bevatten die het totale aantal kalibreringen aangeeft dat met de kaart is uitgevoerd.

340) Een werkplaatskaart moet een teller bevatten die het aantal kalibreringen sinds de laatste download aangeeft.

4.5.4.2.7 Gegevens over voorvallen en fouten

341) Een werkplaatskaart moet records over voorvallen en fouten op dezelfde manier kunnen opslaan als een bestuurderskaart.

342) Een werkplaatskaart moet gegevens over de drie meest recente voorvallen van elke soort (d.w.z. 33 voorvallen) en de zes meest recente fouten van elke soort (d.w.z. 12 fouten) kunnen opslaan.

4.5.4.2.8 Gegevens over de activiteiten van de bestuurder

343) Een werkplaatskaart moet de gegevens over de activiteiten van de bestuurder op dezelfde manier kunnen opslaan als een bestuurderskaart.

344) Een werkplaatskaart moet de gegevens over de activiteiten van de bestuurder ten minste gedurende 1 dag met gemiddelde activiteiten van de bestuurder bewaren.

4.5.4.2.9 Gegevens over de gebruikte voertuigen

345) Een werkplaatskaart moet records over de gebruikte voertuigen op dezelfde manier kunnen opslaan als een bestuurderskaart.

346) Een werkplaatskaart moet ten minste 4 records kunnen opslaan.

4.5.4.2.10 Gegevens over het begin en einde van dagelijkse werkperioden

347) Een werkplaatskaart moet records over het begin en einde van dagelijkse werkperioden op dezelfde manier kunnen opslaan als een bestuurderskaart.

348) Een werkplaatskaart moet ten minste 3 paren van dergelijke records kunnen bewaren.

4.5.4.2.11 Gegevens over kaartsessies

349) Een werkplaatskaart moet gegevens over het downloaden van de kaart op dezelfde manier kunnen opslaan als een bestuurderskaart.

4.5.4.2.12 Gegevens over controleactiviteiten

350) Een werkplaatskaart moet de gegevens over controleactiviteiten op dezelfde manier kunnen opslaan als een bestuurderskaart.

4.5.4.2.13 Gegevens over de gebruikte voertuigunits

351) Een werkplaatskaart moet de volgende gegevens kunnen bewaren in verband met de verschillende voertuigunits waarin ze is gebruikt:

— de datum en het tijdstip waarop het gebruik in de voertuigunit begint (eerste invoer in de VU voor de periode);

— de fabrikant van de voertuigunit;

— het type voertuigunit;

— het nummer van de softwareversie van de VU.

352) Een werkplaatskaart moet ten minste 4 records kunnen opslaan.

4.5.4.2.14 Plaats en tijdstip ononderbroken rijtijd van drie uur

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

— de datum en het tijdstip waarop de ononderbroken rijtijd van de bestuurder een veelvoud van drie uur bereikt;

— de positie van het voertuig;

— de GNSS-nauwkeurigheid, datum en tijdstip waarop de positie is bepaald.

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

4.5.4.2.15 Gegevens over specifieke omstandigheden

355) Een werkplaatskaart moet gegevens over specifieke omstandigheden op dezelfde manier kunnen opslaan als een bestuurderskaart.

356) Een werkplaatskaart moet ten minste 2 records kunnen opslaan.

4.5.5 *Controlekaart*

4.5.5.1 Tachograaftoepassingen (toegankelijk voor voertuigunits van de eerste en tweede generatie)

4.5.5.1.1 Toepassingsidentificatie

357) Een controlekaart moet de volgende toepassingsidentificatiegegevens kunnen opslaan:

— toepassingsidentificatie van de tachograaf;

— type tachograafkaartidentificatie.

4.5.5.1.2 Sleutels en certificaten

358) Een controlekaart moet een aantal cryptografische sleutels en certificaten kunnen opslaan overeenkomstig de specificaties in aanhangsel 11, deel A.

4.5.5.1.3 Identificatie van de kaart

359) Een controlekaart moet de volgende kaartidentificatiegegevens kunnen opslaan:

— kaartnummer;

— lidstaat van afgifte, instantie van afgifte, datum van afgifte;

— ingangsdatum van de geldigheid van de kaart en datum waarop de kaart vervalt (indien van toepassing).

4.5.5.1.4 Identificatie van de kaarthouder

360) Een controlekaart moet de volgende identificatiegegevens van de kaarthouder kunnen opslaan:

— naam van de controle-instantie;

— adres van de controle-instantie;

— naam van de houder;

— voorna(a)m(en) van de houder;

— voorkeurstaal.

4.5.5.1.5 Gegevens over controleactiviteiten

361) Een controlekaart moet de volgende gegevens met betrekking tot controleactiviteiten kunnen opslaan:

— datum en tijdstip van de controle;

— aard van de controle (weergeven en/of afdrukken en/of VU-gegevens downloaden en/of kaartgegevens downloaden en/of kalibreringscontrole langs de weg);

— gedownloade periode (indien van toepassing);

— kentekennummer en lidstaat waarin het gecontroleerde voertuig is ingeschreven;

— kaartnummer en lidstaat die de gecontroleerde bestuurderskaart heeft afgegeven.

362) Een controlekaart moet ten minste 230 records kunnen bewaren.

4.5.5.2 Tachograaftoepassingen van de tweede generatie (niet toegankelijk voor voertuigunits van de eerste generatie)

4.5.5.2.1 Toepassingsidentificatie

363) Een controlekaart moet de volgende toepassingsidentificatiegegevens kunnen opslaan:

— toepassingsidentificatie van de tachograaf;

— type tachograafkaartidentificatie.

4.5.5.2.2 Sleutels en certificaten

364) Een controlekaart moet een aantal cryptografische sleutels en certificaten kunnen opslaan overeenkomstig de specificaties in aanhangsel 11, deel B.

4.5.5.2.3 Identificatie van de kaart

365) Een controlekaart moet de volgende kaartidentificatiegegevens kunnen opslaan:

— kaartnummer;

— lidstaat van afgifte, instantie van afgifte, datum van afgifte;

— ingangsdatum van de geldigheid van de kaart en datum waarop de kaart vervalt (indien van toepassing).

4.5.5.2.4 Identificatie van de kaarthouder

366) Een controlekaart moet de volgende identificatiegegevens van de kaarthouder kunnen opslaan:

— naam van de controle-instantie;

— adres van de controle-instantie;

— naam van de houder;

— voorna(a)m(en) van de houder;

— voorkeurstaal.

4.5.5.2.5 Gegevens over controleactiviteiten

367) Een controlekaart moet de volgende gegevens met betrekking tot controleactiviteiten kunnen opslaan:

— datum en tijdstip van de controle;

— aard van de controle (weergeven en/of afdrukken en/of VU-gegevens downloaden en/of kaartgegevens downloaden en/of kalibreringscontrole langs de weg).

— gedownloade periode (indien van toepassing);

— kentekennummer en lidstaat waarin het gecontroleerde voertuig is ingeschreven;

— kaartnummer en lidstaat die de gecontroleerde bestuurderskaart heeft afgegeven.

368) Een controlekaart moet ten minste 230 records kunnen bewaren.

4.5.6 *Bedrijfskaart*

4.5.6.1 Tachograaftoepassingen (toegankelijk voor voertuigunits van de eerste en tweede generatie)

4.5.6.1.1 Toepassingsidentificatie

369) Een bedrijfskaart moet de volgende toepassingsidentificatiegegevens kunnen opslaan:

— toepassingsidentificatie van de tachograaf;

— type tachograafkaartidentificatie.

4.5.6.1.2 Sleutels en certificaten

370) Een bedrijfskaart moet een aantal cryptografische sleutels en certificaten kunnen opslaan overeenkomstig de specificaties in aanhangsel 11, deel A.

4.5.6.1.3 Identificatie van de kaart

371) Een bedrijfskaart moet de volgende kaartidentificatiegegevens kunnen opslaan:

— kaartnummer;

— lidstaat van afgifte, instantie van afgifte, datum van afgifte;

— ingangsdatum van de geldigheid van de kaart en datum waarop de kaart vervalt (indien van toepassing).

4.5.6.1.4 Identificatie van de kaarthouder

372) Een bedrijfskaart moet de volgende identificatiegegevens van de kaarthouder kunnen opslaan:

— naam van het bedrijf;

— adres van het bedrijf.

4.5.6.1.5 Gegevens over bedrijfsactiviteiten

373) Een bedrijfskaart moet de volgende gegevens over bedrijfsactiviteiten kunnen opslaan:

— datum en tijdstip van de activiteit;

— soort activiteit (vergrendeling en/of ontgrendeling van VU en/of VU-gegevens downloaden en/of kaartgegevens downloaden);

— gedownloade periode (indien van toepassing);

— kentekennummer en registrerende instantie van de lidstaat van het voertuig;

— kaartnummer en lidstaat die de kaart heeft afgegeven (bij het downloaden van de kaart).

374) Een bedrijfskaart moet ten minste 230 van dergelijke records kunnen bewaren.

4.5.6.2 Tachograaftoepassingen van de tweede generatie (niet toegankelijk voor voertuigunits van de eerste generatie)

4.5.6.2.1 Toepassingsidentificatie

375) Een bedrijfskaart moet de volgende toepassingsidentificatiegegevens kunnen opslaan:

— toepassingsidentificatie van de tachograaf;

— type tachograafkaartidentificatie.

4.5.6.2.2 Sleutels en certificaten

376) Een bedrijfskaart moet een aantal cryptografische sleutels en certificaten kunnen opslaan overeenkomstig de specificaties in aanhangsel 11, deel B.

4.5.6.2.3 Identificatie van de kaart

377) Een bedrijfskaart moet de volgende kaartidentificatiegegevens kunnen opslaan:

— kaartnummer;

— lidstaat van afgifte, instantie van afgifte, datum van afgifte;

— ingangsdatum van de geldigheid van de kaart en datum waarop de kaart vervalt (indien van toepassing).

4.5.6.2.4 Identificatie van de kaarthouder

378) Een bedrijfskaart moet de volgende identificatiegegevens van de kaarthouder kunnen opslaan:

— naam van het bedrijf;

— adres van het bedrijf.

4.5.6.2.5 Gegevens over bedrijfsactiviteiten

379) Een bedrijfskaart moet de volgende gegevens over bedrijfsactiviteiten kunnen opslaan:

— datum en tijdstip van de activiteit;

— soort activiteit (vergrendeling en/of ontgrendeling van VU en/of VU-gegevens downloaden en/of kaartgegevens downloaden);

— gedownloade periode (indien van toepassing);

— kentekennummer en registrerende instantie van de lidstaat van het voertuig;

— kaartnummer en lidstaat die de kaart heeft afgegeven (bij het downloaden van de kaart).

380) Een bedrijfskaart moet ten minste 230 van dergelijke records kunnen bewaren.

5 INSTALLATIE VAN HET CONTROLEAPPARAAT

5.1 **Installatie**

381) Nieuwe controleapparaten moeten in niet-geactiveerde toestand geleverd worden aan installateurs of voertuigfabrikanten. Alle kalibreringsparameters, als vermeld in punt 3.21, moeten daarbij ingesteld zijn op de juiste en geldige standaardwaarden. Indien geen specifieke waarde geschikt is, moeten de letters op „?" en de cijfers op „0" worden gezet. Indien nodig kan tijdens de beveiligingscertificering de levering van voor beveiliging relevante onderdelen van het controleapparaat worden beperkt.

382) Vóór de activering moet het controleapparaat toegang geven tot de kalibreringsfunctie, zelfs wanneer het apparaat zich niet in de kalibreringsmodus bevindt.

383) Vóór de activering mag het controleapparaat geen gegevens als bedoeld in de punten 3.12.3, 3.12.9 en 3.12.12 tot en met 3.12.15 opslaan.

384) Tijdens de installatie moeten de voertuigfabrikanten alle bekende parameters instellen.

385) Voertuigfabrikanten of installateurs moeten het geïnstalleerde controleapparaat activeren uiterlijk voordat het voertuig wordt gebruikt in het kader van Verordening (EG) nr. 561/2006.

386) De activering van het controleapparaat moet automatisch worden opgestart bij de eerste invoer van een geldige werkplaatskaart in een van zijn kaartinterfaces.

387) Eventuele specifieke verbindingen tussen de bewegingssensor en de voertuigunit moeten automatisch gebeuren voor of tijdens de activering.

388) Op dezelfde manier moeten het tot stand brengen van de koppeling tussen de externe GNSS-module en de voertuigunit, indien van toepassing, automatisch gebeuren voor of tijdens de activering.

389) Na de activering moet het controleapparaat alle functies uitvoeren en toegang geven tot alle gegevens.

390) Na de activering, stuurt het controleapparaat alle beveiligde gegevens die nodig zijn voor de uitvoering van gerichte wegcontroles door naar het systeem voor controle op afstand.

391) De registratie- en opslagfuncties van het controleapparaat moeten na de activering volledig operationeel zijn.

392) Na de installatie moet een kalibrering volgen. Bij de eerste kalibrering wordt niet noodzakelijk het voertuigregistratienummer (VRN) ingevoerd, wanneer dat niet bekend is bij de erkende werkplaats die de kalibrering uitvoert. In dat geval, en alleen op dat moment, kan de eigenaar van het voertuig het VRN invoeren met behulp van zijn bedrijfskaart voordat het voertuig gebruikt wordt in het kader van Verordening (EG) nr. 561/2006 (bv. door middel van commando's in een juiste menustructuur van de mens-machine-interface van de voertuigunit.) ([1]) Deze invoer mag alleen met behulp van een werkplaatskaart worden bijgewerkt of bevestigd.

393) Voor de installatie van een externe GNSS-module moet dat systeem aan de voertuigunit worden gekoppeld en moet vervolgens de GNSS-positie-informatie worden geverifieerd.

394) Het controleapparaat moet zodanig in het voertuig worden geïnstalleerd dat de bestuurder gemakkelijk vanaf zijn zitplaats toegang heeft tot de noodzakelijke functies.

([1]) PB L 102 van 11.4.2006, blz. 1.

5.2 **Installatieplaatje**

395) Na controle van het controleapparaat bij de installatie wordt op het controleapparaat een gegraveerd of onuitwisbaar bedrukt installatieplaatje aangebracht. Dat plaatje moet duidelijk zichtbaar en gemakkelijk toegankelijk zijn. Waar dat niet mogelijk is, moet het plaatje worden aangebracht op de B-stijl van het voertuig, zodat het duidelijk zichtbaar is. Voor voertuigen zonder B-stijl moet het installatieplaatje worden aangebracht op de deurlijst aan de bestuurderskant van het voertuig, en altijd duidelijk zichtbaar zijn.

Na iedere controle door een erkende installateur of werkplaats dient het oude plaatje door een nieuw te worden vervangen.

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 van het voertuig;

— de aanwezigheid (of afwezigheid) van een externe GNSS-module;

— het serienummer van de externe GNSS-module;

— het serienummer van het systeem voor communicatie op afstand;

— 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 adaptor.

397) Uitsluitend voor voertuigen van categorie M1 en N1 die zijn uitgerust met een adapter volgens Verordening (EG) nr. 68/2009 van de Commissie ([1]), als laatstelijk gewijzigd, en waarbij niet alle benodigde informatie kan worden vermeld, zoals beschreven in voorschrift 396, mag gebruik worden gemaakt van een tweede, extra plaatje. In dergelijke gevallen moeten op dit extra plaatje minimaal de laatste vier in voorschrift 396 beschreven streepjes staan.

Dit tweede plaatje moet worden aangebracht in de buurt van of naast het in voorschrift 396 beschreven eerste primaire plaatje en moet op dezelfde manier worden beschermd. Voorts moeten op het secundaire plaatje eveneens de naam, het adres of de handelsnaam van de erkende installateur of werkplaats die de installatie heeft uitgevoerd, en de datum van installatie zijn vermeld.

([1]) Verordening (EG) nr. 68/2009 van de Commissie van 23 januari 2009 betreffende de negende aanpassing aan de vooruitgang van de techniek van Verordening (EEG) nr. 3821/85 van de Raad betreffende het controleapparaat in het wegvervoer (PB L 21 van 24.1.2009, blz. 3).

5.3 **Verzegeling**

398) De volgende onderdelen moeten worden verzegeld:

— alle verbindingen die, wanneer ze verbroken zouden worden, tot niet-traceerbare wijzigingen of niet-traceerbaar verlies van gegevens zouden leiden (dit kan bv. het geval zijn voor de aansluiting van de bewegingssensor op de versnellingsbank, de adapter voor voertuigen van de categorieën M1/N1, de externe GNSS-verbinding of de voertuigunit);

— het installatieplaatje, tenzij het zodanig is aangebracht dat het niet kan worden verwijderd zonder de daarop aangebrachte aanduidingen te vernietigen.

399) De bovengenoemde verzegelingen mogen worden verwijderd:

— in noodgevallen;

— voor het plaatsen, afstellen of repareren van een snelheidsbegrenzer of alle andere inrichtingen die bijdragen tot de verkeersveiligheid, op voorwaarde dat het controleapparaat betrouwbaar en correct blijft functioneren en na het plaatsen van de snelheidsbegrenzer of andere inrichtingen die bijdragen tot de verkeersveiligheid onmiddellijk opnieuw door een erkende installateur of werkplaats (als bedoeld in hoofdstuk 6) wordt verzegeld; of binnen zeven dagen in andere gevallen.

400) Iedere verbreking van deze zegels moet schriftelijk worden gemotiveerd; deze motivering dient ter beschikking van de bevoegde autoriteit te worden gehouden.

401) Op de zegels is een door de fabrikant toegekend identificatienummer aanwezig. Dat nummer moet uniek zijn en verschillen van alle andere door andere fabrikanten van zegels toegekende zegelnummers.

Het unieke identificatienummer wordt als volgt gedefinieerd: MMNNNNNN 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 NNNNNN een alfanumeriek zegelnummer is binnen het domein van de fabrikant.

402) Op de zegels moet een vrije ruimte beschikbaar zijn waar erkende installateurs, werkplaatsen of voertuigfabrikanten een merkteken kunnen aanbrengen overeenkomstig artikel 22, lid 3, van Verordening (EU) nr. 165/2014.

Het merkteken mag het identificatienummer van het zegel niet bedekken.

403) Zegelfabrikanten worden opgenomen in een specifieke databank en maken hun zegelidentificatienummers bekend door middel van een door de Europese Commissie vastgestelde procedure.

404) Erkende werkplaatsen en voertuigfabrikanten gebruiken in het kader van Verordening (EU) nr. 165/2014 alleen zegels die geproduceerd zijn door in de voornoemde databank opgenomen zegelfabrikanten.

405) Fabrikanten en distributeurs van zegels waarborgen de volledige traceerbaarheid van de voor gebruik in het kader van Verordening (EU) nr. 165/2014 verkochte zegels en zorgen ervoor dat zij die gegevens indien nodig kunnen verstrekken aan de bevoegde nationale instanties.

406) De unieke zegelidentificatienummer moeten zichtbaar zijn op het installatieplaatje.

6 CONTROLES, INSPECTIES EN HERSTELLINGEN

Voorschriften betreffende de omstandigheden waarin verzegelingen verwijderd mogen worden, als bedoeld in artikel 22, lid 5, van Verordening (EU) nr. 165/2014, zijn gedefinieerd in punt 5.3 van deze bijlage.

6.1 **Erkenning van installateurs, werkplaatsen en voertuigfabrikanten**

De lidstaten erkennen, certificeren en controleren regelmatig de instanties die de

— installaties,

— controles,

— inspecties en

— reparaties verrichten.

Werkplaatskaarten worden uitsluitend afgegeven aan voor het activeren en/of kalibreren van controleapparaten erkende installateurs en/of werkplaatsen die voldoen aan deze bijlage en, tenzij voldoende gerechtvaardigd:

— niet in aanmerking komen voor een bedrijfskaart;

— wiens andere bedrijfsactiviteiten geen potentieel gevaar voor de totale veiligheid van het systeem opleveren zoals vereist in aanhangsel 10.

6.2 **Controle van nieuwe of herstelde inrichtingen**

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, door middel van verzegeling overeenkomstig punt 5.3 en kalibrering.

6.3 **Installatie-inspectie**

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.

6.4 **Periodieke controles**

409) Periodieke controles van de in de voertuigen geïnstalleerde inrichtingen moeten plaatsvinden na iedere reparatie van de inrichting, of na iedere wijziging van de kenmerkende coëfficiënt van het voertuig of van de effectieve omtrek van de wielbanden, of wanneer de UTC-tijd van de inrichting meer dan 20 minuten afwijkt, of wanneer het kentekennummer gewijzigd is en ten minste om de twee jaar (24 maanden) na de laatste controle.

410) Die inspecties omvatten de volgende controles:

— de correcte werking van het controleapparaat, met name de gegevensopslag op de tachograafkaart en de communicatie met toestellen om berichten op afstand te lezen;

— de naleving van het bepaalde in de punten 3.2.1 en 3.2.2 inzake de maximumtoleranties bij installatie;

— de naleving van het bepaalde in de punten 3.2.3 en 3.3;

— de aanwezigheid van het typegoedkeuringsmerk op het controleapparaat;

— dat het installatieplaatje, zoals omschreven in voorschrift 396, en het identificatieplaatje, zoals omschreven in voorschrift 225, zijn aangebracht;

— de bandenmaat en de werkelijke omtrek van de banden;

— dat er geen manipulatiemiddelen aanwezig zijn;

— dat de zegels correct zijn aangebracht, in goede staat zijn en over een geldig identificatienummer beschikken (erkende zegelfabrikant in de EC-databank), en dat hun identificatienummer overeenstemt met de merktekens op het identificatieplaatje (zie voorschrift 401).

411) Indien een van de in punt 3.9 (Detectie van voorvallen en/of fouten) genoemde voorvallen zich heeft voorgedaan sinds de laatste inspectie en door tachograaffabrikanten en/of de nationale overheid wordt beschouwd als mogelijke bedreiging voor de beveiliging van het apparaat, moet de werkplaats:

a. een vergelijking maken tussen de identificatiegegevens van de op de versnellingsbak aangesloten bewegingssensor en de in de voertuigunit opgeslagen gegevens van de gekoppelde bewegingssensor;

b. controleren of de informatie op het installatieplaatje overeenkomt met de in de voertuigunit opgeslagen informatie;

c. controleren of het serienummer en het goedkeuringsnummer van de bewegingssensor, indien deze op de bewegingssensor zijn afgedrukt, overeenkomen met de in het geheugen van het controleapparaat opgeslagen informatie;

d. de op het identificatieplaatje van de externe GNSS-module aangebrachte gegevens, indien van toepassing, vergelijken met de in het geheugen van de VU opgeslagen gegevens.

412) Werkplaatsen moeten in hun inspectieverslag melding maken van eventueel aangetroffen verbroken zegels of manipulatiemiddelen. Deze rapporten moeten minstens 2 jaar worden bewaard en op verzoek aan de bevoegde autoriteit worden overgelegd.

413) Bij die controles moet een kalibrering plaatsvinden en moeten de zegels waarvan de aanwezigheid onder de verantwoordelijkheid van de werkplaats valt preventief worden vervangen.

6.5 Meting van afwijkingen

414) De meting van de afwijkingen bij installatie en gebruik gebeurt onder de volgende omstandigheden, die beschouwd moeten worden als normale testomstandigheden:

— onbelast voertuig, in normale rijklare toestand;

— bandenspanning overeenkomstig de door de fabrikant verstrekte gegevens,

— slijtage van de banden binnen de door de nationale voorschriften toegestane grenzen;

— rijdend voertuig:

— het voertuig moet zich, aangedreven door zijn eigen motor, langs een rechte lijn over een vlakke ondergrond bewegen met een snelheid van 50 ± 5 km/u. Het meettraject moet ten minste 1 000 m lang zijn;

— de test mag ook uitgevoerd worden met alternatieve methoden, zoals op een geschikte proefbank, op voorwaarde dat deze even nauwkeurig zijn.

6.6 Reparaties

415) Werkplaatsen kunnen gegevens van het controleapparaat downloaden en deze gegevens teruggeven aan de betreffende vervoersonderneming.

416) Erkende werkplaatsen moeten een certificaat van onmogelijkheid tot het downloaden van gegevens aan de vervoersondernemingen afgeven, wanneer vooraf geregistreerde gegevens ten gevolge van de slechte werking van het controleapparaat zelfs na reparatie door de betrokken werkplaats niet kunnen worden gedownload. De werkplaatsen bewaren een kopie van elk afgegeven certificaat gedurende ten minste twee jaar.

7 AFGIFTE VAN KAARTEN

De door de lidstaten vastgestelde werkwijze voor de afgifte van kaarten moet aan het volgende voldoen:

417) Het kaartnummer van het eerste exemplaar van een tachograafkaart dat aan een aanvrager verstrekt wordt, moet een opeenvolgende index (indien van toepassing), een vervangingsindex en een vernieuwingsindex op de stand „0” hebben.

418) Van de kaartnummers van alle niet-persoonlijke tachograafkaarten, die aan een bepaalde controle-instantie, een bepaalde werkplaats of een bepaalde vervoersonderneming zijn afgegeven, moeten de eerste 13 cijfers hetzelfde zijn. Verder moeten ze allemaal een andere opeenvolgende index hebben.

419) Een tachograafkaart die ter vervanging van een bestaande tachograafkaart wordt afgegeven, moet hetzelfde kaartnummer hebben als de vervangen kaart, met uitzondering van de vervangingsindex die met „1” moet worden verhoogd (in de volgorde 0, …, 9, A, …, Z).

420) Een tachograafkaart die ter vervanging van een bestaande tachograafkaart wordt afgegeven, moet dezelfde vervaldatum hebben als de vervangen kaart.

421) Een tachograafkaart die ter vernieuwing van een bestaande tachograafkaart wordt afgegeven, moet hetzelfde kaartnummer hebben als de bestaande kaart met uitzondering van de vervangingsindex die op „0" moet worden teruggezet en de vernieuwingsindex die met „1" moet worden verhoogd (in de volgorde 0, …, 9, A, …, Z).

422) Het ruilen van een bestaande tachograafkaart met het oog op de wijziging van administratieve gegevens moet in dezelfde lidstaat gebeuren volgens de voorschriften voor vernieuwing, of de voorschriften voor de eerste afgifte wanneer de kaart in een andere lidstaat wordt geruild.

423) In het geval van niet-persoonlijke werkplaats- of controlekaarten moet bij de „naam van de kaarthouder" de naam van de werkplaats of de controle-instantie worden ingevuld, of de naam van de installateur of controleur indien de lidstaten daartoe besluiten.

424) De lidstaten wisselen elektronisch gegevens uit om het unieke karakter te waarborgen van de bestuurderskaarten die zij afgeven overeenkomstig artikel 31 van Verordening (EU) nr. 165/2014.

8 TYPEGOEDKEURING VAN CONTROLEAPPARATEN EN TACHOGRAAFKAARTEN

8.1 **Algemeen**

In dit punt wordt onder „controleapparaat" verstaan: „controleapparaat of de onderdelen 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 van zijn onderdeel met elk willekeurig type bewegingssensor of externe GNSS-module, en omgekeerd, aanvragen op voorwaarde dat elk onderdeel voldoet aan de voorschriften van deze bijlage. Fabrikanten kunnen als alternatief ook een typegoedkeuring voor hun controleapparaten aanvragen.

425) Het controleapparaat moet met alle geïntegreerde aanvullende systemen ter goedkeuring worden aangeboden.

426) De typegoedkeuring van het controleapparaat en van de tachograafkaarten omvat tests van de beveiliging, functietests en interoperabiliteitstests. Positieve testresultaten worden op een relevant certificaat vermeld.

427) De goedkeuringsautoriteiten van de lidstaten verlenen geen typegoedkeuringscertificaat zolang zij niet beschikken over:

— een beveiligingscertificaat,

— een functiecertificaat,

— en een interoperabiliteitscertificaat.

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

428) De autoriteit die de goedkeuring voor het apparaat verleende, moet vooraf in kennis worden gesteld van elke wijziging in de software of hardware van het apparaat of in de aard van de voor de fabricage gebruikte materialen. Deze autoriteit bevestigt de verlenging van de goedkeuring aan de fabrikant of eist een aanpassing of een bevestiging van de relevante functie-, beveiligings- en/of interoperabiliteitscertificaten.

429) Procedures voor een in-situ upgrade van de software van het controleapparaat moeten worden goedgekeurd door de autoriteit die de typegoedkeuring voor het controleapparaat heeft verleend. Een aanpassing van de software mag de in het controleapparaat opgeslagen gegevens over de activiteiten van de bestuurder wijzigen noch verwijderen. Software mag alleen worden aangepast onder de verantwoordelijkheid van de fabrikant van het apparaat.

430) De typegoedkeuring van softwarewijzigingen met het oog op een upgrade van voorheen goedgekeurde apparatuur mag niet worden geweigerd indien de wijzigingen alleen betrekking hebben op functies die niet in deze bijlage zijn gespecificeerd. Indien technisch niet uitvoerbaar, mag de invoering van nieuwe tekensets bij de software-upgrade van controleapparaten achterwege worden gelaten.

8.2 **Veiligheidscertificaat**

431) Het veiligheidscertificaat wordt afgegeven in overeenstemming met de bepalingen van aanhangsel 10 van deze bijlage. De onderdelen van het controleapparaat die moeten worden gecertificeerd, zijn de voertuigunit, de bewegingssensor, de externe GNSS-module en de tachograafkaart.

432) In het uitzonderlijke geval dat de autoriteiten voor beveiligingscertificering weigeren een nieuw apparaat te certificeren op grond van veroudering van de beveiligingsmechanismen, wordt alleen typegoedkeuring verleend in dit specifieke en uitzonderlijke geval en wanneer er geen andere, met de verordening in overeenstemming zijnde oplossing bestaat.

433) In dat geval stelt de lidstaat onverwijld de Europese Commissie op de hoogte, die binnen twaalf kalendermaanden na de verleende typegoedkeuring een procedure start om ervoor te zorgen dat de beveiliging weer op haar oorspronkelijke niveau wordt gebracht.

8.3 **Functiecertificaat**

434) Elke aanvrager van een typegoedkeuring moet de goedkeuringsautoriteit van de lidstaat de door die autoriteit noodzakelijk geachte materialen en documentatie verschaffen.

435) De fabrikanten dienen binnen één maand nadat daarom is verzocht de relevante monsters van goedgekeurde producten en de bijbehorende documentatie te verstrekken die de met het uitvoeren van functionele tests belaste laboratoria nodig hebben. Alle uit dat verzoek voortvloeiende kosten worden gedragen door de partij die daarom vraagt. De laboratoria dienen commercieel gevoelige informatie vertrouwelijk te behandelen.

436) Een functiecertificaat wordt alleen aan de fabrikant afgegeven nadat in elk geval alle functiebeproevingen als gespecificeerd in aanhangsel 9, succesvol afgesloten zijn.

437) De typegoedkeuringsautoriteit geeft het functiecertificaat af. Dit certificaat moet behalve de naam van de ontvanger en de identificatie van het model ook een gedetailleerde lijst van uitgevoerde tests en behaalde resultaten vermelden.

438) Op het functiecertificaat van een controleapparaat moeten ook de typegoedkeuringsnummers zijn aangegeven van alle andere goedgekeurde compatibele onderdelen van dat apparaat die voor de certificering van het controleapparaat zijn getest.

439) Op het functiecertificaat van een onderdeel van een controleapparaat wordt vermeld aan welke ISO of CEN-norm de functionele interface is getoetst.

8.4 **Interoperabiliteitscertificaat**

440) Interoperabiliteitstests worden door een laboratorium uitgevoerd in opdracht en onder verantwoordelijkheid van de Europese Commissie.

441) Het laboratorium moet de verzoeken van fabrikanten om interoperabiliteitstests in chronologische volgorde van ontvangst registreren.

442) Verzoeken worden officieel geregistreerd wanneer het laboratorium in het bezit is van:

— alle materialen en documenten die nodig zijn voor de interoperabiliteitstests;

— het corresponderende beveiligingscertificaat;

— het corresponderende functiecertificaat.

De fabrikant moet over de registratiedatum van het verzoek worden geïnformeerd.

443) Het laboratorium voert geen interoperabiliteitstests uit voor controleapparaten of tachograafkaarten waarvoor geen beveiligingscertificaat en functiecertificaat is afgegeven, behalve in de uitzonderlijke omstandigheden die zijn beschreven in voorschrift 432.

444) Een fabrikant die een interoperabiliteitstest aanvraagt, moet alle materialen en documenten die nodig zijn voor het uitvoeren van de test verstrekken aan het voor deze test verantwoordelijke laboratorium.

445) De interoperabiliteitstests worden, overeenkomstig aanhangsel 9 van deze bijlage, uitgevoerd met alle types controleapparatuur of tachograafkaarten

— waarvan de typegoedkeuring nog steeds geldig is of

— waarvan de typegoedkeuring is aangevraagd en waarvoor een geldig interoperabiliteitscertificaat is verleend.

446) De interoperabiliteitstests bestrijken alle generaties van controleapparaten of tachograafkaarten die nog worden gebruikt.

447) Het laboratorium geeft het interoperabiliteitscertificaat alleen aan de fabrikant af nadat alle vereiste interoperabiliteitstest zijn geslaagd.

448) Indien de interoperabiliteitstests bij een of meer controleapparaten of tachograafkaarten niet zijn geslaagd, wordt het interoperabiliteitscertificaat pas afgegeven nadat de betreffende fabrikant de noodzakelijke wijzigingen heeft aangebracht en de apparatuur respectievelijk kaarten de daaropvolgende interoperabiliteitstest met goed gevolg hebben doorstaan. Het laboratorium moet de oorzaak van het probleem met de hulp van de betreffende fabrikanten vaststellen en moet de fabrikant die het verzoek heeft ingediend, helpen om een technische oplossing te zoeken. Als de fabrikant zijn product heeft gewijzigd, dient hij bij de bevoegde instantie na te vragen of het veiligheidscertificaat en het functiecertificaat geldig blijven.

449) Het interoperabiliteitscertificaat is zes maanden geldig. Aan het einde van deze periode wordt het ingetrokken wanneer de fabrikant geen corresponderend goedkeuringscertificaat heeft ontvangen. Het certificaat moet door de fabrikant naar de goedkeuringsautoriteit van de lidstaat worden gezonden die het functiecertificaat heeft afgegeven.

450) Elk onderdeel dat aan de basis van een interoperabiliteitsfout kan liggen, mag niet worden gebruikt om voordelen of een dominante positie te verkrijgen.

8.5 **Typegoedkeuringscertificaat**

451) De goedkeuringsautoriteit van de lidstaat geeft het goedkeuringscertificaat af zodra de autoriteit in het bezit is van de drie vereiste certificaten.

452) Op het typegoedkeuringscertificaat van onderdelen van een controleapparaat moeten ook de typegoedkeuringsnummers van alle andere goedgekeurde interoperabele controleapparaten worden vermeld

453) Op het moment van afgifte aan de fabrikant moet de typegoedkeuringsautoriteit een kopie van het typegoedkeuringscertificaat aan het voor de interoperabiliteitstest verantwoordelijke laboratorium verstrekken.

454) Het voor de interoperabiliteitstests bevoegde laboratorium moet een publiek toegankelijke website beheren waarop de lijst van types controleapparaten of tachograafkaarten wordt bijgewerkt:

— waarvoor een verzoek tot uitvoering van interoperabiliteitstests is geregistreerd;

— waarvoor een interoperabiliteitscertificaat (ook tijdelijk) is afgegeven;

— waarvoor een typegoedkeuringscertificaat is afgegeven.

8.6 **Bijzondere procedure: eerste interoperabiliteitscertificaten voor controleapparaten en tachograafkaarten van de 2de generatie**

455) Tot vier maanden nadat de eerste combinatie van controleapparaat van de 2de generatie en tachograafkaart van de 2de generatie (bestuurders-, werkplaats-, controle- en bedrijfskaart) als interoperabel gecertificeerd is, wordt een afgegeven interoperabiliteitscertificaat (inclusief de allereerste) met betrekking tot tijdens deze periode geregistreerde verzoeken, als tijdelijk beschouwd.

456) Wanneer aan het einde van deze periode alle betreffende producten onderling interoperabel zijn, worden alle corresponderende interoperabiliteitscertificaten definitief.

457) Wanneer tijdens deze periode interoperabiliteitsfouten worden ontdekt, moet het voor de interoperabiliteitstests verantwoordelijke laboratorium de oorzaak van de problemen met hulp van alle betrokken fabrikanten vaststellen en moeten de fabrikanten de noodzakelijke wijzigingen aanbrengen.

458) Indien zich aan het einde van deze periode nog steeds interoperabiliteitsproblemen voordoen, moet het voor de interoperabiliteitstests verantwoordelijke laboratorium in samenwerking met de betreffende fabrikanten en de goedkeuringsautoriteiten die de corresponderende functiecertificaten hebben afgegeven, de oorzaken van de interoperabiliteitsfouten detecteren en vaststellen welke wijzigingen door de betreffende fabrikanten moeten worden aangebracht. Het zoeken naar technische oplossingen duurt maximaal twee maanden, waarna, indien geen algemene oplossing gevonden wordt, de Commissie na overleg met het voor de interoperabiliteitstests verantwoordelijke laboratorium beslist welke apparaten en kaarten een definitief interoperabiliteitscertificaat krijgen. De Commissie motiveert haar beslissing.

459) Elk verzoek tot uitvoering van interoperabiliteitstests dat door het laboratorium geregistreerd wordt tussen het einde van de periode van vier maanden nadat het eerste tijdelijke interoperabiliteitscertificaat is afgegeven en de datum van het besluit van de Commissie als bedoeld in voorschrift 455, moet worden opgeschort totdat de aanvankelijke interoperabiliteitsproblemen opgelost zijn. Die verzoeken worden vervolgens in chronologische volgorde van registratie behandeld.

Aanhangsel 1

DATA DICTIONARY

INHOUDSOPGAVE

1. INLEIDING 88

1.1. Methoden voor de definitie van soorten gegevens 88

1.2. Referentienormen 88

2. DEFINITIES VAN SOORTEN GEGEVENS 89

2.1. ActivityChangeInfo 89

2.2. Address 90

2.3. AESKey 91

2.4. AES128Key 91

2.5. AES192Key 91

2.6. AES256Key 92

2.7. BCDString 92

2.8. CalibrationPurpose 92

2.9. CardActivityDailyRecord 93

2.10. CardActivityLengthRange 93

2.11. CardApprovalNumber 93

2.12. CardCertificate 94

2.13. CardChipIdentification 94

2.14. CardConsecutiveIndex 94

2.15. CardControlActivityDataRecord 94

2.16. CardCurrentUse 95

2.17. CardDriverActivity 95

2.18. CardDrivingLicenceInformation 95

2.19. CardEventData 96

2.20. CardEventRecord 96

2.21. CardFaultData 96

2.22. CardFaultRecord 97

2.23. CardIccIdentification 97

2.24. CardIdentification 97

2.25. CardMACertificate 98

2.26. CardNumber 98

2.27. CardPlaceDailyWorkPeriod 99

2.28. CardPrivateKey 99

2.29. CardPublicKey 99
2.30. CardRenewalIndex 99
2.31. CardReplacementIndex 99
2.32. CardSignCertificate 100
2.33. CardSlotNumber 100
2.34. CardSlotsStatus 100
2.35. CardSlotsStatusRecordArray 100
2.36. CardStructureVersion 101
2.37. CardVehicleRecord 101
2.38. CardVehiclesUsed 102
2.39. CardVehicleUnitRecord 102
2.40. CardVehicleUnitsUsed 102
2.41. Certificate 103
2.42. CertificateContent 103
2.43. CertificateHolderAuthorisation 104
2.44. CertificateRequestID 104
2.45. CertificationAuthorityKID 104
2.46. CompanyActivityData 105
2.47. CompanyActivityType 106
2.48. CompanyCardApplicationIdentification 106
2.49. CompanyCardHolderIdentification 106
2.50. ControlCardApplicationIdentification 106
2.51. ControlCardControlActivityData 107
2.52. ControlCardHolderIdentification 107
2.53. ControlType 108
2.54. CurrentDateTime 109
2.55. CurrentDateTimeRecordArray 109
2.56. DailyPresenceCounter 109
2.57. Datef 109
2.58. DateOfDayDownloaded 110
2.59. DateOfDayDownloadedRecordArray 110
2.60. Distance 110
2.61. DriverCardApplicationIdentification 110
2.62. DriverCardHolderIdentification 111
2.63. DSRCSecurityData 112
2.64. EGFCertificate 112
2.65. EmbedderIcAssemblerId 112

2.66. EntryTypeDailyWorkPeriod 113
2.67. EquipmentType 113
2.68. EuropeanPublicKey 114
2.69. EventFaultRecordPurpose 114
2.70. EventFaultType 114
2.71. ExtendedSealIdentifier 115
2.72. ExtendedSerialNumber 116
2.73. FullCardNumber 116
2.74. FullCardNumberAndGeneration 117
2.75. Generation 117
2.76. GeoCoordinates 117
2.77. GNSSAccuracy 118
2.78. GNSSContinuousDriving 118
2.79. GNSSContinuousDrivingRecord 118
2.80. GNSSPlaceRecord 118
2.81. HighResOdometer 119
2.82. HighResTripDistance 119
2.83. HolderName 119
2.84. InternalGNSSReceiver 119
2.85. K-ConstantOfRecordingEquipment 119
2.86. KeyIdentifier 120
2.87. KMWCKey 120
2.88. Language 120
2.89. LastCardDownload 120
2.90. LinkCertificate 120
2.91. L-TyreCircumference 121
2.92. MAC 121
2.93. ManualInputFlag 121
2.94. ManufacturerCode 121
2.95. ManufacturerSpecificEventFaultData 121
2.96. MemberStateCertificate 122
2.97. MemberStateCertificateRecordArray 122
2.98. MemberStatePublicKey 122
2.99. Name 122
2.100. NationAlpha 123
2.101. NationNumeric 123
2.102. NoOfCalibrationRecords 123

2.103. NoOfCalibrationsSinceDownload 123
2.104. NoOfCardPlaceRecords 123
2.105. NoOfCardVehicleRecords 124
2.106. NoOfCardVehicleUnitRecords 124
2.107. NoOfCompanyActivityRecords 124
2.108. NoOfControlActivityRecords 124
2.109. NoOfEventsPerType 124
2.110. NoOfFaultsPerType 124
2.111. NoOfGNSSCDRecords 124
2.112. NoOfSpecificConditionRecords 125
2.113. OdometerShort 125
2.114. OdometerValueMidnight 125
2.115. OdometerValueMidnightRecordArray 125
2.116. OverspeedNumber 125
2.117. PlaceRecord 126
2.118. PreviousVehicleInfo 126
2.119. PublicKey 127
2.120. RecordType 127
2.121. RegionAlpha 128
2.122. RegionNumeric 128
2.123. RemoteCommunicationModuleSerialNumber 129
2.124. RSAKeyModulus 129
2.125. RSAKeyPrivateExponent 129
2.126. RSAKeyPublicExponent 129
2.127. RtmData 129
2.128. SealDataCard 129
2.129. SealDataVu 130
2.130. SealRecord 130
2.131. SensorApprovalNumber 130
2.132. SensorExternalGNSSApprovalNumber 131
2.133. SensorExternalGNSSCoupledRecord 131
2.134. SensorExternalGNSSIdentification 131
2.135. SensorExternalGNSSInstallation 132
2.136. SensorExternalGNSSOSIdentifier 132
2.137. SensorExternalGNSSSCIdentifier 132
2.138. SensorGNSSCouplingDate 133

2.139. SensorGNSSSerialNumber 133
2.140. SensorIdentification 133
2.141. SensorInstallation 133
2.142. SensorInstallationSecData 134
2.143. SensorOSIdentifier 134
2.144. SensorPaired 134
2.145. SensorPairedRecord 135
2.146. SensorPairingDate 135
2.147. SensorSCIdentifier 135
2.148. SensorSerialNumber 135
2.149. Handtekening 135
2.150. SignatureRecordArray 136
2.151. SimilarEventsNumber 136
2.152. SpecificConditionRecord 136
2.153. SpecificConditions 136
2.154. SpecificConditionType 137
2.155. Speed 137
2.156. SpeedAuthorised 137
2.157. SpeedAverage 138
2.158. SpeedMax 138
2.159. TachographPayload 138
2.160. TachographPayloadEncrypted 138
2.161. TDesSessionKey 138
2.162. TimeReal 139
2.163. TyreSize 139
2.164. VehicleIdentificationNumber 139
2.165. VehicleIdentificationNumberRecordArray 139
2.166. VehicleRegistrationIdentification 139
2.167. VehicleRegistrationNumber 140
2.168. VehicleRegistrationNumberRecordArray 140
2.169. VuAbility 140
2.170. VuActivityDailyData 141
2.171. VuActivityDailyRecordArray 141
2.172. VuApprovalNumber 141
2.173. VuCalibrationData 142
2.174. VuCalibrationRecord 142
2.175. VuCalibrationRecordArray 143

2.176. VuCardIWData 144
2.177. VuCardIWRecord 144
2.178. VuCardIWRecordArray 145
2.179. VuCardRecord 145
2.180. VuCardRecordArray 146
2.181. VuCertificate 146
2.182. VuCertificateRecordArray 146
2.183. VuCompanyLocksData 147
2.184. VuCompanyLocksRecord 147
2.185. VuCompanyLocksRecordArray 148
2.186. VuControlActivityData 148
2.187. VuControlActivityRecord 148
2.188. VuControlActivityRecordArray 149
2.189. VuDataBlockCounter 149
2.190. VuDetailedSpeedBlock 149
2.191. VuDetailedSpeedBlockRecordArray 150
2.192. VuDetailedSpeedData 150
2.193. VuDownloadablePeriod 150
2.194. VuDownloadablePeriodRecordArray 151
2.195. VuDownloadActivityData 151
2.196. VuDownloadActivityDataRecordArray 151
2.197. VuEventData 152
2.198. VuEventRecord 152
2.199. VuEventRecordArray 153
2.200. VuFaultData 154
2.201. VuFaultRecord 154
2.202. VuFaultRecordArray 155
2.203. VuGNSSCDRecord 155
2.204. VuGNSSCDRecordArray 156
2.205. VuIdentification 156
2.206. VuIdentificationRecordArray 157
2.207. VuITSConsentRecord 157
2.208. VuITSConsentRecordArray 158
2.209. VuManufacturerAddress 158
2.210. VuManufacturerName 158
2.211. VuManufacturingDate 158

2.212. VuOverSpeedingControlData 159
2.213. VuOverSpeedingControlDataRecordArray 159
2.214. VuOverSpeedingEventData 159
2.215. VuOverSpeedingEventRecord 159
2.216. VuOverSpeedingEventRecordArray 160
2.217. VuPartNumber 161
2.218. VuPlaceDailyWorkPeriodData 161
2.219. VuPlaceDailyWorkPeriodRecord 161
2.220. VuPlaceDailyWorkPeriodRecordArray 162
2.221. VuPrivateKey 162
2.222. VuPublicKey 162
2.223. VuSerialNumber 162
2.224. VuSoftInstallationDate 162
2.225. VuSoftwareIdentification 163
2.226. VuSoftwareVersion 163
2.227. VuSpecificConditionData 163
2.228. VuSpecificConditionRecordArray 163
2.229. VuTimeAdjustmentData 164
2.230. VuTimeAdjustmentGNSSRecord 164
2.231. VuTimeAdjustmentGNSSRecordArray 164
2.232. VuTimeAdjustmentRecord 165
2.233. VuTimeAdjustmentRecordArray 165
2.234. WorkshopCardApplicationIdentification 166
2.235. WorkshopCardCalibrationData 166
2.236. WorkshopCardCalibrationRecord 167
2.237. WorkshopCardHolderIdentification 168
2.238. WorkshopCardPIN 168
2.239. W-VehicleCharacteristicConstant 169
2.240. VuPowerSupplyInterruptionRecord 169
2.241. VuPowerSupplyInterruptionRecordArray 169
2.242. VuSensorExternalGNSSCoupledRecordArray 170
2.243. VuSensorPairedRecordArray 170
3. DEFINITIES VAN WAARDEN- EN AFMETINGENBEREIK 171
4. TEKENSETS 171
5. CODERING 171
6. OBJECTIDENTIFICATIE EN TOEPASSINGSIDENTIFICATIE 171
6.1. Objectidentificatie 171
6.2. Toepassingsidentificaties 172

1. INLEIDING

In dit aanhangsel worden gegevensformaten, -elementen en -structuren gespecificeerd voor gebruik in controle-apparaten en op tachograafkaarten.

1.1. **Methoden voor de definitie van soorten gegevens**

In dit aanhangsel wordt Abstract Syntax Notation One (ASN.1) gebruikt om soorten gegevens te definiëren. Daardoor is het mogelijk enkelvoudige en gestructureerde gegevens te definiëren zonder een toepassings- en omgevingsafhankelijke specifieke overdrachtssyntaxis (coderingsregels).

ASN.1-conventies voor soortbenaming worden gebruikt in overeenstemming met ISO/IEC 8824-1. Dat betekent dat:

— waar mogelijk de betekenis van de gegevenssoort door middel van de geselecteerde benamingen wordt aangeduid;

— waar een gegevenssoort een samenstelling van andere gegevenssoorten is, de benaming van de gegevenssoort toch een enkele reeks alfabetische tekens is die begint met een hoofdletter. Hoofdletters worden echter in de benaming gebruikt om de corresponderende betekenis te verduidelijken;

— de benamingen van de soorten gegevens in het algemeen betrekking hebben op de benaming van de soorten gegevens waaruit ze zijn samengesteld, de apparatuur waarin de gegevens zijn opgeslagen en de aan de gegevens gerelateerde functie.

Als een ASN.1-soort reeds als onderdeel van een andere norm is gedefinieerd en als hij relevant is voor gebruik in het controleapparaat, wordt die ASN.1-soort in dit aanhangsel gedefinieerd.

Om verscheidene soorten coderingsregels mogelijk te maken, is een aantal ASN.1-soorten in dit aanhangsel beperkt door identificatiesymbolen voor het waardenbereik. Die identificatiesymbolen voor het waardenbereik zijn gedefinieerd in punt 3 en aanhangsel 2.

1.2. **Referentienormen**

In dit aanhangsel worden de volgende referentienormen gebruikt:

ISO 639	Code voor namen van talen. Eerste uitgave: 1988.
ISO 3166	Codes voor de weergave van landnamen en hun onderverdelingen — Deel 1: Landencodes, 2013.
ISO 3779	Wegvoertuigen — Voertuig-identificatienummer (VIN) — Inhoud en structuur. 2009.
ISO/IEC 7816-5	Identification cards — Integrated circuit cards — Part 5: Registration of application providers. Second edition: 2004.
ISO/IEC 7816-6	Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange, 2004 + Technical Corrigendum 1: 2006.
ISO/IEC 8824-1	Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation. 2008 + Technical Corrigendum 1: 2012 and Technical Corrigendum 2: 2014.
ISO/IEC 8825-2	Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). 2008.
ISO/IEC 8859-1	Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1 First edition: 1998.
ISO/IEC 8859-7	Information technology — 8-bit single-byte coded graphic character sets — Part 7: Latin/Greek alphabet. 2003.

ISO 16844-3	Wegvoertuigen — Tachograafsystemen — Aansluiting van bewegingssensor. 2004 + Technical Corrigendum 1: 2006.
TR-03110-3	BSI / ANSSI Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token — Part 3 Common Specifications, version 2.20, 3. February 2015.

2. DEFINITIES VAN SOORTEN GEGEVENS

Voor elk van de volgende gegevenssoorten bestaat de standaardwaarde voor een "onbekende" of een "niet-toepasbare" inhoud in het opvullen van het dataelement met 'FF'-bytes.

Alle gegevenssoorten worden gebruikt voor toepassingen van de 1e en 2e generatie, tenzij anders bepaald.

2.1. **ActivityChangeInfo**

Met deze gegevenssoort kan de status van een lezer op 00:00 en/of de status van een bestuurder op 00:00 en/of wijzigingen van activiteit en/of wijzigingen in de status van de bestuurder en/of wijzigingen in de status van een kaart voor een bestuurder of een bijrijder gecodeerd worden binnen een woord van twee bytes. Deze gegevenssoort is gerelateerd aan de voorschriften 105, 266, 291, 320, 321, 343 en 344 van bijlage 1C.

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

Waardetoekenning — **Octet-uitgericht**: 'scpaatttttttttt'B (16-bits)

Voor geheugenrecords (of status van de lezer):

's'B	Lezer:
	'0'B: BESTUURDER,
	'1'B: BIJRIJDER,
'c'B	Status van de bestuurder:
	'0'B: ALLEEN,
	'1'B: MET EEN TEAM,
'p'B	Status van de bestuurderskaart (of werkplaatskaart) in de relevante lezer:
	'0'B: INGEBRACHT, een kaart is ingebracht,
	'1'B: NIET INGEBRACHT, er is geen kaart ingebracht (of er is een kaart uitgenomen),
'aa'B	Activiteit:
	'00'B: PAUZE/RUST,
	'01'B: BESCHIKBAARHEID,
	'10'B: WERKEN,
	'11'B: RIJDEN,
'ttttttttttt'B	Tijd van de wijziging: aantal minuten vanaf 00.00 uur op de betreffende dag.

Voor bestuurderskaartregistraties (of werkplaatskaartregistraties) (en status van de bestuurder):

's'B	Lezer (niet relevant als 'p' = 1, behoudens onderstaande opmerking):
	'0'B: BESTUURDER,
	'1'B: BIJRIJDER,
'c'B	Status van de bestuurder (geval 'p' = 0) of
	Volgende activiteitstatus (geval 'p' = 1):
	'0'B: ALLEEN,
	'0'B: ONBEKEND,
	'1'B: MET EEN TEAM,
	'1'B: BEKEND (= manueel ingevoerd)
'p'B	Status van de kaart:
	'0'B: INGEBRACHT, de kaart is in een controleapparaat ingebracht,
	'1'B: NIET INGEBRACHT, de kaart is niet ingebracht (of de kaart is uitgenomen),
'aa'B	Activiteit (niet relevant als 'p' = 1 en 'c' = 0, behoudens onderstaande opmerking):
	'00'B: PAUZE/RUST,
	'01'B: BESCHIKBAARHEID,
	'10'B: WERKEN,
	'11'B: RIJDEN,
'ttttttttttt'B	Tijd van de wijziging: aantal minuten vanaf 00.00 uur op de betreffende dag.

Opmerking in geval van "kaartuitneming":

Als de kaart is uitgenomen:

— 's' is relevant en geeft de lezer aan waar de kaart is uitgenomen,

— 'c' moet op 0 worden gezet,

— 'p' moet op 1 worden gezet,

— 'aa' moet de lopende, op dat moment geselecteerde activiteit coderen.

Ten gevolge van een manuele invoer kunnen de bits 'c' en 'aa' van het (op een kaart opgeslagen) woord later worden overschreven om de invoer weer te geven.

2.2. **Address**

Een adres.

```
Address ::= SEQUENCE {
   codePage                              INTEGER (0..255),
   address                               OCTET STRING (SIZE(35))
}
```

codePage specificeert een tekenset zoals gedefinieerd in hoofdstuk 4,

address is een adres dat is gecodeerd met de gespecificeerde tekenset.

2.3. **AESKey**

2e generatie:

Een AES-sleutel met een lengte van 128, 192 of 256 bits.

```
AESKey ::= CHOICE {
   aes128Key                          AES128Key,
   aes192Key                          AES192Key,
   aes256Key                          AES256Key
}
```

Waardetoekenning: niet nader gespecificeerd.

2.4. **AES128Key**

2e generatie:

Een AES128-sleutel.

```
AES128Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes128Key                          OCTET STRING (SIZE(16))
}
```

length geeft de lengte van de AES128-sleutel in bytes aan.

aes128Key is een AES-sleutel met een lengte van 128 bits.

Waardetoekenning:

de lengte heeft waarde 16.

2.5. **AES192Key**

2e generatie:

Een AES192-sleutel.

```
AES192Key ::= SEQUENCE {
   length                             INTEGER(0..255),
   aes192Key                          OCTET STRING (SIZE(24))
}
```

length geeft de lengte van de AES192-sleutel in bytes aan.

aes192Key is een AES-sleutel met een lengte van 192 bits.

Waardetoekenning:

de lengte heeft waarde 24.

2.6. **AES256Key**

2e generatie:

Een AES256-sleutel.

```
AES256Key ::= SEQUENCE {
   length                                  INTEGER(0..255),
   aes256Key                               OCTET STRING (SIZE(32))
}
```

length geeft de lengte van de AES256-sleutel in bytes aan.

aes256Key is een AES-sleutel met een lengte van 256 bits.

Waardetoekenning:

de lengte heeft waarde 32.

2.7. **BCDString**

BCDString wordt toegepast voor de BCD-weergave (Binary Code Decimal, binair gecodeerde decimaal). Deze datasoort wordt gebruikt om een decimaal cijfer in een semi-byte (4 bits) weer te geven. BCDString is gebaseerd op het 'CharacterStringType' van ISO/IEC 8824-1.

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

BCDString gebruikt een "hstring"-notatie. Het uiterst linkse hexadecimale cijfer moet de meest significante semi-byte van de eerste byte zijn. Om een veelvoud van bytes aan te maken, moeten zoveel semi-bytes eindigend op nul worden ingebracht als nodig zijn vanaf de uiterst linkse semi-bytepositie in de eerste byte.

Toegestane cijfers zijn: 0, 1, …, 9.

2.8. **CalibrationPurpose**

Code die verklaart waarom een verzameling kalibratieparameters werd geregistreerd. Deze gegevenssoort is gerelateerd aan de voorschriften 097 en 098 van bijlage 1B en voorschrift 119 van bijlage 1C.

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

Waardetoekenning:

1e generatie:

'00'H	gereserveerde waarde,
'01'H	activering: registratie van kalibratieparameters die op het moment van activering van de voertuigunit (VU) bekend zijn,
'02'H	eerste installatie: eerste kalibratie van de VU na activering,
'03'H	installatie: eerste kalibratie van de VU in het huidige voertuig,
'04'H	periodieke controle.

2e generatie:

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

'05'H invoering van kentekennummer door de onderneming,

'06'H tijdafstelling zonder kalibratie,

'07'H tot '7F'H RFU,

'80'H tot 'FF'H Specifiek voor de fabrikant.

2.9. **CardActivityDailyRecord**

Op een kaart opgeslagen informatie met betrekking tot de activiteiten van de bestuurder op een bepaalde dag. Deze gegevenssoort is gerelateerd aan de voorschriften 266, 291, 320 en 343 van bijlage 1C.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength         INTEGER(0..CardActivityLengthRange),
   activityRecordLength                 INTEGER(0..CardActivityLengthRange),
   activityRecordDate                   TimeReal,
   activityDailyPresenceCounter         DailyPresenceCounter,
   activityDayDistance                  Distance,
   activityChangeInfo                   SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength is de totale lengte in bytes van de voorafgaande dagelijkse registratie. De maximale waarde wordt toegekend door de lengte van de OCTET STRING die deze records bevat (zie CardActivityLengthRange aanhangsel 2, punt 4). Als die record de oudste dagelijkse registratie is, moet de waarde van activityPreviousRecordLength op 0 worden gezet.

activityRecordLength is de totale lengte in bytes van deze record. De maximale waarde wordt toegekend door de lengte van de OCTET STRING die deze records bevat.

activityRecordDate is de datum van de record.

activityDailyPresenceCounter is de dagelijkse aanwezigheidsteller voor de kaart op die dag.

activityDayDistance is de totale op die dag afgelegde afstand.

activityChangeInfo is de verzameling ActivityChangeInfo-gegevens voor de bestuurder op die dag. Het kan maximaal 1440 waarden bevatten (één activiteitswijziging per minuut). De verzameling bevat altijd de activityChangeInfo waarmee de bestuurderstatus op 00:00 wordt gecodeerd.

2.10. **CardActivityLengthRange**

Aantal beschikbare bytes op een bestuurders- of werkplaatskaart voor het opslaan van records van de activiteiten van de bestuurder.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Waardetoekenning: zie aanhangsel 2.

2.11. **CardApprovalNumber**

Typegoedkeuringsnummer van de kaart.

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

Waardetoekenning:

het goedkeuringsnummer wordt verstrekt zoals het is bekendgemaakt op de overeenkomstige website van de Europese Commissie, bijv. met eventuele koppeltekens. Het goedkeuringsnummer wordt links uitgelijnd.

2.12. **CardCertificate**

1e generatie:

Certificaat van de openbare sleutel van een kaart.

```
CardCertificate ::= Certificate
```

2.13. **CardChipIdentification**

Op een kaart opgeslagen informatie met betrekking tot de identificatie van het geïntegreerd circuit (IC) van de kaart (voorschrift 249 van bijlage 1C). Het icSerialNumber vormt samen met de icManufacturingReferences de unieke identificatie van de kaartchip. Het icSerialNumber alleen is geen unieke identificatie van de kaartchip.

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                    OCTET STRING (SIZE(4)),
   icManufacturingReferences         OCTET STRING (SIZE(4))
}
```

icSerialNumber is het serienummer van het IC.

icManufacturingReferences is het specifieke identificatiesymbool van de fabrikant van het IC.

2.14. **CardConsecutiveIndex**

Opeenvolgende index van de kaart (definitie h)).

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

Waardetoekenning: (zie bijlage 1C, hoofdstuk 7).

Volgorde van verhoging: '0, …, 9, A, …, Z, a, …, z'

2.15. **CardControlActivityDataRecord**

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de laatste controle van de bestuurder (voorschriften 274, 299, 327 en 350 van bijlage 1C).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                       ControlType,
   controlTime                       TimeReal,
   controlCardNumber                 FullCardNumber,
   controlVehicleRegistration        VehicleRegistrationIdentification,
   controlDownloadPeriodBegin        TimeReal,
   controlDownloadPeriodEnd          TimeReal
}
```

controlType is de soort controle.

controlTime is de datum en het tijdstip van de controle.

controlCardNumber is het FullCardNumber van de controleur die de controle heeft uitgevoerd.

controlVehicleRegistration is het kentekennummer en de registrerende lidstaat van het voertuig waarin de controle plaatsvond.

controlDownloadPeriodBegin en **controlDownloadPeriodEnd** is de gedownloade periode in geval van download.

2.16. **CardCurrentUse**

Informatie over het werkelijke gebruik van de kaart (voorschriften 273, 298, 326 en 349 van bijlage 1C).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                    TimeReal,
   sessionOpenVehicle                 VehicleRegistrationIdentification
}
```

sessionOpenTime is het tijdstip waarop de kaart voor het huidige gebruik ingebracht wordt. Dat element wordt bij kaartuitneming op nul gezet.

sessionOpenVehicle is de identificatie van het thans gebruikte voertuig, die wordt ingesteld bij kaartinbrenging. Dat element wordt bij kaartuitneming op nul gezet.

2.17. **CardDriverActivity**

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de activiteiten van de bestuurder (voorschriften 267, 268, 292, 293, 321 en 344 van bijlage 1C).

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

activityPointerOldestDayRecord is de specificatie van het begin van de geheugenplaats (aantal bytes vanaf het begin van de string) van de oudste volledige dagregistratie in de activityDailyRecords-string. De maximale waarde wordt door de lengte van de string aangegeven.

activityPointerNewestRecord is de specificatie van het begin van de geheugenplaats (aantal bytes vanaf het begin van de string) van de meest recente dagregistratie in de activityDailyRecords-string. De maximale waarde wordt door de lengte van de string aangegeven.

activityDailyRecords is de ruimte die beschikbaar is om de gegevens over de activiteit van de bestuurder op te slaan (gegevensstructuur: CardActivityDaily record) voor elke kalenderdag waarop de kaart is gebruikt.

Waardetoekenning: deze bytestring wordt periodiek met registraties van de CardActivityDailyRecord gevuld. Bij het eerste gebruik begint de opslag met de eerste byte van de string. Alle nieuwe records worden aan het einde van de voorgaande record toegevoegd. Als de string vol is, gaat de opslag verder bij de eerste byte van de string, onafhankelijk van een onderbreking binnen een gegevenselement. Voor het invoeren van nieuwe gegevens over activiteiten in de string (uitbreiden van de lopende activityDailyRecord of invoeren van een nieuwe activityDaily-Record), die oudere gegevens over activiteiten vervangen, moet de activityPointerOldestDayRecord worden bijgewerkt om de nieuwe locatie van de oudste volledige dagregistratie weer te geven; de activityPreviousRecord-Length van deze (nieuwe) oudste volledige dagregistratie moet op 0 worden teruggezet.

2.18. **CardDrivingLicenceInformation**

Op een bestuurderskaart opgeslagen informatie met betrekking tot de rijbewijsgegevens van de kaarthouder (voorschriften 259 en 284 van bijlage 1C).

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

drivingLicenceIssuingAuthority is de autoriteit die verantwoordelijk is voor de afgifte van het rijbewijs.

drivingLicenceIssuingNation is de nationaliteit van de autoriteit die het rijbewijs heeft afgegeven.

drivingLicenceNumber is het nummer van het rijbewijs.

2.19. **CardEventData**

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de aan de kaarthouder te wijten voorvallen (voorschriften 260, 285, 318 en 341 van bijlage 1C).

```
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).

2.20. **CardEventRecord**

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot een aan de kaarthouder te wijten voorval (voorschriften 261, 286, 318 en 341 van bijlage 1C).

```
CardEventRecord ::= SEQUENCE {
   eventType                            EventFaultType,
   eventBeginTime                       TimeReal,
   eventEndTime                         TimeReal,
   eventVehicleRegistration             VehicleRegistrationIdentification
}
```

eventType is het soort voorval.

eventBeginTime is de datum en het tijdstip van het begin van het voorval.

eventEndTime is de datum en het tijdstip van het einde van het voorval.

eventVehicleRegistration is het kentekennummer en de registrerende lidstaat van het voertuig waarin het voorval plaatsvond.

2.21. **CardFaultData**

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot aan de kaarthouder te wijten fouten (voorschriften 263, 288, 318 en 341 van bijlage 1C).

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

CardFaultData is een sequentie van een recordsverzameling van controleapparaatfouten gevolgd door een recordsverzameling van kaartfouten.

cardFaultRecords is een reeks foutenrecords van een bepaalde foutencategorie (controleapparaat of kaart).

2.22. **CardFaultRecord**

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot een aan de kaarthouder te wijten fout (voorschriften 264, 289, 318 en 341 van bijlage 1C).

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

faultType is het soort fout.

faultBeginTime is de datum en het tijdstip van het begin van de fout.

faultEndTime is de datum en het tijdstip van het einde van de fout.

faultVehicleRegistration is het kentekennummer en de registrerende lidstaat van het voertuig waarin de fout plaatsvond.

2.23. **CardIccIdentification**

Op een kaart opgeslagen informatie met betrekking tot de identificatie van het geïntegreerde circuit (IC) van de kaart (voorschrift 248 van bijlage 1C).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                          OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber           ExtendedSerialNumber,
   cardApprovalNumber                 CardApprovalNumber,
   cardPersonaliserID                 ManufacturerCode,
   embedderIcAssemblerId              EmbedderIcAssemblerId,
   icIdentifier                       OCTET STRING (SIZE(2))
}
```

clockStop is de klokstopmodus zoals gedefinieerd in aanhangsel 2.

cardExtendedSerialNumber is het unieke serienummer van de IC-kaart zoals verder gespecificeerd door de gegevenssoort ExtendedSerialNumber.

cardApprovalNumber is het typegoedkeuringsnummer van de kaart.

cardPersonaliserID is de persoonlijke identificatie (ID) van de kaart gecodeerd als ManufacturerCode.

embedderIcAssemblerId geeft informatie over de embedder/IC-assembleur.

icIdentifier is het identificatiesymbool van het IC op de kaart en van de fabrikant van het IC zoals gedefinieerd in ISO/IEC 7816-6.

2.24. **CardIdentification**

Op een kaart opgeslagen informatie met betrekking tot de identificatie van de kaart (voorschriften 255, 280, 310, 333, 359, 365, 371 en 377 van bijlage 1C).

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

cardIssuingMemberState is de code van de lidstaat die de kaart heeft afgegeven.

cardNumber is het nummer van de kaart.

cardIssuingAuthorityName is de naam van de autoriteit die de kaart heeft afgegeven.

cardIssueDate is de datum van afgifte van de kaart aan de huidige houder.

cardValidityBegin is de datum waarop de geldigheid van de kaart ingaat.

cardExpiryDate is de datum waarop de geldigheid van de kaart afloopt.

2.25. **CardMACertificate**

2e generatie:

Certificaat van de openbare sleutel van de kaart voor wederzijdse authenticatie met een VU. De structuur van dat certificaat is gespecificeerd in aanhangsel 11.

```
CardMACertificate ::= Certificate
```

2.26. **CardNumber**

Kaartnummer zoals gedefinieerd in definitie g.

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification             IA5String(SIZE(14)),
      cardReplacementIndex             CardReplacementIndex,
      cardRenewalIndex                 CardRenewalIndex
   },
   SEQUENCE {
      ownerIdentification              IA5String(SIZE(13)),
      cardConsecutiveIndex             CardConsecutiveIndex,
      cardReplacementIndex             CardReplacementIndex,
      cardRenewalIndex                 CardRenewalIndex
   }
}
```

driverIdentification is de unieke identificatie van een bestuurder in een lidstaat.

ownerIdentification is de unieke identificatie van een bedrijf of een werkplaats of een controle-instantie in een lidstaat.

cardConsecutiveIndex is de opeenvolgende index van de kaart.

cardReplacementIndex is de vervangingsindex van de kaart.

cardRenewalIndex is de vernieuwingsindex van de kaart.

De eerste keuzesequentie is geschikt voor het coderen van een bestuurderskaartnummer, de tweede keuzesequentie is geschikt voor het coderen van werkplaats-, controle- en bedrijfskaartnummers.

2.27. **CardPlaceDailyWorkPeriod**

Op een bestuurders- en werkplaatskaart opgeslagen informatie met betrekking tot de plaatsen waar dagelijkse werkperioden beginnen en/of eindigen (voorschriften 272, 297, 325 en 348 van bijlage 1C).

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

placePointerNewestRecord is de index van de laatst bijgewerkte plaatsrecords.

Waardetoekenning: cijfer dat correspondeert met de teller van de plaatsrecord, beginnend met '0' voor de eerste plaatsrecord in de structuur.

placeRecords is de reeks records die de informatie met betrekking tot ingevoerde plaatsen bevat.

2.28. **CardPrivateKey**

1e generatie:

De particuliere sleutel van een kaart.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. **CardPublicKey**

De openbare sleutel van een kaart.

```
CardPublicKey ::= PublicKey
```

2.30. **CardRenewalIndex**

Vernieuwingsindex van de kaart (definitie i).

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

Waardetoekenning: (zie hoofdstuk VII van deze bijlage)

'0' Eerste afgifte.

Volgorde van verhoging: '0, …, 9, A, …, Z'

2.31. **CardReplacementIndex**

Vervangingsindex van de kaart (definitie j).

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

Waardetoekenning: (zie hoofdstuk VII van deze bijlage).

'0' Originele kaart.

Volgorde van verhoging: '0, …, 9, A, …, Z'

2.32. **CardSignCertificate**

2e generatie:

Certificaat van de openbare sleutel van de kaart voor ondertekening. De structuur van dat certificaat is gespecificeerd in aanhangsel 11.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Code ter onderscheiding van de twee lezers van een VU.

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

Waardetoekenning: niet nader gespecificeerd.

2.34. **CardSlotsStatus**

Code die de soort kaarten aangeeft die in de twee lezers van de VU zijn ingebracht.

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

Waardetoekenning — Octet-uitgericht: 'ccccdddd'B

'cccc'B Identificatie van de soort kaart die is ingebracht in de lezer van de bijrijder,

'dddd'B Identificatie van de soort kaart die is ingebracht in de lezer van de bestuurder,

met de volgende identificatiecodes:

'0000'B er is geen kaart ingebracht,

'0001'B er is een bestuurderskaart ingebracht,

'0010'B er is een werkplaatskaart ingebracht,

'0011'B er is een controlekaart ingebracht,

'0100'B er is een bedrijfskaart ingebracht.

2.35. **CardSlotsStatusRecordArray**

2e generatie:

De CardSlotsStatus plus metagegevens zoals gebruikt in het downloadprotocol.

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

recordType geeft de soort record aan (CardSlotsStatus). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van de CardSlotsStatus in bytes.

noOfRecords is het aantal records in de reeks records.

records is de reeks CardSlotsStatus-records.

2.36. **CardStructureVersion**

Code die de versie aangeeft van de in een tachograafkaart geïmplementeerde structuur.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Waardetoekenning: 'aabb'H:

'aa'H Index voor wijzigingen van de structuur.

'00'H voor toepassingen van de 1e generatie.

'01'H voor toepassingen van de 2e generatie.

'bb'H Index voor wijzigingen betreffende het gebruik van de voor de structuur gedefinieerde gegevenselementen, gegeven door de high byte.

'00'H voor deze versie van toepassingen van de 1e generatie.

'00'H voor deze versie van toepassingen van de 2e generatie.

2.37. **CardVehicleRecord**

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de gebruiksperiode van een voertuig gedurende een kalenderdag (voorschriften 269, 294, 322 en 345 van bijlage 1C).

1e generatie:

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

vehicleOdometerBegin is de kilometerstand van het voertuig aan het begin van de gebruiksperiode van het voertuig.

vehicleOdometerEnd is de kilometerstand van het voertuig aan het einde van de gebruiksperiode van het voertuig.

vehicleFirstUse is de datum en het tijdstip van het begin van de gebruiksperiode van het voertuig.

vehicleLastUse is de datum en het tijdstip van het einde van de gebruiksperiode van het voertuig.

vehicleRegistration is het kentekennummer en de registrerende lidstaat van het voertuig.

vuDataBlockCounter is de waarde van de VuDataBlockCounter bij de laatste selectie van de gebruiksperiode van het voertuig.

2e generatie:

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

Als aanvulling op de 1e generatie wordt het volgende gegevenselement gebruikt:

VehicleIdentificationNumber is het identificatienummer van het voertuig dat naar het voertuig als geheel verwijst.

2.38. **CardVehiclesUsed**

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de door de kaarthouder gebruikte voertuigen (voorschriften 270, 295, 323 en 346 van bijlage 1C).

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

vehiclePointerNewestRecord is de index van de laatst bijgewerkte voertuigrecords.

Waardetoekenning: cijfer dat correspondeert met de teller van de voertuigrecords, beginnend met '0' voor de eerste voertuigrecords in de structuur.

cardVehicleRecords is de reeks records die informatie over gebruikte voertuigen bevat.

2.39. **CardVehicleUnitRecord**

2e generatie:

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot een gebruikte voertuigunit (voorschriften 303 en 351 van bijlage 1C).

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

timeStamp is het begin van de gebruiksperiode van de VU (d.w.z. de eerste invoering van de kaart in de VU voor die periode).

manufacturerCode identificeert de fabrikant van de VU.

deviceID identificeert de soort VU van een fabrikant. De waarde is fabrikantspecifiek.

vuSoftwareVersion is het nummer van de softwareversie van de VU.

2.40. **CardVehicleUnitsUsed**

2e generatie:

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de door de kaarthouder gebruikte voertuigunits (voorschriften 306 en 352 van bijlage 1C).

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

vehiclePointerNewestRecord is de index van de laatst bijgewerkte VU-record.

Waardetoekenning: cijfer dat correspondeert met de teller van de VU-record, beginnend met '0' voor de eerste VU-record in de structuur.

cardVehicleRecords is de reeks records die informatie over gebruikte VU's bevat.

2.41. **Certificate**

Het certificaat van een openbare sleutel afgegeven door een certificeringsautoriteit.

1e generatie:

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

Waardetoekenning: digitale handtekening met gedeeltelijk herstel van een CertificateContent overeenkomstig de algemene beveiligingsmechanismen in aanhangsel 11: handtekening (128 bytes) || restant openbare sleutel (58 bytes) || referentie certificeringsautoriteit (8 bytes).

2e generatie:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Waardetoekenning: zie aanhangsel 11.

2.42. **CertificateContent**

1e generatie:

De (duidelijke) inhoud van het certificaat van een openbare sleutel overeenkomstig de algemene beveiligingsmechanismen in aanhangsel 11.

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier         INTEGER(0..255),
   certificationAuthorityReference      KeyIdentifier,
   certificateHolderAuthorisation       CertificateHolderAuthorisation,
   certificateEndOfValidity             TimeReal,
   certificateHolderReference           KeyIdentifier,
   publicKey                            PublicKey
}
```

certificateProfileIdentifier is de versie van het corresponderende certificaat.

Waardetoekenning: '01h' voor deze versie.

certificationAuthorityReference identificeert de certificeringsautoriteit die het certificaat afgeeft. Het verwijst ook naar de openbare sleutel van die certificeringsautoriteit.

certificateHolderAuthorisation identificeert de rechten van de certificaathouder.

certificateEndOfValidity is de datum waarop het certificaat administratief vervalt.

certificateHolderReference identificeert de certificaathouder. Het verwijst ook naar zijn openbare sleutel.

publicKey is de openbare sleutel die door dat certificaat gecertificeerd wordt.

2.43. **CertificateHolderAuthorisation**

Identificatie van de rechten van een certificaathouder.

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

1e generatie:

tachographApplicationID is het toepassingsidentificatiesymbool voor de tachograaftoepassing.

Waardetoekenning: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Dit AID is een particulier niet-geregistreerd toepassings-identificatiesymbool overeenkomstig ISO/IEC 7816-5.

equipmentType is de identificatie van het type apparaat waarvoor het certificaat bedoeld is.

Waardetoekenning: overeenkomstig gegevenssoort EquipmentType. **0** als het een certificaat van een lidstaat betreft.

2e generatie:

tachographApplicationID verwijst naar de zes significantste bytes van het toepassingsidentificatiesymbool (AID) van de tachograafkaart van de 2e generatie. De AID voor de tachograafkaarttoepassing is gespecificeerd in hoofdstuk 6.2.

Waardetoekenning: 'FF 53 4D 52 44 54'.

equipmentType is de identificatie van het type voor de 2e generatie gespecificeerde apparaat waarvoor het certificaat bedoeld is.

Waardetoekenning: overeenkomstig gegevenssoort EquipmentType.

2.44. **CertificateRequestID**

Unieke identificatie van een certificaatverzoek. Dit kan ook als een identificatiesymbool van de openbare sleutel van een VU worden gebruikt als het serienummer van de VU waarvoor de sleutel bedoeld is, ten tijde van de ontwikkeling van het certificaat niet bekend is.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber                  INTEGER(0..2^32-1),
   requestMonthYear                     BCDString(SIZE(2)),
   crIdentifier                         OCTET STRING(SIZE(1)),
   manufacturerCode                     ManufacturerCode
}
```

requestSerialNumber is een serienummer voor het certificaatverzoek, uniek voor de fabrikant en de hieronder genoemde maand.

requestMonthYear is de identificatie van de maand en het jaar van het certificaatverzoek.

Waardetoekenning: BCD-codering van maand (twee cijfers) en jaar (twee laatste cijfers).

crIdentifier: is een identificatiesymbool om een certificaatverzoek van een toegevoegd serienummer te kunnen onderscheiden.

Waardetoekenning: 'FFh'.

manufacturerCode: is de numerieke code van de fabrikant die het certificaat aanvraagt.

2.45. **CertificationAuthorityKID**

Identificatiesymbool van de openbare sleutel van een certificeringsautoriteit (een lidstaat of de Europese certificeringsautoriteit).

```
CertificationAuthorityKID ::= SEQUENCE{
   nationNumeric                        NationNumeric,
   nationAlpha                          NationAlpha,
   keySerialNumber                      INTEGER(0..255),
   additionalInfo                       OCTET STRING(SIZE(2)),
   caIdentifier                         OCTET STRING(SIZE(1))
}
```

nationNumeric is de numerieke nationale code van de certificeringsautoriteit.

nationAlpha is de alfanumerieke nationale code van de certificeringsautoriteit.

keySerialNumber is een serienummer om de verschillende sleutels van de certificeringsautoriteit te onderscheiden in het geval dat sleutels worden gewijzigd.

additionalInfo is een veld van twee bytes voor aanvullende codering (specifiek voor de certificeringsautoriteit).

caIdentifier is een identificatiesymbool om het sleutelidentificatiesymbool van een certificeringsautoriteit van andere sleutelidentificatiesymbolen te onderscheiden.

Waardetoekenning: '01h'.

2.46. **CompanyActivityData**

Op een bedrijfskaart opgeslagen informatie met betrekking tot activiteiten die met de kaart worden uitgevoerd (voorschriften 373 en 379 van bijlage 1C).

```
CompanyActivityData ::= SEQUENCE {
   companyPointerNewestRecord         INTEGER(0..NoOfCompanyActivityRecords-1),
   companyActivityRecords             SET SIZE(NoOfCompanyActivityRecords) OF
    companyActivityRecord              SEQUENCE {
     companyActivityType                CompanyActivityType,
     companyActivityTime                TimeReal,
     cardNumberInformation              FullCardNumber,
     vehicleRegistrationInformation     VehicleRegistrationIdentification,
     downloadPeriodBegin                TimeReal,
     downloadPeriodEnd                  TimeReal
    }
}
```

companyPointerNewestRecord is de index van het laatst bijgewerkte companyActivityRecord.

Waardetoekenning: cijfer corresponderend met de teller van de records van bedrijfsactiviteiten, beginnend met '0' voor de eerste record van bedrijfsactiviteiten in de structuur.

companyActivityRecords is de verzameling van alle records van bedrijfsactiviteiten.

companyActivityRecord is de sequentie van informatie met betrekking tot één bedrijfsactiviteit.

companyActivityType is de soort bedrijfsactiviteit.

companyActivityTime is de datum en het tijdstip van de bedrijfsactiviteit.

cardNumberInformation is het kaartnummer en de lidstaat van afgifte van de gedownloade kaart, indien van toepassing.

vehicleRegistrationInformation is het kentekennummer en de registrerende lidstaat van het gedownloade, vergrendelde of ontgrendelde voertuig.

downloadPeriodBegin en **downloadPeriodEnd** is de vanaf de VU gedownloade periode, indien van toepassing.

2.47. **CompanyActivityType**

Code die een activiteit aangeeft die door een bedrijf met gebruikmaking van zijn bedrijfskaart is uitgevoerd.

```
CompanyActivityType ::= INTEGER {
   card downloading                    (1),
   VU downloading                      (2),
   VU lock-in                          (3),
   VU lock-out                         (4)
}
```

2.48. **CompanyCardApplicationIdentification**

Op een bedrijfskaart opgeslagen informatie met betrekking tot de toepassingsidentificatie van de kaart (voorschriften 369 en 375 van bijlage 1C).

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

typeOfTachographCardId specificeert de geïmplementeerde kaartsoort.

cardStructureVersion specificeert de versie van de op de kaart geïmplementeerde structuur.

noOfCompanyActivityRecords specificeert het aantal bedrijfsactiviteiten dat op de kaart kan worden opgeslagen.

2.49. **CompanyCardHolderIdentification**

Op een bedrijfskaart opgeslagen informatie met betrekking tot de identificatie van de kaarthouder (voorschriften 372 en 378 van bijlage 1C).

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

companyName is de naam van het bedrijf van de houder.

companyAddress is het adres van het bedrijf van de houder.

cardHolderPreferredLanguage is de voorkeurtaal van de kaarthouder.

2.50. **ControlCardApplicationIdentification**

Op een controlekaart opgeslagen informatie met betrekking tot de toepassingsidentificatie van de kaart (voorschriften 357 en 363 van bijlage 1C).

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

typeOfTachographCardId specificeert de geïmplementeerde kaartsoort.

cardStructureVersion specificeert de versie van de structuur die op de kaart geïmplementeerd is.

noOfControlActivityRecords is het aantal records van controleactiviteiten dat op de kaart kan worden opgeslagen.

2.51. **ControlCardControlActivityData**

Op een controlekaart opgeslagen informatie met betrekking tot controleactiviteiten die met de kaart worden uitgevoerd (voorschriften 361 en 367 van bijlage 1C).

```
ControlCardControlActivityData ::= SEQUENCE {
   controlPointerNewestRecord        INTEGER(0.. NoOfControlActivityRecords-1),
   controlActivityRecords            SET SIZE(NoOfControlActivityRecords) OF
    controlActivityRecord             SEQUENCE {
     controlType                       ControlType,
     controlTime                       TimeReal,
     controlledCardNumber              FullCardNumber,
     controlledVehicleRegistration     VehicleRegistrationIdentification,
     controlDownloadPeriodBegin        TimeReal,
     controlDownloadPeriodEnd          TimeReal
    }
}
```

controlPointerNewestRecord is de index van de laatst gewijzigde record van controleactiviteiten.

Waardetoekenning: cijfer corresponderend met de teller van de record van controleactiviteiten, beginnend met '0' voor de eerste record van de controleactiviteiten die in de structuur voorkomt.

controlActivityRecords is de verzameling van alle records van controleactiviteiten.

controlActivityRecord is de sequentie van informatie met betrekking tot een controle.

controlType is de soort controle.

controlTime is de datum en het tijdstip van de controle.

controlledCardNumber is het kaartnummer en de lidstaat van afgifte van de gecontroleerde kaart.

controlledVehicleRegistration is het kentekennummer en de registrerende lidstaat van het voertuig waarin de controle plaatsvond.

controlDownloadPeriodBegin en **controlDownloadPeriodEnd** is de mogelijk gedownloade periode.

2.52. **ControlCardHolderIdentification**

Op een controlekaart opgeslagen informatie met betrekking tot de identificatie van de kaarthouder (voorschriften 360 en 366 van bijlage 1C).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                    Name,
   controlBodyAddress                 Address,
   cardHolderName                     HolderName,
   cardHolderPreferredLanguage        Language
}
```

controlBodyName is de naam van de controle-instantie van de kaarthouder.

controlBodyAddress is het adres van de controle-instantie van de kaarthouder.

cardHolderName is de naam en voorna(a)m(en) van de houder van de controlekaart.

cardHolderPreferredLanguage is de voorkeurtaal van de kaarthouder.

2.53. **ControlType**

Code die de tijdens een controle uitgevoerde activiteiten aangeeft. Deze gegevenssoort is gerelateerd aan de voorschriften 126, 274, 299, 327 en 350 van bijlage 1C.

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

1e generatie:

Waardetoekenning — **Octet-uitgericht**: 'cvpdxxxx'B (8-bits)

'c'B	kaartdownload:
	'0'B: kaart niet gedownload tijdens deze controleactiviteit,
	'1'B: kaart gedownload tijdens deze controleactiviteit
'v'B	VU-download:
	'0'B: VU niet gedownload tijdens deze controleactiviteit,
	'1'B: voertuig gedownload tijdens deze controleactiviteit
'p'B	afdrukken:
	'0'B: geen afdrukken gemaakt tijdens deze controleactiviteit,
	'1'B: afdrukken gemaakt tijdens deze controleactiviteit
'd'B	display:
	'0'B: geen display gebruikt tijdens deze controleactiviteit,
	'1'B: display gebruikt tijdens deze controleactiviteit
'xxxx'B	Niet gebruikt.

2e generatie:

Waardetoekenning — **Octet-uitgericht**: 'cvpdexxx'B (8-bits)

'c'B	kaartdownload:
	'0'B: kaart niet gedownload tijdens deze controleactiviteit,
	'1'B: kaart gedownload tijdens deze controleactiviteit
'v'B	VU-download:
	'0'B: VU niet gedownload tijdens deze controleactiviteit,
	'1'B: VU gedownload tijdens deze controleactiviteit
'p'B	afdrukken:
	'0'B: geen afdrukken gemaakt tijdens deze controleactiviteit,
	'1'B: afdrukken gemaakt tijdens deze controleactiviteit
'd'B	display:
	'0'B: geen display gebruikt tijdens deze controleactiviteit,
	'1'B: display gebruikt tijdens deze controleactiviteit

'e'B	kalibratiecontrole langs de weg:
	'0'B: kalibratieparameters niet gecontroleerd tijdens deze controleactiviteit,
	'1'B: kalibratieparameters gecontroleerd tijdens deze controleactiviteit,
'xxx'B	RFU.

2.54. **CurrentDateTime**

De huidige datum en het tijd van het controleapparaat.

```
CurrentDateTime ::= TimeReal
```

Waardetoekenning: niet nader gespecificeerd.

2.55. **CurrentDateTimeRecordArray**

2e generatie:

De huidige datum en tijd plus metagegevens zoals gebruikt in het downloadprotocol.

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

recordType geeft de soort record aan (CurrentDateTime). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van CurrentDateTime in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks records van de huidige datum en tijd.

2.56. **DailyPresenceCounter**

Op een bestuurders- of werkplaatskaart opgeslagen teller die met één wordt verhoogd voor elke kalenderdag waarop de kaart in een VU is ingebracht. Deze gegevenssoort is gerelateerd aan de voorschriften 266, 299, 320 en 343 van bijlage 1C.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Waardetoekenning: opeenvolgend getal met een maximale waarde = 9 999, waarna het opnieuw met 0 begint. Bij de eerste afgifte van de kaart wordt het getal op 0 gezet.

2.57. **Datef**

Datum weergegeven in een gemakkelijk af te drukken numerieke vorm.

```
Datef ::= SEQUENCE {
   year        BCDString(SIZE(2)),
   month       BCDString(SIZE(1)),
   day         BCDString(SIZE(1))
}
```

Waardetoekenning:

yyyy	jaar
mm	maand
dd	dag
'00000000'H	geeft expliciet geen datum aan.

2.58. **DateOfDayDownloaded**

2e generatie:

De datum en het tijdstip van de download.

```
DateOfDayDownloaded ::= TimeReal
```

Waardetoekenning: niet nader gespecificeerd.

2.59. **DateOfDayDownloadedRecordArray**

2e generatie:

De datum en tijd van de download plus metagegevens zoals gebruikt in het downloadprotocol.

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

recordType geeft de soort record aan (DateOfDayDownloaded). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van CurrentDateTime in bytes.

noOfRecords is het aantal records in de reeks records.

records is de verzameling van datums en tijden van de downloadrecords.

2.60. **Distance**

Een afgelegde afstand (resultaat van de berekening van het verschil tussen twee kilometerstanden van het voertuig in kilometers).

```
Distance ::= INTEGER(0..2^16-1)
```

Waardetoekenning: niet-getekend binair getal. Waarde in km in het operationele bereik van 0 tot 9 999 km.

2.61. **DriverCardApplicationIdentification**

Op een bestuurderskaart opgeslagen informatie met betrekking tot de toepassingsidentificatie van de kaart (voorschriften 253 en 278 van bijlage 1C).

1e generatie:

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

typeOfTachographCardId specificeert de geïmplementeerde kaartsoort.

cardStructureVersion specificeert de versie van de op de kaart geïmplementeerde structuur.

noOfEventsPerType is het aantal voorvallen per soort voorval dat de kaart kan registreren.

noOfFaultsPerType is het aantal fouten per soort fout dat de kaart kan registreren.

activityStructureLength geeft het aantal beschikbare bytes aan voor het opslaan van records van activiteiten.

noOfCardVehicleRecords is het aantal voertuigrecords dat de kaart kan bevatten.

noOfCardPlaceRecords is het aantal plaatsen dat de kaart kan registreren.

2e generatie:

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

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

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

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

2.62. DriverCardHolderIdentification

Op een bestuurderskaart opgeslagen informatie met betrekking tot de identificatie van de kaarthouder (voorschriften 256 en 281 van bijlage 1C).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                      HolderName,
   cardHolderBirthDate                 Datef,
   cardHolderPreferredLanguage         Language
}
```

cardHolderName is de naam en voorna(a)m(en) van de houder van de bestuurderskaart.

cardHolderBirthDate is de geboortedatum van de houder van de bestuurderskaart.

cardHolderPreferredLanguage is de voorkeurtaal van de kaarthouder.

2.63. **DSRCSecurityData**

2e generatie:

De informatie in normale tekst en de MAC die via DSRC van de tachograaf naar het systeem voor ondervraging op afstand (remote interrogator, RI) moeten worden verzonden; zie voor meer informatie aanhangsel 11, deel B, hoofdstuk 13.

```
DSRCSecurityData ::= SEQUENCE {
   tagLenthPlainText                    OCTET STRING(SIZE(2)),
   currentDateTime                      CurrentDateTime,
   counter                              INTEGER(0..2^24-1),
   vuSerialNumber                       VuSerialNumber,
   dSRCMKVersionNumber                  INTEGER(SIZE(1)),
   tagLengthMac                         OCTET STRING(SIZE(2)),
   mac                                  MAC
}
```

tagLength is onderdeel van de DER-TLV-codering en wordt op '81 10' gezet (zie aanhangsel 11, deel B, hoofdstuk 13).

currentDateTime is de huidige datum en tijd van de VU.

counter somt de RTM-berichten op.

vuSerialNumber is het serienummer van de VU.

dSRCMKVersionNumber is het versienummer van de DSRC-hoofdsleutel waarvan de VU-specifieke DSRC-sleutels zijn afgeleid.

tagLengthMac is het label en de lengte van het MAC-gegevensobject als onderdeel van de DER-TLV-codering. Het label wordt op '8E' gezet; de lengte codeert de lengte van de MAC in bytes (zie aanhangsel 11, deel B, hoofdstuk 13).

mac is de MAC die is berekend voor het RTM-bericht (zie aanhangsel 11, deel B, hoofstuk 13).

2.64. **EGFCertificate**

2e generatie:

Certificaat van de openbare sleutel van de externe GNSS-module voor wederzijdse authenticatie met een VU. De structuur van dat certificaat is gespecificeerd in aanhangsel 11.

```
EGFCertificate ::= Certificate
```

2.65. **EmbedderIcAssemblerId**

Geeft informatie over de IC-embedder.

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

countryCode is de tweeletterige landcode van de embedder van de module, overeenkomstig ISO 3166.

moduleEmbedder identificeert de embedder van de module.

manufacturerInformation voor intern gebruik door de fabrikant.

2.66. EntryTypeDailyWorkPeriod

Code die een onderscheid maakt tussen begin en einde van invoer van een plaats van de dagelijkse werkperiode en voorwaarde van de invoer.

1e generatie

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5)
}
```

Waardetoekenning: overeenkomstig ISO/IEC8824-1.

2e generatie

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5),
   Begin,  related time based on GNSS data                             (6),
   End     related time based on GNSS data                             (7)
}
```

Waardetoekenning: overeenkomstig ISO/IEC8824-1.

2.67. EquipmentType

Code die de verschillende soorten apparatuur voor de tachograaftoepassing onderscheidt.

```
EquipmentType ::= INTEGER(0..255)
```

1e generatie:

```
--Reserved                          (0),
--Driver Card                       (1),
--Workshop Card                     (2),
--Control Card                      (3),
--Company Card                      (4),
--Manufacturing Card                (5),
--Vehicle Unit                      (6),
--Motion Sensor                     (7),
--RFU                               (8..255)
```

Waardetoekenning: overeenkomstig ISO/IEC8824-1.

Waarde 0 is gereserveerd voor vermelding van een lidstaat of Europa in het CHA-veld van certifikaten.

2e generatie:

Er worden dezelfde waarden gebruikt 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
--RFU                                    (17..255)
```

Opmerking: 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.

2.68. **EuropeanPublicKey**

1e generatie:

De Europese openbare sleutel.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

Code die aangeeft waarom een voorval of een fout geregistreerd werd.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Waardetoekenning:

'00'H	een van de 10 meest recente (of laatste) voorvallen of fouten
'01'H	het langste voorval gedurende een van de laatste 10 dagen waarin het is opgetreden
'02'H	een van de 5 langste voorvallen gedurende de afgelopen 365 dagen
'03'H	het laatste voorval gedurende een van de laatste 10 dagen waarin het is opgetreden
'04'H	het ernstigste voorval gedurende een van de laatste 10 dagen waarin het is opgetreden
'05'H	een van de 5 ernstigste voorvallen gedurende de afgelopen 365 dagen
'06'H	eerste na de laatste kalibrering opgetreden voorval of fout
'07'H	een actief(actieve)/aan de gang zijnd(e) voorval of fout
'08'H to '7F'H	RFU
'80'H to 'FF'H	specifiek voor de fabrikant

2.70. **EventFaultType**

Code die een voorval of een fout aanduidt.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Waardetoekenning:

1e 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	Snelheidsoverschrijding,
'08'H	Onderbreking in de stroomvoorziening,
'09'H	Fout in de bewegingsgegevens,
'0A'H	Tegenstrijdige bewegingsgegevens,
'0B' to '0F'H	RFU,

	Poging tot inbreuk op de beveiliging van de voertuigunit,
‘1x’H	Geen verdere details,
‘10’H	Authenticatiefout van de bewegingssensor,
‘11’H	Authenticatiefout van de tachograafkaart,
‘12’H	Niet-geautoriseerde wijziging van de bewegingssensor,
‘13’H	Integriteitsfout in de gegevensinvoer op de kaart,
‘14’H	Integriteitsfout in de opgeslagen gebruikersgegevens,
‘15’H	Overdrachtsfout in de interne gegevens,
‘16’H	Niet-geautoriseerde opening van de unit,
‘17’H	Hardwaresabotage,
‘18’H	RFU,
‘19’H to ‘1F’H	
‘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 to ‘2F’H	RFU,
‘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 to ‘3F’H	RFU,
‘4x’H	Kaartfouten,
‘40’H	Geen verdere details,
‘41’H to ‘4F’H	RFU,
‘50’H to ‘7F’H	RFU,
‘80’H to ‘FF’H	Specifiek voor de fabrikant.

2e generatie:

Er worden dezelfde waarden gebruikt als in de 1e generatie, met de volgende aanvullingen:

‘0B’H	Tijdsconflict (tussen GNSS en de interne klok van de VU)
‘0C’ to ‘0F’H	RFU,
‘5x’H	GNSS-gerelateerde fouten,
‘50’H	Geen verdere details,
‘51’H	Fout in de interne GNSS-ontvanger,
‘52’H	Fout in de externe GNSS-ontvanger,
‘53’H	Externe GNSS-communicatiefout,
‘54’H	Geen GNSS-positiegegevens,
‘55’H	GNSS is gemanipuleerd,
‘56’H	Certificaat van de externe GNSS-module is vervallen,
‘57’H to ‘5F’H	RFU,
‘6x’H	Fouten die verband houden met de module voor communicatie op afstand,
‘60’H	Geen verdere details,
‘61’H	Fout in de module voor communicatie op afstand,
‘62’H	Communicatiefout in de module voor communicatie op afstand,
‘63’H to ‘6F’H	RFU,
‘7x’H	ITS-interfacefout,
‘70’H	Geen verdere details,
‘71’H to ‘7F’H	RFU.

2.71. **ExtendedSealIdentifier**

2e generatie:

De verlengde zegelidentificatiecode identificeert een zegel op unieke wijze (voorschrift 401 van bijlage 1C).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode is een code van de zegelfabrikant.

sealIdentifier is een zegelidentificatienummer dat uniek is voor de fabrikant.

2.72. **ExtendedSerialNumber**

Unieke identificatie van een apparaat. Dit kan ook als een identificatiesymbool van de openbare sleutel van het apparaat worden gebruikt.

1e generatie:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

serialNumber is een serienummer voor het apparaat, uniek voor de fabrikant, het soort apparaat en onderstaande maand en jaar.

monthYear is de identificatie van de maand en het jaar van fabricage (of van toekenning van het serienummer).

Waardetoekenning: BCD-codering van maand (twee cijfers) en jaar (twee laatste cijfers).

type is een identificatiesymbool voor het soort apparaat.

Waardetoekenning: specifiek voor de fabrikant, met gereserveerde waarde 'FFh'.

manufacturerCode: de numerieke code aan de hand waarvan een fabrikant van een apparaat met typegoedkeuring wordt geïdentificeerd.

2e generatie:

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

serialNumber zie 1e generatie

monthYear zie 1e generatie

type geeft het soort apparaat aan

manufacturerCode: zie 1e generatie.

2.73. **FullCardNumber**

Code die een tachograafkaart volledig identificeert.

```
FullCardNumber ::= SEQUENCE {
   cardType                              EquipmentType,
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber
}
```

cardType is de soort tachograafkaart.

cardIssuingMemberState is de code van de lidstaat die de kaart heeft afgegeven.

cardNumber is het kaartnummer.

2.74. **FullCardNumberAndGeneration**

2e generatie:

Code die een tachograafkaart en haar generatie volledig identificeert.

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

fullcardNumber identificeert de tachograafkaart.

generation geeft de generatie van de gebruikte tachograafkaart aan.

2.75. **Generation**

2e generatie:

Geeft de generatie van de gebruikte tachograafkaart aan.

```
Generation ::= INTEGER(0..255)
```

Waardetoekenning:

'00'H	RFU
'01'H	1e generatie
'02'H	2e generatie
'03'H .. 'FF'H	RFU

2.76. **GeoCoordinates**

2e generatie:

De geografische coördinaten zijn gecodeerd als gehele getallen. Die gehele getallen zijn veelvouden van de ± DDMM.M-codering voor de breedte en ± DDDMM.M-codering voor de lengte. In dit geval worden met ± DD en ± DDD de graden en met MM.M de minuten aangeduid.

```
GeoCoordinates ::= SEQUENCE {
   latitude                              INTEGER(-90000..90001),
   longitude                             INTEGER(-180000..180001)
}
```

latitude is gecodeerd als een veelvoud (factor 10) van de ± DDMM.M-weergave.

longitude is gecodeerd als een veelvoud (factor 10) van de ± DDDMM.M-weergave.

2.77. **GNSSAccuracy**

2e generatie:

De nauwkeurigheid van de GNSS-positiegegevens (definitie eee). De nauwkeurigheid is gecodeerd als een geheel getal en is een veelvoud (factor 10) van de X.Y-waarde in de GSA NMEA-zin.

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

2e generatie:

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de GNSS-positie van het voertuig als de rijtijdperiode van de bestuurder een veelvoud van drie uur bereikt (voorschriften 306 en 354 van bijlage 1C).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord            INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords         SET SIZE(NoOfGNSSCDRecords) OF
                                        GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord is de index van de laatst gewijzigde GNSS-record van ononderbroken rijtijd.

Waardetoekenning: cijfer dat correspondeert met de teller van de GNSS-record van ononderbroken rijtijd, beginnend met '0' voor de eerste GNSS-record van ononderbroken rijtijd in de structuur.

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

2.79. **GNSSContinuousDrivingRecord**

2e generatie:

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de GNSS-positie van het voertuig als de rijtijdperiode van de bestuurder een veelvoud van drie uur bereikt (voorschriften 305 en 353 van bijlage 1C).

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

timeStamp is de datum en tijd waarop de ononderbroken rijtijd van de kaarthouder een veelvoud van drie uur bereikt.

gnssPlaceRecord bevat informatie over de positie van het voertuig.

2.80. **GNSSPlaceRecord**

2e generatie:

Informatie met betrekking tot de GNSS-positie van het voertuig (voorschriften 108, 109, 110, 296, 305, 347 en 353 van bijlage 1C).

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

timeStamp is de datum en tijd waarop de GNSS-positie van het voertuig werd bepaald.

gnssAccuracy is de nauwkeurigheid van de GNSS-positiegegevens.

geoCoordinates is de met gebruik van GNSS geregistreerde plaats.

2.81. **HighResOdometer**

Kilometerstand van het voertuig: totale door het voertuig afgelegde afstand tijdens de gebruiksperiode.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

Waardetoekenning: niet-getekend binair getal. Waarde in 1/200 km in het operationele bereik van 0 tot 21 055 406 km.

2.82. **HighResTripDistance**

Een afgelegde afstand tijdens de gehele reis of een gedeelte daarvan.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Waardetoekenning: niet-getekend binair getal. Waarde in 1/200 km in het operationele bereik van 0 tot 21 055 406 km.

2.83. **HolderName**

Naam en voorna(a)men van een kaarthouder.

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

holderSurname is de achternaam (familienaam) van de houder. Deze achternaam bevat geen titels.

Waardetoekenning: Wanneer een kaart niet persoonlijk is, bevat de holderSurname dezelfde informatie als companyName of workshopName of controlBodyName.

holderFirstNames omvat de voornaam (voornamen) en initialen van de houder.

2.84. **InternalGNSSReceiver**

2e generatie:

Geeft aan of de voertuigunit over een interne of externe GNSS-ontvanger beschikt. "True" betekent dat de VU een interne GNSS-ontvanger heeft. "False" betekent dat het om een externe GNSS-ontvanger gaat.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Constante van het controleapparaat (definitie m).

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Waardetoekenning: pulsen per kilometer in het operationele bereik van 0 tot 64 255 pulsen/km.

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 of tachograafkaart.

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.

2.87. **KMWCKey**

2e generatie:

AES-sleutel en de geassocieerde sleutelversie die wordt gebruikt om de VU te verbinden met de bewegingssensor. Zie voor details aanhangsel 11.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                             AESKey,
   keyVersion                          INTEGER (SIZE(1))
}
```

kMWCKey is de lengte van de AES-sleutel aaneengeschakeld met de sleutel die wordt gebruikt om de VU te verbinden met de bewegingssensor.

keyVersion duidt de sleutelversie van de AES-sleutel aan.

2.88. **Language**

Code die een taal identificeert.

```
Language ::= IA5String(SIZE(2))
```

Waardetoekenning: een code van twee onderkastletters overeenkomstig ISO 639.

2.89. **LastCardDownload**

Op een bestuurderskaart opgeslagen datum en tijd van het downloaden van de laatste kaart (voor andere doeleinden dan controle) (voorschriften 257 en 282 van bijlage 1C). Deze datum kan worden aangepast door een VU of een kaartlezer.

```
LastCardDownload ::= TimeReal
```

Waardetoekenning: niet nader gespecificeerd.

2.90. **LinkCertificate**

2e generatie:

Het verbindingscertificaat tussen European Root CA-sleutelparen.

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

Effectieve omtrek van de wielbanden (definitie u).

```
L-TyreCircumference ::= INTEGER(0.. 2^16-1)
```

Waardetoekenning: niet-getekend binair getal, waarde in 1/8 mm in het operationele bereik van 0 tot 8 031 mm.

2.92. **MAC**

2e generatie:

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

```
MAC ::= CHOICE {
   mac8                                 OCTET STRING (SIZE(8)),
   mac12                                OCTET STRING (SIZE(12)),
   mac16                                OCTET STRING (SIZE(12))
}
```

2.93. **ManualInputFlag**

Code die aangeeft of een kaarthouder manueel activiteiten van de bestuurder bij kaartinbrenging heeft ingevoerd of niet (voorschrift 081 van bijlage 1B en voorschrift 102 van bijlage 1C).

```
ManualInputFlag ::= INTEGER {
   noEntry                              (0)
   manualEntries                        (1)
}
```

Waardetoekenning: niet nader gespecificeerd.

2.94. **ManufacturerCode**

Code die een fabrikant van apparatuur met typegoedkeuring identificeert.

```
ManufacturerCode ::= INTEGER(0..255)
```

Het voor interoperabiliteitstests bevoegde laboratorium onderhoudt de lijst met fabrikantcodes en publiceert die lijst op zijn website (voorschrift 454 van bijlage 1C).

ManufacturerCodes worden tijdelijk toegewezen aan ontwikkelaars van apparatuur voor tachografen, op aanvraag bij het laboratorium dat bevoegd is voor interoperabiliteitstests.

2.95. **ManufacturerSpecificEventFaultData**

2e generatie:

Foutcodes die specifiek voor een fabrikant zijn, vereenvoudigen de foutenanalyse en het onderhoud van voertuigunits.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                     ManufacturerCode,
   manufacturerSpecificErrorCode        OCTET STRING(SIZE(3))
}
```

manufacturerCode identificeert de fabrikant van de VU.

manufacturerSpecificErrorCode is een foutcode specifiek voor de fabrikant.

2.96. **MemberStateCertificate**

Het door de Europese certificeringsautoriteit afgegeven certificaat van de openbare sleutel van een lidstaat.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

2e generatie:

Het lidstaatcertificaat plus metagegevens zoals gebruikt in het downloadprotocol.

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

recordType geeft de soort record aan (MemberStateCertificate). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van MemberStateCertificate in bytes.

noOfRecords is het aantal records in de reeks records. De waarde wordt op 1 gezet, omdat certificaten een verschillende lengte kunnen hebben.

records is de reeks lidstaatcertificaten.

2.98. **MemberStatePublicKey**

1e generatie:

De openbare sleutel van een lidstaat.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Name**

Een naam.

```
Name ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   name                                OCTET STRING (SIZE(35))
}
```

codePage specificeert een tekenset zoals gedefinieerd in hoofdstuk 4,

name is een naam die is gecodeerd met de gespecificeerde tekenset.

2.100. **NationAlpha**

Alfabetische verwijzing naar een land in overeenstemming met de kentekens op voertuigen in internationaal verkeer (Verdrag van Wenen inzake wegverkeer, 1968, van de Verenigde Naties).

```
NationAlpha ::= IA5String(SIZE(3))
```

De codes NationAlpha en NationNumeric worden bijgehouden op een lijst die wordt onderhouden op de website van het laboratorium dat belast is met het uitvoeren van de interoperabiliteitstests, zoals vastgesteld in voorschrift 440 van bijlage 1C.

2.101. **NationNumeric**

Numerieke referentie naar een land.

```
NationNumeric ::= INTEGER(0 .. 255)
```

Waardetoekenning: zie gegevenssoort 2.100 (NationAlpha)

De hierboven beschreven specificatie van NationAlpha of NationNumeric wordt pas gewijzigd of bijgewerkt nadat het aangewezen laboratorium de fabrikanten van typegoedgekeurde voertuigunits van digitale en slimme tachografen heeft geraadpleegd.

2.102. **NoOfCalibrationRecords**

Aantal kalibreringsrecords dat op een werkplaatskaart kan worden opgeslagen.

1e generatie:

```
NoOfCalibrationRecords ::= INTEGER(0..255)
```

Waardetoekenning: zie aanhangsel 2.

2e generatie:

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

Waardetoekenning: zie aanhangsel 2.

2.103. **NoOfCalibrationsSinceDownload**

Teller die het aantal met een werkplaatskaart uitgevoerde kalibreringen sinds de laatste download aangeeft (voorschriften 317 en 340 van bijlage 1C).

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

Waardetoekenning: niet nader gespecificeerd.

2.104. **NoOfCardPlaceRecords**

Aantal plaatsrecords dat op een bestuurders- of werkplaatskaart kan worden opgeslagen.

1e generatie:

```
NoOfCardPlaceRecords ::= INTEGER(0..255)
```

Waardetoekenning: zie aanhangsel 2.

2e generatie:

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

Waardetoekenning: zie aanhangsel 2.

2.105. **NoOfCardVehicleRecords**

Aantal records van gebruikte voertuigen dat op een bestuurders- of werkplaatskaart kan worden opgeslagen.

```
NoOfCardVehicleRecords ::= INTEGER(0.. 2^16-1)
```

Waardetoekenning: zie aanhangsel 2.

2.106. **NoOfCardVehicleUnitRecords**

2e generatie:

Aantal records van gebruikte voertuigunits dat op een bestuurders- of werkplaatskaart kan worden opgeslagen.

```
NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2^16-1)
```

Waardetoekenning: zie aanhangsel 2.

2.107. **NoOfCompanyActivityRecords**

Aantal records van bedrijfsactiviteiten dat op een bedrijfskaart kan worden opgeslagen.

```
NoOfCompanyActivityRecords ::= INTEGER(0.. 2^16-1)
```

Waardetoekenning: zie aanhangsel 2.

2.108. **NoOfControlActivityRecords**

Aantal records van controleactiviteiten dat op een controlekaart kan worden opgeslagen.

```
NoOfControlActivityRecords ::= INTEGER(0.. 2^16-1)
```

Waardetoekenning: zie aanhangsel 2.

2.109. **NoOfEventsPerType**

Aantal voorvallen per soort voorval dat op een kaart kan worden opgeslagen.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Waardetoekenning: zie aanhangsel 2.

2.110. **NoOfFaultsPerType**

Aantal fouten per soort fout dat opeen kaart kan worden opgeslagen.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Waardetoekenning: see Appendix 2.

2.111. **NoOfGNSSCDRecords**

2e generatie:

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

```
NoOfGNSSCDRecords ::= INTEGER(0..2^16-1)
```

Waardetoekenning: zie aanhangsel 2.

2.112. **NoOfSpecificConditionRecords**

2e generatie:

Aantal records van specifieke omstandigheden dat op een kaart kan worden opgeslagen.

```
NoOfSpecificConditionRecords ::= INTEGER(0..2^16-1)
```

Waardetoekenning: zie aanhangsel 2.

2.113. **OdometerShort**

Kilometerstand van het voertuig in een verkorte vorm.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Waardetoekenning: niet-getekend binair getal. Waarde in km in het operationele bereik van 0 tot 9 999 999 km.

2.114. **OdometerValueMidnight**

De kilometerstand van het voertuig om 0.00 uur op een bepaalde dag (voorschrift 090 van bijlage 1B en voorschrift 113 van bijlage 1C).

```
OdometerValueMidnight ::= OdometerShort
```

Waardetoekenning: niet nader gespecificeerd.

2.115. **OdometerValueMidnightRecordArray**

2e generatie:

De OdometerValueMidnight plus metagegevens zoals gebruikt in het downloadprotocol.

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

recordType geeft de soort record aan (OdometerValueMidnight). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van OdometerValueMidnight in bytes.

noOfRecords is het aantal records in de reeks records.

records is de reeks OdometerValueMidnight-records.

2.116. **OverspeedNumber**

Aantal snelheidsoverschrijdingen sinds de laatste controle van snelheidsoverschrijdingen.

```
OverspeedNumber ::= INTEGER(0..255)
```

Waardetoekenning: 0 betekent dat er sinds de laatste controle van snelheidsoverschrijdingen geen snelheidsoverschrijding heeft plaatsgevonden; 1 betekent dat er sinds de laatste controle van snelheidsoverschrijdingen een snelheidsoverschrijding heeft plaatsgevonden; … 255 betekent 255 of meer snelheidsoverschrijdingen sinds de laatste controle van snelheidsoverschrijdingen.

2.117. **PlaceRecord**

Informatie met betrekking tot een plaats waar een dagelijkse werkperiode begint of eindigt (voorschriften 108, 271, 296, 324 en 347 van bijlage 1C).

1e generatie:

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort
}
```

entryTime is een datum en tijdstip met betrekking tot de invoer.

entryTypeDailyWorkPeriod is de soort invoer.

dailyWorkPeriodCountry is het ingevoerde land.

dailyWorkPeriodRegion is de ingevoerde regio.

vehicleOdometerValue is de kilometerstand op het moment van invoer van de plaats.

2e generatie:

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort,
   entryGNSSPlaceRecord               GNSSPlaceRecord
}
```

Als aanvulling op de 1e generatie wordt de volgende component gebruikt:

entryGNSSPlaceRecord is de geregistreerde plaats en tijd.

2.118. **PreviousVehicleInfo**

Informatie met betrekking tot het vorige door een bestuurder gebruikte voertuig wanneer hij zijn kaart in een voertuigunit inbrengt (voorschrift 081 van bijlage 1B en voorschrift 102 van bijlage 1C).

1e generatie:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal
}
```

vehicleRegistrationIdentification is het kentekennummer en de registrerende lidstaat van het voertuig.

cardWithdrawalTime is de datum en het tijdstip van kaartuitneming.

2e generatie:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal,
   vuGeneration                           Generation
}
```

Als aanvulling op de 1e generatie wordt het volgende gegevenselement gebruikt:

vuGeneration identificeert de generatie van de VU.

2.119. **PublicKey**

1e generatie:

Een openbare RSA-sleutel.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                    RSAKeyModulus,
   rsaKeyPublicExponent             RSAKeyPublicExponent
}
```

rsaKeyModulus is de modulus van het sleutelpaar.

rsaKeyPublicExponent is de openbare exponent van het sleutelpaar.

2.120. **RecordType**

2e generatie:

Verwijzing naar een soort record. Deze gegevenssoort wordt gebruikt in RecordArrays.

```
RecordType ::= OCTET STRING(SIZE(1))
```

Waardetoekenning:

'01'H	ActivityChangeInfo,
'02'H	CardSlotsStatus,
'03'H	CurrentDateTime,
'04'H	MemberStateCertificate,
'05'H	OdometerValueMidnight,
'06'H	DateOfDayDownloaded,
'07'H	SensorPaired,
'08'H	Signature,
'09'H	SpecificConditionRecord,
'0A'H	VehicleIdentificationNumber,
'0B'H	VehicleRegistrationNumber,
'0C'H	VuCalibrationRecord,
'0D'H	VuCardIWRecord,
'0E'H	VuCardRecord,
'0F'H	VuCertificate,
'10'H	VuCompanyLocksRecord,
'11'H	VuControlActivityRecord,
'12'H	VuDetailedSpeedBlock,
'13'H	VuDownloadablePeriod,
'14'H	VuDownloadActivityData,
'15'H	VuEventRecord,
'16'H	VuGNSSCDRecord,
'17'H	VuITSConsentRecord,
'18'H	VuFaultRecord,
'19'H	VuIdentification,
'1A'H	VuOverSpeedingControlData,
'1B'H	VuOverSpeedingEventRecord,
'1C'H	VuPlaceDailyWorkPeriodRecord,
'1D'H	VuTimeAdjustmentGNSSRecord,
'1E'H	VuTimeAdjustmentRecord,
'1F'H	VuPowerSupplyInterruptionRecord,
'20'H	SensorPairedRecord,
'21'H	SensorExternalGNSSCoupledRecord,
'22'H to '7F'H	RFU,
'80'H to 'FF'H	Specifiek voor de fabrikant.

2.121. **RegionAlpha**

Alfabetische verwijzing naar een regio in een gespecificeerd land.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

1e generatie:

Waardetoekenning:

```
‘   ’         No information available,
Spain:
‘AN ’         Andalucía,
‘AR ’         Aragón,
‘AST’         Asturias,
‘C  ’         Cantabria,
‘CAT’         Cataluña,
‘CL ’         Castilla-León,
‘CM ’         Castilla-La-Mancha,
‘CV’          Valencia,
‘EXT’         Extremadura,
‘G  ’         Galicia,
‘IB ’         Baleares,
‘IC ’         Canarias,
‘LR ’         La Rioja,
‘M  ’         Madrid,
‘MU ’         Murcia,
‘NA ’         Navarra,
‘PV ’         País Vasco
```

2e generatie:

De RegionAlpha-codes worden bijgehouden op een lijst die wordt onderhouden op de website van het laboratorium dat belast is met het uitvoeren van de interoperabiliteitstests.

2.122. **RegionNumeric**

Numerieke verwijzing naar een regio in een gespecificeerd land.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

1e generatie:

Waardetoekenning:

```
‘00’H         No information available,
Spain:
‘01’H         Andalucía,
‘02’H         Aragón,
‘03’H         Asturias,
‘04’H         Cantabria,
‘05’H         Cataluña,
‘06’H         Castilla-León,
‘07’H         Castilla-La-Mancha,
‘08’H         Valencia,
‘09’H         Extremadura,
‘0A’H         Galicia,
‘0B’H         Baleares,
‘0C’H         Canarias,
‘0D’H         La Rioja,
‘0E’H         Madrid,
‘0F’H         Murcia,
‘10’H         Navarra,
‘11’H         País Vasco
```

2e generatie:

De RegionNumeric-codes worden bijgehouden op een lijst die wordt onderhouden op de website van het laboratorium dat belast is met het uitvoeren van de interoperabiliteitstests.

2.123. **RemoteCommunicationModuleSerialNumber**

2e generatie:

Serienummer van de module voor communicatie op afstand.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

1e generatie:

De modulus van een RSA-sleutelpaar.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Waardetoekenning: niet gespecificeerd.

2.125. **RSAKeyPrivateExponent**

1e generatie:

De particuliere exponent van een RSA-sleutelpaar.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Waardetoekenning: niet gespecificeerd.

2.126. **RSAKeyPublicExponent**

1e generatie:

De openbare exponent van een RSA-sleutelpaar.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Waardetoekenning: niet gespecificeerd.

2.127. **RtmData**

2e generatie:

Zie aanhangsel 14 voor de definitie van deze gegevenssoort.

2.128. **SealDataCard**

2e generatie:

Deze gegevenssoort slaat informatie op over de zegels die aan de verschillende onderdelen van een voertuig zijn gehecht en dient te worden opgeslagen op een kaart. Deze gegevenssoort is gerelateerd aan voorschrift 337 van bijlage 1C.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                        INTEGER(1..5),
   sealRecords                            SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords is het aantal records in sealRecords.

sealRecords is een reeks zegelrecords.

2.129. **SealDataVu**

2e generatie:

Deze gegevenssoort slaat informatie op over de zegels die aan de verschillende onderdelen van een voertuig zijn gehecht en dient te worden opgeslagen in een voertuigunit.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                            SealRecord
}
```

sealRecords is een reeks zegelrecords. Als er minder dan vijf zegels zijn, wordt de waarde van EquipmentType in alle ongebruikte sealRecords op 16 gezet, d.w.z. ongebruikt.

2.130. **SealRecord**

2e generatie:

Deze gegevenssoort slaat informatie op over een zegel dat aan een onderdeel is gehecht. Deze gegevenssoort is gerelateerd aan voorschrift 337 van bijlage 1C.

```
SealRecord ::= SEQUENCE {
   equipmentType                          EquipmentType,
   extendedSealIdentifier                 ExtendedSealIdentifier
}
```

equipmentType identificeert het soort apparaat waaraan het zegel is gehecht.

extendedSealIdentifier is het identificatiesymbool van het zegel dat aan het apparaat is gehecht.

2.131. **SensorApprovalNumber**

Typegoedkeuringsnummer van de sensor.

1e generatie:

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

Waardetoekenning: niet gespecificeerd.

2e generatie:

```
SensorApprovalNumber ::= IA5String(SIZE(16))
```

Waardetoekenning:

Het goedkeuringsnummer wordt verstrekt zoals het is bekendgemaakt op de overeenkomstige website van de Europese Commissie, bijv. met eventuele koppeltekens. Het goedkeuringsnummer wordt links uitgelijnd.

2.132. **SensorExternalGNSSApprovalNumber**

2e generatie:

Typegoedkeuringsnummer van de externe GNSS-module.

```
SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))
```

Waardetoekenning:

Het goedkeuringsnummer wordt verstrekt zoals het is bekendgemaakt op de overeenkomstige website van de Europese Commissie, bijv. met eventuele koppeltekens. Het goedkeuringsnummer wordt links uitgelijnd.

2.133. **SensorExternalGNSSCoupledRecord**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot de identificatie van de met de voertuigunit verbonden externe GNSS-module (voorschrift 100 van bijlage 1C).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber is het serienummer van de met de voertuigunit verbonden externe GNSS-module.

sensorApprovalNumber is het goedkeuringsnummer van deze externe GNSS-module.

sensorCouplingDate is de datum waarop deze externe GNSS-module met de voertuigunit is verbonden.

2.134. **SensorExternalGNSSIdentification**

2e generatie:

Informatie met betrekking tot de identificatie van de externe GNSS-module (voorschrift 98 van bijlage 1C).

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                  SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                  SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber is het verlengde serienummer van de externe GNSS-module.

sensorApprovalNumber is het goedkeuringsnummer van de externe GNSS-module.

sensorSCIdentifier is het identificatiesymbool van de beveiligingscomponent van de externe GNSS-module.

sensorOSIdentifier is het identificatiesymbool van het besturingssysteem van de externe GNSS-module.

2.135. **SensorExternalGNSSInstallation**

2e generatie:

In de externe GNSS-module opgeslagen informatie met betrekking tot de installatie van de externe GNSS-sensor (voorschrift 123 van bijlage 1C).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst              SensorGNSSCouplingDate,
   firstVuApprovalNumber                VuApprovalNumber,
   firstVuSerialNumber                  VuSerialNumber,
   sensorCouplingDateCurrent            SensorGNSSCouplingDate,
   currentVuApprovalNumber              VuApprovalNumber,
   currentVUSerialNumber                VuSerialNumber
}
```

sensorCouplingDateFirst is de datum van de eerste verbinding van de externe GNSS-module met een voertuigunit.

firstVuApprovalNumber is het goedkeuringsnummer van de eerste voertuigunit die met de externe GNSS-module verbonden wordt.

firstVuSerialNumber is het serienummer van de eerste voertuigunit die met de externe GNSS-module verbonden wordt.

sensorCouplingDateCurrent is de datum van de huidige verbinding van de externe GNSS-module met een voertuigunit.

currentVuApprovalNumber is het goedkeuringsnummer van de voertuigunit die op dat moment met de externe GNSS-module verbonden is.

currentVuSerialNumber is het serienummer van de voertuigunit die op dat moment met de externe GNSS-module verbonden is.

2.136. **SensorExternalGNSSOSIdentifier**

2e generatie:

Identificatiesymbool van het besturingssysteem van de externe GNSS-module.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Waardetoekenning: specifiek voor de fabrikant.

2.137. **SensorExternalGNSSSCIdentifier**

2e generatie:

Deze soort wordt gebruikt om bijv. de cryptografische module van de externe GNSS-module te identificeren.

Identificatiesymbool van de beveiligingscomponent van de externe GNSS-module.

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

Waardetoekenning: specifiek voor de fabrikant van het onderdeel.

2.138. **SensorGNSSCouplingDate**

2e generatie:

Datum van een verbinding van de externe GNSS-module met een voertuigunit.

```
SensorGNSSCouplingDate ::= TimeReal
```

Waardetoekenning: niet gespecificeerd.

2.139. **SensorGNSSSerialNumber**

2e generatie:

Deze soort wordt gebruikt om het serienummer van de GNSS-ontvanger op te slaan, zowel binnen als buiten de VU.

Serienummer van de GNSS-ontvanger.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

In een bewegingssensor opgeslagen informatie met betrekking tot de identificatie van de bewegingssensor (voorschrift 077 van bijlage 1B en voorschrift 95 van bijlage 1C).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorSCIdentifier                  SensorSCIdentifier,
   sensorOSIdentifier                  SensorOSIdentifier
}
```

sensorSerialNumber is het verlengde serienummer van de bewegingssensor (inclusief onderdeelnummer en code van de fabrikant).

sensorApprovalNumber is het goedkeuringsnummer van de bewegingssensor.

sensorSCIdentifier is het identificatiesymbool van de beveiligingscomponent van de bewegingssensor.

sensorOSIdentifier is het identificatiesymbool van het besturingssysteem van de bewegingssensor.

2.141. **SensorInstallation**

In een bewegingssensor opgeslagen informatie met betrekking tot de installatie van de bewegingssensor (voorschrift 099 van bijlage 1B en voorschrift 122 van bijlage 1C).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst              SensorPairingDate,
   firstVuApprovalNumber               VuApprovalNumber,
   firstVuSerialNumber                 VuSerialNumber,
   sensorPairingDateCurrent            SensorPairingDate,
   currentVuApprovalNumber             VuApprovalNumber,
   currentVUSerialNumber               VuSerialNumber
}
```

sensorPairingDateFirst is de datum van de eerste verbinding van de bewegingssensor met een voertuigunit.

firstVuApprovalNumber is het goedkeuringsnummer van de eerste voertuigunit die met de bewegingssensor verbonden wordt.

firstVuSerialNumber is het serienummer van de eerste met de bewegingssensor verbonden voertuigunit.

sensorPairingDateCurrent is de datum van de huidige verbinding van de bewegingssensor met de voertuigunit.

currentVuApprovalNumber is het goedkeuringsnummer van de op dat moment met de bewegingssensor verbonden voertuigunit.

currentVUSerialNumber is het serienummer van de op dat moment met de bewegingssensor verbonden voertuigunit.

2.142. **SensorInstallationSecData**

Op een werkplaatskaart opgeslagen informatie met betrekking tot de benodigde beveiligingsgegevens bij verbinding van een bewegingssensor met een voertuigunit (voorschriften 308 en 331 van bijlage 1C).

1e generatie:

```
SensorInstallationSecData ::= TdesSessionKey
```

Waardetoekenning: overeenkomstig ISO 16844-3.

2e generatie:

Zoals beschreven in aanhangsel 11 worden op een werkplaatskaart maximaal drie sleutels voor de verbinding van de VU met de bewegingssensor opgeslagen. Die sleutels hebben verschillende sleutelversies.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                              KMWCKey,
   kMWCKey2                              KMWCKey OPTIONAL,
   kMWCKey3                              KMWCKey OPTIONAL
}
```

2.143. **SensorOSIdentifier**

Identificatiesymbool van het besturingssysteem van de bewegingssensor.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Waardetoekenning: specifiek voor de fabrikant.

2.144. **SensorPaired**

1e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot de identificatie van de met de voertuigunit verbonden bewegingssensor (voorschrift 079 van bijlage 1B).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorPairingDateFirst                SensorPairingDate
}
```

sensorSerialNumber is het serienummer van de op dat moment met de voertuigunit verbonden bewegingssensor.

sensorApprovalNumber is het goedkeuringsnummer van de op dat moment met de voertuigunit verbonden bewegingssensor.

sensorPairingDateFirst is de datum van de eerste verbinding met een voertuigunit van de op dat moment met de voertuigunit verbonden bewegingssensor.

2.145. **SensorPairedRecord**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot de identificatie van de met de voertuigunit verbonden bewegingssensor (voorschrift 97 van bijlage 1C).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorPairingDate                   SensorPairingDate
}
```

sensorSerialNumber is het serienummer van een met de voertuigunit verbonden bewegingssensor.

sensorApprovalNumber is het goedkeuringsnummer van die bewegingssensor.

sensorPairingDate is een datum waarop die externe bewegingssensor met de voertuigunit is verbonden.

2.146. **SensorPairingDate**

Datum van een verbinding van de bewegingssensor met een voertuigunit.

```
SensorPairingDate ::= TimeReal
```

Waardetoekenning: niet gespecificeerd.

2.147. **SensorSCIdentifier**

Identificatiesymbool van de beveiligingscomponent van de bewegingssensor.

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

Waardetoekenning: specifiek voor de fabrikant van de component.

2.148. **SensorSerialNumber**

Serienummer van de bewegingssensor.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Handtekening**

Een digitale handtekening.

1e generatie:

```
Signature ::= OCTET STRING (SIZE(128))
```

Waardetoekenning: overeenkomstig de algemene beveiligingsmechanismen in aanhangsel 11.

2e generatie:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Waardetoekenning: overeenkomstig de algemene beveiligingsmechanismen in aanhangsel 11.

2.150. **SignatureRecordArray**

2e generatie:

Een reeks handtekeningen plus metagegevens zoals gebruikt in het downloadprotocol.

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

recordType geeft de soort record aan (Signature). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van Signature in bytes.

noOfRecords is het aantal records in de reeks records. De waarde wordt op 1 gezet, omdat de handtekeningen een verschillende lengte kunnen hebben.

records is de reeks handtekeningen.

2.151. **SimilarEventsNumber**

Het aantal soortgelijke voorvallen op een bepaalde dag (voorschrift 094 van bijlage 1B en voorschrift 117 van bijlage 1C).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Waardetoekenning: 0 is niet-gebruikt; 1 betekent dat er op die dag maar een voorval van die soort heeft plaatsgevonden en opgeslagen is; 2 betekent dat 2 voorvallen van die soort op die dag hebben plaatsgevonden (een ervan is opgeslagen), … 255 betekent dat 255 of meer voorvallen van die soort hebben plaatsgevonden op die dag.

2.152. **SpecificConditionRecord**

Op een bestuurderskaart, een werkplaatskaart of in een voertuigunit opgeslagen informatie met betrekking tot een specifieke omstandigheid (voorschriften 130, 276, 301, 328 en 355 van bijlage 1C).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                           TimeReal,
   specificConditionType               SpecificConditionType
}
```

entryTime is de datum en het tijdstip van de invoer.

specificConditionType is de code die de specifieke omstandigheid identificeert.

2.153. **SpecificConditions**

Op een bestuurderskaart, een werkplaatskaart of in een voertuigunit opgeslagen informatie met betrekking tot een specifieke omstandigheid (voorschriften 131, 277, 302, 329 en 356 van bijlage 1C).

2e generatie:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord        INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords            SET SIZE(NoOfSpecificConditionRecords) OF
                                       SpecificConditionRecord
}
```

contditionPointerNewestRecord is de index van de laatst gewijzigde record van een specifieke omstandigheid.

Waardetoekenning: cijfer dat correspondeert met de teller van de record van specifieke omstandigheden, beginnend met '0' voor de eerste record van specifieke omstandigheden in de structuur.

specificConditionRecords is de reeks records die informatie over de geregistreerde specifieke omstandigheden bevat.

2.154. **SpecificConditionType**

Code die een specifieke omstandigheid identificeert (voorschriften 050b, 105a, 212a en 230a van bijlage 1B en voorschrift 62 van bijlage 1C).

```
SpecificConditionType ::= INTEGER(0..255)
```

1e generatie:

Waardetoekenning:

'00'H	RFU
'01'H	niet verplicht — Begin
'02'H	niet verplicht — Einde
'03'H	Vervoer per veerboot/trein
'04'H .. 'FF'H	RFU

2e generatie:

Waardetoekenning:

'00'H	RFU
'01'H	niet verplich — Begin
'02'H	niet verplicht — Einde
'03'H	Vervoer per veerboot/trein — Begin
'04'H	Vervoer per veerboot/trein — Einde
'05'H .. 'FF'H	RFU

2.155. **Speed**

Snelheid van het voertuig (km/u).

```
Speed ::= INTEGER(0..255)
```

Waardetoekenning: kilometer per uur in het operationele bereik van 0 tot 220 km/u.

2.156. **SpeedAuthorised**

Toegestane maximumsnelheid van het voertuig (definitie hh).

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

Gemiddelde snelheid tijdens een vooraf gedefinieerde periode (km/u).

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Maximumsnelheid gemeten tijdens een vooraf gedefinieerde periode.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

2e generatie:

Zie aanhangsel 14 voor de definitie van deze datasoort.

2.160. **TachographPayloadEncrypted**

2e generatie:

De DER-TLV-gecodeerde payloadgegevens van de tachograaf, d.w.z. de in het RTM-bericht gecodeerd verzonden gegevens. Zie aanhangsel 11, deel B, hoofdstuk 13, voor de codering.

```
TachographPayloadEncrypted ::= SEQUENCE {
   tag                                  OCTET STRING(SIZE(1)),
   length                               OCTET STRING(SIZE(1..2)),
   paddingContentIndicatorByte          OCTET STRING(SIZE(1)),
   encryptedData                        OCTET STRING(SIZE(16..192))
}
```

tag is onderdeel van de DER-TLV-codering en wordt op '87' gezet (zie aanhangsel 11, deel B, hoofdstuk 13).

length is onderdeel van de DER-TLV-codering en codeert de lengte van de volgende paddingContentIndicatorByte en de encryptedData.

paddingContentIndicatorByte wordt op '00' gezet.

encryptedData is gecodeerde tachographPayload zoals gespecificeerd in aanhangsel 11, deel B, hoofdstuk 13. De lengte in bytes van deze gegevens is altijd een veelvoud van 16.

2.161. **TDesSessionKey**

1e generatie:

Een triple DES-sessiesleutel.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                             OCTET STRING (SIZE(8)),
   tDesKeyB                             OCTET STRING (SIZE(8))
}
```

Waardetoekenning: niet nader gespecificeerd.

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 GMT.

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

Waardetoekenning — Octet-uitgericht: aantal seconden sinds middernacht 1 januari 1970 GMT.

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

2.163. **TyreSize**

Aanduiding van de afmetingen van de banden.

```
TyreSize ::= IA5String(SIZE(15))
```

Waardetoekenning: overeenkomstig Richtlijn 92/23/EEG van 31 maart 1992 (PB L 129 van 14.5.1992, blz. 95).

2.164. **VehicleIdentificationNumber**

Identificatienummer van het voertuig (VIN) dat verwijst naar het voertuig als geheel, in de regel het chassisnummer.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Waardetoekenning: zoals gedefinieerd in ISO 3779.

2.165. **VehicleIdentificationNumberRecordArray**

2e generatie:

Het identificatienummer van het voertuig plus metagegevens zoals gebruikt in het downloadprotocol.

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

recordType geeft de soort record aan (VehicleIdentificationNumber). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VehicleIdentificationNumber in bytes.

noOfRecords is het aantal records in de reeks records.

records is de reeks identificatienummers van voertuigen.

2.166. **VehicleRegistrationIdentification**

Identificatie van een voertuig, uniek voor Europa (kentekennummer en lidstaat).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation           NationNumeric,
   vehicleRegistrationNumber           VehicleRegistrationNumber
}
```

vehicleRegistrationNation is het land waar het voertuig geregistreerd is.

vehicleRegistrationNumber is het kentekennummer van het voertuig (VRN).

2.167. **VehicleRegistrationNumber**

Kentekennummer van het voertuig (VRN). Het kentekennummer wordt toegewezen door de vergunningverlenende autoriteit.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   vehicleRegNumber                    OCTET STRING (SIZE(13))
}
```

codePage specificeert een tekenset zoals gedefinieerd in hoofdstuk 4,

vehicleRegNumber is een VRN die is gecodeerd met de gespecificeerde tekenset.

Waardetoekenning: specifiek voor een land.

2.168. **VehicleRegistrationNumberRecordArray**

2e generatie:

Het kentekennummer van het voertuig plus metagegevens zoals gebruikt in het downloadprotocol.

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

recordType geeft de soort record aan (VehicleRegistrationNumber). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VehicleregistrationNumber in bytes.

noOfRecords is het aantal records in de reeks records.

records is de reeks kentekennummers van voertuigen.

2.169. **VuAbility**

2e generatie:

In een voertuigunit opgeslagen informatie over de mogelijkheid om in de VU al dan niet tachograafkaarten van de eerste generatie te gebruiken (voorschrift 121 van bijlage 1C).

```
VuAbility ::= OCTET STRING (SIZE(1))
```

Waardetoekenning — Octet-uitgericht: 'xxxxxxxa'B (8-bits)

Mogelijkheid om 1e generatie te ondersteunen:

'a'B	Mogelijkheid om tachograafkaarten van de 1e generatie te ondersteunen:
	'0'B 1e generatie ondersteund
	'1'B 1e generatie niet ondersteund
'xxxxxxx'B	RFU

2.170. **VuActivityDailyData**

1e generatie:

In een VU opgeslagen informatie met betrekking tot wijzigingen in de activiteiten en/of wijzigingen in de rijstatus en/of wijzigingen in de kaartstatus voor een bepaalde kalenderdag (voorschrift 084 van bijlage 1B en voorschriften 105, 106 en 107 van bijlage 1C) en in de status van lezers op 00:00 die dag.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                INTEGER SIZE(0..1440),
   activityChangeInfos                SET SIZE(noOfActivityChanges) OF
                                      ActivityChangeInfo
}
```

noOfActivityChanges is het aantal ActivityChangeInfo-woorden in de reeks activityChangeInfos.

activityChangeInfos is de reeks ActivityChangeInfo-woorden die in de VU is opgeslagen die dag. Het bevat altijd twee ActivityChangeInfo-woorden waarin de status van de twee lezers wordt gegeven op 00:00 die dag.

2.171. **VuActivityDailyRecordArray**

2e generatie:

In een VU opgeslagen informatie met betrekking tot wijzigingen in de activiteiten en/of wijzigingen in de rijstatus en/of wijzigingen in de kaartstatus voor een bepaalde kalenderdag (voorschriften 105, 106 en 107 van bijlage 1C) en in de status van lezers op 00:00 die dag.

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

recordType geeft de soort record aan (ActivityChangeInfo). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van ActivityChangeInfo in bytes.

noOfRecords is het aantal records in de reeks records.

records is de reeks ActivityChangeInfo-woorden die in de VU is opgeslagen die dag. Het bevat altijd twee ActivityChangeInfo-woorden waarin de status van de twee lezers wordt gegeven op 00:00 die dag.

2.172. **VuApprovalNumber**

Typegoedkeuringsnummer van de voertuigunit.

1e generatie:

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

Waardetoekenning: niet gespecificeerd.

2e generatie:

```
VuApprovalNumber ::= IA5String(SIZE(16))
```

Waardetoekenning:

Het goedkeuringsnummer wordt verstrekt zoals het is bekendgemaakt op de overeenkomstige website van de Europese Commissie, bijv. met eventuele koppeltekens. Het goedkeuringsnummer wordt links uitgelijnd.

2.173. **VuCalibrationData**

1e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot de kalibreringen van het controleapparaat (voorschrift 098 van bijlage 1B).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords             INTEGER(0..255),
   vuCalibrationRecords                 SET SIZE(noOfVuCalibrationRecords) OF
                                        VuCalibrationRecord
}
```

noOfVuCalibrationRecords is het aantal records in de vuCalibrationRecords-reeks.

vuCalibrationRecords is de reeks kalibreringsrecords.

2.174. **VuCalibrationRecord**

In een voertuigunit opgeslagen informatie met betrekking tot de kalibrering van het controleapparaat (voorschrift 098 van bijlage 1B en voorschriften 119 en 120 van bijlage 1C).

1e generatie:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                   CalibrationPurpose,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber,
   workshopCardExpiryDate               TimeReal,
   vehicleIdentificationNumber          VehicleIdentificationNumber,
   vehicleRegistrationIdentification    VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant       W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment        K-ConstantOfRecordingEquipment,
   lTyreCircumference                   L-TyreCircumference,
   tyreSize                             TyreSize,
   authorisedSpeed                      SpeedAuthorised,
   oldOdometerValue                     OdometerShort,
   newOdometerValue                     OdometerShort,
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   nextCalibrationDate                  TimeReal
}
```

calibrationPurpose is het doel van de kalibrering.

workshopName, workshopAddress zijn de naam en het adres van de werkplaats.

workshopCardNumber identificeert de werkplaatskaart die tijdens de kalibrering wordt gebruikt.

workshopCardExpiryDate is de vervaldatum van de kaart.

vehicleIdentificationNumber is het VIN.

vehicleRegistrationIdentification bevat het kentekennummer en de registerende lidstaat.

wVehicleCharacteristicConstant is de kenmerkende coëfficiënt van het voertuig.

kConstantOfRecordingEquipment is de constante van het controleapparaat.

lTyreCircumference is de effectieve omtrek van de wielbanden.

tyreSize is de aanduiding van de afmeting van de banden waarmee het voertuig uitgerust is.

authorisedSpeed is de toegestane snelheid van het voertuig.

oldOdometerValue, **newOdometerValue** zijn de oude en nieuwe kilometerstanden.

oldTimeValue, newTimeValue zijn de oude en nieuwe waarden van datum en tijd.

nextCalibrationDate is de datum van de volgende in CalibrationPurpose gespecificeerde soort kalibrering die door de bevoegde controleautoriteit moet worden uitgevoerd.

2e generatie:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal,
   sealDataVu                            SealDataVu
}
```

Als aanvulling op de 1e generatie wordt het volgende gegevenselement gebruikt:

sealDataVu geeft informatie over de zegels die aan de verschillende onderdelen van het voertuig zijn gehecht.

2.175. **VuCalibrationRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot de kalibreringen van het controleapparaat (voorschrift 119 en 120 van bijlage 1C).

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

recordType geeft de soort record aan (VuCalibrationRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuCalibrationRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is de reeks kalibreringsrecords.

2.176. **VuCardIWData**

1e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot cycli van inbrengen in en uitnemen uit een voertuigunit van bestuurders- of werkplaatskaarten (voorschrift 081 van bijlage 1B en voorschrift 103 van bijlage 1C).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                       INTEGER(0..2^16-1),
   vuCardIWRecords                     SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords is het aantal records in de reeks vuCardIWRecords.

vuCardIWRecords is een reeks records met betrekking tot cycli van inbrengen en uitnemen van een kaart.

2.177. **VuCardIWRecord**

In een voertuigunit opgeslagen informatie met betrekking tot cycli van inbrengen in en uitnemen uit een voertuigunit van bestuurders- of werkplaatskaarten (voorschrift 081 van bijlage 1B en voorschrift 102 van bijlage 1C).

1e generatie:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                      HolderName,
   fullCardNumber                      FullCardNumber,
   cardExpiryDate                      TimeReal,
   cardInsertionTime                   TimeReal,
   vehicleOdometerValueAtInsertion     OdometerShort,
   cardSlotNumber                      CardSlotNumber,
   cardWithdrawalTime                  TimeReal,
   vehicleOdometerValueAtWithdrawal    OdometerShort,
   previousVehicleInfo                 PreviousVehicleInfo,
   manualInputFlag                     ManualInputFlag
}
```

cardHolderName is de op de kaart opgeslagen naam en voornaam (voornamen) van de houder van de bestuurders- of werkplaatskaart.

fullCardNumber is de op de kaart opgeslagen soort kaart, de lidstaat van afgifte en het kaartnummer.

cardExpiryDate is de op de kaart opgeslagen vervaldatum van de kaart.

cardInsertionTime is de datum en het tijdstip van inbrenging.

vehicleOdometerValueAtInsertion is de kilometerstand van het voertuig bij kaartinbrenging.

cardSlotNumber is de lezer waarin de kaart is ingebracht.

cardWithdrawalTime is de datum en het tijdstip van uitneming.

vehicleOdometerValueAtWithdrawal is de kilometerstand van het voertuig bij kaartuitneming.

previousVehicleInfo bevat de op de kaart opgeslagen informatie over het vorige door de bestuurder gebruikte voertuig.

manualInputFlag is een teken dat identificeert of de kaarthouder bij de kaartinbrenging manueel activiteiten van de bestuurder heeft ingevoerd.

2e generatie:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                       HolderName,
   fullCardNumberAndGeneration          FullCardNumberAndGeneration,
   cardExpiryDate                       TimeReal,
   cardInsertionTime                    TimeReal,
   vehicleOdometerValueAtInsertion      OdometerShort,
   cardSlotNumber                       CardSlotNumber,
   cardWithdrawalTime                   TimeReal,
   vehicleOdometerValueAtWithdrawal     OdometerShort,
   previousVehicleInfo                  PreviousVehicleInfo,
   manualInputFlag                      ManualInputFlag
}
```

In de gegevensstructuur van de 2e generatie is fullCardNumber vervangen door het volgende gegevenselement:

fullCardNumberAndGeneration is de op de kaart opgeslagen soort kaart, de lidstaat van afgifte, het kaartnummer en de generatie.

2.178. **VuCardIWRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot cycli van inbrengen in en uitnemen uit een voertuigunit van bestuurders- of werkplaatskaarten (voorschrift 103 van bijage 1C).

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

recordType geeft de soort record aan (VuCardIWRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuCardIWRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks records met betrekking tot cycli van inbrengen en uitnemen van een kaart.

2.179. **VuCardRecord**

2e generatie:

In een voertuigunit opgeslagen informatie over een gebruikte tachograafkaart (voorschrift 132 van bijlage 1C).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

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

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

typeOfTachographCardId zoals afgelezen uit het bestand EF_Application_Identification onder DF Tachograaf_G2.

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.

2.180. **VuCardRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie over de in die VU gebruikte tachograafkaarten. Deze informatie is bedoeld voor de analyse van VU- of kaartproblemen (voorschrift 132 van bijlage 1C).

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

recordType geeft de soort record aan (VuCardRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuCardRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks records met betrekking tot de in de VU gebruikte tachograafkaarten.

2.181. **VuCertificate**

Certificaat van de openbare sleutel van een voertuigunit.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

2e generatie:

Het VU-certificaat plus metagegevens zoals gebruikt in het downloadprotocol.

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

recordType geeft de soort record aan (VuCertificate). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuCertificate in bytes.

noOfRecords is het aantal records in de reeks records. De waarde wordt op 1 gezet, omdat certificaten een verschillende lengte kunnen hebben.

records is een reeks VU-certificaten.

2.183. **VuCompanyLocksData**

1e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot bedrijfsvergrendelingen (voorschrift 104 van bijlage 1B).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                          INTEGER(0..255),
   vuCompanyLocksRecords              SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks is het aantal in vuCompanyLocksRecords opgenomen vergrendelingen.

vuCompanyLocksRecords is de reeks records van bedrijfsvergrendelingen.

2.184. **VuCompanyLocksRecord**

In een voertuigunit opgeslagen informatie met betrekking tot een bedrijfsvergrendeling (voorschrift 104 van bijlage 1B en voorschrift 128 van bijlage 1C).

1e generatie:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumber                  FullCardNumber
}
```

lockInTime, lockOutTime zijn de datum en het tijdstip van vergrendeling en ontgrendeling.

companyName, companyAddress zijn de naam en het adres van het vergrendelende bedrijf.

companyCardNumber identificeert de kaart die bij de vergrendeling wordt gebruikt.

2e generatie:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                         TimeReal,
   lockOutTime                        TimeReal,
   companyName                        Name,
   companyAddress                     Address,
   companyCardNumberAndGeneration     FullCardNumberAndGeneration
}
```

In de gegevensstructuur van de 2e generatie is companyCardNumber vervangen door het volgende gegevenselement:

companyCardNumberAndGeneration identificeert de kaart, inclusief de generatie, die bij de vergrendeling wordt gebruikt.

2.185. **VuCompanyLocksRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot bedrijfsvergrendelingen (voorschrift 128 van bijlage 1C.

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

recordType geeft de soort record aan (VuCompanyLocksRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuCompanyLocksRecord in bytes.

noOfRecords is het aantal records in de reeks registraties. Waarde 0..255.

records is de reeks records van bedrijfsvergrendelingen.

2.186. **VuControlActivityData**

1e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot controles die met deze VU worden uitgevoerd (voorschrift 102 van bijlage 1B).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

noOfControls is het aantal in vuControlActivityRecords opgenomen controles.

vuControlActivityRecords is de reeks records van controleactiviteiten.

2.187. **VuControlActivityRecord**

In een voertuigunit opgeslagen informatie met betrekking tot een controle die met deze VU wordt uitgevoerd (voorschrift 102 van bijlage 1B en voorschrift 126 van bijlage 1C).

1e generatie:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                         ControlType,
   controlTime                         TimeReal,
   controlCardNumber                   FullCardNumber,
   downloadPeriodBeginTime             TimeReal,
   downloadPeriodEndTime               TimeReal
}
```

controlType is de soort controle.

controlTime is de datum en het tijdstip van de controle.

ControlCardNumber identificeert de bij de controle gebruikte controlekaart.

downloadPeriodBeginTime is de begintijd van de gedownloade periode, in geval van download.

downloadPeriodEndTime is de eindtijd van de gedownloade periode, in geval van download.

2e generatie:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

In de gegevensstructuur van de 2e generatie is controlCardNumber vervangen door het volgende gegevenselement:

ControlCardNumberAndGeneration identificeert de bij de controle gebruikte controlekaart, inclusief de generatie.

2.188. **VuControlActivityRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot controles die met deze VU worden uitgevoerd (voorschrift 126 van bijlage 1C).

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

recordType geeft de soort record aan (VuControlActivityRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuControlActivityRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is de reeks records van VU-controleactiviteiten.

2.189. **VuDataBlockCounter**

Op een kaart opgeslagen teller die de cycli van kaartinbrenging in en kaartuitneming uit voertuigunits opeenvolgend identificeert.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Waardetoekenning: opeenvolgend cijfer met een maximale waarde van 9 999, waarna het opnieuw met 0 begint.

2.190. **VuDetailedSpeedBlock**

In een voertuigunit opgeslagen informatie met betrekking tot de gedetailleerde snelheid van het voertuig gedurende een minuut waarin het voertuig rijdt (voorschrift 093 van bijlage 1B en voorschrift 116 van bijlage 1C).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate    TimeReal,
   speedsPerSecond        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate is de datum en het tijdstip van de eerste snelheidswaarde in het blok.

speedsPerSecond is de chronologische sequentie van gemeten snelheden gedurende elke seconde van de minuut die begint met speedBlockBeginDate (inclusief).

2.191. **VuDetailedSpeedBlockRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot de gedetailleerde snelheid van het voertuig.

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

recordType geeft de soort record aan (VuDetailedSpeedBlock). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuDetailedSpeedBlock in bytes.

noOfRecords is het aantal records in de reeks records.

records is de reeks gedetailleerde snelheidsblokken.

2.192. **VuDetailedSpeedData**

1e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot de gedetailleerde snelheid van het voertuig.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                     INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks               SET SIZE(noOfSpeedBlocks) OF
                                       VuDetailedSpeedBlock
}
```

noOfSpeedBlocks is het aantal snelheidsblokken in de vuDetailedSpeedBlocks-reeks.

vuDetailedSpeedBlocks is de reeks gedetailleerde snelheidsblokken.

2.193. **VuDownloadablePeriod**

De eerste en laatste datum waarvan een voertuigunit gegevens met betrekking tot activiteiten van de bestuurder bewaart (voorschriften 081, 084 of 087 van bijlage 1B en voorschriften 102, 105 en 108 van bijlage 1C).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                 TimeReal
   maxDownloadableTime                 TimeReal
}
```

minDownloadableTime is de datum en het tijdstip van de eerste in de VU opgeslagen kaartinbrenging, van de wijziging van activiteiten of van de invoer van de plaats.

maxDownloadableTime is de datum en het tijdstip van de laatste in de VU opgeslagen kaartuitneming, van de wijziging van activiteiten of van invoer van de plaats.

2.194. **VuDownloadablePeriodRecordArray**

2e generatie:

De VUDownloadablePeriod plus metagegevens zoals gebruikt in het downloadprotocol.

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

recordType geeft de soort record aan (VuDownloadablePeriod). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuDownloadablePeriod in bytes.

noOfRecords is het aantal records in de reeks records.

records is de reeks VuDownloadablePeriod-records.

2.195. **VuDownloadActivityData**

In een voertuigunit opgeslagen informatie met betrekking tot de laatste download (voorschrift 105 van bijlage 1B en voorschrift 129 van bijlage 1C).

1e generatie:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumber                      FullCardNumber,
   companyOrWorkshopName               Name
}
```

downloadingTime is de datum en het tijdstip van downloaden.

fullCardNumber identificeert de kaart die wordt gebruikt om de download te autoriseren.

companyOrWorkshopName is de naam van het bedrijf of de werkplaats.

2e generatie:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                     TimeReal,
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   companyOrWorkshopName               Name
}
```

In de gegevensstructuur van de 2e generatie is fullCardNumber vervangen door het volgende gegevenselement:

fullCardNumberAndGeneration identificeert de kaart die wordt gebruikt om de download te autoriseren.

2.196. **VuDownloadActivityDataRecordArray**

2e generatie:

Informatie met betrekking tot de laatste VU-download (voorschrift 129 van bijlage 1C).

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

recordType geeft de soort record aan (VuDownloadActivityData). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuDownloadActivityData in bytes.

noOfRecords is het aantal records in de reeks records.

records is de reeks records van downloadactiviteitgegevens.

2.197. **VuEventData**

1e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot voorvallen (voorschrift 094 van bijlage 1B, met uitzondering van snelheidsoverschrijding).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                          INTEGER(0..255),
   vuEventRecords                        SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents is het aantal in de vuEventRecords-reeks opgenomen voorvallen.

vuEventRecords is een reeks voorvallenrecords.

2.198. **VuEventRecord**

In een voertuigunit opgeslagen informatie met betrekking tot een voorval (voorschrift 094 van bijlage 1B en voorschrift 117 van bijlage 1C, met uitzondering van snelheidsoverschrijding).

1e generatie:

```
VuEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType is het soort voorval.

eventRecordPurpose is het doel waarvoor dit voorval geregistreerd werd.

eventBeginTime is de datum en het tijdstip van het begin van het voorval.

eventEndTime is de datum en het tijdstip van het einde van het voorval.

cardNumberDriverSlotBegin identificeert de aan het begin van het voorval in de lezer van de bestuurder ingebrachte kaart.

cardNumberCodriverSlotBegin identificeert de aan het begin van het voorval in de lezer van de bijrijder ingebrachte kaart.

cardNumberDriverSlotEnd identificeert de aan het einde van het voorval in de lezer van de bestuurder ingebrachte kaart.

cardNumberCodriverSlotEnd identificeert de aan het einde van het voorval in de lezer van de bijrijder ingebrachte kaart.

similarEventsNumber is het aantal vergelijkbare voorvallen op die dag.

Deze sequentie kan worden gebruikt voor alle voorvallen met uitzondering van snelheidsoverschrijdingen.

2e generatie:

```
VuEventRecord ::= SEQUENCE {
   eventType                           EventFaultType,
   eventRecordPurpose                  EventFaultRecordPurpose,
   eventBeginTime                      TimeReal,
   eventEndTime                        TimeReal,
   cardNumberAndGenDriverSlotBegin     FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin   FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd       FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd     FullCardNumberAndGeneration,
   similarEventsNumber                 SimilarEventsNumber,
   manufacturerSpecificEventFaultData  ManufacturerSpecificEventFaultData
}
```

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

manufacturerSpecificEventFaultData bevat aanvullende informatie over het voorval, specifiek voor de fabrikant.

In de gegevensstructuur van de 2e generatie zijn cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd en cardNumberCodriverSlotEnd vervangen door de volgende gegevenselementen:

cardNumberAndGenDriverSlotBegin identificeert de aan het begin van het voorval in de lezer van de bestuurder ingebrachte kaart, inclusief de generatie.

cardNumberAndGenCodriverSlotBegin identificeert de aan het begin van het voorval in de lezer van de bijrijder ingebrachte kaart, inclusief de generatie.

cardNumberAndGenDriverSlotEnd identificeert de aan het einde van het voorval in de lezer van de bestuurder ingebrachte kaart, inclusief de generatie.

cardNumberAndGenCodriverSlotEnd identificeert de aan het einde van het voorval in de lezer van de bijrijder ingebrachte kaart, inclusief de generatie.

Als het om een tijdsconflict gaat, moeten eventBeginTime en eventEndTime als volgt worden geïnterpreteerd:

eventBeginTime is de datum en het tijdstip van het controleapparaat.

eventEndTime is de datum en het tijdstip van het GNSS.

2.199. **VuEventRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot voorvallen (voorschrift 117 van bijlage 1C, met uitzondering van snelheidsoverschrijding).

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

recordType geeft de soort record aan (VuEventRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuEventRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks voorvallenrecords.

2.200. **VuFaultData**

1e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot fouten (voorschrift 096 van bijlage 1B).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                          INTEGER(0..255),
   vuFaultRecords                        SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults is het aantal in de vuFaultRecords-reeks opgenomen fouten.

vuFaultRecords is een reeks foutenrecords.

2.201. **VuFaultRecord**

In een voertuigunit opgeslagen informatie met betrekking tot een fout (voorschrift 096 van bijlage 1B en voorschrift 118 van bijlage 1C).

1e generatie:

```
VuFaultRecord ::= SEQUENCE {
   faultType                             EventFaultType,
   faultRecordPurpose                    EventFaultRecordPurpose,
   faultBeginTime                        TimeReal,
   faultEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber
}
```

faultType is de soort fout van het controleapparaat.

faultRecordPurpose is het doel waarvoor deze fout geregistreerd werd.

faultBeginTime is de datum en het tijdstip van het begin van de fout.

faultEndTime is de datum en het tijdstip van het einde van de fout.

cardNumberDriverSlotBegin identificeert de aan het begin van de fout in de lezer van de bestuurder ingebrachte kaart.

cardNumberCodriverSlotBegin identificeert de aan het begin van de fout in de lezer van de bijrijder ingebrachte kaart.

cardNumberDriverSlotEnd identificeert de aan het einde van de fout in de lezer van de bestuurder ingebrachte kaart.

cardNumberCodriverSlotEnd identificeert de aan het einde van de fout in de lezer van de bijrijder ingebrachte kaart.

2e generatie:

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Als aanvulling op de 1e generatie wordt het volgende gegevenselement gebruikt:

manufacturerSpecificEventFaultData bevat aanvullende informatie over de fout, specifiek voor de fabrikant.

In de gegevensstructuur van de 2e generatie zijn cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd en cardNumberCodriverSlotEnd vervangen door de volgende gegevenselementen:

cardNumberAndGenDriverSlotBegin identificeert de aan het begin van de fout in de lezer van de bestuurder ingebrachte kaart, inclusief de generatie.

cardNumberAndGenCodriverSlotBegin identificeert de aan het begin van de fout in de lezer van de bijrijder ingebrachte kaart, inclusief de generatie.

cardNumberAndGenDriverSlotEnd identificeert de aan het einde van de fout in de lezer van de bestuurder ingebrachte kaart, inclusief de generatie.

cardNumberAndGenCodriverSlotEnd identificeert de aan het einde van de fout in de lezer van de bijrijder ingebrachte kaart, inclusief de generatie.

2.202. **VuFaultRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot fouten (voorschrift 118 van bijlage 1C).

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

recordType geeft de soort record aan (VuFaultRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuFaultRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks foutrecords.

2.203. **VuGNSSCDRecord**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot de GNSS-positie van het voertuig als de lopende rijtijdperiode van de bestuurder een veelvoud van drie uur bereikt (voorschriften 108 en 110 van bijlage 1C).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   cardNumberAndGenDriverSlot             FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot           FullCardNumberAndGeneration,
   gnssPlaceRecord                        GNSSPlaceRecord
}
```

timeStamp is de datum en het tijdstip waarop de ononderbroken rijtijd van de kaarthouder 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 met betrekking tot de positie van het voertuig.

2.204. **VuGNSSCDRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot de GNSS-positie van het voertuig als de lopende rijtijdperiode van de bestuurder een veelvoud van drie uur bereikt (voorschriften 108 en 110 van bijlage 1C).

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

recordType geeft de soort record aan (VuGNSSCDRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuGNSSCDRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks GNSS-records van de ononderbroken rijtijd.

2.205. **VuIdentification**

In een voertuigunit opgeslagen informatie met betrekking tot de identificatie van het controleapparaat (voorschrift 075 van bijlage 1B en voorschriften 93 en 121 van bijlage 1C).

1e generatie:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                     VuManufacturerName,
   vuManufacturerAddress                  VuManufacturerAddress,
   vuPartNumber                           VuPartNumber,
   vuSerialNumber                         VuSerialNumber,
   vuSoftwareIdentification               VuSoftwareIdentification,
   vuManufacturingDate                    VuManufacturingDate,
   vuApprovalNumber                       VuApprovalNumber
}
```

vuManufacturerName is de naam van de fabrikant van de voertuigunit.

vuManufacturerAddress is het adres van de fabrikant van de voertuigunit.

vuPartNumber is het onderdeelnummer van de voertuigunit.

vuSerialNumber is het serienummer van de VU.

vuSoftwareIdentification identificeert de software die in de voertuigunit geïmplementeerd is.

vuManufacturingDate is het bouwjaar van de voertuigunit.

vuApprovalNumber is het typegoedkeuringsnummer van de voertuigunit.

2e generatie:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                  VuManufacturerName,
   vuManufacturerAddress               VuManufacturerAddress,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   vuSoftwareIdentification            VuSoftwareIdentification,
   vuManufacturingDate                 VuManufacturingDate,
   vuApprovalNumber                    VuApprovalNumber,
   vuGeneration                        Generation,
   vuAbility                           VuAbility
}
```

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

vuGeneration identificeert de generatie van de VU.

vuAbility geeft aan of de voertuigunit al dan niet tachograafkaarten van de 1e generatie ondersteunt

2.206. **VuIdentificationRecordArray**

2e generatie:

De VuIdentification plus metagegevens zoals gebruikt in het downloadprotocol.

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

recordType geeft de soort record aan (VuIdentification). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuIdentification in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks VuIdentification-records.

2.207. **VuITSConsentRecord**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot de toestemming van de bestuurder om intelligente vervoerssystemen te gebruiken.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAndGen identificeert de kaart, inclusief de generatie. Dit moet een bestuurders- of werkplaatskaart zijn.

consent is een teken dat aangeeft of de bestuurder toestemming heeft gegeven om in zijn voertuig/voertuigunit intelligente vervoerssystemen te gebruiken.

Waardetoekenning:

TRUE geeft dat de bestuurder heeft toegestemd om intelligente vervoerssystemen te gebruiken

FALSE geeft dat de bestuurder heeft geweigerd om intelligente vervoerssystemen te gebruiken

2.208. **VuITSConsentRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot de toestemming van de bestuurder om intelligente vervoerssystemen te gebruiken (voorschrift 200 van bijlage 1C).

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

recordType geeft de soort record aan (VuITSConsentRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuITSConsentRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is de reeks records van toestemmingen om ITS te gebruiken.

2.209. **VuManufacturerAddress**

Adres van de fabrikant van de voertuigunit.

```
VuManufacturerAddress ::= Address
```

Waardetoekenning: niet gespecificeerd.

2.210. **VuManufacturerName**

Naam van de fabrikant van de voertuigunit.

```
VuManufacturerName ::= Name
```

Waardetoekenning: niet gespecificeerd.

2.211. **VuManufacturingDate**

Bouwjaar van de voertuigunit.

```
VuManufacturingDate ::= TimeReal
```

Waardetoekenning: niet gespecificeerd.

2.212. **VuOverSpeedingControlData**

In een voertuigunit opgeslagen informatie met betrekking tot snelheidsoverschrijdingen sinds de laatste controle van de snelheidsoverschrijding (voorschrift 095 van bijlage 1B en voorschrift 117 van bijlage 1C).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime            TimeReal,
   firstOverspeedSince                 TimeReal,
   numberOfOverspeedSince              OverspeedNumber
}
```

lastOverspeedControlTime is de datum en het tijdstip van de laatste controle van de snelheidsoverschrijding.

firstOverspeedSince is de datum en het tijdstip van de eerste snelheidsoverschrijding na deze controle van de snelheidsoverschrijding.

numberOfOverspeedSince is het aantal snelheidsoverschrijdingen na de laatste controle van de snelheidsoverschrijding.

2.213. **VuOverSpeedingControlDataRecordArray**

2e generatie:

De VuOverSpeedingControlData plus metagegevens zoals gebruikt in het downloadprotocol.

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

recordType geeft de soort records aan (VuOverSpeedingControlData). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuOverSpeedingControlData in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks records van gegevens over snelheidsoverschrijdingscontroles.

2.214. **VuOverSpeedingEventData**

1e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot voorvallen van snelheidsoverschrijding (voorschrift 094 van bijlage 094).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents            INTEGER(0..255),
   vuOverSpeedingEventRecords          SET SIZE(noOfVuOverSpeedingEvents) OF
                                       VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents is het aantal in de vuOverSpeedingEventRecords-reeks opgenomen voorvallen.

vuOverSpeedingEventRecords is een reeks voorvallenrecords van snelheidsoverschrijding.

2.215. **VuOverSpeedingEventRecord**

1e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot voorvallen van snelheidsoverschrijding (voorschrift 094 van bijlage 1B en voorschrift 117 van bijlage 1C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberDriverSlotBegin          FullCardNumber,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType is het soort voorval.

eventRecordPurpose is het doel waarvoor dit voorval geregistreerd werd.

eventBeginTime is de datum en het tijdstip van het begin van het voorval.

eventEndTime is de datum en het tijdstip van het einde van het voorval.

maxSpeedValue is de tijdens het voorval gemeten maximumsnelheid.

averageSpeedValue is de tijdens het voorval gemeten rekenkundige gemiddelde snelheid.

cardNumberDriverSlotBegin identificeert de aan het begin van het voorval in de lezer van de bestuurder ingebrachte kaart.

similarEventsNumber is het aantal vergelijkbare voorvallen op die dag.

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot voorvallen van snelheidsoverschrijding (voorschrift 094 van bijlage 1B en voorschrift 117 van bijlage 1C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

In de gegevensstructuur van de 2e generatie is cardNumberDriverSlotBegin vervangen door het volgende gegevenselement:

cardNumberAndGenDriverSlotBegin identificeert de aan het begin van het voorval in de lezer van de bestuurder ingebrachte kaart, inclusief de generatie.

2.216. **VuOverSpeedingEventRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot voorvallen van snelheidsoverschrijding (voorschrift 117 van bijlage 1C).

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

recordType geeft de soort record aan (VuOverSpeedingEventRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuOverSpeedingEventRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks voorvallenrecords van snelheidsoverschrijding.

2.217. **VuPartNumber**

Onderdeelnummer van de voertuigunit.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Waardetoekenning: specifiek voor de fabrikant van de VU.

2.218. **VuPlaceDailyWorkPeriodData**

1e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot plaatsen waar bestuurders een dagelijkse werkperiode beginnen of eindigen (voorschrift 087 van bijlage 1B en voorschriften 108 en 110 van bijlage 1C).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                    INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords       SET SIZE(noOfPlaceRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords is het aantal in de vuPlaceDailyWorkPeriodRecords-reeks opgenomen records.

vuPlaceDailyWorkPeriodRecords is een reeks records met betrekking tot de plaats.

2.219. **VuPlaceDailyWorkPeriodRecord**

1e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot plaatsen waar een bestuurder een dagelijkse werkperiode begint of eindigt (voorschrift 087 van bijlage 1B en voorschriften 108 en 110 van bijlage 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                      FullCardNumber,
   placeRecord                         PlaceRecord
}
```

fullCardNumber is de soort bestuurderskaart, de lidstaat van afgifte en het kaartnummer.

placeRecord bevat de informatie met betrekking tot de ingevoerde plaats.

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot een plaats waar een bestuurder een dagelijkse werkperiode begint of eindigt (voorschrift 087 van bijlage 1B en voorschriften 108 en 110 van bijlage 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

In de gegevensstructuur van de 2e generatie is fullCardNumber vervangen door het volgende gegevenselement:

fullCardNumberAndGeneration is de op de kaart opgeslagen soort kaart, de lidstaat van afgifte, het kaartnummer en de generatie.

2.220. **VuPlaceDailyWorkPeriodRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot plaatsen waar bestuurders een dagelijkse werkperiode beginnen of eindigen (voorschrift 108 en 110 van bijlage 1C).

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

recordType geeft de soort record aan (VuPlaceDailyWorkPeriodRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuPlaceDailyWorkPeriodRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks records met betrekking tot de plaats.

2.221. **VuPrivateKey**

1e generatie:

De particuliere sleutel van een voertuigunit.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

1e generatie:

De openbare sleutel van een voertuigunit.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

Serienummer van de voertuigunit (voorschrift 075 van bijlage 1B en voorschrift 93 van bijlage 1C).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

Datum van installatie van de softwareversie in de voertuigunit.

```
VuSoftInstallationDate ::= TimeReal
```

Waardetoekenning: niet gespecificeerd.

2.225. **VuSoftwareIdentification**

In een voertuigunit opgeslagen informatie met betrekking tot de geïnstalleerde software.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                    VuSoftwareVersion,
   vuSoftInstallationDate               VuSoftInstallationDate
}
```

vuSoftwareVersion is het nummer van de softwareversie van de VU.

vuSoftInstallationDate is de datum van installatie van de softwareversie.

2.226. **VuSoftwareVersion**

Nummer van de softwareversie van de voertuigunit.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Waardetoekenning: niet gespecificeerd.

2.227. **VuSpecificConditionData**

1e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot specifieke omstandigheden.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords is het aantal in de specificConditionRecords-reeks opgenomen records.

specificConditionRecords is een reeks records met betrekking tot specifieke omstandigheden.

2.228. **VuSpecificConditionRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot specifieke omstandigheden (voorschrift 130 van bijlage 1C).

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

recordType geeft de soort record aan (SpecificConditionRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van SpecificConditionRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks records met betrekking tot specifieke omstandigheden.

2.229. **VuTimeAdjustmentData**

1e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot de buiten het kader van een geregelde kalibrering uitgevoerde tijdafstellingen (voorschrift 101 van bijlage 1B).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                INTEGER(0..6),
   vuTimeAdjustmentRecords             SET SIZE(noOfVuTimeAdjRecords) OF
                                       VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords is het aantal records in de vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords is een reeks tijdafstellingsrecords.

2.230. **VuTimeAdjustmentGNSSRecord**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot een tijdafstelling op basis van GNSS-tijdsgegevens (voorschriften 124 en 125 van bijlage 1C).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal
}
```

oldTimeValue, newTimeValue zijn de oude en nieuwe waarden van datum en tijd.

2.231. **VuTimeAdjustmentGNSSRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot een tijdafstelling mede op basis van GNSS-tijdsgegevens (voorschriften 124 en 125 van bijlage 1C).

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

recordType geeft de soort record aan (VuTimeAdjustmentGNSSRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuTimeAdjustmentGNSSRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks records van GNSS-tijdafstellingen.

2.232. **VuTimeAdjustmentRecord**

In een voertuigunit opgeslagen informatie met betrekking tot de buiten het kader van een geregelde kalibrering uitgevoerde tijdafstellingen (voorschrift 101 van bijlage 1B en voorschriften 124 en 125 van bijlage 1C).

1e generatie:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber
}
```

oldTimeValue, newTimeValue zijn de oude en nieuwe waarden van datum en tijd.

workshopName, workshopAddress zijn de naam en het adres van de werkplaats.

workshopCardNumber identificeert de voor de tijdafstelling gebruikte werkplaatskaart.

2e generatie:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

In de gegevensstructuur van de 2e generatie is workshopCardNumber vervangen door het volgende gegevenselement:

workshopCardNumberAndGeneration identificeert de voor de tijdafstelling gebruikte werkplaatskaart, inclusief de generatie.

2.233. **VuTimeAdjustmentRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot de buiten het kader van een geregelde kalibrering uitgevoerde tijdafstellingen (voorschriften 124 en 125 van bijlage 1C).

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

recordType geeft de soort record aan (VuTimeAdjustmentRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuTimeAdjustmentRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks records van tijdafstellingen.

2.234. **WorkshopCardApplicationIdentification**

Op een werkplaatskaart opgeslagen informatie met betrekking tot de toepassingsidentificatie van de kaart (voorschriften 307 en 330 van bijlage 1C).

1e generatie:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords
}
```

typeOfTachographCardId specificeert de geïmplementeerde kaartsoort.

cardStructureVersion specificeert de versie van de op de kaart geïmplementeerde structuur.

noOfEventsPerType is het aantal voorvallen per soort voorval dat de kaart kan registreren.

noOfFaultsPerType is het aantal fouten per soort fout dat de kaart kan registreren.

activityStructureLength geeft het aantal beschikbare bytes aan voor het opslaan van activiteitenrecords.

noOfCardVehicleRecords is het aantal voertuigregistraties dat de kaart kan bevatten.

noOfCardPlaceRecords is het aantal plaatsen dat de kaart kan registreren.

noOfCalibrationRecords is het aantal kalibreringsrecords dat de kaart kan opslaan.

2e generatie:

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

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

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

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

2.235. **WorkshopCardCalibrationData**

Op een werkplaatskaart opgeslagen informatie met betrekking tot de met de kaart uitgevoerde activiteiten van de werkplaats (voorschriften 314, 316, 337 en 339 van bijlage 1C).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber              INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord      INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                  SET SIZE(NoOfCalibrationRecords) OF
                                       WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber is het totale aantal met de kaart uitgevoerde kalibreringen.

calibrationPointerNewestRecord is de index van de laatst bijgewerkte kalibreringsrecord.

Waardetoekenning: getal dat correspondeert met de teller van de kalibreringsrecord, beginnend met '0' voor de eerste kalibreringsrecord in de structuur.

calibrationRecords is de reeks records die informatie over kalibrering en/of tijdafstelling bevat.

2.236. **WorkshopCardCalibrationRecord**

Op een werkplaatskaart opgeslagen informatie met betrekking tot een met de kaart uitgevoerde kalibrering (voorschriften 314 en 337 van bijlage 1C).

1e generatie:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber
}
```

calibrationPurpose is het doel van de kalibrering.

vehicleIdentificationNumber is het VIN.

vehicleRegistration bevat het kentekennummer en de registrerende lidstaat.

wVehicleCharacteristicConstant is de kenmerkende coëfficiënt van het voertuig.

kConstantOfRecordingEquipment is de constante van het controleapparaat.

lTyreCircumference is de effectieve omtrek van de wielbanden.

tyreSize is de aanduiding van de afmeting van de banden waarmee het voertuig uitgerust is.

authorisedSpeed is de toegestane maximumsnelheid van het voertuig.

oldOdometerValue, newOdometerValue zijn de oude en nieuwe kilometerstanden.

oldTimeValue, newTimeValue zijn de oude en nieuwe waarden van datum en tijd.

nextCalibrationDate is de datum van de volgende in CalibrationPurpose gespecificeerde soort kalibrering die door de bevoegde controleautoriteit moet worden uitgevoerd.

vuPartNumber, vuSerialNumber en **sensorSerialNumber** zijn de gegevenselementen voor identificatie van het controleapparaat.

2e generatie:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber,
   sensorGNSSSerialNumber              SensorGNSSSerialNumber,
   rcmSerialNumber                     RemoteCommunicationModuleSerialNumber,
   sealDataCard                        SealDataCard
}
```

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

sensorGNSSSerialNumber identificeert een externe GNSS-module.

rcmSerialNumber identificeert een module voor communicatie op afstand.

sealDataCard geeft informatie over de zegels die aan de verschillende onderdelen van het voertuig zijn gehecht.

2.237. **WorkshopCardHolderIdentification**

Op een werkplaatskaart opgeslagen informatie met betrekking tot de identificatie van de kaarthouder (voorschriften 311 en 334 van bijlage 1C).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                        Name,
   workshopAddress                     Address,
   cardHolderName                      HolderName,
   cardHolderPreferredLanguage         Language
}
```

workshopName is de naam van de werkplaats van de kaarthouder.

workshopAddress is het adres van de werkplaats van de kaarthouder.

cardHolderName is de naam en voornaam (voornamen) van de houder (bijv. de naam van de monteur).

cardHolderPreferredLanguage is de voorkeurtaal van de kaarthouder.

2.238. **WorkshopCardPIN**

Persoonlijk identificatienummer (PIN-code) van de werkplaatskaart (voorschriften 309 en 332 van bijlage 1C).

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

Waardetoekenning: de bij de kaarthouder bekende PIN-code, rechts met 'FF' bytes tot maximaal 8 bytes opgevuld.

2.239. **W-VehicleCharacteristicConstant**

Kenmerkende coëfficiënt van het voertuig (definitie k).

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Waardetoekenning: pulsen per kilometer in het operationele bereik van 0 tot 64 255 pulsen/km.

2.240. **VuPowerSupplyInterruptionRecord**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot onderbrekingen in de stroomvoorziening (voorschrift 117 van bijlage 1C).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd      FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin  FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType is het soort voorval.

eventRecordPurpose is het doel waarvoor dit voorval geregistreerd werd.

eventBeginTime is de datum en het tijdstip van het begin van het voorval.

eventEndTime is de datum en het tijdstip van het einde van het voorval.

cardNumberAndGenDriverSlotBegin identificeert de aan het begin van het voorval in de lezer van de bestuurder ingebrachte kaart, inclusief de generatie.

cardNumberAndGenDriverSlotEnd identificeert de aan het eind van het voorval in de lezer van de bestuurder ingebrachte kaart, inclusief de generatie.

cardNumberAndGenCodriverSlotBegin identificeert de aan het begin van het voorval in de lezer van de bijrijder ingebrachte kaart, inclusief de generatie.

cardNumberAndGenCodriverSlotEnd identificeert de aan het eind van het voorval in de lezer van de bijrijder ingebrachte kaart, inclusief de generatie.

similarEventsNumber is het aantal vergelijkbare voorvallen op die dag.

2.241. **VuPowerSupplyInterruptionRecordArray**

2e generatie:

In een voertuigunit opgeslagen informatie met betrekking tot onderbrekingen in de stroomvoorziening (voorschrift 117 van bijlage 1C).

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

recordType staat voor de soort record (VuPowerSupplyInterruptionRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van VuPowerSupplyInterruptionRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks records van onderbrekingen in de stroomvoorziening.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

2e generatie:

Een reeks SensorExternalGNSSCoupledRecord plus metagegevens die worden gebruikt in het downloadprotocol.

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

recordType staat voor de soort record (SensorExternalGNSSCoupledRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van SensorExternalGNSSCoupledRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks SensorExternalGNSSCoupledRecords.

2.243. **VuSensorPairedRecordArray**

2e generatie:

Een reeks SensorPairedRecord plus metagegevens die worden gebruikt in het downloadprotocol.

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

recordType staat voor de soort record (SensorPairedRecord). **Waardetoekenning**: zie RecordType.

recordSize is de grootte van SensorPairedRecord in bytes.

noOfRecords is het aantal records in de reeks records.

records is een reeks SensorPairedRecords.

3. DEFINITIES VAN WAARDEN- EN AFMETINGENBEREIK

Definitie van variabele waarden die gebruikt zijn bij de definities in paragraaf 2.

```
TimeRealRange ::= 2^32-1
```

4. TEKENSETS

IA5-Strings gebruiken de ASCII-tekens zoals gedefinieerd in ISO/IEC 8824-1. Voor de leesbaarheid en voor gemakkelijke verwijzing wordt de waardetoekenning hieronder gegeven. In geval van afwijkingen geldt ISO/IEC 8824-1 boven deze informatieve notitie.

```
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

Andere tekenstrings (Address, Name, VehicleRegistrationNumber) gebruiken bovendien tekens die worden gedefinieerd door de codes 161 tot en met 255 van de volgende 8-bits standaardtekensets, gespecificeerd door het CodePagenummer: Standaardtekenset	Code Page (decimaal)
ISO/IEC 8859-1 Latijns-1 West-Europees	1
ISO/IEC 8859-2 Latijns-2 Centraal-Europees	2
ISO/IEC 8859-3 Latijns-3 Zuid-Europees	3
ISO/IEC 8859-5 Latijns / Cyrillisch	5
ISO/IEC 8859-7 Latijns / Grieks	7
ISO/IEC 8859-9 Latijns-5 Turks	9
ISO/IEC 8859-13 Latijns-7 Baltische regio	13
ISO/IEC 8859-15 Latijns-9	15
ISO/IEC 8859-16 Latijns-10 Zuid-Oost-Europees	16
KOI8-R Latijns / Cyrillisch	80
KOI8-U Latijns / Cyrillisch	85

5. CODERING

In het geval van codering met ASN.1-coderegels moeten alle gedefinieerde gegevenssoorten gecodeerd worden overeenkomstig ISO/IEC 8825-2, uitgerichte variant.

6. OBJECTIDENTIFICATIE EN TOEPASSINGSIDENTIFICATIE

6.1. **Objectidentificatie**

De in dit hoofdstuk opgenomen objectidentificatiesymbolen (OID's) hebben alleen betrekking op de 2e generatie. Die OID's zijn gespecificeerd in TR-03110-3 en worden hier voor de volledigheid herhaald. Ze zijn opgenomen in de substructuur van bsi-de:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

VU-authenticatieprotocolidentificatoren

```
id-TA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 2}

id-TA-ECDSA                 OBJECT IDENTIFIER ::= {id-TA 2}

id-TA-ECDSA-SHA-256 OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}

id-TA-ECDSA-SHA-384 OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}

id-TA-ECDSA-SHA-512 OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}
```

Voorbeeld: Als VU-authenticatie moet worden uitgevoerd met SHA-384, is het te gebruiken objectidentificatiesymbool (in ASN.1-notatie) `bsi-de protocols(2) smartcard(2) 2 2 4`. De waarde van dit objectidentificatiesymbool in puntnotatie is `0.4.0.127.0.7.2.2.2.2.4`.

	Puntnotatie	Bytenotatie
`id-TA-ECDSA-SHA-256`	`0.4.0.127.0.7.2.2.2.2.3`	‘04 00 7F 00 07 02 02 02 02 03’
`id-TA-ECDSA-SHA-384`	`0.4.0.127.0.7.2.2.2.2.4`	‘04 00 7F 00 07 02 02 02 02 04’
`id-TA-ECDSA-SHA-512`	`0.4.0.127.0.7.2.2.2.2.5`	‘04 00 7F 00 07 02 02 02 02 05’

Chipauthenticatieprotocolidentificatoren

```
id-CA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 3}

id-CA-ECDH                          OBJECT IDENTIFIER ::= {id-CA 2}

id-CA-ECDH-AES-CBC-CMAC-128         OBJECT IDENTIFIER ::= {id-CA-ECDH 2}

id-CA-ECDH-AES-CBC-CMAC-192         OBJECT IDENTIFIER ::= {id-CA-ECDH 3}

id-CA-ECDH-AES-CBC-CMAC-256         OBJECT IDENTIFIER ::= {id-CA-ECDH 4}
```

Voorbeeld: Veronderstel dat chipauthenticatie moet worden uitgevoerd met het ECDH-algoritme, wat resulteert in een AES-sessiesleutel met een lengte van 128 bits. Die sessiesleutel wordt vervolgens gebruikt in CBC-modus om de vertrouwelijkheid van de gegevens te verzekeren en met het CMAC-algoritme om de authenticiteit van de gegevens te verzekeren. Het te gebruiken objectidentificatiesymbool (in ASN.1-notatie) is daarom `bsi-de protocols(2) smartcard(2) 3 2 2`. De waarde van dit objectidentificatiesymbool in puntnotatie is `0.4.0.127.0.7.2.2.3.2.2`.

	Puntnotatie	Bytenotatie
`id-CA-ECDH-AES-CBC-CMAC-128`	`0.4.0.127.0.7.2.2.3.2.2`	‘04 00 7F 00 07 02 02 03 02 02’
`id-CA-ECDH-AES-CBC-CMAC-192`	`0.4.0.127.0.7.2.2.3.2.3`	‘04 00 7F 00 07 02 02 03 02 03’
`id-CA-ECDH-AES-CBC-CMAC-256`	`0.4.0.127.0.7.2.2.3.2.4`	‘04 00 7F 00 07 02 02 03 02 04’

6.2. Toepassingsidentificaties

2e generatie:

Het toepassingsidentificatiesymbool (AID) voor de externe GNSS-module (2e generatie) wordt gegeven door ‘FF 44 54 45 47 4D’. Dit is een particuliere AID overeenkomstig ISO/IEC 7816-4.

Opmerking: De laatste 5 bytes coderen DTEGM voor een externe GNSS-module van een slimme tachograaf.

Het toepassingsidentificatiesymbool (AID) voor de tachograafkaartapplicatie van de 2e generatie) wordt gegeven door 'FF 53 4D 52 44 54'. Dit is een particuliere AID overeenkomstig ISO/IEC 7816-4.

Aanhangsel 2

SPECIFICATIE VAN TACHOGRAAFKAARTEN

INHOUDSOPGAVE

1. INLEIDING 175
1.1. Afkortingen 175
1.2. Referentienormen 176
2. ELEKTRONISCHE EN FYSIEKE KENMERKEN 176
2.1. Toevoerspanning en stroomverbruik 177
2.2. Programmeerspanning V_{pp} 177
2.3. Klokgenerering en klokfrequentie 177
2.4. I/O-contact 177
2.5. Statussen van de kaart 177
3. HARDWARE EN COMMUNICATIE 177
3.1. Inleiding 177
3.2. Overbrengingsprotocol 178
3.2.1 Protocollen 178
3.2.2 ATR 179
3.2.3 PTS 179
3.3. Toegangsregels 180
3.4. Overzicht van commando's en foutcodes 183
3.5. Beschrijving van commando's 185
3.5.1 SELECT (Selecteer) 186
3.5.2 READ BINARY (Lees binair getal) 187
3.5.3 UPDATE BINARY (Werk binair getal bij) 194
3.5.4 GET CHALLENGE (Vraag naar identiteit) 200
3.5.5 VERIFY (Verifieer) 200
3.5.6 GET RESPONSE (Haal antwoord op) 202
3.5.7 PSO: VERIFY CERTIFICATE (PSO: verifieer certificaat) 202
3.5.8 INTERNAL AUTHENTICATE (Interne authenticatie) 204
3.5.9 EXTERNAL AUTHENTICATE (Externe authenticatie) 205
3.5.10 GENERAL AUTHENTICATE (Algemene authenticatie) 206
3.5.11 MANAGE SECURITY ENVIRONMENT (Beheer beveiligingsomgeving) 207
3.5.12 PSO: HASH 210
3.5.13 PERFORM HASH OF FILE (Voer hash van bestand uit) 211
3.5.14 PSO: COMPUTE DIGITAL SIGNATURE (PSO: bereken digitale handtekening) 212
3.5.15 PSO: VERIFY DIGITAL SIGNATURE (PSO: verifieer digitale handtekening) 213
3.5.16 PROCESS DSRC MESSAGE (Verwerk dsrc-bericht) 214
4. BESTANDSSTRUCTUUR VAN DE TACHOGRAAFKAARTEN 216
4.1. Stambestand (MF) 216

4.2. Tachograaftoepassingen voor de bestuurderskaart 217
4.2.1 Tachograaftoepassing van de eerste generatie voor de bestuurderskaart 217
4.2.2 Tachograaftoepassing van de tweede generatie voor de bestuurderskaart 221
4.3. Tachograaftoepassingen voor de werkplaatskaart 224
4.3.1 Tachograaftoepassing van de eerste generatie voor de werkplaatskaart 224
4.3.2 Tachograaftoepassing van de tweede generatie voor de werkplaatskaart 228
4.4. Tachograaftoepassingen voor de controlekaart 233
4.4.1 Tachograaftoepassing van de eerste generatie voor de controlekaart 233
4.4.2 Tachograaftoepassing van de tweede generatie voor de controlekaart 235
4.5. Tachograaftoepassingen voor de bedrijfskaart 237
4.5.1 Tachograaftoepassing van de eerste generatie voor de bedrijfskaart 237
4.5.2 Tachograaftoepassing van de tweede generatie voor de bedrijfskaart 238

1. INLEIDING

1.1. **Afkortingen**

In dit aanhangsel worden de volgende afkortingen gebruikt.

AC	Toegangscondities
AES	Advanced Encryption Standard
AID	Toepassingsidentificator
ALW	Altijd
APDU	Toepassingsprotocol gegevensunit (commandostructuur)
ATR	Antwoord op terugstellen
AUT	Geauthenticeerd
C6, C7	Contacten nr. 6 en 7 van de kaart, zoals beschreven in ISO/IEC 7816-2
cc	Klokcycli
CHV	Verificatie-informatie van de kaarthouder
CLA	Bytecategorie van het APDU-commando
DSRC	Speciale korteafstandscommunicatie
DF	Toepassingsgericht bestand. Een DF kan andere bestanden (EF of DF) bevatten
ECC	Elliptische-krommecryptografie
EF	Hoofdbestand
etu	Elementaire tijdeenheid
G1	Eerste generatie
G2	Tweede generatie
IC	Geïntegreerde schakeling
ICC	Chipkaart
ID	Identificator
IFD	Interface-inrichting
IFS	Grootte van het informatieveld
IFSC	Grootte van het informatieveld voor de kaart

IFSD	Inrichting voor de grootte van het informatieveld (voor het werkstation)
INS	Instructiebyte van een APDU-commando
Lc	Lengte van invoergegevens voor een APDU-commando
Le	Lengte van de verwachte gegevens (uitvoergegevens voor een commando)
MF	Stambestand (hoofd-DF)
NAD	Knooppuntadres gebruikt in het protocol T = 1
NEV	Nooit
P1-P2	Parameterbytes
PIN	Persoonlijk identificatienummer (pincode)
PRO SM	Beschermd door beveiligde berichtenuitwisseling
PTS	Protocol voor transmissieselectie
RFU	Gereserveerd voor toekomstig gebruik
RST	Terugstellen (van de kaart)
SFID	Korte EF-identificator
SM	Beveiligde berichtenuitwisseling
SW1-SW2	Statusbytes
TS	Initieel ATR-teken
VPP	Programmeerspanning
VU	Voertuigunit
XXh	Waarde XX in hexadecimale notatie
'XXh'	Waarde XX in hexadecimale notatie
||	Samenvoegingssymbool 03||04 = 0304

1.2. **Referentienormen**

De onderstaande referentienormen worden in dit aanhangsel gebruikt:

ISO/IEC 7816-2 Identification cards — Integrated circuit cards — Part 2: Dimensions and location of the contacts. ISO/IEC 7816-2:2007.

ISO/IEC 7816-3 Identification cards — Integrated circuit cards — Part 3: Electrical interface and transmission protocols. ISO/IEC 7816-3:2006.

ISO/IEC 7816-4 Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange. ISO/IEC 7816-4:2013 + Cor 1: 2014.

ISO/IEC 7816-6 Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange. ISO/IEC 7816-6:2004 + Cor 1: 2006.

ISO/IEC 7816-8 Identification cards — Integrated circuit cards — Part 8: Commands for security operations. ISO/IEC 7816-8:2004.

ISO/IEC 9797-2 Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function. ISO/IEC 9797-2:2011.

2. ELEKTRISCHE EN FYSIEKE KENMERKEN

TCS_01 Tenzij anders gespecificeerd, zijn alle elektronische signalen in overeenstemming met ISO/IEC 7816-3.

TCS_02 De plaats en afmetingen van de contacten van de kaart voldoen aan ISO/IEC 7816-2.

2.1. **Toevoerspanning en stroomverbruik**

TCS_03 De kaart werkt overeenkomstig de specificaties binnen de in ISO/IEC 7816-3 gespecificeerde verbruikslimieten.

TCS_04 De kaart werkt met Vcc = 3 V (± 0,3 V) of met Vcc = 5 V (± 0,5 V).

De spanning wordt geselecteerd overeenkomstig ISO/IEC 7816-3.

2.2. **Programmeerspanning V_{pp}**

TCS_05 De kaart gebruikt geen programmeerspanning op pin C6. Pin C6 wordt naar verwachting niet aangesloten in een IFD. Contact C6 kan worden verbonden met V_{cc} in de kaart, maar niet met de aarde. Deze spanning mag in geen geval worden omgezet.

2.3. **Klokgenerering en klokfrequentie**

TCS_06 De kaart werkt binnen een frequentiebereik van 1 tot 5 MHz en kan hogere frequenties ondersteunen. Tijdens een kaartsessie kan de klokfrequentie ± 2 % variëren. De klokfrequentie wordt door de voertuigunit en niet door de kaart zelf gegenereerd. De inschakelduur kan variëren tussen 40 en 60 %.

TCS_07 Onder de in het kaartbestand EF ICC opgenomen voorwaarden kan de externe klok worden stilgezet ("klokstop"). De eerste byte van het EF ICC-bestandsdeel codeert de voorwaarden voor de klokstop.

Laag	Hoog		
Bit 3	Bit 2	Bit 1	
0	0	1	klokstop toegestaan, geen voorkeurniveau
0	1	1	klokstop toegestaan, bij voorkeur hoog niveau
1	0	1	klokstop toegestaan, bij voorkeur laag niveau
0	0	0	klokstop niet toegestaan
0	1	0	klokstop alleen toegestaan op hoog niveau
1	0	0	klokstop alleen toegestaan op laag niveau

De bits 4 tot en met 8 worden niet gebruikt.

2.4. **I/O-contact**

TCS_08 Het I/O-contact C7 wordt gebruikt om gegevens te ontvangen van en over te brengen naar de IFD. Alleen tijdens de werking staat ofwel de kaart, ofwel de IFD in overbrengingsmodus. Indien beide units in overbrengingsmodus staan, mag er geen schade aan de kaart ontstaan. De kaart staat in ontvangstmodus, tenzij gegevens worden overgebracht.

2.5. **Statussen van de kaart**

TCS_09 De kaart werkt in twee statussen wanneer de toevoerspanning aangesloten is:

operationele status wanneer commando's worden uitgevoerd of verbinding wordt gemaakt met de digitale unit,

inactieve status op alle andere tijdstippen; in deze status blijven alle gegevens bewaard op de kaart.

3. HARDWARE EN COMMUNICATIE

3.1. **Inleiding**

In dit punt wordt een beschrijving gegeven van de minimaal vereiste functionaliteit voor tachograafkaarten en VU's om een correcte werking en interoperabiliteit te waarborgen.

Tachograafkaarten voldoen zo veel mogelijk aan de beschikbare, toepasselijke ISO/IEC-normen (in het bijzonder ISO/IEC 7816). Commando's en protocollen worden echter volledig beschreven om beperkt gebruik of eventueel aanwezige verschillen te specificeren. Tenzij anders aangegeven, voldoen de gespecificeerde commando's integraal aan de genoemde normen.

3.2. **Overbrengingsprotocol**

TCS_10 Het overbrengingsprotocol voldoet aan ISO/IEC 7816-3 voor T = 0 en T = 1. De VU herkent in het bijzonder door de kaart verzonden verlengingen van de wachttijd.

3.2.1 *Protocollen*

TCS_11 De kaart biedt zowel protocol **T = 0** als protocol **T = 1**. Bovendien kan de kaart aanvullende contactgerichte protocollen ondersteunen.

TCS_12 **T = 0** is het standaardprotocol; bijgevolg is een **PTS**-commando noodzakelijk om het protocol te wijzigen in **T = 1**.

TCS_13 Inrichtingen ondersteunen de **directe conventie** in beide protocollen: bijgevolg is de directe conventie verplicht voor de kaart.

TCS_14 De byte voor de **grootte van het informatieveld** wordt weergegeven in teken TA3 van het ATR. Deze waarde is ten minste gelijk aan 'F0h' (= 240 bytes).

De onderstaande beperkingen zijn van toepassing op de protocollen:

TCS_15 **T = 0**

— De interface-inrichting ondersteunt een antwoord op I/O na de oplopende rand van het signaal bij RST vanaf 400 cc.

— De interface-inrichting kan met 12 etu's gescheiden tekens lezen.

— De interface-inrichting kan een foutief teken en de herhaling daarvan lezen, indien gescheiden met 13 etu's. Indien een foutief teken wordt vastgesteld, kan de I/O-foutsignalering tussen 1 etu en 2 etu's voorkomen. De inrichting ondersteunt een vertraging van 1 etu.

— De interface-inrichting accepteert een ATR van 33 bytes (TS + 32).

— Indien TC1 in het ATR staat, is Extra Guard Time aanwezig voor door de interface-inrichting verzonden tekens. Niettemin kunnen door de kaart verzonden tekens nog steeds met 12 etu's worden gescheiden. Dit geldt ook voor het door de kaart verzonden ACK-teken na een door de interface-inrichting gezonden P3-teken.

— De interface-inrichting houdt rekening met een door de kaart gezonden NUL-teken.

— De interface-inrichting accepteert de complementaire modus voor ACK.

— Het GET RESPONSE-commando kan niet in kettingmodus worden gebruikt om een gegeven op te halen dat langer kan zijn dan 255 bytes.

TCS_16 **T = 1**

— NAD-byte: niet gebruikt (NAD wordt op '00' gezet).

— S-blok ABORT: niet gebruikt.

— S-blok VPP state error: niet gebruikt.

— De totale kettinglengte voor een gegevensveld bedraagt ten hoogste 255 bytes (te waarborgen door de IFD).

— De inrichting voor de grootte van het informatieveld (IFSD) wordt onmiddellijk na het ATR door de IFD aangegeven: de IFD brengt het S-blok IFS-verzoek na het ATR over en de kaart zendt het S-blok IFS terug. De aanbevolen waarde voor IFSD is 254 bytes.

— De kaart vraagt geen IFS-bijstelling.

3.2.2 *ATR*

TCS_17 De inrichting controleert de ATR-bytes overeenkomstig ISO/IEC 7816-3. Historische tekens van het ATR worden niet geverifieerd.

Voorbeeld van basis-biprotocol ATR overeenkomstig ISO/IEC 7816-3

Teken	Waarde	Opmerkingen
TS	'3Bh'	Geeft directe conventie aan
T0	'85h'	TD1 aanwezig; 5 historische bytes zijn aanwezig
TD1	'80h'	TD2 aanwezig; T=0 moet worden gebruikt
TD2	'11h'	TA3 aanwezig; T=1 moet worden gebruikt
TA3	'XXh' (ten minste 'F0h')	Grootte van het informatieveld voor de kaart (IFSC)
TH1 t/m TH5	'XXh'	Historische tekens
TCK	'XXh'	Controleer teken (exclusieve OF (XOR))

TCS_18 Het stambestand (MF) wordt na het ATR impliciet geselecteerd en geldt als geldige map (directory).

3.2.3 *PTS*

TCS_19 Het standaardprotocol is T = 0. Om het protocol T = 1 in te stellen, moet de inrichting een PTS (ook PPS genoemd) naar de kaart verzenden.

TCS_20 Aangezien de protocollen T = 0 en T = 1 verplicht zijn voor de kaart, is het basis-PTS voor protocolwisseling verplicht voor de kaart.

Zoals aangegeven in ISO/IEC 7816-3, kan het PTS worden gebruikt om te wisselen naar hogere baudsnelheden dan de standaardsnelheid die de kaart in het eventuele ATR aangeeft (TA(1) byte).

Hogere baudsnelheden zijn facultatief voor de kaart.

TCS_21 Indien geen andere baudsnelheid dan de standaardsnelheid wordt ondersteund (of indien de geselecteerde baudsnelheid niet wordt ondersteund), reageert de kaart correct op het PTS, overeenkomstig ISO/IEC 7816-3, door de PPS1-byte weg te laten.

Voorbeelden van het basis-PTS voor protocolselectie:

Teken	Waarde	Opmerkingen
PPSS	'FFh'	Startteken
PPS0	'00h' of '01h'	PPS1 t/m PPS3 niet aanwezig; '00h' om T0 te selecteren, '01h' om T1 te selecteren
PK	'XXh'	Controleteken: 'XXh' = 'FFh' als PPS0 = '00h' 'XXh' = 'FEh' als PPS0 = '01h'

3.3. **Toegangsregels**

TCS_22 Een toegangsregel specificeert de toepasselijke beveiligingsvoorwaarden voor een toegangsmodus, dat wil zeggen een commando. Indien aan deze beveiligingsvoorwaarden is voldaan, wordt het corresponderende commando verwerkt.

TCS_23 De volgende beveiligingsvoorwaarden worden gebruikt voor de tachograafkaart:

Afkorting	Betekenis
ALW	De actie is altijd mogelijk en kan zonder enige beperking worden uitgevoerd. Het APDU-commando en -antwoord worden ongecodeerd verzonden, dat wil zeggen zonder beveiligde berichtenuitwisseling.
NEV	De actie is nooit mogelijk.
PLAIN-C	Het APDU-commando wordt ongecodeerd verzonden, dat wil zeggen zonder beveiligde berichtenuitwisseling.
PWD	De actie kan alleen worden uitgevoerd indien de pincode van de werkplaatskaart met succes is geverifieerd, dat wil zeggen indien de interne beveiligingsstatus van de kaart is ingesteld op „PIN_Verified". Het commando moet zonder beveiligde berichtenuitwisseling worden verzonden.
EXT-AUT-G1	De actie kan alleen worden uitgevoerd indien het External Authenticate-commando voor authenticatie van de eerste generatie (zie ook aanhangsel 11, deel A) met succes werd uitgevoerd.
SM-MAC-G1	Het APDU-commando en -antwoord moeten worden toegepast met beveiligde berichtenuitwisseling van de eerste generatie in alleen-authenticeren-modus (zie aanhangsel 11, deel A).
SM-C-MAC-G1	Het APDU-commando moet worden toegepast met beveiligde berichtenuitwisseling van de eerste generatie in alleen-authenticeren-modus (zie aanhangsel 11, deel A).
SM-R-ENC-G1	Het APDU-antwoord moet worden toegepast met beveiligde berichtenuitwisseling van de eerste generatie in coderingsmodus (zie aanhangsel 11, deel A); er wordt bijgevolg geen berichtauthenticatiecode teruggezonden.
SM-R-ENC-MAC-G1	Het APDU-antwoord moet worden toegepast met beveiligde berichtenuitwisseling van de eerste generatie in eerst-coderen-dan-authenticeren-modus (zie aanhangsel 11, deel A).
SM-MAC-G2	Het APDU-commando en -antwoord moeten worden toegepast met beveiligde berichtenuitwisseling van de tweede generatie in alleen-authenticeren-modus (zie aanhangsel 11, deel B).
SM-C-MAC-G2	Het APDU-commando moet worden toegepast met beveiligde berichtenuitwisseling van de tweede generatie in alleen-authenticeren-modus (zie aanhangsel 11, deel B).
SM-R-ENC-MAC-G2	Het APDU-antwoord moet worden toegepast met beveiligde berichtenuitwisseling van de tweede generatie in eerst-coderen-dan-authenticeren-modus (zie aanhangsel 11, deel B).

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.

TCS_25 In de toepassing DF Tachograaf G1 worden de volgende toegangsregels gebruikt:

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
PSO: 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

TCS_26 In de toepassing DF Tachograaf_G2 worden de volgende toegangsregels gebruikt:

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

Commando	Bestuurderskaart	Werkplaatskaart	Controlekaart	Bedrijfskaart
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
PSO: 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

TCS_27 In het stambestand (MF) worden de volgende toegangsregels gebruikt:

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

Commando	Bestuurderskaart	Werkplaatskaart	Controlekaart	Bedrijfskaart
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
PSO: Hash of File	Niet van toepassing	Niet van toepassing	Niet van toepassing	Niet van toepassing
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Niet van toepassing	ALW	Niet van toepassing	Niet van toepassing

TCS_28 Een tachograafkaart kan al dan niet een commando accepteren met een hoger beveiligingsniveau dan in de beveiligingsvoorwaarden is voorgeschreven. Indien bijvoorbeeld ALW (of PLAIN-C) geldt als beveiligingsvoorwaarde, kan de kaart een commando ontvangen met beveiligde berichtenuitwisseling (in coderings- en/of authenticatiemodus). Indien in de beveiligingsvoorwaarde beveiligde berichtenuitwisseling in authenticatiemodus wordt opgelegd, kan de tachograafkaart een commando met beveiligde berichtenuitwisseling van dezelfde generatie accepteren in authenticatie- en coderingsmodus.

Opmerking: in de beschrijving van commando's wordt nader toegelicht welke commando's door de verschillende soorten tachograafkaarten en DF's worden ondersteund.

3.4. **Overzicht van commando's en foutcodes**

De commando's en bestandsorganisatie zijn afgeleid van en voldoen aan ISO/IEC 7816-4.

In dit punt wordt een beschrijving gegeven van de volgende APDU-commando-antwoordparen. In de beschrijving van commando's wordt aangegeven welke varianten van commando's door toepassingen van de eerste en tweede generatie worden ondersteund.

Commando	INS
SELECT	'A4h'
READ BINARY	'B0h', 'B1h'
UPDATE BINARY	'D6h', 'D7h'
GET CHALLENGE	'84h'
VERIFY	'20h'
GET RESPONSE	'C0h'
PERFORM SECURITY OPERATION	'2Ah'
— VERIFY CERTIFICATE	
— COMPUTE DIGITAL SIGNATURE	
— VERIFY DIGITAL SIGNATURE	
— HASH	
— PERFORM HASH OF FILE	
— PROCESS DSRC MESSAGE	

Commando	INS
INTERNAL AUTHENTICATE	'88h'
EXTERNAL AUTHENTICATE	'82h'
MANAGE SECURITY ENVIRONMENT	'22h'
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	'86h'

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
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	82	Beveiligde berichtenuitwisseling niet ondersteund
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)

SW1	SW2	Betekenis
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

TCS_30 Indien in een APDU-commando meerdere foutcondities vervuld zijn, kan de kaart een van de toepasselijke statuswoorden terugzenden.

3.5. **Beschrijving van commando's**

In dit hoofdstuk wordt een beschrijving gegeven van de verplichte commando's voor de tachograafkaarten.

In aanhangsel 11 „Algemene beveiligingsmechanismen" worden nadere bijzonderheden verstrekt over de betrokken cryptografische bewerkingen voor tachograaftoepassingen van de eerste en de tweede generatie.

Alle commando's worden onafhankelijk van het gebruikte protocol (T = 0 of T = 1) beschreven. De APDU-bytes CLA, INS, P1, P2, Lc en Le worden altijd aangegeven. Indien Lc of Le niet nodig is voor het beschreven commando, zijn de daarmee samenhangende lengte, waarde en omschrijving leeg.

TCS_31 Indien beide lengtebytes (Lc en Le) vereist zijn, moet het beschreven commando in twee delen worden gesplitst wanneer de IFD protocol T = 0 gebruikt: de IFD verzendt het commando zoals beschreven met P3 = Lc + gegevens, en verzendt vervolgens een GET RESPONSE-commando (zie punt 3.5.6) met P3 = Le.

TCS_32 Indien beide lengtebytes vereist zijn en Le = 0 (beveiligde berichtenuitwisseling):

— Bij gebruik van protocol T = 1 beantwoordt de kaart Le = 0 door alle beschikbare uitvoergegevens te verzenden.

— Bij gebruik van protocol T = 0 verzendt de IFD het eerste commando met P3 = Lc + gegevens, en beantwoordt de kaart (deze impliciete Le = 0) met de statusbytes '**61La**', waarbij La het aantal beschikbare antwoordbytes is. De IFD genereert vervolgens een GET RESPONSE-commando met P3 = La om de gegevens te kunnen lezen.

TCS_33 Overeenkomstig ISO/IEC 7816-4 kan een tachograafkaart facultatief velden met uitgebreide lengte ondersteunen. Een tachograafkaart die velden met uitgebreide lengte ondersteunt:

— geeft in het ATR aan dat velden met uitgebreide lengte worden ondersteund;

— verstrekt de ondersteunde buffergrootte via de informatie over de uitgebreide lengte in EF ATR/INFO (zie TCS_146);

— geeft in EF Extended_Length aan of velden met uitgebreide lengte worden ondersteund voor T = 1 en/of T = 0 (zie TCS_147).

— ondersteunt velden met uitgebreide lengte voor tachograaftoepassingen van de eerste en de tweede generatie.

Opmerkingen:

Alle commando's worden gespecificeerd voor velden met een korte lengte. Het gebruik van APDU's met uitgebreide lengte wordt verduidelijkt in ISO/IEC 7816-4.

Doorgaans worden de commando's gespecificeerd voor de ongecodeerde modus, dat wil zeggen zonder beveiligde berichtenuitwisseling, aangezien de laag voor beveiligde berichtenuitwisseling wordt gespecificeerd in aanhangsel 11. De toegangsregels voor een commando verduidelijken of het commando beveiligde berichtenuitwisseling al dan niet ondersteunt, en of het commando beveiligde berichtenuitwisseling van de eerste en/of de tweede generatie ondersteunt. Sommige varianten van commando's worden beschreven met beveiligde berichtenuitwisseling om het gebruik daarvan te verduidelijken.

TCS_34 De VU voert voor een sessie het volledige protocol voor wederzijdse authenticatie van VU-kaarten van de tweede generatie uit, met inbegrip van de certificaatverificatie (indien vereist) in DF Tachograaf, DF Tachograaf_G2 of in het MF.

3.5.1 *SELECT*

Dit commando voldoet aan ISO/IEC 7816-4, maar heeft een beperkt gebruik vergeleken met het in deze norm gedefinieerde commando.

Het SELECT-commando wordt gebruikt:

— om een DF-toepassing te selecteren (er moet op naam worden geselecteerd);

— om een hoofdbestand te selecteren dat overeenstemt met de opgegeven bestandsidentificator.

3.5.1.1 Selectie op naam (AID)

Met dit commando wordt een DF-toepassing op de kaart geselecteerd.

TCS_35 Dit commando kan overal in de bestandsstructuur worden uitgevoerd (na het ATR of wanneer dan ook).

TCS_36 Indien een toepassing wordt geselecteerd, wordt de huidige beveiligingsomgeving teruggesteld. Na het selecteren van de toepassing wordt geen actuele openbare sleutel meer geselecteerd. De EXT-AUT-G1-toegangsconditie is ook verloren gegaan. Indien het commando zonder beveiligde berichtenuitwisseling (SM) werd uitgevoerd, zijn de vorige SM-sessiesleutels niet langer beschikbaar.

TCS_37 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Selectie op naam (AID)
P2	1	'0Ch'	Geen antwoord verwacht
Lc	1	'NNh'	Aantal naar de kaart verzonden bytes (lengte van AID): '06h' voor de tachograaftoepassing
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' voor de tachograaftoepassing van de eerste generatie AID: 'FF 53 4D 52 44 54' voor de tachograaftoepassing van de tweede generatie

Een antwoord op het SELECT-commando is niet nodig (Le afwezig in T = 1, of geen antwoord gevraagd in T = 0).

TCS_38 **Antwoordbericht (geen antwoord gevraagd)**

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien de met de AID corresponderende toepassing niet wordt gevonden, wordt de verwerkingsstatus '**6A82**' teruggezonden.

— In T = 1, indien byte Le aanwezig is, wordt de status '**6700**' teruggezonden.

— In T= 0, indien na het SELECT-commando een antwoord wordt gevraagd, wordt de status '**6900**' teruggezonden.

— Indien de geselecteerde toepassing beschadigd is (integriteitsfout vastgesteld in de bestandsattributen), wordt de verwerkingsstatus '**6400**' of '**6581**' teruggezonden.

3.5.1.2 Selectie van een hoofdbestand (EF) op basis van de bestandsidentificator

TCS_39 **Commandobericht**

TCS_40 Voor deze commandovariant ondersteunt een tachograafkaart beveiligde berichtenuitwisseling van de tweede generatie, zoals gespecificeerd in aanhangsel 11, deel B.

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Selectie van EF in de geldige DF
P2	1	'0Ch'	Geen antwoord verwacht
Lc	1	'02h'	Aantal naar de kaart verzonden bytes
#6-#7	2	'XXXXh'	Bestandsidentificator

Een antwoord op het SELECT-commando is niet nodig (Le afwezig in T = 1, of geen antwoord gevraagd in T = 0).

TCS_41 **Antwoordbericht (geen antwoord gevraagd)**

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien het met de bestandsidentificator corresponderende bestand niet wordt gevonden, wordt de verwerkingsstatus '**6A82**' teruggezonden.

— In T = 1, indien byte Le aanwezig is, wordt de status '**6700**' teruggezonden.

— In T = 0, indien na het SELECT-commando een antwoord wordt gevraagd, wordt de status '**6900**' teruggezonden.

— Indien het geselecteerde bestand beschadigd is (integriteitsfout vastgesteld in de bestandsattributen), wordt de verwerkingsstatus '**6400**' of '**6581**' teruggezonden.

3.5.2 *READ BINARY*

Dit commando voldoet aan ISO/IEC 7816-4, maar heeft een beperkt gebruik vergeleken met het in deze norm gedefinieerde commando.

Het READ BINARY-commando wordt gebruikt om gegevens van een transparant bestand te lezen.

Het antwoord van de kaart bestaat uit het terugzenden van de gelezen gegevens, facultatief ingekapseld in een structuur van beveiligde berichtenuitwisseling.

3.5.2.1 Commando met offset in P1-P2

Met dit commando kan de IFD gegevens in het thans geselecteerde hoofdbestand (EF) lezen zonder beveiligde berichtenuitwisseling.

Opmerking: dit commando zonder beveiligde berichtenuitwisseling kan alleen worden gebruikt voor het lezen van een bestand dat de ALW-beveiligingsvoorwaarde voor de toegangsmodus van de Read-functie ondersteunt.

TCS_42 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'B0h'	READ BINARY (Lees binair getal)
P1	1	'XXh'	Offset in bytes vanaf het begin van het bestand: meest significante byte
P2	1	'XXh'	Offset in bytes vanaf het begin van het bestand: minst significante byte
Le	1	'XXh'	Lengte van verwachte gegevens. Aantal te lezen bytes

Opmerking: bit 8 van P1 moet op '0' worden gezet.

TCS_43 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
#1-#X	X	'XX..XXh'	Gelezen gegevens
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien geen EF is geselecteerd, wordt de verwerkingsstatus '**6986**' teruggezonden.

— Indien niet wordt voldaan aan de beveiligingsvoorwaarden van het geselecteerde bestand, wordt het commando onderbroken met '**6982**'.

— Indien de offset niet compatibel is met de grootte van het hoofdbestand (offset > grootte EF), wordt de verwerkingsstatus '**6B00**' teruggezonden.

— Indien de grootte van de te lezen gegevens niet compatibel is met de grootte van het hoofdbestand (Offset + Le > grootte EF), wordt de verwerkingsstatus '**6700**' of '**6Cxx**' teruggezonden, waarbij 'xx' de exacte lengte aangeeft.

— Indien in de bestandsattributen een integriteitsfout wordt vastgesteld, beschouwt de kaart het bestand als beschadigd en definitief verloren en wordt de verwerkingsstatus '**6400**' of '**6581**' teruggezonden.

— Indien in de opgeslagen gegevens een integriteitsfout wordt vastgesteld, zendt de kaart de gevraagde gegevens terug en wordt de verwerkingsstatus '**6281**' teruggezonden.

3.5.2.1.1 Commando met beveiligde berichtenuitwisseling (voorbeelden)

Met dit commando kan de IFD gegevens van het thans geselecteerde hoofdbestand (EF) met beveiligde berichtenuitwisseling lezen om de integriteit van de ontvangen gegevens te verifiëren en de vertrouwelijkheid van de gegevens te beschermen in het geval dat de beveiligingsvoorwaarde SM-R-ENC-MAC-G1 (eerste generatie) of SM-R-ENC-MAC-G2 (tweede generatie) wordt toegepast.

TCS_44 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'0Ch'	Beveiligde berichtenuitwisseling gevraagd
INS	1	'B0h'	READ BINARY (Lees binair getal)
P1	1	'XXh'	P1 (offset in bytes vanaf het begin van het bestand): meest significante byte
P2	1	'XXh'	P2 (offset in bytes vanaf het begin van het bestand): minst significante byte
Lc	1	'XXh'	Lengte van invoergegevens voor beveiligde berichtenuitwisseling
#6	1	'97h'	T_{LE}: label voor verwachte lengtespecificatie
#7	1	'01h'	L_{LE}: lengte van verwachte lengte
#8	1	'NNh'	Verwachte lengtespecificatie (originele Le): aantal te lezen bytes
#9	1	'8Eh'	T_{CC}: label voor cryptografische controlesom
#10	1	'XXh'	L_{CC}: 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-sleutellengte voor beveiligde berichtenuitwisseling van de tweede generatie (zie aanhangsel 11, deel B)
#11-#(10+L)	L	'XX..XXh'	Cryptografische controlesom
Le	1	'00h'	Zoals gespecificeerd in ISO/IEC 7816-4

TCS_45 **Antwoordbericht indien SM-R-ENC-MAC-G1 (eerste generatie) / SM-R-ENC-MAC-G2 (tweede generatie) niet vereist is en indien het invoerformaat van de beveiligde berichtenuitwisseling correct is:**

Byte	Lengte	Waarde	Omschrijving
#1	1	'99h'	Label voor verwerkingsstatus (SW1-SW2) — facultatief voor beveiligde berichtenuitwisseling van de eerste generatie
#2	1	'02h'	Lengte van verwerkingsstatus
#3 — #4	2	'XX XXh'	Verwerkingsstatus van het onbeveiligde APDU-antwoord
#5	1	'81h'	T_{PV}: label voor gegevens met ongecodeerde waarde
#6	L	'NNh' of '81 NNh'	L_{PV}: lengte van teruggezonden gegevens (= originele Le) L is 2 bytes indien L_{PV}>127 bytes

Byte	Lengte	Waarde	Omschrijving
#(6+L)-#(5+L+NN)	NN	'XX..XXh'	Ongecodeerde gegevenswaarde
#(6+L+NN)	1	'8Eh'	T_{CC}: label voor cryptografische controlesom
#(7+L+NN)	1	'XXh'	L_{CC}: 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-sleutellengte voor beveiligde berichtenuitwisseling van de tweede generatie (zie aanhangsel 11, deel B)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Cryptografische controlesom
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

TCS_46 **Antwoordbericht indien SM-R-ENC-MAC-G1 (eerste generatie) / SM-R-ENC-MAC-G2 (tweede generatie) vereist is en indien het invoerformaat van de beveiligde berichtenuitwisseling correct is:**

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 $L_{PI\ CG} > 127$ 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
#(4+L+MM) — #(5+L+MM)	2	'XX XXh'	Verwerkingsstatus van het onbeveiligde APDU-antwoord
#(6+L+MM)	1	'8Eh'	T_{CC}: label voor cryptografische controlesom
#(7+L+MM)	1	'XXh'	L_{CC}: 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-sleutellengte 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)

Het READ BINARY-commando kan gewone verwerkingsstatussen terugzenden die worden opgesomd in TCS_43 onder de label '99h' (zie beschrijving in TCS_59), met gebruikmaking van beveiligde antwoordberichtstructuren.

Bovendien kunnen bepaalde fouten optreden die meer in het bijzonder verband houden met de beveiligde berichtenuitwisseling. In dit geval wordt de verwerkingsstatus gewoon teruggezonden zonder beveiligde berichtenuitwisselingsstructuur.

TCS_47 **Antwoordbericht indien het invoerformaat van de beveiligde berichtenuitwisseling niet correct is:**

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien geen lopende sessiesleutel beschikbaar is, wordt de verwerkingsstatus '**6A88**' teruggezonden. Dit is het geval wanneer de sessiesleutel nog niet werd gegenereerd of wanneer de geldigheid van de sessiesleutel verlopen is (in dit geval moet de IFD opnieuw een wederzijdse authenticatie uitvoeren om een nieuwe sessiesleutel te genereren).

— Indien een aantal verwachte gegevensobjecten (zoals hierboven gespecificeerd) ontbreekt in het formaat van de beveiligde berichtenuitwisseling, wordt de verwerkingsstatus '**6987**' teruggezonden: deze fout treedt op wanneer een verwacht label ontbreekt of wanneer het commandoveld niet correct samengesteld is.

— Indien een aantal gegevensobjecten niet correct is, wordt de verwerkingsstatus '**6988**' teruggezonden: deze fout treedt op wanneer alle vereiste labels aanwezig zijn, maar een aantal lengtes afwijkt van de verwachte lengtes.

— Indien de verificatie van de cryptografische controlesom mislukt, wordt de verwerkingsstatus '**6688**' teruggezonden.

3.5.2.2 Commando met korte EF (Elementary File)-identificator

Met deze commandovariant kan de IFD een hoofdbestand (EF) selecteren met behulp van een korte EF-identificator, en gegevens van deze EF lezen.

TCS_48 Een tachograafkaart ondersteunt deze commandovariant voor alle hoofdbestanden met een specifieke korte EF-identificator. Deze korte EF-identificatoren worden gespecificeerd in hoofdstuk 4.

TCS_49 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'B0h'	READ BINARY (Lees binair getal)
P1	1	'XXh'	Bit 8 wordt op '1' gezet Bits 7 en 6 worden op '00' gezet Bits 5 t/m 1 coderen de korte EF-identificator van de corresponderende EF
P2	1	'XXh'	Codeert een offset van 0 t/m 255 bytes in de EF waarnaar P1 verwijst
Le	1	'XXh'	Lengte van verwachte gegevens. Aantal te lezen bytes

Opmerking: de korte EF-identificatoren die voor tachograaftoepassingen van de tweede generatie worden gebruikt, worden gespecificeerd in hoofdstuk 4.

Indien P1 een korte EF-identificator codeert en het commando succesvol is, wordt het geïdentificeerde hoofdbestand (EF) de thans geselecteerde (geldige) EF.

TCS_50 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
#1-#L	L	'XX..XXh'	Gelezen gegevens
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien het met de korte EF-identificator corresponderende bestand niet wordt gevonden, wordt de verwerkingsstatus '**6A82**' teruggezonden.

— Indien niet wordt voldaan aan de beveiligingsvoorwaarden van het geselecteerde bestand, wordt het commando onderbroken met '**6982**'.

— Indien de offset niet compatibel is met de grootte van het hoofdbestand (offset > grootte EF), wordt de verwerkingsstatus '**6B00**' teruggezonden.

— Indien de grootte van de te lezen gegevens niet compatibel is met de grootte van het hoofdbestand (Offset + Le > grootte EF), wordt de verwerkingsstatus '**6700**' of '**6Cxx**' teruggezonden, waarbij 'xx' de exacte lengte aangeeft.

— Indien in de bestandsattributen een integriteitsfout wordt vastgesteld, beschouwt de kaart het bestand als beschadigd en definitief verloren en wordt de verwerkingsstatus '**6400**' of '**6581**' teruggezonden.

— Indien in de opgeslagen gegevens een integriteitsfout wordt vastgesteld, zendt de kaart de gevraagde gegevens terug en wordt de verwerkingsstatus '**6281**' teruggezonden.

3.5.2.3 Commando met oneven instructiebyte

Met deze commandovariant kan de IFD gegevens lezen van een hoofdbestand (EF) dat 32 768 bytes of meer bevat.

TCS_51 Een tachograafkaart die ondersteuning biedt aan EF's met 32 768 bytes of meer, ondersteunt deze commandovariant voor die EF's. Voor andere EF's, met uitzondering van de EF Sensor_Installation_Data, kan een tachograafkaart deze commandovariant al dan niet ondersteunen (zie TCS_156 en TCS_160).

TCS_52 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'B1h'	READ BINARY (Lees binair getal)
P1	1	'00h'	Geldige EF
P2	1	'00h'	
Lc	1	'NNh'	Lc lengte van offset-gegevensobject
#6-#(5+NN)	NN	'XX..XXh'	Offset-gegevensobject: Label '54h' Lengte '01h' of '02h' Waarde offset
Le	1	'XXh'	Aantal te lezen bytes

De IFD codeert de lengte van het offset-gegevensobject met zo weinig mogelijk bytes, en gebruikt met andere woorden de lengtebyte '01h' om een offset te coderen van 0 tot en met 255 bytes, en de lengtebyte '02h' om een offset te coderen van 256 tot en met 65 535 bytes.

TCS_53 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
#1-#L	L	'XX..XXh'	Gelezen gegevens, ingekapseld in een discretionair gegevensobject met label '53h'.
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien geen EF is geselecteerd, wordt de verwerkingsstatus '**6986**' teruggezonden.

— Indien niet wordt voldaan aan de beveiligingsvoorwaarden van het geselecteerde bestand, wordt het commando onderbroken met '**6982**'.

— Indien de offset niet compatibel is met de grootte van het hoofdbestand (offset > grootte EF), wordt de verwerkingsstatus '**6B00**' teruggezonden.

— Indien de grootte van de te lezen gegevens niet compatibel is met de grootte van het hoofdbestand (offset + Le > grootte EF), wordt de verwerkingsstatus '**6700**' of '**6Cxx**' teruggezonden, waarbij 'xx' de exacte lengte aangeeft.

— Indien in de bestandsattributen een integriteitsfout wordt vastgesteld, beschouwt de kaart het bestand als beschadigd en definitief verloren en wordt de verwerkingsstatus '**6400**' of '**6581**' teruggezonden.

— Indien in de opgeslagen gegevens een integriteitsfout wordt vastgesteld, zendt de kaart de gevraagde gegevens terug en wordt de verwerkingsstatus '**6281**' teruggezonden.

3.5.2.3.1 Commando met beveiligde berichtenuitwisseling (voorbeeld)

Het volgende voorbeeld verduidelijkt het gebruik van beveiligde berichtenuitwisseling indien de beveiligingsvoorwaarde SM-MAC-G2 van toepassing is.

TCS_54 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'0Ch'	Beveiligde berichtenuitwisseling gevraagd
INS	1	'B1h'	READ BINARY (Lees binair getal)
P1	1	'00h'	Geldige EF
P2	1	'00h'	
Lc	1	'XXh'	Lengte van het beveiligde gegevensveld
#6	1	'B3h'	Label voor ongecodeerde waarde van met BER-TLV gecodeerde gegevens
#7	1	'NNh'	L_{PV}: lengte van overgebrachte gegevens
#(8)-#(7+NN)	NN	'XX..XXh'	Ongecodeerde waarde van met BER-TLV gecodeerde gegevens, d.w.z. het offset-gegevensobject met label '54'
#(8+NN)	1	'97h'	T_{LE}: label voor verwachte lengtespecificatie
#(9+NN)	1	'01h'	L_{LE}: lengte van verwachte lengtespecificatie
#(10+NN)	1	'XXh'	Verwachte lengtespecificatie (originele Le): aantal te lezen bytes
#(11+NN)	1	'8Eh'	T_{CC}: label voor cryptografische controlesom
#(12+NN)	1	'XXh'	L_{CC}: lengte van volgende cryptografische controlesom '08h', '0Ch' of '10h' afhankelijk van de AES-sleutellengte voor beveiligde berichtenuitwisseling van de tweede generatie (zie aanhangsel 11, deel B)
#(13+NN)-#(12+M+NN)	M	'XX..XXh'	Cryptografische controlesom
Le	1	'00h'	Zoals gespecificeerd in ISO/IEC 7816-4

TCS_55 Antwoordbericht indien het commando succesvol is

Byte	Lengte	Waarde	Omschrijving
#1	1	'B3h'	Ongecodeerde waarde van met BER-TLV gecodeerde gegevens
#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 waarde van met BER-TLV gecodeerde gegevens, d.w.z. gelezen gegevens, ingekapseld in een discretionair gegevensobject met label '53h'
#(2+L+NN)	1	'99h'	Verwerkingsstatus van het onbeveiligde APDU-antwoord
#(3+L+NN)	1	'02h'	Lengte van verwerkingsstatus
#(4+L+NN) — #(5+L+NN)	2	'XX XXh'	Verwerkingsstatus van het onbeveiligde APDU-antwoord
#(6+L+NN)	1	'8Eh'	T_{CC}: label voor cryptografische controlesom
#(7+L+NN)	1	'XXh'	L_{CC}: lengte van volgende cryptografische controlesom '08h', '0Ch' of '10h' afhankelijk van de AES-sleutellengte voor beveiligde berichtenuitwisseling van de tweede generatie (zie aanhangsel 11, deel B)
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Cryptografische controlesom
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

3.5.3 *UPDATE BINARY*

Dit commando voldoet aan ISO/IEC 7816-4, maar heeft een beperkt gebruik vergeleken met het in die norm gedefinieerde commando.

Het UPDATE BINARY-commandobericht start het bijwerken (wissen + schrijven) van de bits die al in een binair getal van een EF aanwezig zijn met de in het APDU-commando gegeven bits.

3.5.3.1 Commando met offset in P1-P2

Met dit commando kan de IFD gegevens schrijven in de thans geselecteerde EF, zonder dat de kaart de integriteit van de ontvangen gegevens verifieert.

Opmerking: dit commando zonder beveiligde berichtenuitwisseling kan alleen worden gebruikt voor het bijwerken van een bestand dat de ALW-beveiligingsvoorwaarde van de toegangsmodus van de Update-functie ondersteunt.

TCS_56 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'D6h'	Update Binary (Werk binair getal bij)

Byte	Lengte	Waarde	Omschrijving
P1	1	'XXh'	Offset in bytes vanaf het begin van het bestand: meest significante byte
P2	1	'XXh'	Offset in bytes vanaf het begin van het bestand: minst significante byte
Lc	1	'NNh'	Lc lengte van bij te werken gegevens. Aantal te schrijven bytes
#6-#(5+NN)	NN	'XX..XXh'	Te schrijven gegevens

Opmerking: bit 8 van P1 moet op '0' worden gezet.

TCS_57 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien geen EF is geselecteerd, wordt de verwerkingsstatus '**6986**' teruggezonden.

— Indien niet wordt voldaan aan de beveiligingsvoorwaarden van het geselecteerde bestand, wordt het commando onderbroken met '**6982**'.

— Indien de offset niet compatibel is met de grootte van het hoofdbestand (offset > grootte EF), wordt de verwerkingsstatus '**6B00**' teruggezonden.

— Indien de grootte van de te schrijven gegevens niet compatibel is met de grootte van het hoofdbestand (offset + Lc > grootte EF), wordt de verwerkingsstatus '**6700**' teruggezonden.

— Indien in de bestandsattributen een integriteitsfout wordt vastgesteld, beschouwt de kaart het bestand als beschadigd en definitief verloren en wordt de verwerkingsstatus '**6400**' of '**6500**' teruggezonden.

— Indien het schrijven mislukt, wordt de verwerkingsstatus '**6581**' teruggezonden.

3.5.3.1.1 Commando met beveiligde berichtenuitwisseling (voorbeelden)

Met dit commando kan de IFD gegevens schrijven in de thans geselecteerde EF, waarbij de kaart de integriteit van de ontvangen gegevens verifieert. Aangezien geen vertrouwelijkheid vereist is, worden de gegevens niet gecodeerd.

TCS_58 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'0Ch'	Beveiligde berichtenuitwisseling gevraagd
INS	1	'D6h'	Update Binary (Werk binair getal bij)
P1	1	'XXh'	Offset in bytes vanaf het begin van het bestand: meest significante byte
P2	1	'XXh'	Offset in bytes vanaf het begin van het bestand: minst significante byte
Lc	1	'XXh'	Lengte van het beveiligde gegevensveld

Byte	Lengte	Waarde	Omschrijving
#6	1	'81h'	T_{PV}: label voor gegevens met ongecodeerde waarde
#7	L	'NNh' of '81 NNh'	L_{PV}: lengte van overgebrachte gegevens L is 2 bytes indien L_{PV} > 127 bytes
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Ongecodeerde gegevenswaarde (te schrijven gegevens)
#(7+L+NN)	1	'8Eh'	T_{CC}: label voor cryptografische controlesom
#(8+L+NN)	1	'XXh'	L_{CC}: lengte van volgende cryptografische controlesom '04h' voor beveiligde berichtenuitwisseling van de eerste generatie (zie deel A van aanhangsel 11) '08h', '0Ch' of '10h' afhankelijk van de AES-sleutellengte voor beveiligde berichtenuitwisseling van de tweede generatie (zie aanhangsel 11, deel B)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Cryptografische controlesom
Le	1	'00h'	Zoals gespecificeerd in ISO/IEC 7816-4

TCS_59 **Antwoordbericht indien het invoerformaat van de beveiligde berichtenuitwisseling correct is**

Byte	Lengte	Waarde	Omschrijving
#1	1	'99h'	T_{SW}: label voor statuswoorden (te beveiligen door CC)
#2	1	'02h'	L_{SW}: lengte van teruggezonden statuswoorden
#3-#4	2	'XXXXh'	Verwerkingsstatus van het onbeveiligde APDU-antwoord
#5	1	'8Eh'	T_{CC}: label voor cryptografische controlesom (CC)
#6	1	'XXh'	L_{CC}: lengte van volgende cryptografische controlesom (CC) '04h' voor beveiligde berichtenuitwisseling van de eerste generatie (zie aanhangsel 11, deel A) '08h', '0Ch' of '10h' afhankelijk van de AES-sleutellengte voor beveiligde berichtenuitwisseling van de tweede generatie (zie aanhangsel 11, deel B)
#7-#(6+L)	L	'XX..XXh'	Cryptografische controlesom (CC)
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

De „gewone" verwerkingsstatussen voor het UPDATE BINARY-commando zonder beveiligde berichtenuitwisseling (zie beschrijving in punt 3.5.3.1) kunnen met gebruikmaking van de hierboven omschreven antwoordberichtstructuur worden teruggezonden.

Bovendien kunnen bepaalde fouten optreden die meer in het bijzonder verband houden met de beveiligde berichtenuitwisseling. In dit geval wordt de verwerkingsstatus gewoon teruggezonden zonder beveiligde berichtenuitwisselingsstructuur.

TCS_60 **Antwoordbericht bij een fout in de beveiligde berichtenuitwisseling**

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien geen lopende sessiesleutel beschikbaar is, wordt de verwerkingsstatus '**6A88**' teruggezonden.

— Indien een aantal verwachte gegevensobjecten (zoals hierboven gespecificeerd) ontbreekt in het formaat van de beveiligde berichtenuitwisseling, wordt de verwerkingsstatus '**6987**' teruggezonden: deze fout treedt op wanneer een verwacht label ontbreekt of wanneer het commandoveld niet correct samengesteld is.

— Indien een aantal gegevensobjecten niet correct is, wordt de verwerkingsstatus '**6988**' teruggezonden: deze fout treedt op wanneer alle vereiste labels aanwezig zijn, maar een aantal lengtes afwijkt van de verwachte lengtes.

— Indien de verificatie van de cryptografische controlesom mislukt, wordt de verwerkingsstatus '**6688**' teruggezonden.

3.5.3.2 Commando met korte EF-identificator

Met deze commandovariant kan de IFD een hoofdbestand (EF) selecteren met behulp van een korte EF-identificator, en gegevens van deze EF schrijven.

TCS_61 Een tachograafkaart ondersteunt deze commandovariant voor alle hoofdbestanden met een specifieke korte EF-identificator. Deze korte EF-identificatoren worden gespecificeerd in hoofdstuk 4.

TCS_62 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'D6h'	Update Binary (Werk binair getal bij)
P1	1	'XXh'	Bit 8 wordt op '1' gezet Bits 7 en 6 worden op '00' gezet Bits 5 t/m 1 coderen de korte EF-identificator van de corresponderende EF
P2	1	'XXh'	Codeert een offset van 0 t/m 255 bytes in de EF waarnaar P1 verwijst
Lc	1	'NNh'	Lc lengte van bij te werken gegevens. Aantal te schrijven bytes
#6-#(5+NN)	NN	'XX..XXh'	Te schrijven gegevens

TCS_63 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

Opmerking: de korte EF-identificatoren die voor tachograaftoepassingen van de tweede generatie worden gebruikt, worden gespecificeerd in hoofdstuk 4.

Indien P1 een korte EF-identificator codeert en het commando succesvol is, wordt het geïdentificeerde hoofdbestand (EF) de thans geselecteerde (geldige) EF.

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien het met de korte EF-identificator corresponderende bestand niet wordt gevonden, wordt de verwerkingsstatus '**6A82**' teruggezonden.

— Indien niet wordt voldaan aan de beveiligingsvoorwaarden van het geselecteerde bestand, wordt het commando onderbroken met '**6982**'.

— Indien de offset niet compatibel is met de grootte van het hoofdbestand (offset > grootte EF), wordt de verwerkingsstatus '**6B00**' teruggezonden.

— Indien de grootte van de te schrijven gegevens niet compatibel is met de grootte van het hoofdbestand (offset + Lc > grootte EF), wordt de verwerkingsstatus '**6700**' teruggezonden.

— Indien in de bestandsattributen een integriteitsfout wordt vastgesteld, beschouwt de kaart het bestand als beschadigd en definitief verloren en wordt de verwerkingsstatus '**6400**' of '**6581**' teruggezonden.

— Indien het schrijven mislukt, wordt de verwerkingsstatus '**6581**' teruggezonden.

3.5.3.3 Commando met oneven instructiebyte

Met deze commandovariant kan de IFD gegevens schrijven in een hoofdbestand (EF) dat 32 768 bytes of meer bevat.

TCS_64 Een tachograafkaart die ondersteuning biedt aan EF's met 32 768 bytes of meer, ondersteunt deze commandovariant voor die EF's. Een tachograafkaart kan deze commandovariant al dan niet ondersteunen voor andere EF's.

TCS_65 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'D7h'	Update Binary (Werk binair getal bij)
P1	1	'00h'	Geldige EF
P2	1	'00h'	
Lc	1	'NNh'	Lc Lengte van gegevens in het gegevensveld van het commando
#6-#(5+NN)	NN	'XX..XXh'	Offset-gegevensobject met label '54h' || Discretionair gegevensobject met label '53h', waarin de te schrijven gegevens zijn ingekapseld

De IFD codeert de lengte van het offset-gegevensobject en het discretionair gegevensobject met zo weinig mogelijk bytes, en gebruikt met andere woorden de lengtebyte '01h' om een offset/lengte te coderen van 0 tot en met 255 bytes, en de lengtebyte '02h' om een offset/lengte te coderen van 256 tot en met 65 535 bytes.

TCS_66 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien geen EF is geselecteerd, wordt de verwerkingsstatus '**6986**' teruggezonden.

— Indien niet wordt voldaan aan de beveiligingsvoorwaarden van het geselecteerde bestand, wordt het commando onderbroken met '**6982**'.

— Indien de offset niet compatibel is met de grootte van het hoofdbestand (offset > grootte EF), wordt de verwerkingsstatus '**6B00**' teruggezonden.

— Indien de grootte van de te schrijven gegevens niet compatibel is met de grootte van het hoofdbestand (offset + Lc > grootte EF), wordt de verwerkingsstatus '**6700**' teruggezonden.

— Indien in de bestandsattributen een integriteitsfout wordt vastgesteld, beschouwt de kaart het bestand als beschadigd en definitief verloren en wordt de verwerkingsstatus '**6400**' of '**6500**' teruggezonden.

— Indien het schrijven mislukt, wordt de verwerkingsstatus '**6581**' teruggezonden.

3.5.3.3.1 Commando met beveiligde berichtenuitwisseling (voorbeeld)

Het volgende voorbeeld verduidelijkt het gebruik van beveiligde berichtenuitwisseling indien de beveiligingsvoorwaarde SM-MAC-G2 van toepassing is.

TCS_67 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'0Ch'	Beveiligde berichtenuitwisseling gevraagd
INS	1	'D7h'	Update Binary (Werk binair getal bij)
P1	1	'00h'	Geldige EF
P2	1	'00h'	
Lc	1	'XXh'	Lengte van het beveiligde gegevensveld
#6	1	'B3h'	Label voor ongecodeerde waarde van met BER-TLV gecodeerde gegevens
#7	L	'NNh' of '81 NNh'	L_{PV}: lengte van overgebrachte gegevens L is 2 bytes indien L_{PV} > 127 bytes
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Ongecodeerde waarde van met BER-TLV gecodeerde gegevens, d.w.z. offset-gegevensobject met label '54h' || Discretionair gegevensobject met label '53h', waarin de te schrijven gegevens zijn ingekapseld
#(7+L+NN)	1	'8Eh'	T_{CC}: label voor cryptografische controlesom
#(8+L+NN)	1	'XXh'	L_{CC}: lengte van volgende cryptografische controlesom '08h', '0Ch' of '10h' afhankelijk van de AES-sleutellengte voor beveiligde berichtenuitwisseling van de tweede generatie (zie aanhangsel 11, deel B)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Cryptografische controlesom
Le	1	'00h'	Zoals gespecificeerd in ISO/IEC 7816-4

TCS_68 Antwoordbericht indien het commando succesvol is

Byte	Lengte	Waarde	Omschrijving
#1	1	'99h'	T_{SW}: label voor statuswoorden (te beveiligen door CC)
#2	1	'02h'	L_{SW}: lengte van teruggezonden statuswoorden
#3-#4	2	'XXXXh'	Verwerkingsstatus van het onbeveiligde APDU-antwoord
#5	1	'8Eh'	T_{CC}: label voor cryptografische controlesom

Byte	Lengte	Waarde	Omschrijving
#6	1	'XXh'	L_{CC}: lengte van volgende cryptografische controlesom '08h', '0Ch' of '10h' afhankelijk van de AES-sleutellengte voor beveiligde berichtenuitwisseling van de tweede generatie (zie aanhangsel 11, deel B)
#7-#(6+L)	L	'XX..XXh'	Cryptografische controlesom
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

3.5.4 *GET CHALLENGE*

Dit commando voldoet aan ISO/IEC 7816-4, maar heeft een beperkt gebruik vergeleken met het in die norm gedefinieerde commando.

Via het GET CHALLENGE-commando wordt de kaart gevraagd een identiteit af te geven voor gebruik in een beveiligingsprocedure waarbij een cryptogram of een aantal gecodeerde gegevens naar de kaart wordt verzonden.

TCS_69 De door de kaart afgegeven identiteit geldt alleen voor het volgende naar de kaart verzonden commando dat een identiteit gebruikt.

TCS_70 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (lengte van de verwachte identiteit)

TCS_71 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
#1-#8	8	'XX..XXh'	Identiteit
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien Le verschilt van '08h', is de verwerkingsstatus '**6700**'.

— Indien de parameters P1-P2 niet correct zijn, is de verwerkingsstatus '**6A86**'.

3.5.5 *VERIFY*

Dit commando voldoet aan ISO/IEC 7816-4, maar heeft een beperkt gebruik vergeleken met het in die norm gedefinieerde commando.

Alleen de werkplaatskaart is vereist om dit commando te ondersteunen.

Op andere soorten tachograafkaarten kan dit commando al dan niet worden geïmplementeerd. Voor deze kaarten wordt echter geen referentie-CHV gepersonaliseerd. Bijgevolg kunnen deze kaarten dit commando niet met succes uitvoeren. Indien dit commando wordt verzonden voor andere tachograafkaarten dan werkplaatskaarten, valt de werking — dat wil zeggen de teruggezonden foutcode — buiten het toepassingsgebied van deze specificatie.

Het VERIFY-commando start de vergelijking in de kaart van de door het commando verzonden CHV-gegevens (pincode) met de op de kaart opgeslagen referentie-CHV.

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 Workshop-CardPIN in aanhangsel 1).

TCS_73 Tachograaftoepassingen van de eerste en de tweede generatie gebruiken dezelfde referentie-CHV.

TCS_74 De tachograafkaart controleert of het commando juist gecodeerd is. Indien het commando niet juist gecodeerd is, beëindigt de kaart het commando zonder de CHV-waarden te vergelijken, zonder de teller voor resterende CHV-pogingen te verlagen en zonder de beveiligingsstatus „PIN_Verified" terug te stellen. Een commando geldt als juist gecodeerd indien de bytes CLA, INS, P1, P2 en Lc de voorgeschreven waarden bevatten, indien Le afwezig is en indien het gegevensveld van het commando de juiste lengte heeft.

TCS_75 Indien het commando succesvol is, wordt de teller voor resterende CHV-pogingen opnieuw geïnitialiseerd. De beginwaarde van de teller voor resterende CHV-pogingen is 5. Indien het commando succesvol is, stelt de kaart de interne beveiligingsstatus in op „PIN_Verified". De kaart stelt deze beveiligingsstatus terug indien de kaart wordt teruggesteld of indien de in het commando overgebrachte CHV-code niet overeenstemt met de opgeslagen referentie-CHV.

Opmerking: door gebruik te maken van dezelfde referentie-CHV en van een algemene beveiligingsstatus, wordt vermeden dat de werkplaatsmedewerker de pincode opnieuw moet invoeren na het selecteren van een andere DF van de tachograaftoepassing.

TCS_76 Een niet-succesvolle vergelijking wordt op de kaart geregistreerd door de teller voor resterende CHV-pogingen met 1 te verlagen ter beperking van het aantal latere pogingen om de referentie-CHV te gebruiken.

TCS_77 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (de geverifieerde CHV is impliciet bekend)
Lc	1	'08h'	Lengte van de overgebrachte CHV-code
#6-#13	8	'XX..XXh'	CHV

TCS_78 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien de referentie-CHV niet wordt gevonden, wordt de verwerkingsstatus '**6A88**' teruggezonden.

— Indien de CHV geblokkeerd is (de teller voor resterende CHV-pogingen staat op nul), wordt de verwerkingsstatus '**6983**' teruggezonden. Zodra die status actief is, kan de CHV niet meer met succes worden aangeboden.

— Indien de vergelijking niet succesvol is, wordt de teller voor resterende pogingen verlaagd en wordt de status '**63CX**' teruggezonden (waarbij 'X' groter is dan nul en gelijk aan de teller voor resterende CHV-pogingen).

— Indien de referentie-CHV beschadigd is, wordt de verwerkingsstatus '**6400**' of '**6581**' teruggezonden.

— Indien Lc verschilt van '08h', is de verwerkingsstatus '**6700**'.

3.5.6 *GET RESPONSE*

Dit commando voldoet aan ISO/IEC 7816-4.

Dit commando is alleen nodig en beschikbaar voor het protocol T = 0. Met dit commando worden de voorbereide gegevens van de kaart overgebracht naar de interface-inrichting (IFD) voor zover zowel Lc als Le in het commando was opgenomen.

Het GET RESPONSE-commando moet worden gegeven onmiddellijk na het commando om de gegevens voor te bereiden. Zo niet, gaan de gegevens verloren. Na de uitvoering van het GET RESPONSE-commando (tenzij de fout '**61xx**' of '**6Cxx**' optreedt, zie hieronder) zijn de eerder voorbereide gegevens niet langer beschikbaar.

TCS_79 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Aantal verwachte bytes

TCS_80 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
#1-#X	X	'XX..XXh'	Gegevens
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien de kaart geen gegevens heeft voorbereid, wordt de verwerkingsstatus '**6900**' of '**6F00**' teruggezonden.

— Indien Le het aantal beschikbare bytes overschrijdt of gelijk is aan nul, wordt de verwerkingsstatus '**6Cxx**' teruggezonden, waarbij 'xx' het exacte aantal beschikbare bytes aangeeft. In dit geval zijn de voorbereide gegevens nog beschikbaar voor een volgend GET RESPONSE-commando.

— Indien Le verschilt van nul en kleiner is dan het aantal beschikbare bytes, worden de vereiste gegevens gewoon door de kaart verzonden en wordt de verwerkingsstatus '**61xx**' teruggezonden, waarbij 'xx' een aantal extra bytes aangeeft dat nog beschikbaar is voor een volgend GET RESPONSE-commando.

— Indien het commando niet wordt ondersteund (protocol T = 1), zendt de kaart '**6D00**' terug.

3.5.7 *PSO: VERIFY CERTIFICATE*

Dit commando voldoet aan ISO/IEC 7816-8, maar heeft een beperkt gebruik vergeleken met het in deze norm gedefinieerde commando.

De kaart gebruikt het VERIFY CERTIFICATE-commando om een externe openbare sleutel te verkrijgen en de geldigheid ervan te controleren.

3.5.7.1 Commando-antwoordpaar voor de eerste generatie

TCS_81 Deze commandovariant wordt alleen ondersteund door tachograaftoepassingen van de eerste generatie.

TCS_82 Wanneer een VERIFY CERTIFICATE-commando succesvol is, wordt de openbare sleutel in de beveiligingsomgeving opgeslagen voor toekomstig gebruik. Deze sleutel wordt expliciet ingesteld voor gebruik in beveiligingsgerelateerde commando's (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE of VERIFY CERTIFICATE) door het MSE-commando (zie punt 3.5.11) met behulp van de bijbehorende sleutelidentificator.

TCS_83 Het VERIFY CERTIFICATE-commando gebruikt hoe dan ook de openbare sleutel die het MSE-commando eerder heeft geselecteerd om het certificaat te openen. Deze openbare sleutel moet die van een lidstaat of van Europa zijn.

TCS_84 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'2Ah'	Voer beveiligingsoperatie uit (PSO)
P1	1	'00h'	P1
P2	1	'AEh'	P2: niet met BER-TLV gecodeerde gegevens (samenvoeging van gegevenselementen)
Lc	1	'C2h'	Lc: lengte van het certificaat, 194 bytes
#6-#199	194	'XX..XXh'	Certificaat: samenvoeging van gegevenselementen (zoals omschreven in aanhangsel 11)

TCS_85 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien de certificaatverificatie mislukt, wordt de verwerkingsstatus '**6688**' teruggezonden. De procedure voor certificaatverificatie en openmaken van het certificaat wordt nader omschreven in aanhangsel 11 voor tachograaftoepassingen van de eerste en de tweede generatie.

— Indien geen openbare sleutel in de beveiligingsomgeving aanwezig is, wordt '**6A88**' teruggezonden.

— Indien de geselecteerde openbare sleutel (waarmee het certificaat wordt opengemaakt) beschadigd is, wordt de verwerkingsstatus '**6400**' of '**6581**' teruggezonden.

— Alleen voor tachograaftoepassingen van de eerste generatie: Indien de geselecteerde openbare sleutel (waarmee het certificaat wordt opengemaakt) een andere CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) heeft dan '00' (dat wil zeggen niet die van een lidstaat of van Europa is), wordt de verwerkingsstatus '**6985**' teruggezonden.

3.5.7.2 Commando-antwoordpaar voor tachograaftoepassingen van de tweede generatie

In verband met de grootte van de elliptische kromme kunnen ECC-certificaten zo lang zijn dat het niet mogelijk is om ze in een enkele APDU te verzenden. In dit geval moeten de commando's aan elkaar worden gekoppeld ("geketend") overeenkomstig ISO/IEC 7816-4, en wordt het certificaat verzonden in twee opeenvolgende APDU-commando's PSO: Verify Certificate.

De certificaatstructuur en domeinparameters zijn gedefinieerd in aanhangsel 11.

TCS_86 Het commando kan worden uitgevoerd in MF, DF Tachograaf en DF Tachograaf_G2 (zie ook TCS_33).

TCS_87 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'X0h'	CLA-byte die aangeeft dat de commando's worden geketend '00h' het enige of laatste commando van de keten '10h' niet het laatste commando van de keten
INS	1	'2Ah'	Voer beveiligingsoperatie uit (PSO)
P1	1	'00h'	
P2	1	'BEh'	Verifieer zelfbeschrijvend certificaat
Lc	1	'XXh'	Lengte van het gegevensveld van het commando (zie TCS_88 en TCS_89).
#6-#5+L	L	'XX..XXh'	Met DER-TLV gecodeerde gegevens: inhoud van het ECC-certificaat als eerste gegevensobject samengevoegd met de handtekening van het ECC-certificaat als tweede gegevensobject of met een deel van deze samenvoeging. Het label '7F21' en de bijbehorende lengte worden niet verzonden. Deze gegevensobjecten hebben een vastgelegde volgorde.

TCS_88 Voor APDU's met korte lengte geldt het volgende: de IFD gebruikt het minimaal vereiste aantal APDU's om de payloadgegevens van het commando over te brengen en om het maximumaantal bytes in het eerste APDU-commando te verzenden volgens de waarde van de byte voor de grootte van het informatieveld (IFS), zie TCS_14. Indien de IFD anders reageert, valt de werking van de kaart buiten het toepassingsgebied van deze specificatie.

TCS_89 Voor APDU's met uitgebreide lengte geldt het volgende: indien het certificaat niet in een enkele APDU past, ondersteunt de kaart het ketenen van commando's. De IFD gebruikt het minimaal vereiste aantal APDU's om de payloadgegevens van het commando over te brengen en om het maximumaantal bytes in het eerste APDU-commando te verzenden. Indien de IFD anders reageert, valt de werking van de kaart buiten het toepassingsgebied van deze specificatie.

Opmerking: overeenkomstig aanhangsel 11 slaat de kaart het certificaat of de toepasselijke inhoud daarvan op, en werkt de kaart de currentAuthenticatedTime bij.

De antwoordberichtstructuur en statuswoorden zijn vastgelegd in TCS_85.

TCS_90 Naast de in TCS_85 opgesomde foutcodes kan de kaart de volgende foutcodes terugzenden:

— Indien de geselecteerde openbare sleutel (waarmee het certificaat wordt opengemaakt) een CHA. LSB (CertificateHolderAuthorisation.equipmentType) heeft die niet geschikt is voor certificaatverificatie overeenkomstig aanhangsel 11, wordt de verwerkingsstatus '**6985**' teruggezonden.

— Indien de currentAuthenticatedTime van de kaart valt na de datum waarop de geldigheid van het certificaat afloopt, wordt de verwerkingsstatus '**6985**' teruggezonden.

— Indien het laatste commando van de keten wordt verwacht, zendt de kaart '**6883**' terug.

— Indien onjuiste parameters worden verzonden in het gegevensveld van het commando, zendt de kaart '**6A80**' terug (dat is ook het geval indien de gegevensobjecten niet in de voorgeschreven volgorde worden verzonden).

3.5.8 *INTERNAL AUTHENTICATE*

Dit commando voldoet aan ISO/IEC 7816-4.

TCS_91 Alle tachograafkaarten ondersteunen dit commando in DF Tachograaf G1. Dit commando kan al dan niet toegankelijk zijn in MF en/of in DF Tachograaf_G2. Als dat het geval is, wordt het commando beëindigd met de toepasselijke foutcode aangezien de particuliere sleutel van de kaart (Card.SK) voor het authenticatieprotocol van de eerste generatie alleen toegankelijk is in DF_Tachograaf van de eerste generatie.

Met het INTERNAL AUTHENTICATE-commando kan de IFD de kaart authenticeren. De authenticatieprocedure wordt uiteengezet in aanhangsel 11. Hierbij worden de onderstaande instructies toegepast.

TCS_92 Het INTERNAL AUTHENTICATE-commando gebruikt de (impliciet geselecteerde) particuliere sleutel van de kaart ter ondertekening van de authenticatiegegevens met inbegrip van K1 (eerste element voor sleutelovereenstemming tijdens de sessie) en RND1, en gebruikt de thans geselecteerde openbare sleutel (via het laatste MSE-commando) om de handtekening te coderen en het authenticatieteken te genereren (zie aanhangsel 11 voor meer informatie).

TCS_93 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Lengte van naar de kaart verzonden gegevens
#6 — #13	8	'XX..XXh'	Identiteit gebruikt om de kaart te authenticeren
#14 -#21	8	'XX..XXh'	VU.CHR (zie aanhangsel 11)
Le	1	'80h'	Lengte van de gegevens die van de kaart worden verwacht

TCS_94 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
#1-#128	128	'XX..XXh'	Kaartauthenticatieteken (zie aanhangsel 11)
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien geen openbare sleutel in de beveiligingsomgeving aanwezig is, wordt de verwerkingsstatus '**6A88**' teruggezonden.

— Indien geen particuliere sleutel in de beveiligingsomgeving aanwezig is, wordt de verwerkingsstatus '**6A88**' teruggezonden.

— Indien VU.CHR niet overeenstemt met de identificator van de huidige openbare sleutel, wordt de verwerkingsstatus '**6A88**' teruggezonden.

— Indien de geselecteerde particuliere sleutel beschadigd is, wordt de verwerkingsstatus '**6400**' of '**6581**' teruggezonden.

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

3.5.9 *EXTERNAL AUTHENTICATE*

Dit commando voldoet aan ISO/IEC 7816-4.

Met het EXTERNAL AUTHENTICATE-commando kan de kaart de IFD authenticeren. De authenticatieprocedure wordt uiteengezet in aanhangsel 11 voor tachograaftoepassingen van de eerste en de tweede generatie (VU-authenticatie).

TCS_96 Wat betreft het mechanisme voor wederzijdse authenticatie van de eerste generatie wordt deze commandovariant uitsluitend ondersteund door tachograaftoepassingen van de eerste generatie.

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).

TCS_98 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Sleutels en algoritmen impliciet bekend
P2	1	'00h'	
Lc	1	'XXh'	Lc: lengte van de naar de kaart verzonden gegevens
#6-#(5+L)	L	'XX..XXh'	Authenticatie van de eerste generatie: cryptogram (zie aanhangsel 11, deel A) Authenticatie van de tweede generatie: handtekening gegenereerd door de IFD (zie aanhangsel 11, deel B)

TCS_99 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien de CHA van de thans ingestelde openbare sleutel niet de samenvoeging is van de AID van de tachograaftoepassing en van een model van VU-apparatuur, wordt de verwerkingsstatus '**6F00**' teruggezonden.

— Indien het commando niet onmiddellijk wordt voorafgegaan door een GET CHALLENGE-commando, wordt de verwerkingsstatus '**6985**'teruggezonden.

De tachograaftoepassing van de eerste generatie kan de volgende aanvullende foutcodes terugzenden:

— Indien geen openbare sleutel in de beveiligingsomgeving aanwezig is, wordt '**6A88**' teruggezonden.

— Indien geen particuliere sleutel in de beveiligingsomgeving aanwezig is, wordt de verwerkingsstatus '**6A88**' teruggezonden.

— Indien de verificatie van het cryptogram mislukt, wordt de verwerkingsstatus '**6688**' teruggezonden.

— Indien de geselecteerde particuliere sleutel beschadigd is, wordt de verwerkingsstatus '**6400**' of '**6581**' teruggezonden.

De commandovariant voor authenticatie van de tweede generatie kan de volgende aanvullende foutcode terugzenden:

— Indien de handtekeningverificatie mislukt is, zendt de kaart '**6300**' terug.

3.5.10 *GENERAL AUTHENTICATE*

Dit commando wordt gebruikt voor het chipauthenticatieprotocol van de tweede generatie, zoals gespecificeerd in deel B van aanhangsel 11, en voldoet aan ISO/IEC 7816-4.

TCS_100 Het commando kan worden uitgevoerd in MF, DF Tachograaf en DF Tachograaf_G2 (zie ook TCS_34).

TCS_101 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	Sleutels en protocol impliciet bekend
P2	1	'00h'	
Lc	1	'NNh'	Lc: lengte van het volgende gegevensveld
#6-#(5+L)	L	'7Ch' + L_{7C} + '80h' + L_{80} + 'XX..XXh'	Met DER-TLV gecodeerde waarde van de tijdelijke openbare sleutel (zie aanhangsel 11) De VU verzendt de gegevensobjecten in deze volgorde.

TCS_102 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
#1-#L	L	'7Ch' + L_{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L_{82} + 'XX..XXh'	Met DER-TLV gecodeerde dynamische authenticatiegegevens: *nonce* (willekeurig getal) en authenticatieteken (zie aanhangsel 11)
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— De kaart zendt '**6A80**' terug om te wijzen op onjuiste parameters in het gegevensveld.

— De kaart zendt '**6982**' terug indien het External Authenticate-commando niet met succes werd uitgevoerd.

Het antwoord van het gegevensobject voor dynamische authenticatie '7Ch':

— moet aanwezig zijn indien de bewerking succesvol is, dat wil zeggen wanneer de statuswoorden gelijk zijn aan '**9000**',

— moet afwezig zijn in geval van een uitvoerings- of controlefout, dat wil zeggen wanneer de statuswoorden liggen tussen '**6400**' en '**6FFF**', en

— kan afwezig zijn in geval van een waarschuwing, dat wil zeggen wanneer de statuswoorden liggen tussen '**6200**' en '**63FF**'.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Het MSE-commando wordt gebruikt om een openbare sleutel voor authenticatiedoeleinden in te stellen.

3.5.11.1 Commando-antwoordpaar voor tachograaftoepassingen van de eerste generatie

Dit commando voldoet aan ISO/IEC 7816-4. Het gebruik van dit commando is beperkt vergeleken met de toepasselijke norm.

TCS_103 Dit commando wordt alleen ondersteund door tachograaftoepassingen van de eerste generatie.

TCS_104 De in het MSE-gegevensveld genoemde sleutel blijft de huidige openbare sleutel tot het volgende correcte MSE-commando, totdat een DF wordt geselecteerd of totdat de kaart wordt teruggesteld.

TCS_105 Indien de genoemde sleutel (nog) niet in de kaart aanwezig is, blijft de beveiligingsomgeving ongewijzigd.

TCS_106 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: genoemde sleutel, geldig voor alle cryptografische bewerkingen
P2	1	'B6h'	P2: genoemde gegevens met betrekking tot de digitale handtekening
Lc	1	'0Ah'	Lc: lengte van het volgende gegevensveld
#6	1	'83h'	Label ter verwijzing naar een openbare sleutel in asymmetrische gevallen
#7	1	'08h'	Lengte van de sleutelreferentie (sleutelidentificator)
#8-#15	8	'XX..XXh'	Sleutelidentificator zoals gespecificeerd in aanhangsel 11

TCS_107 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien de genoemde sleutel niet op de kaart aanwezig is, wordt de verwerkingsstatus'**6A88**' teruggezonden.

— Indien een aantal verwachte gegevensobjecten in het beveiligde berichtenuitwisselingsformaat ontbreekt, wordt de verwerkingsstatus '**6987**' teruggezonden. Dit kan gebeuren wanneer het label '83h' ontbreekt.

— Indien een aantal gegevensobjecten niet correct is, wordt de verwerkingsstatus '**6988**' teruggezonden. Dit kan gebeuren wanneer de lengte van de sleutelidentificator verschilt van '08h'.

— Indien de geselecteerde sleutel beschadigd is, wordt de verwerkingsstatus '**6400**' of '**6581**' teruggezonden.

3.5.11.2 Commando-antwoordparen voor tachograaftoepassingen van de tweede generatie

Voor de authenticatie van de tweede generatie ondersteunt de tachograafkaart de volgende MSE: Set-commandoversies die voldoen aan ISO/IEC 7816-4. Deze commandoversies worden niet ondersteund voor de authenticatie van de eerste generatie.

3.5.11.2.1 MSE:SET AT-commando voor chipauthenticatie

Het volgende MSE:SET AT-commando wordt gebruikt om de parameters te selecteren voor de chipauthenticatie die wordt uitgevoerd door een volgend General Authenticate-commando.

TCS_108 Het commando kan worden uitgevoerd in MF, DF Tachograaf en DF Tachograaf_G2 (zie ook TCS_34).

TCS_109 **MSE:SET AT-commandobericht voor chipauthenticatie**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'22h'	

Byte	Lengte	Waarde	Omschrijving
P1	1	'41h'	Ingesteld voor interne authenticatie
P2	1	'A4h'	Authenticatie
Lc	1	'NNh'	Lc: lengte van het volgende gegevensveld
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Met DER-TLV gecodeerde referentie voor het cryptografisch mechanisme: objectidentificator van de chipauthenticatie (alleen waarde, label '06h' wordt weggelaten). Zie aanhangsel 1 voor de waarden van de objectidentificatoren; de notatie in byte wordt gebruikt. Zie aanhangsel 11 voor meer uitleg over de wijze waarop een van deze objectidentificatoren wordt geselecteerd.

3.5.11.2.2 MSE:SET AT-commando voor VU-authenticatie

Het volgende MSE:SET AT-commando wordt gebruikt om de parameters en sleutels te selecteren voor de VU-authenticatie die wordt uitgevoerd door een volgend External Authenticate-commando.

TCS_110 Het commando kan worden uitgevoerd in MF, DF Tachograaf en DF Tachograaf_G2 (zie ook TCS_34).

TCS_111 **MSE:SET AT-commandobericht voor VU-authenticatie**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Ingesteld voor externe authenticatie
P2	1	'A4h'	Authenticatie
Lc	1	'NNh'	Lc: lengte van het volgende gegevensveld
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Met DER-TLV gecodeerde referentie voor het cryptografisch mechanisme: objectidentificator van de VU-authenticatie (alleen waarde, label '06h' wordt weggelaten). Zie aanhangsel 1 voor de waarden van de objectidentificatoren; de notatie in byte wordt gebruikt. Zie aanhangsel 11 voor meer uitleg over de wijze waarop een van deze objectidentificatoren wordt geselecteerd.
		'83h' + '08h' + 'XX..XXh'	Met DER-TLV gecodeerde referentie van de openbare VU-sleutel op basis van de referentie van de certificaathouder die in zijn certificaat vermeld staat.
		'91h' + L_{91} + 'XX..XXh'	Met DER-TLV gecodeerde gecomprimeerde voorstelling van de tijdelijke openbare sleutel van de VU die tijdens de chipauthenticatie wordt gebruikt (zie aanhangsel 11)

3.5.11.2.3 MSE:SET DST

Het volgende MSE:SET DST-commando wordt gebruikt om een openbare sleutel in te stellen:

— ter verificatie van een handtekening die in een volgend PSO: Verify Digital Signature-commando wordt verstrekt, of

— voor de handtekeningverificatie van een certificaat dat in een volgend PSO: Verify Certificate-commando wordt verstrekt.

TCS_112 Het commando kan worden uitgevoerd in MF, DF Tachograaf en DF Tachograaf_G2 (zie ook TCS_33).

TCS_113 **MSE:SET DST-commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Ingesteld ter verificatie
P2	1	'B6h'	Digitale handtekening
Lc	1	'NNh'	Lc: lengte van het volgende gegevensveld
#6-#(5+L)	L	'83h' + '08h' + 'XX...XXh'	Met DER-TLV gecodeerde referentie van een openbare sleutel, dat wil zeggen de referentie van de certificaathouder in het openbare-sleutel-certificaat (zie aanhangsel 11)

Voor alle commandoversies worden de antwoordberichtstructuur en statuswoorden verstrekt door:

TCS_114 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug. Het protocol is geselecteerd en geïnitialiseerd.

— '**6A80**' wijst op onjuiste parameters in het gegevensveld van het commando.

— '**6A88**' geeft aan dat het genoemde gegeven (dat wil zeggen een genoemde sleutel) niet beschikbaar is.

3.5.12 *PSO: HASH*

Dit commando wordt gebruikt om het resultaat van een hashberekening van een aantal gegevens over te brengen op de kaart. Dit commando dient ter verificatie van digitale handtekeningen. De hashwaarde wordt tijdelijk opgeslagen voor het volgende PSO: Verify Digital Signature-commando.

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

Alleen de controlekaart is 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. Dit commando kan al dan niet toegankelijk zijn in het stambestand (MF).

Controlekaarten voor tachograaftoepassingen van de eerste generatie ondersteunen alleen SHA-1.

TCS_115 De tijdelijk opgeslagen hashwaarde wordt verwijderd indien een nieuwe hashwaarde wordt berekend met behulp van het PSO: HASH-commando, indien een DF wordt geselecteerd, en indien de tachograafkaart wordt teruggesteld.

TCS_116 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	CLA
INS	1	'2Ah'	Voer beveiligingsoperatie uit (PSO)
P1	1	'90h'	Zend hashcode terug
P2	1	'A0h'	Label: gegevensveld bevat voor hashfunctie relevante gegevensobjecten (DO's)
Lc	1	'XXh'	Lengte Lc van het volgende gegevensveld
#6	1	'90h'	Label voor de hashcode
#7	1	'XXh'	Lengte L van de hashcode '14h' voor tachograaftoepassingen van de eerste generatie (zie aanhangsel 11, deel A) '20h', '30h' of '40h' voor tachograaftoepassingen van de tweede generatie (zie aanhangsel 11, deel B)
#8-#(7+L)	L	'XX..XXh'	Hashcode

TCS_117 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien een aantal verwachte gegevensobjecten (zoals hierboven gespecificeerd) ontbreekt, wordt de verwerkingsstatus '**6987**' teruggezonden. Dit kan gebeuren wanneer een van de labels '90h' ontbreekt.

— Indien een aantal gegevensobjecten niet correct is, wordt de verwerkingsstatus '**6988**' teruggezonden. Deze fout treedt op wanneer het vereiste label aanwezig is, maar een lengte heeft die verschilt van: '14h' voor SHA-1, '20h' voor SHA-256, '30h' voor SHA-384, '40h' voor SHA-512 (tachograaftoepassing van de tweede generatie).

3.5.13 *PERFORM HASH OF FILE*

Dit commando voldoet niet aan ISO/IEC 7816-8. De CLA-byte van dit commando geeft dus een particulier gebruik van PERFORM SECURITY OPERATION/HASH.

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. Voor een bedrijfs- of controlekaart wordt dit commando geïmplementeerd op de in dit hoofdstuk vastgelegde wijze.

Dit commando kan al dan niet toegankelijk zijn in het stambestand (MF). Als dat het geval is, wordt het commando geïmplementeerd op de in dit hoofdstuk vastgelegde wijze: er wordt met andere woorden geen hashwaarde berekend, maar het commando wordt beëindigd met een geschikte foutcode.

TCS_118 Het PERFORM HASH of FILE-commando wordt gebruikt om het gegevensgebied van de thans geselecteerde transparante EF te hashen.

TCS_119 Een tachograafkaart ondersteunt dit commando alleen voor de hoofdbestanden (EF's) die worden opgesomd in hoofdstuk 4 onder DF Tachograaf en DF Tachograaf_G2, zij het met de volgende uitzondering: een tachograafkaart ondersteunt het commando niet voor de EF Sensor_Installation_Data van DF Tachograaf_G2.

TCS_120 Het resultaat van de hashbewerking wordt tijdelijk in de kaart opgeslagen. Het kan vervolgens worden gebruikt om een digitale handtekening van het bestand te krijgen met gebruikmaking van het PSO: COMPUTE DIGITAL SIGNATURE-commando.

TCS_121 De tijdelijk opgeslagen hashwaarde wordt verwijderd indien een nieuwe hashwaarde wordt berekend met behulp van het PSO: Hash of File-commando, indien een DF wordt geselecteerd, en indien de tachograafkaart wordt teruggesteld.

TCS_122 Tachograaftoepassingen van de eerste generatie ondersteunen SHA-1.

TCS_123 Tachograaftoepassingen van de tweede generatie ondersteunen SHA-1 en SHA-2 (256, 384 en 512 bits).

TCS_124 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'80h'	CLA
INS	1	'2Ah'	Voer beveiligingsoperatie uit (PSO)
P1	1	'90h'	Label: Hash
P2	1	'XXh'	P2: geeft aan welk algoritme wordt gebruikt om de gegevens van het thans geselecteerde transparante bestand te hashen: '00h' voor SHA-1 '01h' voor SHA-256 '02h' voor SHA-384 '03h' voor SHA-512

TCS_125 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien de geldige EF dit commando niet toestaat (EF Sensor_Installation_Data in DF Tachograaf_G2), wordt de verwerkingsstatus '**6985**' teruggezonden.

— Indien de geselecteerde EF beschadigd is (integriteitsfouten in bestandsattributen of opgeslagen gegevens), wordt de verwerkingsstatus '**6400**' of '**6581**' teruggezonden.

— Indien het geselecteerde bestand geen transparant bestand is of indien er geen geldige EF is, wordt de verwerkingsstatus '**6986**' teruggezonden.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

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. Deze kaarten hebben echter geen handtekeningsleutel. Bijgevolg wordt dit commando op deze kaarten niet met succes uitgevoerd, maar beëindigd met een geschikte foutcode.

Dit commando kan al dan niet toegankelijk zijn in het stambestand (MF). Als dat het geval is, wordt het commando beëindigd met een geschikte foutcode.

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

TCS_126 Dit commando berekent geen digitale handtekening van een eerder met het PSO: HASH-commando berekende hashcode.

TCS_127 De particuliere sleutel van de kaart wordt gebruikt om de digitale handtekening te berekenen en is impliciet bij de kaart bekend.

TCS_128 Tachograaftoepassingen van de eerste generatie gebruiken voor de digitale handtekening een paddingmethode overeenkomstig PKCS1 (zie aanhangsel 11 voor meer bijzonderheden).

TCS_129 Tachograaftoepassingen van de tweede generatie berekenen de digitale handtekening op basis van een elliptische kromme (zie aanhangsel 11 voor meer bijzonderheden).

TCS_130 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	CLA
INS	1	'2Ah'	Voer beveiligingsoperatie uit (PSO)
P1	1	'9Eh'	Terug te zenden digitale handtekening
P2	1	'9Ah'	Label: gegevensveld bevat te ondertekenen gegevens. Als geen gegevensveld opgenomen is, wordt aangenomen dat de gegevens al op de kaart aanwezig zijn (hashwaarde van bestand)
Le	1	'NNh'	Lengte van de verwachte handtekening

TCS_131 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
#1-#L	L	'XX..XXh'	Handtekening van de eerder berekende hashwaarde
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien de impliciet geselecteerde particuliere sleutel beschadigd is, wordt de verwerkingsstatus '**6400**' of '**6581**' teruggezonden.

— Indien de eerder met een Perform Hash of File-commando berekende hashwaarde niet beschikbaar is, wordt de verwerkingsstatus '**6985**' teruggezonden.

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Dit commando wordt gebruikt ter verificatie van de digitale handtekening die als invoer is opgegeven en waarvan de hashwaarde bij de kaart bekend is. Het handtekeningalgoritme is impliciet bij de kaart bekend.

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

Alleen de controlekaart is 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. Dit commando kan al dan niet toegankelijk zijn in het stambestand (MF).

TCS_132 Het VERIFY DIGITAL SIGNATURE-commando gebruikt altijd de door het voorafgaande MSE: SET DST-commando geselecteerde openbare sleutel en de voorafgaande, door een PSO: HASH-commando ingevoerde hashcode.

TCS_133 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	CLA
INS	1	'2Ah'	Voer beveiligingsoperatie uit (PSO)
P1	1	'00h'	
P2	1	'A8h'	Label: gegevensveld bevat voor verificatie relevante DO's
Lc	1	'83h'	Lengte Lc van het volgende gegevensveld
6	1	'9Eh'	Label voor digitale handtekening
#7-#8	2	'81 XXh'	Lengte van digitale handtekening: 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)
#9-#(8+L)	L	'XX..XXh'	Inhoud van de digitale handtekening

TCS_134 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— Indien de handtekeningverificatie mislukt, wordt de verwerkingsstatus '**6688**' teruggezonden. De verificatieprocedure wordt uiteengezet in aanhangsel 11.

— Indien geen openbare sleutel wordt geselecteerd, wordt de verwerkingsstatus '**6A88**' teruggezonden.

— Indien een aantal verwachte gegevensobjecten (zoals hierboven gespecificeerd) ontbreekt, wordt de verwerkingsstatus '**6987**' teruggezonden. Dit kan gebeuren wanneer een van de vereiste labels ontbreekt.

— Indien geen hashcode beschikbaar is om het commando te verwerken (als gevolg van een voorafgaand PSO: Hash-commando), wordt de verwerkingsstatus '**6985**' teruggezonden.

— Indien een aantal gegevensobjecten niet correct is, wordt de verwerkingsstatus '**6988**' teruggezonden. Dit kan gebeuren wanneer de lengte van een van vereiste gegevensobjecten niet correct is.

— Indien de geselecteerde openbare sleutel beschadigd is, wordt de verwerkingsstatus '**6400**' of '**6581**' teruggezonden.

3.5.16 *PROCESS DSRC MESSAGE*

Dit commando wordt gebruikt om de integriteit en authenticiteit van het DSRC-bericht te verifiëren, alsook om de gegevens te decoderen die via de DSRC-verbinding worden overgebracht van een VU naar een controleautoriteit of een werkplaats. De kaart bepaalt de coderingssleutel en de MAC-sleutel waarmee het DSRC-bericht is beveiligd (zie beschrijving in aanhangsel 11, deel B, hoofdstuk 13).

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

Op andere soorten tachograafkaarten kan dit commando al dan niet worden geïmplementeerd. Deze kaarten hebben echter geen DSRC-hoofdsleutel („master key"). Bijgevolg wordt dit commando op deze kaarten niet met succes uitgevoerd, maar beëindigd met een geschikte foutcode.

Dit commando kan al dan niet toegankelijk zijn in MF en/of in DF Tachograaf. Als dat het geval is, wordt het commando beëindigd met een geschikte foutcode.

TCS_135 De DSRC-hoofdsleutel is alleen toegankelijk in DF Tachograaf G2; de controle- en werkplaatskaart ondersteunen met andere woorden alleen een succesvolle uitvoering van dit commando in DF Tachograaf G2.

TCS_136 Dit commando decodeert alleen de DSRC-gegevens en controleert de cryptografische controlesom, zij het zonder de invoergegevens te interpreteren.

TCS_137 De volgorde van de gegevensobjecten (DO's) in het gegevensveld van het commando wordt vastgelegd in deze specificatie.

TCS_138 **Commandobericht**

Byte	Lengte	Waarde	Omschrijving
CLA	1	'80h'	Particuliere CLA
INS	1	'2Ah'	Voer beveiligingsoperatie uit (PSO)
P1	1	'80h'	Antwoordgegevens: ongecodeerde waarde
P2	1	'B0h'	Commandogegevens: ongecodeerde waarde van met BER-TLV gecodeerde gegevens, met inbegrip van SM DO's
Lc	1	'NNh'	Lengte Lc van het volgende gegevensveld
#6-#(5+L)	L	'87h' + L_{87} + 'XX..XXh'	Met DER-TLV gecodeerde padding-indicatorbyte gevolgd door gecodeerde payloadgegevens van de tachograaf. Voor de padding-indicatorbyte wordt de waarde '00h' („geen nadere details" overeenkomstig ISO/IEC 7816-4:2013, tabel 52) gebruikt. Zie aanhangsel 11, deel B, hoofdstuk 13 voor meer informatie over het coderingsmechanisme. De toegestane waarden voor de lengte L_{87} zijn veelvouden van de AES-bloklengte + 1 voor de padding-indicatorbyte, dat wil zeggen van 17 bytes tot en met 193 bytes. *Opmerking:* zie ISO/IEC 7816-4:2013, tabel 49 voor het SM-gegevensobject met label '87h'.
		'81h' + '10h'	Met DER-TLV gecodeerd referentiemodel (template) voor vertrouwelijkheidscontrole, waarin de samenvoeging van de volgende gegevenselementen is ingesloten (zie DSRCSecurityData in aanhangsel 1 en zie aanhangsel 11, deel B, hoofdstuk 13): — tijdaanduiding van 4 bytes — teller van 3 bytes — VU-serienummer van 8 bytes — versie van DSRC-hoofdsleutel van 1 byte *Opmerking:* zie ISO/IEC 7816-4:2013, tabel 49 voor het SM-gegevensobject met label '81h'.
		'8Eh' + L_{8E} + 'XX..XXh'	Met DER-TLV gecodeerde MAC van het DSRC-bericht. Zie aanhangsel 11, deel B, hoofdstuk 13 voor meer informatie over het MAC-algoritme en de berekening van deze berichtauthenticatiecode. *Opmerking:* zie ISO/IEC 7816-4:2013, tabel 49 voor het SM-gegevensobject met label '8Eh'.

TCS_139 **Antwoordbericht**

Byte	Lengte	Waarde	Omschrijving
#1-#L	L	'XX..XXh'	Afwezige gegevens (in geval van fout) of gedecodeerde gegevens (padding verwijderd)
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '**9000**' terug.

— '**6A80**' wijst op onjuiste parameters in het gegevensveld van het commando (ook gebruikt wanneer de gegevensobjecten niet in de voorgeschreven volgorde worden verzonden).

— '**6A88**' geeft aan dat het genoemde gegeven (dat wil zeggen de genoemde DSRC-hoofdsleutel) niet beschikbaar is.

— '**6900**' geeft aan dat de verificatie van de cryptografische controlesom of de decodering van de gegevens is mislukt.

4. STRUCTUUR VAN DE TACHOGRAAFKAARTEN

In dit punt worden de bestandsstructuren van de tachograafkaarten gespecificeerd voor het opslaan van toegankelijke gegevens.

De interne bestandsstructuren die specifiek zijn voor de fabrikant van de kaart, zoals de beginlabels (headers) van bestanden, worden niet gespecificeerd, evenmin als de opslag en verwerking van gegevenselementen voor intern gebruik zoals `EuropeanPublicKey`, `CardPrivateKey`, `TdesSessionKey` of `WorkshopCardPin`.

TCS_140 Een tachograafkaart van de tweede generatie bevat het stambestand (MF) alsook een gelijksoortige tachograaftoepassing van de eerste en de tweede generatie (bijvoorbeeld toepassingen voor de bestuurderskaart).

TCS_141 Een tachograafkaart ondersteunt ten minste het minimumaantal registraties dat voor de bijbehorende toepassingen is gespecificeerd, en ondersteunt niet meer registraties dan het maximumaantal dat voor de bijbehorende tachograaftoepassingen is gespecificeerd.

Het maximum- en minimumaantal registraties voor de verschillende tachograaftoepassingen worden in dit hoofdstuk gespecificeerd.

Zie punt 3.3 voor meer informatie over de beveiligingsvoorwaarden die in dit hoofdstuk worden toegepast op de toegangsregels. Doorgaans verwijst de toegangsmodus van de Read-functie naar het READ BINARY-commando met een even en — voor zover ondersteund — oneven instructiebyte (INS), met uitzondering van de EF Sensor_Installation_Data op de werkplaatskaart (zie TCS_156 en TCS_160). De toegangsmodus van de Update-functie verwijst naar het Update Binary-commando met een even en — voor zover ondersteund — oneven instructiebyte (INS). De toegangsmodus voor de Select-functie verwijst naar het SELECT-commando.

4.1. Stambestand (MF)

TCS_142 Na personalisatie heeft het stambestand (MF) de onderstaande permanente bestandsstructuur en bestandstoegangsregels:

Opmerking: de korte EF-identificator SFID wordt opgegeven als decimaal getal; zo komt de waarde '30' overeen met '11110' in binaire notatie.

			Toegangsregels	
Bestand	**Bestands-identificator**	**SFID**	**Lezen/selecteren**	**Bijwerken**
MF	'3F00h'			
├─ EF ICC	'0002h'		ALW	NEV
├─ EF IC	'0005h'		ALW	NEV
├─ EF DIR	'2F00h'	30	ALW	NEV
├─ EF ATR/INFO (conditional)	'2F01h'	29	ALW	NEV
├─ EF Extended_Length (conditional)	'0006h'	28	ALW	NEV
├─ DF Tachograph	'0500h'		SC1	
└─ DF Tachograph_G2			SC1	

In deze tabel wordt de volgende afkorting voor de beveiligingsvoorwaarde gebruikt:

SC1 ALW OR SM-MAC-G2

TCS_143 Alle EF-structuren zijn transparant.

TCS_144 Het stambestand (MF) heeft de onderstaande gegevensstructuur:

Bestand/gegevenselement	No of Records	Size (bytes) Min	Max	Default Values
MF		*63*	*184*	
EF ICC		*25*	*25*	
CardIccIdentification		*25*	*25*	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		*8*	*8*	
CardChipIdentification		*8*	*8*	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
EF DIR		*20*	*20*	
See TCS_145		*20*	*20*	{00..00}
EF ATR/INFO		*7*	*128*	
See TCS_146		*7*	*128*	{00..00}
EF EXTENDED_LENGTH		*3*	*3*	
See TCS_147		*3*	*3*	{00..00}
DF Tachograph				
DF Tachograph_G2				

TCS_145 Het hoofdbestand EF DIR bevat de volgende toepassingsgerelateerde gegevensobjecten: '61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54'

TCS_146 Het hoofdbestand EF ATR/INFO is aanwezig indien de tachograafkaart in het ATR aangeeft dat velden met uitgebreide lengte worden ondersteund. In dit geval bevat EF ATR/INFO het gegevensobject van informatie met uitgebreide lengte (DO '7F66'), zoals gespecificeerd in ISO/IEC 7816-4:2013 onder 12.7.1.

TCS_147 Het hoofdbestand EF Extended_Length is aanwezig indien de tachograafkaart in het ATR aangeeft dat velden met uitgebreide lengte worden ondersteund. In dit geval bevat het hoofdbestand (EF) het volgende gegevensobject: '02 01 xx' waarbij 'xx' aangeeft of velden met uitgebreide lengte worden ondersteund voor het protocol T = 1 en/of T = 0.

De waarde '01' betekent dat velden met uitgebreide lengte worden ondersteund voor het protocol T = 1.

De waarde '10' betekent dat velden met uitgebreide lengte worden ondersteund voor het protocol T = 0.

De waarde '11' betekent dat velden met uitgebreide lengte worden ondersteund voor het protocol T = 1 en T = 0.

4.2. Toepassingen voor de bestuurderskaart

4.2.1 *Toepassing van de eerste generatie voor de bestuurderskaart*

TCS_148 Na personalisatie heeft de toepassing van de eerste generatie voor de bestuurderskaart de onderstaande permanente bestandsstructuur en bestandstoegangsregels:

File	Bestands-identificator	Toegangsregels		
		Lezen	Selecteren	Bijwerken
└─DF Tachograph	'0500h'		SC1	
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	SC2	SC1	NEV
├─EF Card_Download	'050Eh'	SC2	SC1	SC1
├─EF Driving_Licence_Info	'0521h'	SC2	SC1	NEV
├─EF Events_Data	'0502h'	SC2	SC1	SC3
├─EF Faults_Data	'0503h'	SC2	SC1	SC3
├─EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├─EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├─EF Places	'0506h'	SC2	SC1	SC3
├─EF Current_Usage	'0507h'	SC2	SC1	SC3
├─EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└─EF Specific_Conditions	'0522h'	SC2	SC1	SC3

In deze tabel worden de volgende afkortingen voor de beveiligingsvoorwaarden gebruikt:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

TCS_149 Alle EF-structuren zijn transparant.

TCS_150 De tachograaftoepassing van de eerste generatie voor de bestuurderskaart heeft de onderstaande gegevensstructuur:

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
DF Tachograph		*11378*	*24926*	
EF Application_Identification		*10*	*10*	
DriverCardApplicationIdentification		*10*	*10*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				

├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
└CardDriverActivity		*5548*	*13780*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
└CardVehiclesUsed		*2606*	*6202*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*2604*	*6200*	
└─CardVehicleRecord	n_3	*31*	*31*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
└─vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
└CardPlaceDailyWorkPeriod		*841*	*1121*	
├─placePointerNewestRecord		1	1	{00}
└─placeRecords		*840*	*1120*	
└─PlaceRecord	n_4	*10*	*10*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
└─vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
└SpecificConditionRecord	56	*5*	*5*	
├─entryTime		4	4	{00..00}
└─SpecificConditionType		1	1	{00}

TCS_151 De volgende waarden geven de grootte in de bovenstaande tabel aan en komen overeen met het minimum- en maximumaantal registraties dat de gegevensstructuur van de bestuurderskaart moet gebruiken voor een toepassing van de eerste generatie:

		Min.	**Max.**
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 bytes (28 dagen * 93 wijzigingen van activiteit)	13 776 bytes (28 dagen * 240 wijzigingen van activiteit)

4.2.2 *Toepassing van de tweede generatie voor de bestuurderskaart*

TCS_152 Na personalisatie heeft de toepassing van de tweede generatie voor de bestuurderskaart de onderstaande permanente bestandsstructuur en bestandstoegangsregels:

Opmerking: de korte EF-identificator SFID wordt opgegeven als decimaal getal; zo komt de waarde '30' overeen met '11110' in binaire notatie.

			Toegangsregels	
File	**Bestands-identificator**	**SFID**	**Lezen/selecteren**	**Bijwerken**
└─ DF Tachograph_G2			SC1	
├─ EF Application_Identification	'0501h'	1	SC1	NEV
├─ EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─ EF CardSignCertificate	'C101h'	3	SC1	NEV
├─ EF CA_Certificate	'C108h'	4	SC1	NEV
├─ EF Link_Certificate	'C109h'	5	SC1	NEV
├─ EF Identification	'0520h'	6	SC1	NEV
├─ EF Card_Download	'050Eh'	7	SC1	SC1
├─ EF Driving_Licence_Info	'0521h'	10	SC1	NEV
├─ EF Events_Data	'0502h'	12	SC1	SM-MAC-G2
├─ EF Faults_Data	'0503h'	13	SC1	SM-MAC-G2
├─ EF Driver_Activity_Data	'0504h'	14	SC1	SM-MAC-G2
├─ EF Vehicles_Used	'0505h'	15	SC1	SM-MAC-G2
├─ EF Places	'0506h'	16	SC1	SM-MAC-G2
├─ EF Current_Usage	'0507h'	17	SC1	SM-MAC-G2
├─ EF Control_Activity_Data	'0508h'	18	SC1	SM-MAC-G2
├─ EF Specific_Conditions	'0522h'	19	SC1	SM-MAC-G2
├─ EF VehicleUnits_Used	'0523h'	20	SC1	SM-MAC-G2
└─ EF GNSS_Places	'0524h'	21	SC1	SM-MAC-G2

In deze tabel wordt de volgende afkorting voor de beveiligingsvoorwaarde gebruikt:

SC1 ALW OR SM-MAC-G2

TCS_153 Alle EF-structuren zijn transparant.

TCS_154 De toepassing van de tweede generatie voor de bestuurderskaart heeft de onderstaande gegevensstructuur:

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
DF Tachograph_G2		*19510*	*39306*	
EF Application_Identification		*15*	*15*	
DriverCardApplicationIdentification		*15*	*15*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*1584*	*3168*	
CardEventData		*1584*	*3168*	
cardEventRecords	11	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	

faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*4034*	*9602*	
CardVehiclesUsed		*4034*	*9602*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*4032*	*9600*	
CardVehicleRecord	n_3	*48*	*48*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		17	17	{20..20}
EF Places		*1766*	*2354*	
CardPlaceDailyWorkPeriod		*1766*	*2354*	
placePointerNewestRecord		2	2	{00 00}
placeRecords		*1764*	*2352*	
PlaceRecord	n_4	*21*	*21*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
entryGNSSPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

EF Specific_Conditions		*282*	*562*	
SpecificConditions		*282*	*562*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		*280*	*560*	
SpecificConditionRecord	n_9	*5*	*5*	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF VehicleUnits_Used		*842*	*2002*	
CardVehicleUnitsUsed		*842*	*2002*	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		*840*	*2000*	
CardVehicleUnitRecord	n_7	*10*	*10*	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*3782*	*5042*	
GNSSContinuousDriving		*3782*	*5042*	
gnssCDPointerNewestRecord		2	2	{00 00}
gnssContinuousDrivingRecords		3780	5040	{00}
GNSSContinuousDrivingRecord	n_8	*15*	*15*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}

TCS_155 De volgende waarden geven de grootte in de bovenstaande tabel aan en komen overeen met het minimum- en maximumaantal registraties dat de gegevensstructuur van de bestuurderskaart moet gebruiken voor een toepassing van de tweede generatie:

		Min.	**Max.**
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 bytes (28 dagen * 93 wijzigingen van activiteit)	13 776 bytes (28 dagen * 240 wijzigingen van activiteit)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. Toepassingen voor de werkplaatskaart

4.3.1 *Toepassing van de eerste generatie voor de werkplaatskaart*

TCS_156 Na personalisatie heeft de toepassing van de eerste generatie voor de werkplaatskaart de onderstaande permanente bestandsstructuur en bestandstoegangsregels:

		Access rules		
File	**File ID**	**Read**	**Select**	**Update**
└─DF Tachograph	'0500h'		SC1	
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	SC2	SC1	NEV
├─EF Card_Download	'0509h'	SC2	SC1	**SC1**
├─EF Calibration	'050Ah'	SC2	SC1	SC3
├─EF Sensor_Installation_Data	'050Bh'	**SC4**	SC1	NEV
├─EF Events_Data	'0502h'	SC2	SC1	SC3
├─EF Faults_Data	'0503h'	SC2	SC1	SC3
├─EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├─EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├─EF Places	'0506h'	SC2	SC1	SC3
├─EF Current_Usage	'0507h'	SC2	SC1	SC3
├─EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└─EF Specific_Conditions	'0522h'	SC2	SC1	SC3

In deze tabel worden de volgende afkortingen voor de beveiligingsvoorwaarden gebruikt:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

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

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

TCS_157 Alle EF-structuren zijn transparant.

TCS_158 De toepassing van de eerste generatie voor de werkplaatskaart heeft de onderstaande gegevensstructuur:

File / Data element	No of Records	Size (Bytes) Min	Size (Bytes) Max	Default Values
DF Tachograph		*11055*	*29028*	
EF Application_Identification		*11*	*11*	
WorkshopCardApplicationIdentification		*11*	*11*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}

EF Sensor_Installation_Data		*16*	*16*	
└SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
└CardEventData		*432*	*432*	
└cardEventRecords	6	*72*	*72*	
└CardEventRecord	n_1	*24*	*24*	
├eventType		1	1	{00}
├eventBeginTime		4	4	{00..00}
├eventEndTime		4	4	{00..00}
└eventVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
└CardFaultData		*288*	*288*	
└cardFaultRecords	2	*144*	*144*	
└CardFaultRecord	n_2	*24*	*24*	
├faultType		1	1	{00}
├faultBeginTime		4	4	{00..00}
├faultEndTime		4	4	{00..00}
└faultVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
└CardDriverActivity		*202*	*496*	
├activityPointerOldestDayRecord		2	2	{00 00}
├activityPointerNewestRecord		2	2	{00 00}
└activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
└CardVehiclesUsed		*126*	*250*	
├vehiclePointerNewestRecord		2	2	{00 00}
└cardVehicleRecords		*124*	*248*	
└CardVehicleRecord	n_3	*31*	*31*	
├vehicleOdometerBegin		3	3	{00..00}
├vehicleOdometerEnd		3	3	{00..00}
├vehicleFirstUse		4	4	{00..00}
├vehicleLastUse		4	4	{00..00}
├vehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
└vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
└CardPlaceDailyWorkPeriod		*61*	*81*	
├placePointerNewestRecord		1	1	{00}
└placeRecords		*60*	*80*	
└PlaceRecord	n_4	*10*	*10*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
└vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}

EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*10*	*10*	
SpecificConditionRecord	*2*	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_159 De volgende waarden geven de grootte in de bovenstaande tabel aan en komen overeen met het minimum- en maximumaantal registraties dat de gegevensstructuur van de werkplaatskaart moet gebruiken voor een toepassing van de eerste generatie:

		Min.	**Max.**
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bytes (1 dag * 93 wijzigingen van activiteit)	492 bytes (1 dag * 240 wijzigingen van activiteit)

4.3.2 *Toepassing van de tweede generatie voor de werkplaatskaart*

TCS_160 Na personalisatie heeft de toepassing van de tweede generatie voor de werkplaatskaart de onderstaande permanente bestandsstructuur en bestandstoegangsregels:

Opmerking: de korte EF-identificator SFID wordt opgegeven als decimaal getal; zo komt de waarde '30' overeen met '11110' in binaire notatie.

			Access rules		
File	**File ID**	**SFID**	**Read**	**Select**	**Update**
└─DF Tachograph_G2			SC1	SC1	
├─EF Application_Identification	'0501h'	1	SC1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	SC1	NEV
├─EF CardSignCertificate	'C101h'	3	SC1	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	SC1	NEV
├─EF Identification	'0520h'	6	SC1	SC1	NEV
├─EF Card_Download	'0509h'	7	SC1	SC1	SC1
├─EF Calibration	'050Ah'	10	SC1	SC1	SM-MAC-G2
├─EF Sensor_Installation_Data	'050Bh'	11	**SC5**	SM-MAC-G2	NEV
├─EF Events_Data	'0502h'	12	SC1	SC1	SM-MAC-G2
├─EF Faults_Data	'0503h'	13	SC1	SC1	SM-MAC-G2
├─EF Driver_Activity_Data	'0504h'	14	SC1	SC1	SM-MAC-G2
├─EF Vehicles_Used	'0505h'	15	SC1	SC1	SM-MAC-G2
├─EF Places	'0506h'	16	SC1	SC1	SM-MAC-G2
├─EF Current_Usage	'0507h'	17	SC1	SC1	SM-MAC-G2
├─EF Control_Activity_Data	'0508h'	18	SC1	SC1	SM-MAC-G2
├─EF Specific_Conditions	'0522h'	19	SC1	SC1	SM-MAC-G2
├─EF VehicleUnits_Used	'0523h'	20	SC1	SC1	SM-MAC-G2
└─EF GNSS_Places	'0524h'	21	SC1	SC1	SM-MAC-G2

In deze tabel worden de volgende afkortingen voor de beveiligingsvoorwaarden gebruikt:

SC1 ALW OR SM-MAC-G2

SC5 Voor het READ BINARY-commando met even instructiebyte (INS): SM-C-MAC-G2 AND SM-R-ENC-MAC-G2

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

TCS_161 Alle EF-structuren zijn transparant.

TCS_162 De tachograaftoepassing van de tweede generatie voor de werkplaatskaart heeft de onderstaande gegevensstructuur:

File / Data element	No of Records	Size (Bytes) Min	Size (Bytes) Max	Default Values
DF Tachograph_G2		*17837*	*47163*	
EF Application_Identification		*17*	*17*	
WorkshopCardApplicationIdentification		*17*	*17*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfCalibrationRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*14788*	*42844*	
WorkshopCardCalibrationData		*14788*	*42844*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*14784*	*42840*	
WorkshopCardCalibrationRecord	n_5	*168*	*168*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}

oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
sensorGNSSSerialNumber		8	8	{00..00}
rcmSerialNumber		8	8	{00..00}
vuAbility		1	1	{00}
sealDataCard		46	46	
noOfSealRecords		1	1	{00}
SealRecords		45	45	
SealRecord	5	9	9	
equipmentType		1	1	{00}
extendedSealIdentifier		8	8	{00..00}
EF Sensor_Installation_Data		*18*	*102*	
SensorInstallationSecData		18	102	{00..00}
EF Events_Data		*792*	*792*	
CardEventData		*792*	*792*	
cardEventRecords	11	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*194*	*386*	
CardVehiclesUsed		*194*	*386*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*192*	*384*	
CardVehicleRecord	n_3	*48*	*48*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		*17*	17	{20..20}
EF Places		*128*	*170*	

└CardPlaceDailyWorkPeriod		*128*	*170*	
├placePointerNewestRecord		2	2	{00 00}
└placeRecords		*126*	*168*	
└PlaceRecord	n_4	*21*	*21*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
├vehicleOdometerValue		3	3	{00..00}
└entryGNSSPlaceRecord		11	11	{00..00}
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}
EF VehicleUnits_Used		*42*	*42*	
└CardVehicleUnitsUsed		*42*	*82*	
├vehicleUnitPointerNewestRecord		2	2	{00 00}
└cardVehicleUnitRecords		*40*	*80*	
└CardVehicleUnitRecord	n_7	*10*	*10*	
├timeStamp		4	4	{00..00}
├manufacturerCode		1	1	{00..00}
├deviceID		1	1	{00..00}
└vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*262*	*362*	
└GNSSContinuousDriving		*262*	*362*	
├gnssCDPointerNewestRecord		2	2	{00 00}
└gnssContinuousDrivingRecords		*260*	*360*	
└GNSSContinuousDrivingRecord	n_8	*15*	*15*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		11	11	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Specific_Conditions		*12*	*22*	
└SpecificConditions		*12*	*22*	
├conditionPointerNewestRecord		2	2	{00 00}
└specificConditionRecords		10	20	
└SpecificConditionRecord	n_9	*5*	*5*	
├entryTime		4	4	{00..00}
└specificConditionType		1	1	{00}

TCS_163 De volgende waarden geven de grootte in de bovenstaande tabel aan en komen overeen met het minimum- en maximumaantal registraties dat de gegevensstructuur van de werkplaatskaart moet gebruiken voor een toepassing van de tweede generatie:

		Min.	Max.
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bytes (1 dag * 93 wijzigingen van activiteit)	492 bytes (1 dag * 240 wijzigingen van activiteit)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Toepassingen voor de controlekaart

4.4.1 *Toepassing van de eerste generatie voor de controlekaart*

TCS_164 Na personalisatie heeft de toepassing van de eerste generatie voor de controlekaart de onderstaande permanente bestandsstructuur en bestandstoegangsregels:

		Access rules		
File	**File ID**	**Read**	**Select**	**Update**
└─DF Tachograph	'0500h'			
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	**SC6**	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	SC2	SC1	SC3

In deze tabel worden de volgende afkortingen voor de beveiligingsvoorwaarden gebruikt:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_165 Alle EF-structuren zijn transparant.

TCS_166 De toepassing van de eerste generatie voor de controlekaart heeft de onderstaande gegevensstructuur:

File / Data element	No of Records	Size (Bytes) Min	Max	
DF Tachograph		*11186*	*24526*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 De volgende waarden geven de grootte in de bovenstaande tabel aan en komen overeen met het minimum- en maximumaantal registraties dat de gegevensstructuur van de controlekaart moet gebruiken voor een toepassing van de eerste generatie:

		Min.	Max.
n_7	NoOfControlActivityRecords	230	520

4.4.2 *Toepassing van de tweede generatie voor de controlekaart*

TCS_168 Na personalisatie heeft de toepassing van de tweede generatie voor de controlekaart de onderstaande permanente bestandsstructuur en bestandstoegangsregels:

Opmerking: de korte EF-identificator SFID wordt opgegeven als decimaal getal; zo komt de waarde '30' overeen met '11110' in binaire notatie.

File	File ID	SFID	Access rules	
			Read / Select	Update
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	14	SC1	SM-MAC-G2

In deze tabel wordt de volgende afkorting voor de beveiligingsvoorwaarde gebruikt:

SC1 ALW OR SM-MAC-G2

TCS_169 Alle EF-structuren zijn transparant.

TCS_170 De toepassing van de tweede generatie voor de controlekaart heeft de onderstaande gegevensstructuur:

File / Data element	No of Records	Size (Bytes) Min	Max	
DF Tachograph_G2		*11410*	*25161*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_171 De volgende waarden geven de grootte in de bovenstaande tabel aan en komen overeen met het minimum- en maximumaantal registraties dat de gegevensstructuur van de controlekaart moet gebruiken voor een toepassing van de tweede generatie:

		Min.	Max.
n_7	NoOfControlActivityRecords	230	520

4.5. Toepassingen voor de bedrijfskaart

4.5.1 *Toepassing van de eerste generatie voor de bedrijfskaart*

TCS_172 Na personalisatie heeft de toepassing van de eerste generatie voor de bedrijfskaart de onderstaande permanente bestandsstructuur en bestandstoegangsregels:

		Access rules		
File	**File ID**	**Read**	**Select**	**Update**
DF Tachograph	'0500h'		SC1	
EF Application_Identification	'0501h'	SC2	SC1	NEV
EF Card_Certificate	'C100h'	SC2	SC1	NEV
EF CA_Certificate	'C108h'	SC2	SC1	NEV
EF Identification	'0520h'	**SC6**	SC1	NEV
EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

In deze tabel worden de volgende afkortingen voor de beveiligingsvoorwaarden gebruikt:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_173 Alle EF-structuren zijn transparant.

TCS_174 De toepassing van de eerste generatie voor de bedrijfskaart heeft de onderstaande gegevensstructuur:

File / Data element	**No of Records**	**Size (bytes) Min**	**Max**	**Default Values**
DF Tachograph		*11114*	*24454*	
EF Application_Identification		*5*	*5*	
CompanyCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*139*	*139*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		*74*	*74*	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		*10580*	*23920*	
companyActivityRecord	n_8	*46*	*46*	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_175 De volgende waarden geven de grootte in de bovenstaande tabel aan en komen overeen met het minimum- en maximumaantal registraties dat de gegevensstructuur van de bedrijfskaart moet gebruiken voor een toepassing van de eerste generatie:

		Min.	**Max.**
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *Toepassing van de tweede generatie voor de bedrijfskaart*

TCS_176 Na personalisatie heeft de toepassing van de tweede generatie voor de bedrijfskaart de onderstaande permanente bestandsstructuur en bestandstoegangsregels:

Opmerking: de korte EF-identificator SFID wordt opgegeven als decimaal getal; zo komt de waarde '30' overeen met '11110' in binaire notatie.

			Access rules	
File	**File ID**	**SFID**	**Read / Select**	**Update**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Company_Activity_Data	'050Dh'	14	SC1	SM-MAC-G2

In deze tabel wordt de volgende afkorting voor de beveiligingsvoorwaarde gebruikt:

SC1 ALW OR SM-MAC-G2

TCS_177 Alle EF-structuren zijn transparant.

TCS_178 De toepassing van de tweede generatie voor de bedrijfskaart heeft de onderstaande gegevensstructuur:

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
DF Tachograph_G2		*11338*	*25089*	
EF Application_Identification		*5*	*5*	
CompanyCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*139*	*139*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		*74*	*74*	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		*10580*	*23920*	
companyActivityRecord	n_8	*46*	*46*	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_179 De volgende waarden geven de grootte in de bovenstaande tabel aan en komen overeen met het minimum- en maximumaantal registraties dat de gegevensstructuur van de bedrijfskaart moet gebruiken voor een toepassing van de tweede generatie:

		Min.	Max.
n_8	NoOfCompanyActivityRecords	230	520

Aanhangsel 3

PICTOGRAMMEN

PIC_001 Het controleapparaat kan naar keuze gebruik maken van de volgende pictogrammen en combinaties van pictogrammen (of pictogrammen of combinaties daarvan die voldoende gelijkenis vertonen om ermee vereenzelvigd te worden):

1. BASISPICTOGRAMMEN

	Personen	**Activiteiten**	**Werkingsmodi**
	Bedrijf		Bedrijfsmodus
	Controleur	Controle	Controlemodus
	Bestuurder	Rijden	Operationele modus
	Werkplaats/controlestation	Controle/kalibrering	Kalibreringsmodus
	Fabrikant		
	Activiteiten	**Duur**	
	Beschikbaar	Lopende periode van beschikbaarheid	
	Rijden	Ononderbroken rijtijd	
	Rust	Lopende rustperiode	
	Andere werkzaamheden	Lopende werkperiode	
	Pauze	Cumulatieve pauzetijd	
	Onbekend		
	Apparatuur	**Functies**	
	Lezer bestuurder		
	Lezer bijrijder		
	Kaart		
	Klok		
	Display	Weergeven	
	Externe opslag	Downloaden	
	Stroomvoorziening		
	Printer/afdruk	Afdrukken	
	Sensor		
	Bandenmaat		
	Voertuig/voertuigunit		
	GNSS-module		
	Voorziening voor detectie op afstand		
	ITS-interface		
	Specifieke omstandigheden		
OUT	Niet verplicht		
	Vervoer per veerboot/trein		

Diversen

!	Voorvallen	✕	Fouten
⏵	Begin van de dagelijkse werkperiode	⏹	Einde van de dagelijkse werkperiode
●	Plaats		
M	Manuele invoer van werkzaamheden bestuurder		
🔒	Beveiliging		
>	Snelheid		
🕒	Tijd		
Σ	Totaal/overzicht		

Kwalificerende elementen

24 h	Dagelijks
|	Wekelijks
||	Om de twee weken
+	Van of tot

2. PICTOGRAMCOMBINATIES

Diversen

●	Controleplaats		
● ⏵	Plaats begin dagelijkse werkperiode	⏹ ●	Plaats einde dagelijkse werkperiode
🕒 +	Van (tijd)	+ 🕒	Tot (tijd)
🚙 +	Van voertuig		
OUT +	Niet verplicht (begin)	+ OUT	Niet verplicht (einde)

Kaarten

🪪	Bestuurderskaart
🏢 🪪	Bedrijfskaart
● 🪪	Controlekaart
T 🪪	Werkplaatskaart
🪪 – – –	Geen kaart

Rijden

🪪 🪪	Rijden met een team
🪪 |	Rijtijd van een week
🪪 ||	Rijtijd van twee weken

Afdrukken

24 h 🪪 🖨	Dagelijkse afdruk van de kaart van de activiteiten van de bestuurder
24 h 🚙 🖨	Dagelijkse afdruk van de voertuigunit van de activiteiten van de bestuurder
! ✕ 🪪 🖨	Afdruk van de kaart van voorvallen en fouten
! ✕ 🚙 🖨	Afdruk van de voertuigunit van voorvallen en fouten
T 🕒 🖨	Afdruk van technische gegevens
> > 🖨	Afdruk van snelheidsoverschrijding.

Voorvallen

	Inbrengen van een ongeldige kaart
	Kaartconflict
	Tijdsoverlapping
	Rijden zonder een geschikte kaart
	Inbrengen van de kaart tijdens het rijden
	Laatste kaartsessie niet correct afgesloten
	Snelheidsoverschrijding
	Onderbreking in de stroomvoorziening
	Fout in de bewegingsgegevens
	Tegenstrijdige bewegingsgegevens
	Inbreuk op de beveiliging
	Tijdafstelling (door werkplaats)
	Controle op snelheidsoverschrijding

Fouten

	Kaartfout (lezer van de bestuurder)
	Kaartfout (lezer van de bijrijder)
	Displayfout
	Downloadfout
	Printerfout
	Sensorfout
	Interne fout in de VU
	GNSS-fout
	Fout in de detectie op afstand

Procedure bij manuele invoer

	Nog altijd dezelfde dagelijkse werkperiode?
	Einde van de voorafgaande werkperiode?
	Bevestig plaats van het einde van de werkperiode of voer deze in
	Voer begintijd in
	Voer plaats van het begin van de werkperiode in.

Opmerking: Aanvullende pictogramcombinaties voor het vormen van een afdrukblok of recordidentificatiesymbolen worden in aanhangsel 4 gedefinieerd.

Aanhangsel 4

AFDRUKKEN

INHOUDSOPGAVE

1. ALGEMEEN 243
2. SPECIFICATIE VAN GEGEVENSBLOKKEN 243
3. AFDRUKSPECIFICATIES 250
3.1. Dagelijkse afdruk van de kaart met de bestuurdersactiviteiten 250
3.2. Dagelijkse afdruk van de VU met de bestuurdersactiviteiten 251
3.3. Afdruk van de kaart van voorvallen en fouten 252
3.4. Afdruk van de voertuigunit van voorvallen en fouten 252
3.5. Afdruk van technische gegevens 253
3.6. Afdruk van snelheidsoverschrijding 253
3.7. Geschiedenis van ingebrachte kaarten 254

1. ALGEMEEN

Elke afdruk wordt opgebouwd door het achter elkaar plaatsen van diverse gegevensblokken, mogelijk geïdentificeerd met een blokidentificatiesymbool.

Een gegevensblok bevat een of meer records, mogelijk geïdentificeerd met een recordidentificatiesymbool.

PRT_001 Wanneer een blokidentificatiesymbool onmiddellijk voorafgaat aan een recordidentificatiesymbool, wordt het recordidentificatiesymbool niet afgedrukt.

PRT_002 Als een gegevensbestanddeel onbekend is of niet afgedrukt mag worden wegens gegevenstoegangsrechten, worden in plaats daarvan spaties afgedrukt.

PRT_003 Als de inhoud van een volledige regel onbekend is of niet afgedrukt hoeft te worden, wordt de volledige regel weggelaten.

PRT_004 Numerieke gegevensvelden worden rechts uitgelijnd afgedrukt, met een spatie voor duizendtallen en miljoenen en zonder voorafgaande nullen.

PRT_005 Gegevensvelden met opeenvolgende tekens worden links uitgelijnd afgedrukt en opgevuld met spaties tot de lengte van het gegevensbestanddeel of, indien nodig, afgekapt tot de lengte van het gegevensbestanddeel (namen en adressen).

PRT_006 Als een regel wordt afgebroken als gevolg van een lange tekst, moet een bijzonder teken (een punt op halve regelhoogte, "•") worden afgedrukt als eerste teken van de nieuwe regel.

2. SPECIFICATIE VAN GEGEVENSBLOKKEN

In dit hoofdstuk zijn de onderstaande opmaakcriteria gehanteerd:

— **vet** gedrukte letters geven standaardtekst aan die afgedrukt moet worden (afdrukken gebeurt in gewone letters);

— gewone letters geven variabelen aan (pictogrammen of gegevens) die door hun afdrukwaarden moeten worden vervangen;

— namen van variabelen zijn onderstreept om de lengte van het gegevensbestanddeel te tonen die voor de variabele ter beschikking is;

— datums worden gespecificeerd in de vorm "dd/mm/jjjj" (dag, maand, jaar). De vorm "dd.mm.jjjj" mag ook worden gebruikt;

— de term "kaartidentificatie" verwijst naar: de kaartsoort door middel van een pictogramcombinatie van de kaart, de code van de lidstaat van afgifte, een schuine streep en het kaartnummer waarin de vervangingsindex en de vernieuwingsindex door een spatie gescheiden zijn:

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Kaartpictogramcombinaties		Code van de lidstaat van afgifte				Eerste 14 tekens van het kaartnummer (bevat eventueel een opeenvolgende index)														Vervangingsindex		Vernieuwingsindex

PRT_007 Afdrukken maken gebruik van de volgende gegevensblokken en/of -records overeenkomstig de volgende betekenissen en opmaken:

Blok- of recordnummer Betekenis	Data Format
1 ***Datum en tijdstip waarop het document is afgedrukt.***	▼ dd/mm/yyyy hh:mm **(UTC)**
2 ***Soort afdruk.*** Blokidentificatiesymbool Afdruk pictogramcombinatie (zie aanh. 3), instelling snelheidsbegrenzer (uitsluitend afdruk snelheidsoverschrijding)	----------▼---------- Picto xxx **km/h**
3 ***Identificatie van de kaarthouder.*** Blokidentificatiesymbool. P = pictogram voor personen Naam van de kaarthouder Voornaam of voornamen van de kaarthouder (indien van toepassing) Identificatie van de kaart Vervaldatum van de kaart (indien van toepassing) en generatienummer van de kaart (GEN 1 of GEN 2) (*)	----------P---------- P Last_Name_____ First_Name_____ Card_Identification_____ dd/mm/yyyy - GEN 2
4 ***Identificatie van het voertuig.*** Blokidentificatiesymbool VIN Lidstaat van registratie en VRN	----------🚘---------- 🚘 VIN_____ Nat/VRN_____
5 ***VU-identificatie.*** Blokidentificatiesymbool Naam van de fabrikant van de VU Onderdeelnummer van de VU Generatienummer van de VU (*)	----------⊟---------- ⊟ VU_Manufacturer_____ VU_Part_Number__ GEN 2
6 ***Laatste kalibrering van de tachograaf*** Blokidentificatiesymbool Naam van de werkplaats Identificatie van de werkplaatskaart Datum van de kalibrering	----------🔧---------- 🔧 Last_Name_____ Card_Identification_____ 🔧 dd/mm/yyyy

Ingeval de kaart een niet-persoonlijke kaart is en er geen naam van een kaarthouder op staat, wordt in plaats daarvan de naam van het bedrijf, de werkplaats of de controle-instantie afgedrukt.

(*) Het generatienummer van de kaart kan alleen worden afgedrukt door een slimme tachograaf.

(*) Het generatienummer van de VU kan alleen worden afgedrukt door een slimme tachograaf.

7 ***Laatste controle (door een controleur)***

Blokidentificatiesymbool
Identificatie van de controleurskaart
Datum, tijd en soort controle

```
----------▯----------
Card_Identification_____
▯ dd/mm/yyyy hh:mm ppppp
```

Soort controle: Tot vijf pictogrammen. De soort controle kan (een combinatie) zijn (van):
▮: downloaden kaart, ↧: downloaden VU, ↟: afdrukken, ▯: zichtbaar maken, ↑: Kalibreringscontrole langs de weg

8 ***Bestuurdersactiviteiten opgeslagen op een kaart in chronologische volgorde***

Blokidentificatiesymbool
Datum van opvraging (kalenderdag van de afdruk) + dagelijkse aanwezigheidsteller voor de kaart

```
----------⊙----------
    dd/mm/yyyy  xxx
```

8a *Toestand "niet verplicht" aan het begin van deze dag* (niets invullen indien geen "niet-verplicht"-toestand openstaat)

```
----------OUT----------
```

8.1 *Periode waarin de kaart niet was ingebracht*
8.1a Recordidentificatiesymbool (begin van periode)
8.1b *Onbekende periode*. Begintijd, duur
8.1c *Manueel ingevoerde activiteit*.
Activiteitspictogram, begintijd, duur

```
  --------------------
?       hh:mm hhhmm
A       hh:mm hhhmm
```

8.2 *Inbrengen van de kaart in lezer S*
Recordidentificatiesymbool; S = pictogram van de lezer
Lidstaat waar het voertuig is geregistreerd en VRN
Kilometerstand bij inbrengen van de kaart

```
  ---------S---------
🚗 Nat/VRN__________
  x xxx xxx km
```

8.3 *Activiteit (bij ingebrachte kaart)*
Activiteitspictogram, begintijd, duur, status ploeg (teampictogram indien MET EEN TEAM, leeg indien ALLEEN).

```
A       hh:mm hhhmm ⊙⊙
```

8.3a *Specifieke omstandigheid*. Tijd van invoer, pictogram van specifieke omstandigheid (of combinatie van pictogrammen).

```
        hh:mm ---pppp---
```

8.4 *Uitnemen van kaart*
Kilometerstand en afgelegde afstand sinds laatste inbrenging waarvan een kilometerstand bekend is

```
  x xxx xxx km; x xxx km
```

9 ***Bestuurdersactiviteiten opgeslagen in een VU per lezer in chronologische volgorde***

Blokidentificatiesymbool
Datum van opvraging (kalenderdag van de afdruk)
Kilometerstand om 00:00 en 24:00

```
----------⊙----------
       dd/mm/yyyy
x xxx xxx - x xxx xxx km
```

10 ***Activiteiten voor lezer S***

Blokidentificatiesymbool

```
----------S----------
```

10a *Toestand "niet verplicht" aan het begin van deze dag* (niets invullen indien geen "niet-verplicht"-toestand openstaat)

```
----------OUT----------
```

10.1 *Periode zonder in lezer S ingebrachte kaart*
Recordidentificatiesymbool.
Geen kaart ingebracht
Kilometerstand aan begin van periode

```
  --------------------
⊙▮---
  x xxx xxx km
```

10.2 *Inbrengen van kaart*
Recordidentificatiesymbool voor inbrengen van kaart
Naam van de bestuurder

```
  --------------------
⊙ Last_Name_____________
```

	Voornaam van de bestuurder	First_Name_____
	Identificatie bestuurderskaart	Card_Identification_____
	Vervaldatum van de kaart (indien van toepassing) en generatienummer van de kaart (GEN 1 of GEN 2) (*)	dd/mm/yyyy - GEN 2
	Registrerende lidstaat en VRN van eerder gebruikt voertuig	+Nat/VRN_____
	Datum en tijdstip waarop de kaart uit het vorige voertuig is genomen	dd/mm/yyyy hh:mm
	Blanco regel	
	Kilometerstand bij het inbrengen van de kaart, teken voor manuele invoer bestuurdersactiviteit (M bij manuele invoer, blanco bij geen manuele invoer)	x xxx xxx **km** M
	Indien een bestuurderskaart niet is ingebracht op de dag waarvoor de afdruk wordt gemaakt, wordt voor blok 10.2 de kilometerstand van de laatst beschikbare inbrenging voorafgaand aan die dag gebruikt.	
10.3	*Activiteit*	
	Activiteitspictogram, begintijd, duur, status ploeg (teampictogram indien MET EEN TEAM, leeg indien ALLEEN).	A hh:mm hh**h**mm
10.3a	*Specifieke omstandigheid*. Tijd van invoer, pictogram van specifieke omstandigheid (of combinatie van pictogrammen).	hh:mm ---pppp---
10.4	*Uitnemen van kaart of einde van periode "Geen kaart"*	
	Kilometerstand bij het uitnemen van de kaart of aan het einde van periode "Geen kaart" en de afgelegde afstand sinds inbrengen of sinds het begin van de periode "Geen kaart"	x xxx xxx **km**; x xxx **km**

(*) Het generatienummer van de kaart kan alleen worden afgedrukt door een slimme tachograaf.

11	***Dagelijks overzicht***	
	Blokidentificatiesymbool	----------Σ----------
11.1	***Overzicht van perioden zonder kaart in de bestuurderslezer van de VU***	
	Blokidentificatiesymbool	1----
11.2	***Overzicht van perioden zonder kaart in de lezer van de bijrijder***	
	Blokidentificatiesymbool	2----
11.3	***Dagelijks overzicht per bestuurder voor VU***	
	Recordidentificatiesymbool	----------
	Achternaam van de bestuurder	Last_Name_____
	Voornaam (voornamen) van de bestuurder	First_Name_____
	Identificatie bestuurderskaart	Card_Identification_____
11.4	*Invoeren van de plaats waar een dagelijkse werkperiode begint en/of eindigt*	
	pi = pictogram van begin-/eindlocatie, tijd, land, regio	pihh:mm Cou Reg
	Kilometerteller	x xxx xxx **km**
11.5	*Invoeren van de plaats waar een dagelijkse werkperiode begint en/of eindigt*	
	en na 3 uur ononderbroken rijtijd	hh:mm
	Kilometerteller	x xxx xxx **km**
11.6	*Totaal van de activiteiten (van een kaart)*	
	Totale rijtijd, afgelegde afstand	hh**h**mm x xxx **km**
	Totale werkduur en duur van beschikbaarheid	hh**h**mm hh**h**mm
	Totale rusttijd en duur van onbekende activiteit	hh**h**mm ? hh**h**mm
	Totale duur van teamactiviteiten	hh**h**mm
11.7	*Totaal van de activiteiten (perioden zonder kaart in lezer bestuurder)*	
	Totale rijtijd, afgelegde afstand	hh**h**mm x xxx **km**
	Totale werkduur en duur van beschikbaarheid	hh**h**mm hh**h**mm
	Totale rusttijd	hh**h**mm

11.8	*Totaal activiteiten (perioden zonder kaart in lezer bijrijder)*	
	Totale werkduur en duur van beschikbaarheid	`hhhmm  hhhmm`
	Totale rusttijd	`hhhmm`
11.9	*Totaal activiteiten (per bestuurder, beide lezers inbegrepen)*	
	Totale rijtijd, afgelegde afstand	`hhhmm  x xxx km`
	Totale werkduur en duur van beschikbaarheid	`hhhmm  hhhmm`
	Totale rusttijd	`hhhmm`
	Totale duur van teamactiviteiten	`hhhmm`

Wanneer een dagelijkse afdruk voor de lopende dag vereist is, wordt de informatie voor het dagelijkse overzicht berekend met gegevens die beschikbaar zijn op het tijdstip van de afdruk.

12	***Op een kaart opgeslagen voorvallen en/of fouten***	
12.1	Blokidentificatiesymbool van de laatste 5 "voorvallen en fouten" van een kaart	`----------!×----------`
12.2	Blokidentificatiesymbool van alle op een kaart geregistreerde "voorvallen"	`----------!----------`
12.3	Blokidentificatiesymbool van alle op een kaart geregistreerde "fouten"	`----------×----------`
12.4	*Record van voorvallen en/of fouten*	

	Recordidentificatiesymbool
	Pictogram van voorval/fout, doel van record, begindatum en -tijd
	Bijkomende code van voorval/fout (indien van toepassing), duur
	Lidstaat van registratie & VRN van het voertuig waarin het voorval of de fout zich voordeed
		`--------------------`
		`Pic (p) dd/mm/yyyy hh:mm`
		`!xx hhhmm`
		`Nat/VRN__________`

13	***Voorvallen en/of fouten die zijn opgeslagen of aan de gang zijn in een VU***	
13.1	Blokidentificatiesymbool van laatste 5 "voorvallen en fouten" uit VU	`----------!×----------`
13.2	Blokidentificatiesymbool van alle geregistreerde of lopende "voorvallen" in een VU	`----------!----------`
13.3	Blokidentificatiesymbool van alle geregistreerde of lopende "fouten" in een VU	`----------×----------`
13.4	*Record van voorvallen en/of fouten*	

	Recordidentificatiesymbool
	Pictogram van voorval/fout, doel van record, begindatum en -tijd
	Aanvullende voorval-/foutcode (indien van toepassing), aantal soortgelijke voorvallen gedurende deze dag, duur
	Identificatie van de kaarten die waren ingebracht aan het begin of het einde van het voorval of de fout (tot 4 regels zonder tweemaal dezelfde kaartnummers te herhalen)
	
	Geval waarin geen kaart was ingebracht
	Specifiek kenmerk fabrikant
		`--------------------`
		`Pic (p) dd/mm/yyyy hh:mm`
		`!xx (xxx) hhhmm`
		
		`Card_Identification_____`
		`Card_Identification_____`
		`Card_Identification_____`
		`Card_Identification_____`
		`---`
		`< Literal><ErrorCode>`

Het registratiedoel (p) is een numerieke code die zegt waarom het voorval of de fout werd geregistreerd en gecodeerd volgens gegevenselement `EventFaultRecordPurpose`.

`Literal` is een lettercode van maximaal 12 tekens, specifiek voor tachograaffabrikanten

`ErrorCode` is een foutcode van 12 tekens, specifiek voor tachograaffabrikanten.

14	***VU-identificatie***	
	Blokidentificatiesymbool	----------B----------
	Naam van de fabrikant van de VU	B Name_____
	Adres van de fabrikant van de VU	Address_____
	Onderdeelnummer van de VU	PartNumber_____
	Goedkeuringsnummer van de VU	Apprv_____
	Serienummer van de VU	S/N_____
	Bouwjaar van de VU	yyyy
	Softwareversie en datum van installatie van de VU	V xxxx dd/mm/yyyy
15	***Identificatie van de sensor***	
	Blokidentificatiesymbool	----------J----------
15.1	*Koppelingsrecord*	
	Serienummer van de sensor	J S/N_____
	Goedkeuringsnummer van de sensor	Apprv_____
	Datum van sensorkoppeling	dd/mm/yyyy hh:mm
16	***GNSS-identificatie***	
	Blokidentificatiesymbool	---------- ----------
16.1	*Koppelingsrecord*	
	Serienummer van de externe GNSS-module	S/N_____
	Goedkeuringsnummer van de externe GNSS-module	Apprv_____
	Koppelingsdatum van de externe GNSS-module	dd/mm/yyyy hh:mm
17	***Kalibreringsgegevens***	
	Blokidentificatiesymbool	----------T----------
17.1	*Kalibreringsrecord*	
	Recordidentificatiesymbool	----------
	Werkplaats die de kalibrering heeft uitgevoerd	T Workshop_name_____
	Adres van de werkplaats	Workshop_address_____
	Identificatie van de werkplaatskaart	Card_Identification_____
	Vervaldatum van de werkplaatskaart	dd/mm/yyyy
	Blanco regel	
	Kalibreringsdatum + kalibreringsdoel	T dd/mm/yyyy (p)
	VIN	A VIN_____
	Lidstaat van registratie en VRN	Nat/VRN_____
	Kenmerkende coëfficiënt van het voertuig	w xx xxx Imp/km
	Constante van het controleapparaat	k xx xxx Imp/km
	Effective circumference of wheel tyres	l xx xxx mm
	Maat van de gemonteerde banden	● TyreSize_____
	Instelling van de snelheidsbegrenzer	> xxx km/h
	Oude en nieuwe kilometerstand	x xxx xxx – x xxx xxx km

Het registratiedoel (p) is een numerieke code die zegt waarom deze kalibreringsparameters werden geregistreerd en gecodeerd volgens gegevenselement `CalibrationPurpose`.

18	***Tijdafstelling***	
	Blokidentificatiesymbool	----------◷----------
18.1	*Tijdafstellingsrecord*	
	Recordidentificatiesymbool	----------
	Oude datum en tijd	!◷ dd/mm/yyyy hh:mm
	Nieuwe datum en tijd	◷ dd/mm/yyyy hh:mm
	Werkplaats die de kalibrering heeft uitgevoerd	T Workshop_name_____
	Adres van de werkplaats	Workshop_address_____
	Identificatie van de werkplaatskaart	Card_Identification_____
	Vervaldatum van de werkplaatskaart	dd/mm/yyyy
19	***Meest recent(e) door de VU geregistreerd(e) voorval en fout***	
	Blokidentificatiesymbool	----------!×Д----------
	Datum en tijd van het recentste voorval	! dd/mm/yyyy hh:mm
	Datum en tijd van de recentste fout	× dd/mm/yyyy hh:mm
20	***Informatie over snelheidsoverschrijdingscontrole***	
	Blokidentificatiesymbool	----------»»----------
	Datum en tijd van de laatste SNELHEIDSOVERSCHRIJDINGSCONTROLE	»▫dd/mm/yyyy hh:mm
	Datum/tijd van de eerste snelheidsoverschrijding en aantal snelheidsoverschrijdingen sindsdien	»»dd/mm/yyyy hh:mm (nnn)
21	***Snelheidsoverschrijdingsrecord***	
21.1	Blokidentificatiesymbool "eerste snelheidsoverschrijding na de laatste kalibrering"	--------»»T---------
21.2	Blokidentificatiesymbool "5 ernstigste in de afgelopen 365 dagen"	-------»»(365)------
21.3	Blokidentificatiesymbool "ernstigste voor elk van de laatste 10 dagen waarin het is voorgevallen"	-------»»(10)-------
21.4	Recordidentificatiesymbool	----------
	Datum, tijd en duur	»»dd/mm/yyyy hh:mm hhhmm
	Gemiddelde en maximumsnelheid, aantal vergelijkbare voorvallen op die dag	xxx km/h xxx km/h(xxx)
	Naam van de bestuurder	◙ Last_Name_____
	Voornaam (voornamen) van de bestuurder	First_Name_____
	Identificatie bestuurderskaart	Card_Identification_____
21.5	Als een blok geen snelheidsoverschrijdingsrecord bevat	»»---
22	***Handgeschreven informatie***	
	Blokidentificatiesymbool	----------
22.1	Controleplaats	▫● .....
22.2	Handtekening van de controleur	▫ .....
22.3	Van (tijd)	◷+ .....
22.4	Tot (tijd)	+◷ .....
22.5	Handtekening van de bestuurder	◙ .....

"Handgeschreven informatie"; Voeg boven een handgeschreven rubriek voldoende witregels in zodat de vereiste informatie kan worden genoteerd of een handtekening kan worden gezet.

23 ***Laatste in de VU ingebrachte kaarten***
Blokidentificatiesymbool
23.1 Ingebrachte kaart
Recordidentificatiesymbool
Soort kaart, generatie, versie, fabrikant (*)
Identificatie van de kaart
Serienummer van de kaart
Datum en tijdstip van laatste kaartinbrenging

```
-------- ⊟■⊙ --------

----
⍑ <gen> <version> <MC>
Card Identification
Card Serial Number
dd/mm/yyyy hh:mm
```

(*) (alles op één regel)
waarbij
type of card: Pictogram, één teken + spatie
gen: GEN1 of GEN 2, 4 tekens + spatie
version: tot 10 tekens.
MC: code van de fabrikant, 3 tekens.

3. AFDRUKSPECIFICATIES

In dit hoofdstuk worden de onderstaande standaardtekens gebruikt:

N	Afdrukblok of record nummer N
N	Afdrukblok of record nummer N, zo vaak als nodig herhaald
X/Y	Afdrukblokken of records X en/of Y indien nodig, en zo vaak als nodig herhaald

3.1. **Dagelijkse afdruk van de kaart met de bestuurdersactiviteiten**

PRT_008 De dagelijkse afdruk van de kaart met de activiteiten van de bestuurder moet in overeenstemming zijn met onderstaande opmaak:

1	Datum en tijdstip waarop het document is afgedrukt.
2	Soort afdruk
3	Identificatie van de controleur (indien een controlekaart in de VU is ingebracht)
3	Bestuurdersidentificatie (van de kaart die wordt afgedrukt + 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 de bestuurder
8	Begrenzer van de bestuurdersactiviteiten
8a	"Niet verplicht"-toestand aan het begin van deze dag
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Activiteiten van de bestuurder in de volgorde waarin zij zich voordeden
11	Dagelijks overzicht begrenzer

11.4	Ingevoerde plaatsen in chronologische volgorde
11.5	GNSS-gegevens
11.6	Totaal van activiteiten
12.1	Begrenzer van voorvallen of fouten uit kaart
12.4	Voorval/fout-records (laatste 5 op de kaart opgeslagen voorvallen of fouten)
13.1	Begrenzer van voorvallen of fouten uit VU
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
22.5	Handtekening van de bestuurder

3.2. **Dagelijkse afdruk van de VU met de bestuurdersactiviteiten**

PRT_009 De dagelijkse afdruk van de VU van de activiteiten van de bestuurder 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 + 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	GNSS-gegevens
11.6	Totaal van activiteiten
11.2	Overzicht van perioden zonder kaart in lezer voor bijrijder
11.4	Ingevoerde plaatsen in chronologische volgorde
11.5	GNSS-gegevens

11.7	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	GNSS-gegevens
11.8	Totaal van activiteiten voor deze bestuurder
13.1	Begrenzer voorvallen/fouten
12.4	Voorval/fout-records (laatste 5 opgeslagen of lopende voorvallen of fouten in de VU)
13.1	Controleplaats
22.2	Handtekening van de controleur
22.3	Van (tijd) (ruimte voor een bestuurder zonder een kaart om aan te geven welke perioden voor hem relevant zijn)
22.4	Tot (tijd)
22.5	Handtekening van de bestuurder

3.3. **Afdruk van de kaart van voorvallen en fouten**

PRT_010 De afdruk van de kaart met voorvallen en fouten moet in overeenstemming zijn met onderstaande opmaak:

1	Datum en tijdstip waarop het document is afgedrukt.
2	Soort afdruk
3	Identificatie van de controleur (indien een controlekaart in de VU is ingebracht + GEN)
3	Identificatie van de bestuurder (van de kaart waarvan de afdruk gemaakt wordt)
4	Identificatie van het voertuig (voertuig waarvan de afdruk wordt gemaakt)
12.2	Begrenzer van voorvallen
12.4	Voorvalrecords (alle op de kaart opgeslagen voorvallen)
12.3	Begrenzer van fouten
12.4	Foutrecords (alle op de kaart opgeslagen fouten)
22.1	Controleplaats
22.2	Handtekening van de controleur
22.5	Handtekening van de bestuurder

3.4. **Afdruk van de voertuigunit van voorvallen en fouten**

PRT_011 De afdruk van de VU met voorvallen en fouten 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 + GEN)
4	Identificatie van het voertuig (voertuig waarvan de afdruk wordt gemaakt)

13.2	Begrenzer van voorvallen
13.4	Voorvalrecords (alle in de VU opgeslagen of aanhoudende voorvallen)
13.3	Begrenzer van fouten
13.4	Foutrecords (alle in de VU opgeslagen of aanhoudende fouten)
22.1	Controleplaats
22.2	Handtekening van de controleur
22.5	Handtekening van de bestuurder

3.5. **Afdruk van technische gegevens**

PRT_012 De afdruk van technische gegevens 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 + GEN)
4	Identificatie van het voertuig (voertuig waarvan de afdruk wordt gemaakt)
14	VU-identificatie
15	Identificatie van de sensor
15.1	Gegevens over sensorverbinding (alle gegevens in chronologische volgorde)
16	GNSS-identificatie
16.1	Gegevens over verbinding met de GNSS-module (alle gegevens in chronologische volgorde)
17	Begrenzer van kalibreringsgegevens
17.1	Kalibreringsrecords (alle records in chronologische volgorde)
18	Begrenzer van de tijdafstelling
18.1	Tijdafstellingsrecords (alle records van tijdafstelling en kalibreringsgegevens)
19	Meest recent(e) door de VU geregistreerd(e) voorval en fout

3.6. **Afdruk van snelheidsoverschrijding.**

PRT_013 De afdruk van snelheidsoverschrijding 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 + GEN)
4	Identificatie van het voertuig (voertuig waarvan de afdruk wordt gemaakt)
20	Informatie over snelheidsoverschrijdingscontrole
21.1	Identificatiesymbool snelheidsoverschrijdingsgegevens
21.4 / 21.5	Eerste snelheidsoverschrijding na de laatste kalibrering

21.2	Identificatiesymbool snelheidsoverschrijdingsgegevens
21.4 / 21.5	De 5 grootste snelheidsoverschrijdingen in de afgelopen 365 dagen
21.3	Identificatiesymbool snelheidsoverschrijdingsgegevens
21.4 / 21.5	De grootste snelheidsoverschrijding op elk van de laatste 10 dagen waarop snelheidsoverschrijdingen plaatsvonden
22.1	Controleplaats
22.2	Handtekening van de controleur
22.5	Handtekening van de bestuurder

3.7. **Geschiedenis van ingebrachte kaarten**

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

Aanhangsel 5

DISPLAY

In dit aanhangsel worden de onderstaande opmaakcriteria gehanteerd:

— **vet** gedrukte letters geven standaardtekst aan die getoond moet worden (weergave blijft in gewone letters);

— gewone letters geven variabelen aan (pictogrammen of gegevens) die bij de weergave door hun waarden moeten worden vervangen:

  — dd mm yyyy: dag, maand, jaar,

  — hh: uren,

  — mm: minuten,

  — D: duurpictogram,

  — EF: pictogramcombinatie van voorvallen of fouten,

  — O: pictogram van de werkingsmodus.

DIS_001 Het controleapparaat toont de gegevens met gebruikmaking van onderstaande opmaak:

Gegevens	Format
Standaarddisplay	
Plaatselijke tijd	hh:mm
Werkingsmodus	O
Informatie over de bestuurder	1 Dhh**h**mm ‖hh**h**mm
Informatie over de bijrijder	2Dhh**h**mm
"Niet verplicht" -omstandigheid geopend	OUT
Waarschuwingsdisplay	
Overschrijden van de ononderbroken rijtijd	1⊙hh**h**mm ‖hh**h**mm
Voorval of fout	EF
Overige displays	
UTC-datum Tijd	UTC⊙dd/mm/yyyy of UTC⊙dd.mm.yyyy hh:mm
Ononderbroken rijtijd en cumulatieve rusttijd van de bestuurder	1⊙hh**h**mm ‖hh**h**mm
Ononderbroken rijtijd en cumulatieve rusttijd van de bijrijder	2⊙hh**h**mm ‖hh**h**mm
Cumulatieve rijtijd van de bestuurder in de voorafgaande en de lopende week	1⊙‖ hhh**h**mm
Cumulatieve rijtijd van de bijrijder in de voorafgaande en de lopende week	2⊙‖ hhh**h**mm

Aanhangsel 6

FRONTCONNECTOR VOOR KALIBRERING EN DOWNLOADEN

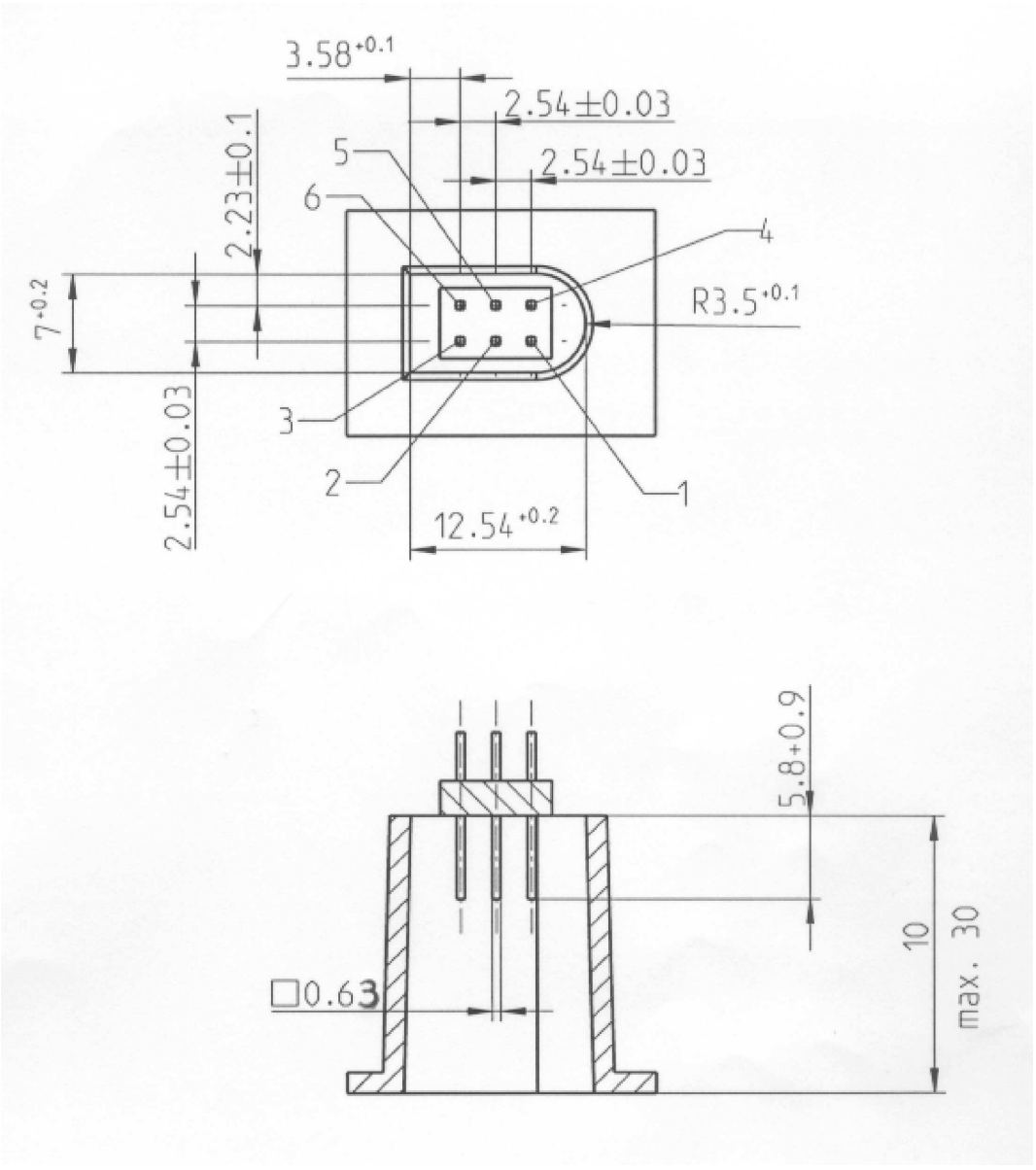
INHOUDSOPGAVE

1. HARDWARE 256
1.1. Connector 256
1.2. Contacttoewijzing 257
1.3. Blokschema 258
2. DOWNLOADINTERFACE 258
3. KALIBRERINGSINTERFACE 259

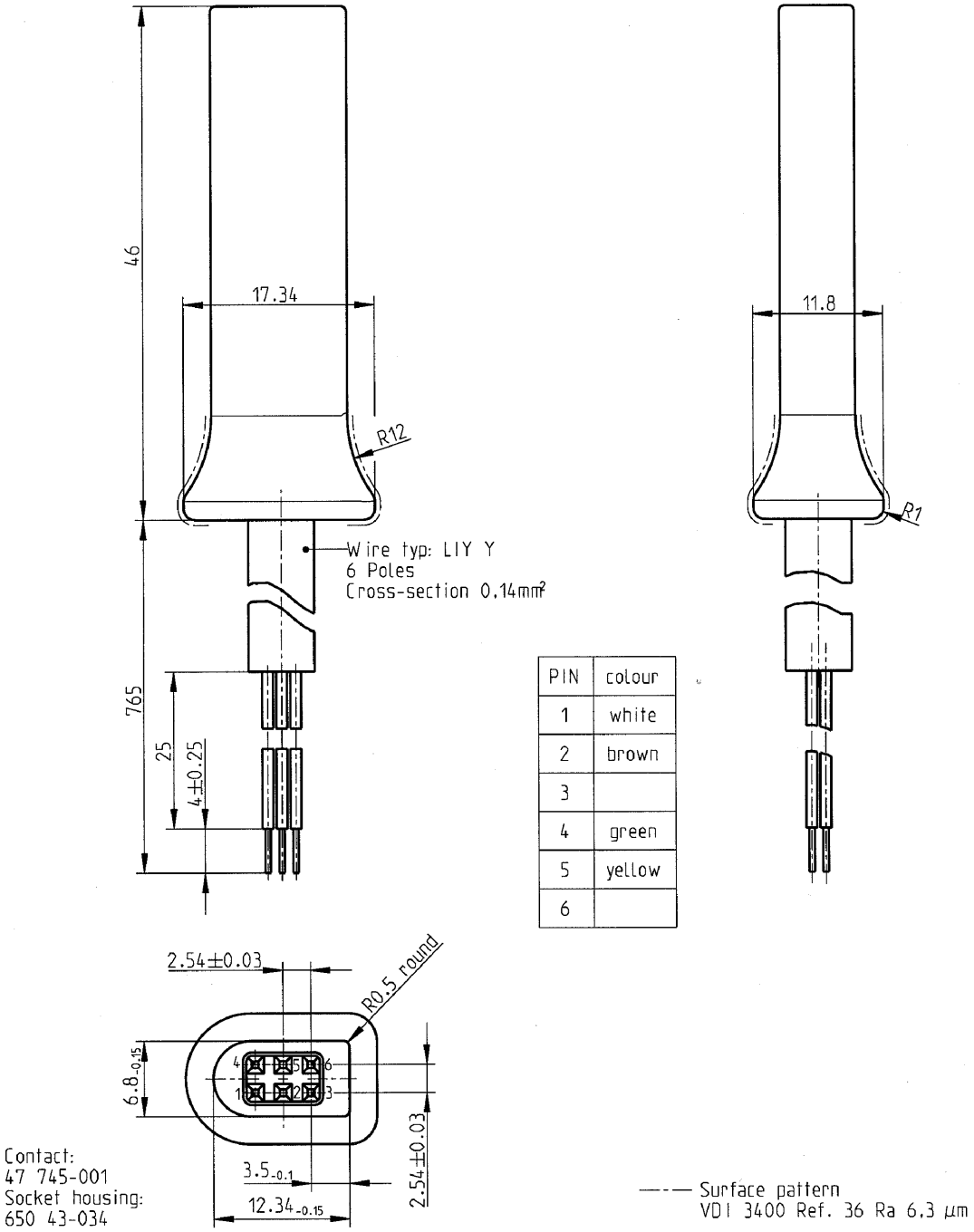
1. HARDWARE

1.1. **Connector**

INT_001 De download-/kalibreringsconnector is een 6-pinsconnector die via het frontpaneel toegankelijk is zonder dat daarvoor delen van de tachograaf moeten worden losgekoppeld. De connector stemt overeen met de onderstaande tekening (alle maten in millimeters):



Het onderstaande schema toont een normale 6-pinscontrastekker:



1.2. **Contacttoewijzing**

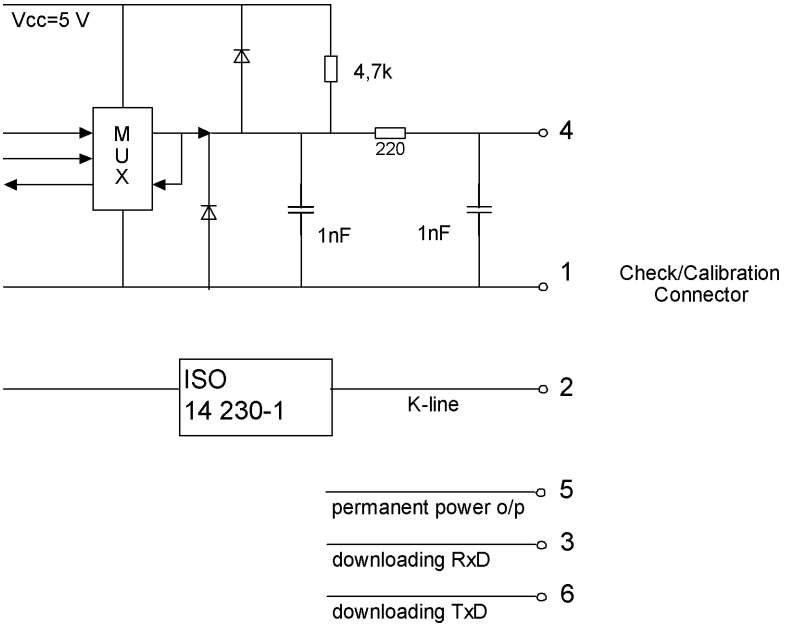
INT_002 Contacten moeten overeenkomstig de onderstaande tabel worden toegewezen:

Pin	Beschrijving	Opmerking
1	Minpool	Verbonden met de minpool van het voertuig
2	Gegevensoverdracht	K-lijn (ISO 14230-1)

Pin	Beschrijving	Opmerking
3	RxD — Download	Gegevensinvoer naar tachograaf
4	Invoer-/uitvoersignaal	Kalibrering
5	Permanente vermogensafgifte	Het spanningsbereik wordt gespecificeerd als het vermogen van het voertuig minus 3 V met het oog op optredend spanningsverlies in de veiligheidsschakelingen Output 40 mA
6	TxD — Download	Gegevensuitvoer van tachograaf

1.3. **Blokschema**

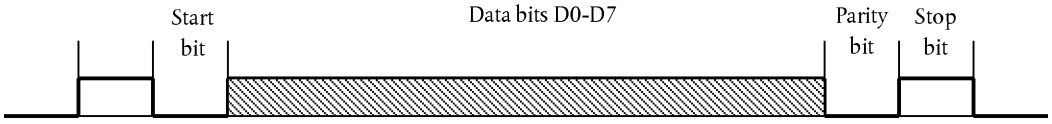
INT_003 Het blokschema moet aan het onderstaande voldoen:



2. DOWNLOADINTERFACE

INT_004 De downloadinterface moet voldoen aan RS232-specificaties.

INT_005 De downloadinterface moet een startbit, 8 gegevensbits met LSB als eerste bit, een even pariteitsbit en 1 stopbit gebruiken.



Organisatie van gegevensbits

Startbit: een bit met logisch niveau 0;

Gegevensbits: verzonden met LSB als eerste bit;

Pariteitsbit: even pariteit

Stopbit: een bit met logisch niveau 1

Wanneer numerieke gegevens verzonden worden die uit meer dan een byte bestaan, wordt de significantste byte het eerst verzonden en de minst significante byte het laatst.

INT_006 Baudsnelheden van de transmissie moeten instelbaar zijn tussen 9 600 bps en 115 200 bps. De transmissie moet met de hoogst mogelijke transmissiesnelheid worden uitgevoerd, waarbij de initiële baudsnelheid na het begin van de overdracht op 9 600 bps moet worden gezet.

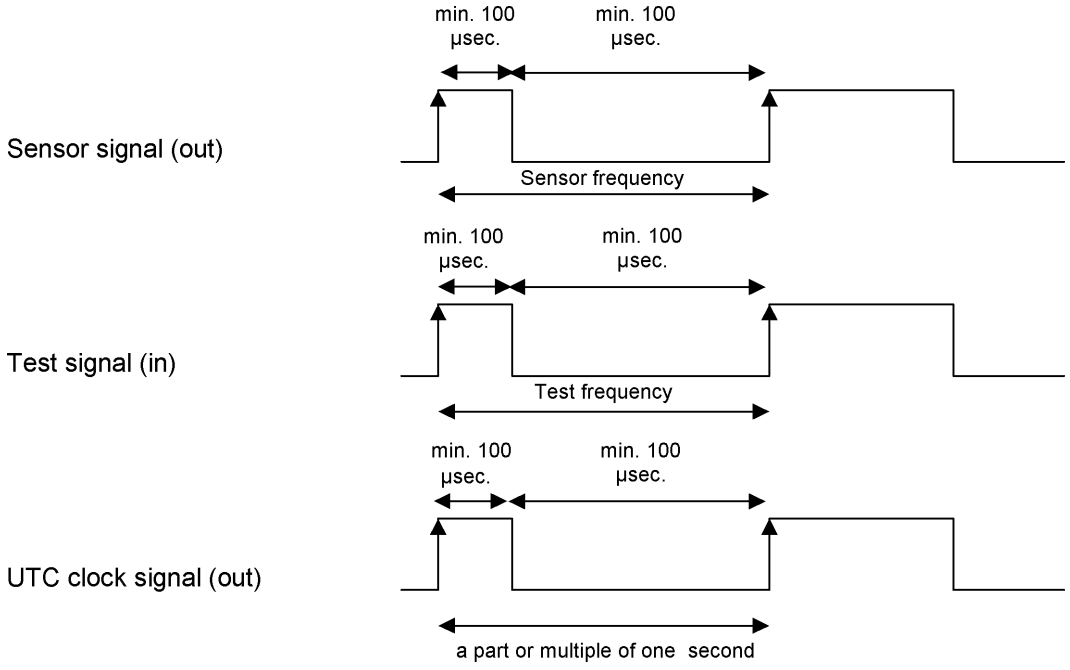
3. KALIBRERINGSINTERFACE

INT_007 De gegevensoverdracht moet voldoen aan ISO 14230-1 Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part 1: Physical layer, First edition: 1999.

INT_008 Het invoer-/uitvoersignaal moet voldoen aan de onderstaande elektrische specificatie:

Parameter	Minimum	Normaal	Maximum	Opmerking
U_{low} (in)			1,0 V	I = 750 µA
U_{high} (in)	4 V			I = 200 µA
Frequentie			4 kHz	
U_{low} (uit)			1,0 V	I = 1 mA
U_{high} (uit)	4 V			I = 1 mA

INT_009 Het invoer-/uitvoersignaal moet voldoen aan de onderstaande tijdschema's:



Aanhangsel 7

PROTOCOL VOOR GEGEVENSOVERDRACHT

INHOUDSOPGAVE

1. INLEIDING 261
1.1. Toepassingsgebied 261
1.2. Acroniemen en notaties 261
2. GEGEVENSOVERDRACHT VAN DE VU 262
2.1. Downloadprocedure 262
2.2. Protocol voor gegevensoverdracht 262
2.2.1 Berichtenstructuur 262
2.2.2 Soorten berichten 264
2.2.2.1 Start Communication Request (SID 81) 266
2.2.2.2 Positive Response Start Communication (SID C1) 266
2.2.2.3 Start Diagnostic Session Request (SID 10) 266
2.2.2.4 Positive Response Start Diagnostic (SID 50) 266
2.2.2.5 Link Control Service (SID 87) 266
2.2.2.6 Link Control Positive Response (SID C7) 266
2.2.2.7 Request Upload (SID 35) 266
2.2.2.8 Positive Response Request Upload (SID 75) 266
2.2.2.9 Transfer Data Request (SID 36) 266
2.2.2.10 Positive Response Transfer Data (SID 76). 267
2.2.2.11 Request Transfer Exit (SID 37) 267
2.2.2.12 Positive Response Request Transfer Exit (SID 77) 267
2.2.2.13 Stop Communication Request (SID 82) 267
2.2.2.14 Positive Response Stop Communication (SID C2) 267
2.2.2.15 Acknowledge Sub Message (SID 83) 267
2.2.2.16 Negative Response (SID 7F) 268
2.2.3 Berichtenstroom 268
2.2.4 Tijdschema 269
2.2.5 Behandeling van fouten 270
2.2.5.1 Start communicatie-fase 270
2.2.5.2 Overbrengingsfase 270
2.2.6 Inhoud van het antwoordbericht 272
2.2.6.1 Positive Response Transfer Data Overview 273
2.2.6.2 Positive Response Transfer Data Activities 274
2.2.6.3 Positive Response Transfer Data Events and Faults 275
2.2.6.4 Positive Response Transfer Data Detailed Speed 276
2.2.6.5 Positive Response Transfer Data Technical Data 276
2.3. ESM bestandsopslag 277

3. DOWNLOADPROTOCOL VAN TACHOGRAAFKAARTEN 277
3.1. Toepassingsgebied 277
3.2. Definities 277
3.3. Kaartdownload 277
3.3.1 Initialisatiesequentie 278
3.3.2 Sequentie voor niet-getekende gegevensbestanden 278
3.3.3 Sequentie voor getekende gegevensbestanden 279
3.3.4 Sequentie voor het resetten van de kalibreringsteller 279
3.4. Opmaak gegevensopslag 280
3.4.1 Inleiding 280
3.4.2 Bestandsopmaak 280
4. DOWNLOADEN VAN EEN TACHOGRAAFKAART VIA EEN VOERTUIGUNIT 281

1. INLEIDING

In dit aanhangsel worden de te volgen procedures gespecificeerd voor het uitvoeren van de verschillende soorten gegevensoverdrachten naar een extern opslagmedium (ESM), alsmede de te implementeren protocollen om de correcte gegevensoverdracht en de volledige compatibiliteit van het overgebrachte gegevensformaat te waarborgen zodat een controleur deze gegevens kan inspecteren en de authenticiteit en integriteit ervan kan controleren voordat hij de gegevens analyseert.

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 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 overgebrachte, 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.

DDP_001 De tijdens een downloadsessie overgebrachte gegevens moeten in het ESM in één bestand worden opgeslagen.

1.2. **Acroniemen en notaties**

In dit aanhangsel worden de onderstaande acroniemen gebruikt:

AID Applicatie-identificatie

ATR Antwoord op reset

CS Controlesombyte

DF Toepassingsgericht bestand

DS_ Diagnostische sessie

EF Hoofdbestand

ESM Extern opslagmedium

FID Bestandsidentificatiesymbool (bestands-ID)

FMT Opmaakbyte (eerste byte van het beginlabel van het bericht)

ICC Chipkaart

IDE Intelligente toepassingsgerichte apparatuur: de apparatuur die wordt gebruikt voor het downloaden van gegevens naar het ESM (bijv. pc)

IFD Interface-apparaat

KWP Sleutelwoordprotocol 2000

LEN Lengtebyte (laatste byte van het beginlabel van het bericht)

PPS Protocol parameterselectie

PSO Voer beveiligingsoperatie uit

SID Dienstidentificatiesymbool

SRC Bronbyte

TGT Doelbyte

TLV Waarde van de labellengte

TREP Parameter overdracht antwoord

TRTP Parameter overdracht verzoek

VU Voertuigunit

2. GEGEVENSOVERDRACHT VAN DE VU

2.1. **Downloadprocedure**

Om gegevens van een VU te downloaden, moet de operator de onderstaande handelingen verrichten:

— zijn tachograafkaart in een kaartlezer van de VU inbrengen (*);

— de IDE met de downloadconnector van de VU verbinden;

— de verbinding tussen de IDE en de VU tot stand brengen;

— de over te brengen gegevens in de IDE selecteren en het verzoek naar de VU sturen;

— de downloadsessie sluiten.

2.2. **Protocol voor gegevensoverdracht**

Het protocol is gestructureerd op een master-slavebasis, waarbij de IDE de rol van master speelt en de VU de rol van slave.

De berichtenstructuur, berichtensoorten en berichtenstroom zijn hoofdzakelijk gebaseerd op het Sleutelwoordprotocol 2000 (KWP) (ISO 14230-2 Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part 2: Data link layer).

De applicatielaag is hoofdzakelijk gebaseerd op het huidige ontwerp van ISO 14229-1 (Road vehicles — Diagnostic systems — Part 1: Diagnostic services, version 6 of 22 February 2001).

2.2.1 *Berichtenstructuur*

DDP_002 Alle tussen de IDE en de VU uitgewisselde berichten zijn opgemaakt volgens een uit drie delen bestaande structuur:

— beginlabel bestaande uit een opmaakbyte (FMT), een doelbyte (TGT), een bronbyte (SRC) en eventueel een lengtebyte (LEN);

— gegevensveld bestaande uit een identificatiebyte van de dienst (SID) en een variabel aantal gegevensbytes, die een facultatieve diagnosesessiebyte (DS_) dan wel een facultatieve overdrachtparameterbyte (TRTP of TREP) kunnen omvatten;

— controlesom bestaande uit een controlesombyte (CS).

Beginlabel				Gegevensveld					Controlesom
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 bytes				Max. 255 bytes					1 byte

(*) De ingebrachte kaart geeft de vereiste toegangsrechten voor het downloaden en tot de gegevens. Het is echter mogelijk gegevens over te brengen van een in één van de VU-lezers ingebrachte kaart als geen andere kaart in de andere lezer is ingebracht.

De TGT- en SRC-byte vertegenwoordigen het fysieke adres van de ontvanger en verzender van het bericht. Waarden zijn F0 Hex voor de IDE en EE Hex voor de VU.

De LEN-byte is de lengte van het gegevensvelddeel.

De controlesombyte is de 8-bits somserie module 256 van alle bytes van het bericht exclusief de CS zelf.

FMT, SID, DS_, TRTP en TREP-bytes worden verderop in dit document gedefinieerd.

DDP_003 Als de door het bericht over te dragen gegevens groter zijn dan de beschikbare ruimte in het gegevensvelddeel, wordt het bericht in een aantal subberichten verzonden. Elk subbericht heeft een beginlabel, hetzelfde SID en dezelfde TREP en een teller van 2 bytes voor de subberichten die het volgnummer van het subbericht binnen het totale bericht aangeeft. Met het oog op fouten-controle en voortijdige beëindiging bevestigt de IDE elk subbericht. De IDE kan het subbericht accepteren, vragen om het opnieuw te zenden, de VU verzoeken om opnieuw te beginnen of de overbrenging afbreken.

DDP_004 Indien het laatste subbericht precies 255 bytes in het gegevensveld bevat, moet een laatste subbericht met een leeg gegevensveld (met uitzondering van SID, TREP en teller van de subberichten) worden toegevoegd dat het einde van het bericht aangeeft.

Voorbeeld:

Beginlabel	SID	TREP	Bericht	CS
4 bytes	Langer dan 255 bytes			

Wordt overgebracht als:

Beginlabel	SID	TREP	00	01	Subbericht 1	CS
4 bytes	255 bytes					

Beginlabel	SID	TREP	00	02	Subbericht 2	CS
4 bytes	255 bytes					

…

Beginlabel	SID	TREP	xx	yy	Subbericht n	CS
4 bytes	Minder dan 255 bytes					

of als:

Beginlabel	SID	TREP	00	01	Subbericht 1	CS
4 bytes	255 bytes					

Beginlabel	SID	TREP	00	02	Subbericht 2	CS
4 bytes	255 bytes					

…

Beginlabel	SID	TREP	xx	yy	Subbericht n	CS
4 bytes	255 bytes					

Beginlabel	SID	TREP	xx	yy + 1	CS
4 bytes	4 bytes				

2.2.2 *Soorten berichten*

Het communicatieprotocol voor de gegevensoverdracht tussen de VU en de IDE vereist de uitwisseling van 8 verschillende berichtensoorten.

De onderstaande tabel vat deze berichten samen.

Berichtstructuur	Max. 4 bytes Beginlabel				Max. 255 bytes Gegevens			1 byte Controle-som
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Start Communication Request	81	EE	F0		81			E0
Positive Response Start Communication	80	F0	EE	03	C1		EA, 8F	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		01,01, 01	EC
19 200 Bd	80	EE	F0	04	87		01,01, 02	ED
38 400 Bd	80	EE	F0	04	87		01,01, 03	EE
57 600 Bd	80	EE	F0	04	87		01,01, 04	EF
115 200 Bd	80	EE	F0	04	87		01,01, 05	F0
Positive Response Verify Baud Rate	80	F0	EE	02	C7		01	28
Transition Baud Rate (stage 2)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0A	35		00,00, 00,00, 00,FF,FF, FF,FF	99
Positive Response Request Upload	80	F0	EE	03	75		00,FF	D5

Berichtstructuur	Max. 4 bytes Beginlabel				Max. 255 bytes Gegevens			1 byte Controle-som
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Transfer Data Request								
Overview	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events & Faults	80	EE	F0	02	36	03		99
Detailed Speed	80	EE	F0	02	36	04		9A
Technical Data	80	EE	F0	02	36	05		9B
Card download	80	EE	F0	02	36	06	Slot	CS
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Gege-vens	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Trans-fer Exit	80	F0	EE	01	77			D6
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Commu-nication	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 Re-quest 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

Opmerkingen:

— Sid Req = het Sid van het corresponderende verzoek.

— TREP = de TRTP van het corresponderende verzoek.

— Zwarte cellen geven aan dat niets wordt overgebracht.

— De term upload (vanaf de IDE) wordt gebruikt voor compatibiliteit met ISO 14229. Het betekent hetzelfde als download (vanaf de VU).

— Potentiële tellers van 2 bytes voor het tellen van subberichten worden in deze tabel niet getoond.

— Lezer is het lezernummer, "1" (kaart in de lezer van de bestuurder) of "2" (kaart in de lezer van de bijrijder).

— Indien de lezer niet is gespecificeerd, kiest de VU lezer 1 indien een kaart in die lezer is ingebracht en kiest hij lezer 2 alleen als die specifiek door de gebruiker wordt geselecteerd.

2.2.2.1 Start Communication Request (SID 81)

DDP_005 Dit bericht wordt door de IDE verstrekt om de overdrachtsverbinding met de VU tot stand te brengen. Aanvankelijk vindt overdracht steeds plaats bij 9 600 baud (tot de baudsnelheid uiteindelijk wordt gewijzigd met behulp van de passende Link Control Service).

2.2.2.2 Positive Response Start Communication (SID C1)

DDP_006 Dit bericht wordt door de VU verstrekt om positief te antwoorden op een verzoek om de start van de overdracht. Het bevat de 2 sleutelbytes 'EA' en '8F', die aangeven dat de unit het protocol met beginlabel inclusief informatie over doel, bron en lengte ondersteunt.

2.2.2.3 Start Diagnostic Session Request (SID 10)

DDP_007 Het bericht Start Diagnostic Session Request wordt door de IDE verstrekt om een nieuwe diagnostische sessie met de VU aan te vragen. De subfunctie 'defaultsessie' (81 Hex) geeft aan dat een standaard diagnostische sessie wordt geopend.

2.2.2.4 Positive Response Start Diagnostic (SID 50)

DDP_008 Het bericht Positive Response Start Diagnostic wordt door de VU gezonden om positief te antwoorden op Diagnostic Session Request.

2.2.2.5 Link Control Service (SID 87)

DDP_052 De Link Control Service wordt door de IDE gebruikt om een wijziging in de baudsnelheid te starten. Dat gebeurt in twee stappen. In stap een stelt de IDE voor de baudsnelheid te wijzigen, met vermelding van de nieuwe snelheid. Na ontvangst van een positief bericht van de VU zendt de IDE bevestiging van de wijziging van de baudsnelheid naar de VU (stap twee). De IDE gaat dan over op de nieuwe baudsnelheid. Na ontvangst van de bevestiging gaat de VU over op de nieuwe baudsnelheid.

2.2.2.6 Link Control Positive Response (SID C7)

DDP_053 De Link Control Positive Response wordt door de VU gegeven om positief te antwoorden op het verzoek van de Link Control Service (stap een). Merk op dat het bevestigingsbericht niet wordt beantwoord (stap twee).

2.2.2.7 Request Upload (SID 35)

DDP_009 Het bericht Request Upload wordt door de IDE verstrekt om aan de VU te melden dat een downloadoperatie wordt gevraagd. Om aan het vereiste in ISO 14229 te voldoen, worden daarin gegevens opgenomen met betrekking tot het adres, de grootte en het formaat voor de gevraagde gegevens. Aangezien de IDE deze vóór de overbrenging niet kent, wordt het geheugenadres op 0 ingesteld, wordt het formaat niet geëncrypteerd en gecomprimeerd en wordt de geheugengrootte op het maximum ingesteld.

2.2.2.8 Positive Response Request Upload (SID 75)

DDP_010 Het bericht Positive Response Request Upload wordt door de VU gezonden om de IDE te laten weten dat de VU gereed is om gegevens te downloaden. Om aan het vereiste in ISO 14229 te voldoen, worden in dit positieve antwoordbericht gegevens opgenomen om de IDE te laten weten dat verdere Positive Response Transfer Data-berichten maximaal 00FF hex bytes zullen bevatten.

2.2.2.9 Transfer Data Request (SID 36)

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

Er zijn zes soorten gegevensoverdracht:

— overzicht (TRTP 01),

— activiteiten van een gespecificeerde datum (TRTP 02),

— voorvallen en fouten (TRTP 03),

— gedetailleerde snelheid (TRTP 04),

— technische gegevens (TRTP 05),

— kaartdownload (TRTP 06).

DDP_054 De IDE is verplicht gedurende een overbrengingssessie de overdracht van overzichtsgegevens (TRTP 01) 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) bevat het bericht Transfer Data Request de aanwijzing van de te downloaden kalenderdag (`TimeReal` opmaak).

2.2.2.10 Positive Response Transfer Data (SID 76).

DDP_012 Het Positive Response Transfer Data wordt door de VU verzonden in antwoord op het Transfer Data Request. Het bericht bevat de gevraagde gegevens met een Transfer Response Parameter (TREP) die correspondeert met de TRTP van het verzoek.

DDP055 In het eerste geval (TREP 01) zendt de VU gegevens waarmee de operator van de IDE kan kiezen welke gegevens hij verder wil overbrengen. 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.

2.2.2.11 Request Transfer Exit (SID 37)

DDP_013 Het bericht Request Transfer Exit wordt door de IDE gezonden om de VU te melden dat de overdrachtssessie beëindigd is.

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

DDP_014 Het bericht Positive Response Request Transfer Exit wordt door de VU gezonden om het Request Transfer Exit te bevestigen.

2.2.2.13 Stop Communication Request (SID 82)

DDP_015 Het bericht Stop Communication Request wordt door de IDE gezonden om de overdrachtsverbinding met de VU te verbreken.

2.2.2.14 Positive Response Stop Communication (SID C2)

DDP_016 Het bericht Positive Response Stop Communication wordt door de VU gezonden om het Stop Communication Request te bevestigen.

2.2.2.15 Acknowledge Sub Message (SID 83)

DDP_017 Het Acknowledge Sub Message wordt door de IDE gezonden om de ontvangst te bevestigen van elk deel van een bericht dat in een aantal subberichten wordt overgebracht. Het gegevensveld bevat het van de VU ontvangen SID en een code van 2 bytes:

— MsgC + 1 bevestigt de correcte ontvangst van het subbericht met de code MsgC.

Verzoek van de IDE aan de VU om het volgende subbericht te zenden.

— MsgC geeft een probleem met de ontvangst van het subbericht met de code MsgC aan.

Verzoek van de IDE aan de VU om het volgende subbericht te zenden.

— FFFF verzoekt om de beëindiging van het bericht.

Dit kan door de IDE worden gebruikt om de overbrenging van het bericht van de VU om welke reden dan ook te beëindigen.

Het laatste subbericht van een bericht (LEN byte < 255) kan met gebruikmaking van een van deze codes bevestigd of niet bevestigd worden.

De uit verschillende subberichten bestaande antwoorden van de VU zijn:

— Positive Response Transfer Data (SID 76).

2.2.2.16 Negative Response (SID 7F)

DDP_018 Het bericht Negative Response wordt door de VU gezonden in antwoord op de bovengenoemde verzoeken wanneer de VU niet aan het verzoek kan voldoen. De gegevensvelden van het bericht bevatten het SID van het antwoord (7F), het SID van het verzoek en een code die de reden van het negatieve antwoord specificeert. De onderstaande codes zijn beschikbaar:

— 10 algemene verwerping

De actie kan niet worden uitgevoerd om een reden die hieronder niet wordt genoemd.

— 11 dienst niet ondersteund

Het SID van het verzoek wordt niet herkend.

— 12 subfunctie niet ondersteund

Het DS_ of TRTP van het verzoek wordt niet herkend of er zijn geen over te brengen subberichten meer.

— 13 onjuiste lengte van het bericht

De lengte van het ontvangen bericht is fout.

— 22 voorwaarden niet correct of verzoeksequentiefout

De gevraagde dienst is niet actief of de sequentie van verzoekberichten is niet correct.

— 31 verzoek buiten bereik

De verzoek parameter record (gegevensveld) is niet geldig.

— 50 upload niet geaccepteerd

Het verzoek kan niet worden uitgevoerd (VU in een niet-geschikte werkingsmodus of interne fout van de VU).

— 78 antwoord in behandeling

De verzochte actie kan niet op tijd worden beëindigd en de VU is niet klaar om een ander verzoek te accepteren.

— FA-gegevens niet beschikbaar

Het gegevensobject van een verzoek om gegevensoverdracht is niet beschikbaar in de VU (omdat er bijv. geen kaart is ingebracht).

2.2.3 *Berichtenstroom*

Een typische berichtenstroom tijdens een normale gegevensdownloadsprocedure ziet er als volgt uit:

IDE		VU
Start Communication Request	⇨ ⇦	Positive Response
Start Diagnostic Service Request	⇨ ⇦	Positive Response
Request Upload	⇨ ⇦	Positive Response

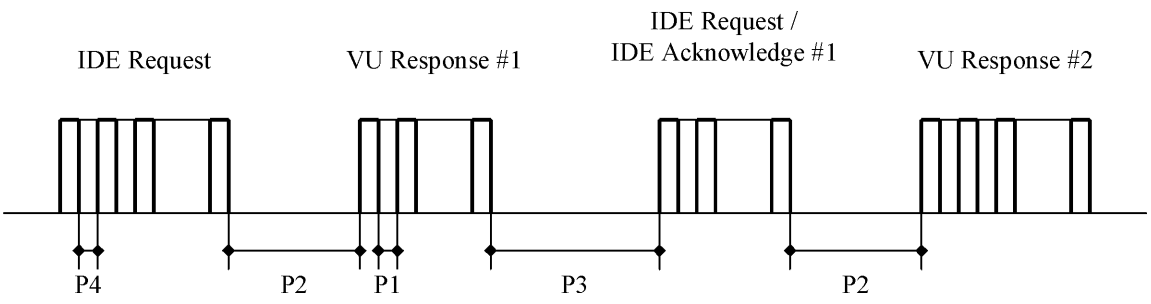
IDE		VU
Transfer Data Request Overview	⇨	
	⇦	Positive Response
Transfer Data Request #2	⇨	
	⇦	Positive Response #1
Acknowledge Sub Message #1	⇨	
	⇦	Positive Response #2
Acknowledge Sub Message #2	⇨	
	⇦	Positive Response #m
Acknowledge Sub Message #m	⇨	
	⇦	Positive Response (Data Field < 255 Bytes)
Acknowledge Sub Message (optional)	⇨	
…		
Transfer Data Request #n	⇨	
	⇦	Positive Response
Request Transfer Exit	⇨	
	⇦	Positive Response
Stop Communication Request	⇨	
	⇦	Positive Response

2.2.4 *Tijdschema*

DDP_019 Tijdens de normale werking zijn de in de onderstaande figuur getoonde timingparameters relevant:

Figuur 1

Berichtenstroom, timing



Waarbij:

P1 = Interbytetijd voor antwoord van de VU.

P2 = Tijd tussen het einde van het verzoek van de IDE en de start van het antwoord van de VU, of tussen het einde van de bevestiging van de IDE en de start van het volgende antwoord van de VU.

P3 = Tijd tussen het einde van het antwoord van de VU en de start van een nieuw verzoek van de IDE, of tussen het einde van het antwoord van de VU en de start van de bevestiging van de IDE, of tussen het einde van het verzoek van de IDE en de start van een nieuw verzoek van de IDE, indien de VU niet antwoordt.

P4 = Interbytetijd voor verzoek van de IDE.

P5 = Toegevoegde waarde van P3 voor kaartdownload.

De toegestane waarden van de timingparameters worden in de onderstaande tabel aangegeven (toebedeelde reeks timingparameters van het KWP, gebruikt in geval van fysieke adressering voor snellere overdracht).

Tijdschemaparameter	Benedengrenswaarde (ms)	Bovengrenswaarde (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minuten

(*) Indien de VU antwoordt met een Negative Response die een code met de betekenis "verzoek correct ontvangen, antwoord in behandeling" bevat, wordt deze waarde toegevoegd aan dezelfde bovengrenswaarde van P3.

2.2.5 *Behandeling van fouten*

Indien tijdens de uitwisseling van berichten een fout optreedt, wordt het berichtenstroomschema gewijzigd volgens de apparatuur die de fout heeft opgespoord en het bericht dat de fout heeft veroorzaakt.

In figuur 2 en figuur 3 worden de procedures voor de behandeling van fouten voor respectievelijk de VU en de IDE getoond.

2.2.5.1 Start communicatie-fase

DDP_020 Indien de IDE tijdens de start communicatie-fase, door timing of door de bitstroom, een fout opspoort, dan moet de IDE een P3min-periode wachten alvorens het verzoek opnieuw te doen.

DDP_021 Indien de VU in de door de IDE gezonden sequentie een fout opspoort, mag de VU geen antwoord zenden maar moet hij wachten op een ander Start Communication Request-bericht binnen een P3max-periode.

2.2.5.2 Overbrengingsfase

Er kunnen twee verschillende gebieden voor de behandeling van fouten worden gedefinieerd:

1. **De VU spoort een overbrengingsfout van de IDE op.**

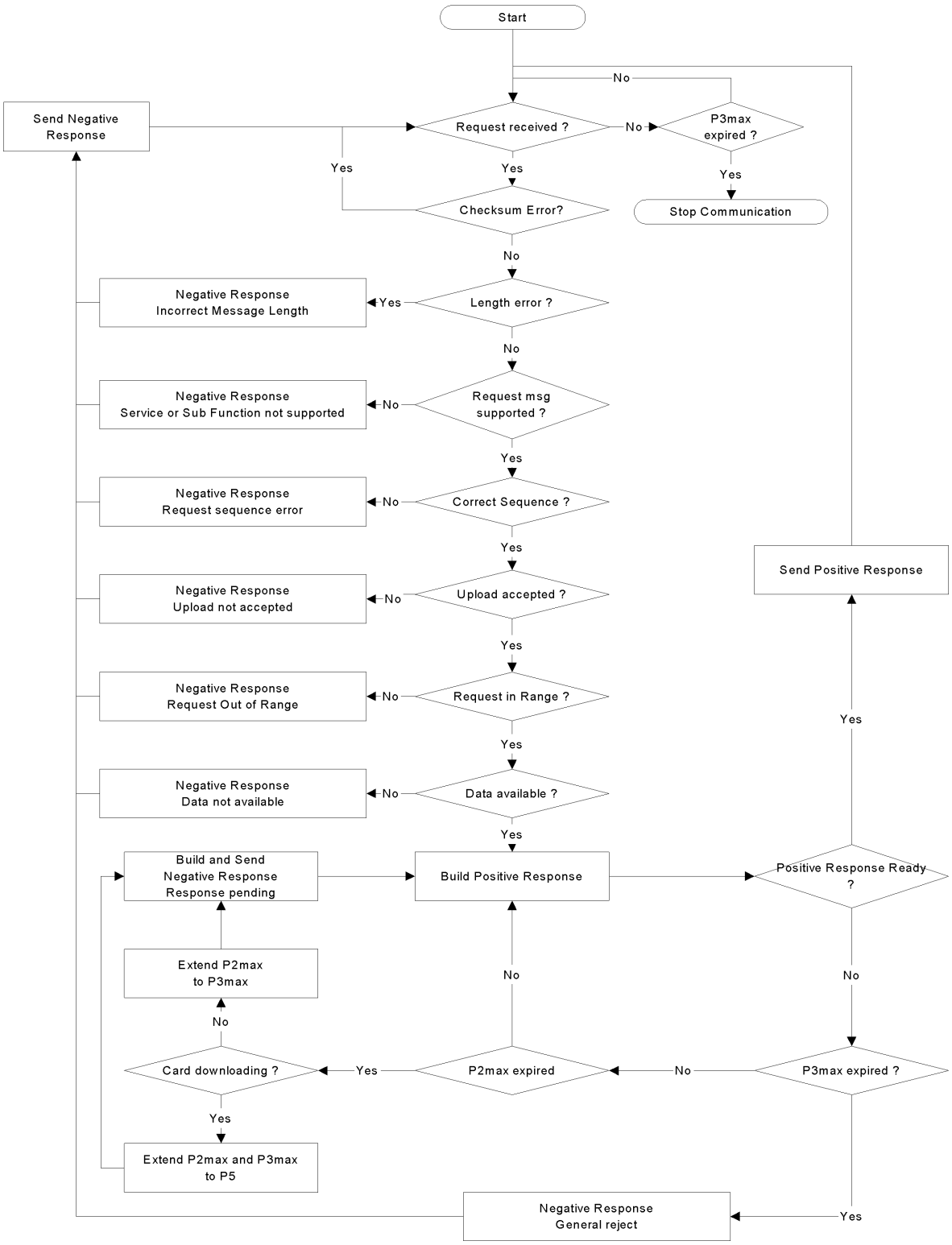
DDP_022 Voor elk ontvangen bericht moet de VU timingfouten, byteopmaakfouten (bijv. foutieve start- en stopbits) en frame errors (verkeerd aantal bytes ontvangen, foutieve controlesombyte) opsporen.

DDP_023 Indien de VU een van de bovengenoemde fouten opspoort, dan zendt hij geen antwoord en negeert hij het ontvangen bericht.

DDP_024 De VU kan andere fouten in de opmaak of inhoud van het ontvangen bericht opsporen (bijv. bericht niet ondersteund), zelfs indien het bericht voldoet aan de lengte- en controlesomeisen; in dat geval moet de VU aan de IDE met een Negative Response-bericht antwoorden waarin de aard van de fout wordt gespecificeerd.

Figuur 2

VU-foutbehandeling



2. **De IDE spoort een overbrengingsfout van de VU op.**

DDP_025 Voor elk ontvangen bericht moet de IDE timingfouten, fouten in de byteopmaak (bijv. foutieve start- en stopbits) en frame errors (verkeerd aantal bytes ontvangen, foutieve controlesombyte) opsporen.

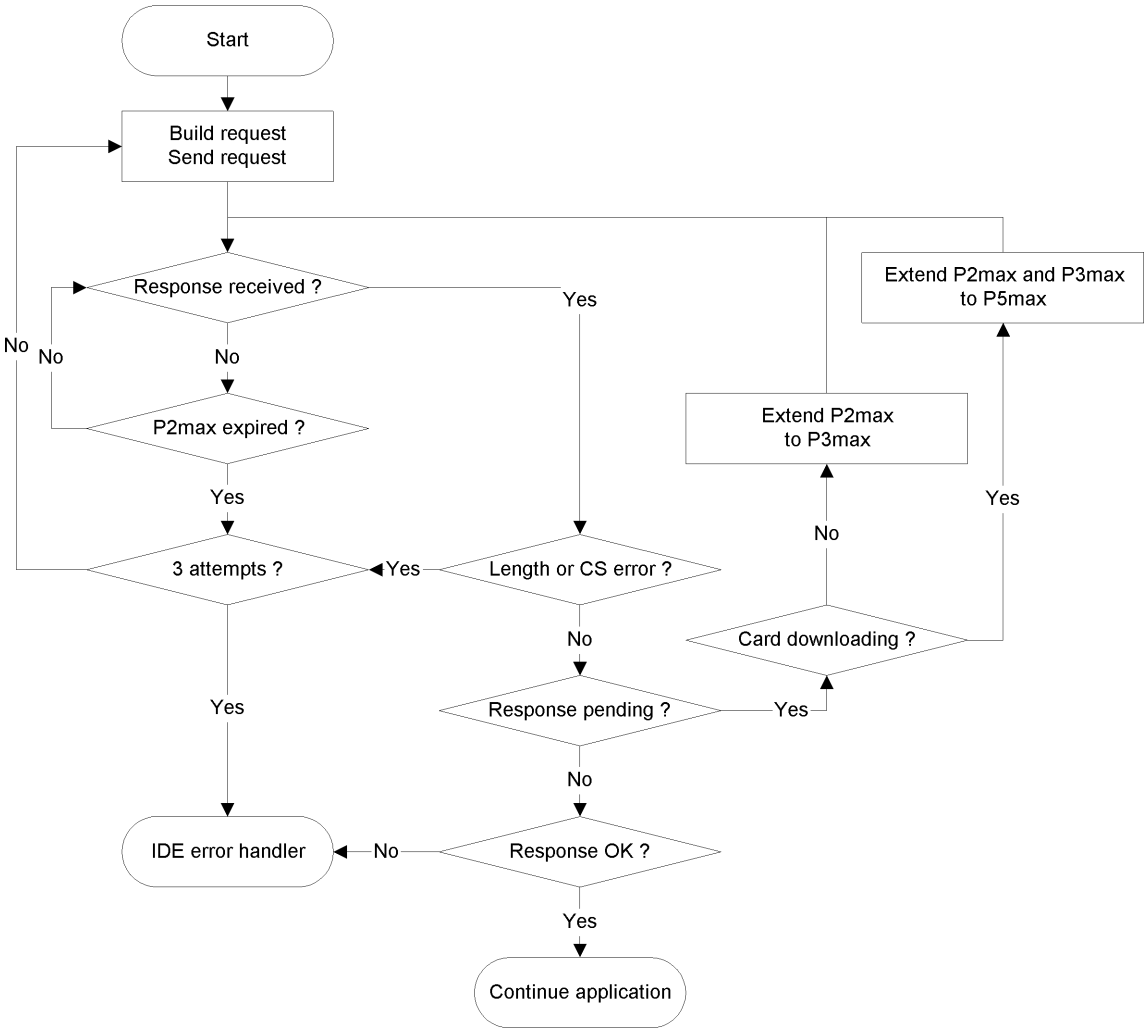
DDP_026 De IDE moet sequentiefouten opsporen, bijv. niet correcte standverhogingen bij de teller van de subberichten bij na elkaar ontvangen berichten.

DDP_027 Indien de IDE een fout opspoort of indien er binnen een P2max-periode geen antwoord van de VU was, wordt het verzoekbericht opnieuw gezonden met een maximum van totaal drie overbrengingen. Voor het doel van deze foutenopsporing wordt de bevestiging van een subbericht beschouwd als een verzoek aan de VU.

DDP_028 De IDE moet ten minste een P3min-periode wachten voor de start van elke overbrenging; de wachttijd moet worden gemeten vanaf de laatst berekende optreding van een stopbit nadat de fout was opgespoord.

Figuur 3

IDE-foutbehandeling



2.2.6 *Inhoud van het antwoordbericht*

Dit punt specificeert de inhoud van de gegevensvelden van de verschillende positieve antwoordberichten.

Gegevenselementen worden gedefinieerd in de data dictionary in aanhangsel 1.

Opmerking: Voor downloads van de 2e generatie wordt elk gegevenselement op het hoogste niveau vertegenwoordigd door een reeks records, zelfs als het maar één record bevat. Een reeks records begint met een beginlabel. Dat beginlabel bevat het soort record, de grootte van het record en het aantal records. Reeksen records worden in de volgende tabellen aangeduid door "…RecordArray" (met beginlabel).

2.2.6.1 Positive Response Transfer Data Overview

DDP_029 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 Hex en de passende splitsing en telling van de subberichten verstrekken:

Gegevensstructuur 1e generatie

Gegevenselement	Opmerking
MemberStateCertificate VUCertificate	VU-veiligheidscertificaten
VehicleIdentificationNumber VehicleRegistrationIdentification	Identificatie van het voertuig
CurrentDateTime	Huidige datum en tijd van de VU
VuDownloadablePeriod	Downloadbare periode
CardSlotsStatus	Soorten in de VU ingebrachte kaarten
VuDownloadActivityData	Vorige VU-download
VuCompanyLocksData	Alle bedrijfsvergrendelingen opgeslagen. Indien dit segment leeg is, wordt alleen noOfLocks = 0 verzonden.
VuControlActivityData	Alle in de VU opgeslagen controlerecords. Indien dit segment leeg is, wordt alleen noOfControls = 0 verzonden.
Signature	RSA-handtekening van alle gegevens (behalve certificaten) vanaf VehicleIdentificationNumber tot de laatste byte van de laatste VuControlActivityData.

Gegevensstructuur 2e generatie

Gegevenselement	Opmerking
MemberStateCertificateRecordArray	Lidstaatcertificaat
VUCertificateRecordArray	VU-certificaat
VehicleIdentificationNumberRecordArray	Identificatie van het voertuig
VehicleRegistrationNumberRecordArray	Voertuigregistratienummer
CurrentDateTimeRecordArray	Huidige datum en tijd van de VU
VuDownloadablePeriodRecordArray	Downloadbare periode
CardSlotsStatusRecordArray	Soorten in de VU ingebrachte kaarten
VuDownloadActivityDataRecordArray	Vorige VU-download
VuCompanyLocksRecordArray	Alle bedrijfsvergrendelingen opgeslagen. Indien het segment leeg is, wordt alleen een beginlabel van een reeks met noOfRecords = 0 verzonden.
VuControlActivityRecordArray	Alle in de VU opgeslagen controlerecords. Indien het segment leeg is, wordt alleen een beginlabel van een reeks met noOfRecords = 0 verzonden.
SignatureRecordArray	ECC-handtekening van alle voorgaande gegevens behalve de certificaten.

2.2.6.2 Positive Response Transfer Data Activities

DDP_030 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 Hex en de passende splitsing en telling van de subberichten verstrekken:

Gegevensstructuur 1e generatie

Gegevenselement	Opmerking
TimeReal	Datum van de gedownloade dag
OdometerValueMidnight	Kilometerstand aan het einde van de gedownloade dag
VuCardIWData	Gegevens over de cycli van inbrengen en uitnemen van kaarten. — Indien deze passage geen beschikbare gegevens bevat, wordt alleen noOfVuCardIWRecords = 0 verzonden. — Wanneer een VuCardIWRecord 00:00 (kaart ingebracht op de vorige dag) of 24:00 (kaart uitgenomen de volgende dag) overschrijdt, wordt het volledig getoond op de twee betrokken dagen.
VuActivityDailyData	Status van de lezers op 00:00 en opgeslagen activiteitswijzigingen op de gedownloade dag.
VuPlaceDailyWorkPeriodData	Opgeslagen plaatsgegevens op de gedownloade dag. Indien dit segment leeg is, wordt alleen noOfPlaceRecords = 0 verzonden.
VuSpecificConditionData	Opgeslagen gegevens over specifieke omstandigheden op de gedownloade dag. Indien dit segment leeg is, wordt alleen noOfSpecificConditionRecords = 0 verzonden.
Signature	RSA-handtekening van alle gegevens vanaf TimeReal tot de laatste byte van de laatste specifieke omstandigheden-record

Gegevensstructuur 2e generatie:

Gegevenselement	Opmerking
DateOfDayDownloadedRecordArray	Datum van de gedownloade dag
OdometerValueMidnightRecordArray	Kilometerstand aan het einde van de gedownloade dag
VuCardIWRecordArray	Gegevens over de cycli van inbrengen en uitnemen van kaarten. — Indien dit segment geen beschikbare gegevens bevat, wordt een beginlabel van een reeks met noOfRecords = 0 verzonden. — Wanneer een VuCardIWRecord 00:00 (kaart ingebracht op de vorige dag) of 24:00 (kaart uitgenomen de volgende dag) overschrijdt, wordt het volledig getoond op de twee betrokken dagen.
VuActivityDailyRecordArray	Status van de lezers op 00:00 en opgeslagen activiteitswijzigingen op de gedownloade dag.
VuPlaceDailyWorkPeriodRecordArray	Opgeslagen plaatsgegevens op de gedownloade dag. Indien het segment leeg is, wordt een beginlabel van een reeks met noOfRecords = 0 verzonden.
VuGNSSCDRecordArray	GNSS-posities van het voertuig indien de rijtijdperiode van de bestuurder een veelvoud van drie uur bereikt. Indien het segment leeg is, wordt alleen een beginlabel van een reeks met noOfRecords = 0 verzonden.
VuSpecificConditionRecordArray	Opgeslagen gegevens over specifieke omstandigheden op de gedownloade dag. Indien het segment leeg is, wordt een beginlabel van een reeks met noOfRecords = 0 verzonden.
SignatureRecordArray	ECC-handtekening van alle voorgaande gegevens.

2.2.6.3 Positive Response Transfer Data Events and Faults

DDP_031 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 Hex en de passende splitsing en telling van de subberichten verstrekken:

Gegevensstructuur 1e generatie

Gegevenselement	Opmerking
VuFaultData	Alle in de VU opgeslagen of lopende fouten. Indien dit segment leeg is, wordt alleen noOfVuFaults = 0 verzonden.
VuEventData	Alle in de VU opgeslagen of lopende voorvallen (behalve snelheidsoverschrijding). Indien het segment leeg is, wordt alleen noOfVuEvents = 0 verzonden.
VuOverSpeedingControlData	Gegevens met betrekking tot de laatste snelheidsoverschrijdingscontrole (standaardwaarde indien er geen gegevens zijn).
VuOverSpeedingEventData	Alle in de VU opgeslagen snelheidsoverschrijdingen. Indien het segment leeg is, wordt alleen noOfVuOverSpeedingEvents = 0 verzonden.
VuTimeAdjustmentData	Alle in de VU opgeslagen tijdafstellingen (buiten het kader van een volledige kalibrering). Indien het segment leeg is, wordt alleen noOfVuTimeAdjrecords = 0 verzonden.
Signature	RSA-handtekening van alle gegevens vanaf noOfVuFaults tot de laatste byte van de laatste tijdafstellingsrecord.

Gegevensstructuur 2e generatie:

Gegevenselement	Opmerking
VuFaultRecordArray	Alle in de VU opgeslagen of lopende fouten. Indien het segment leeg is, wordt een beginlabel van een reeks met noOfRecords = 0 verzonden.
VuEventRecordArray	Alle in de VU opgeslagen of lopende voorvallen (behalve snelheidsoverschrijding). Indien het segment leeg is, wordt een beginlabel van een reeks met noOfRecords = 0 verzonden.
VuOverSpeedingControlDataRecordArray	Gegevens met betrekking tot de laatste snelheidsoverschrijdingscontrole (standaardwaarde indien er geen gegevens zijn).
VuOverSpeedingEventRecordArray	Alle in de VU opgeslagen snelheidsoverschrijdingen. Indien het segment leeg is, wordt een beginlabel van een reeks met noOfRecords = 0 verzonden.
VuTimeAdjustmentRecordArray	Alle in de VU opgeslagen tijdafstellingen (buiten het kader van een volledige kalibrering). Indien het segment leeg is, wordt een beginlabel van een reeks met noOfRecords = 0 verzonden.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	ECC-handtekening van alle voorgaande gegevens.

2.2.6.4 Positive Response Transfer Data Detailed Speed

DDP_032 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 Hex en de passende splitsing en telling van de subberichten verstrekken:

Gegevensstructuur 1e generatie

Gegevenselement	Opmerking
VuDetailedSpeedData	Alle in de VU opgeslagen gegevens over gedetailleerde snelheid (één snelheidsblok per minuut waarin het voertuig rijdt). 60 snelheidswaarden per minuut (één per seconde).
Signature	RSA-handtekening van alle gegevens vanaf noOfSpeedBlocks tot de laatste byte van het laatste snelheidsblok.

Gegevensstructuur 2e generatie:

Gegevenselement	Opmerking
VuDetailedSpeedBlockRecordArray	Alle in de VU opgeslagen gegevens over gedetailleerde snelheid (één snelheidsblok per minuut waarin het voertuig rijdt). 60 snelheidswaarden per minuut (één per seconde).
SignatureRecordArray	ECC-handtekening van alle voorgaande gegevens.

2.2.6.5 Positive Response Transfer Data Technical Data

DDP_033 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 Hex en de passende splitsing en telling van de subberichten verstrekken:

Gegevensstructuur 1e generatie

Gegevenselement	Opmerking
VuIdentification	
SensorPaired	
VuCalibrationData	Alle in de VU opgeslagen kalibreringsrecords.
Signature	RSA-handtekening van alle gegevens vanaf vuManufacturerName tot de laatste byte van de laatste VuCalibrationRecord.

Gegevensstructuur 2e generatie:

Gegevenselement	Opmerking
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Alle in de VU opgeslagen sensorverbindingen.
VuSensorExternalGNSSCoupledRecordArray	Alle in de VU opgeslagen verbindingen met de externe GNSS-module.
VuCalibrationRecordArray	Alle in de VU opgeslagen kalibreringsrecords.
VuCardRecordArray	Alle in de VU opgeslagen gegevens over kaartinbrenging.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	ECC-handtekening van alle voorgaande gegevens.

2.3. **ESM bestandsopslag**

DDP_034 Wanneer tijdens een downloadsessie een gegevensoverdracht van een VU heeft plaatsgevonden, moet de IDE alle tijdens de downloadsessie van de VU in de berichten Positive Response Transfer Data ontvangen gegevens in één fysiek veld opslaan. Opgeslagen gegevens zijn exclusief beginlabels van berichten, tellers van subberichten, lege subberichten en controlesommen maar inclusief het SID en TREP (alleen van het eerste subbericht indien er verscheidene subberichten zijn).

3. DOWNLOADPROTOCOL VAN TACHOGRAAFKAARTEN

3.1. **Toepassingsgebied**

Dit punt beschrijft de directe gegevensoverdracht van een tachograafkaart naar een IDE. De IDE maakt geen deel uit van de beveiligde omgeving; daarom vindt er geen authenticatie tussen de kaart en de IDE plaats.

3.2. **Definities**

Downloadsessie: Elke keer dat er gegevens van de chipkaart worden gedownload. De sessie omvat de volledige procedure vanaf het resetten van de chipkaart door een IFD tot de inactivering van de chipkaart (uitnemen van de kaart of volgende reset).

Getekend gegevensbestand: Een bestand van de chipkaart. Het bestand wordt ongecodeerd naar de IFD overgebracht. Op de chipkaart wordt het bestand gehashed en getekend; de handtekening wordt naar de IFD overgebracht.

3.3. **Kaartdownload**

DDP_035 De download van een tachograafkaart omvat de onderstaande stappen:

— Download van de algemene informatie van de kaart naar de `chipkaart` en `IC` van het EF. Deze informatie is facultatief en wordt niet met een digitale handtekening beveiligd.

— Overdracht van het `Card_Certificate` (of `CardSignCertificate`) 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` en `Tachograph_G2 DF` indien van toepassing) met uitzondering van `Card_Download` van het EF. Deze informatie wordt met een digitale handtekening beveiligd.

— Het is verplicht om ten minste de `Application_Identification` en `ID` 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`,
- `GNSS_Places (indien van toepassing)`,
- `Control_Activity_Data`,
- `Specific_Conditions`.

— Bij de download van een bestuurderskaart moet de datum van de `LastCardDownload` in `Card_Download` van het EF worden aangepast.

— Bij de download van een werkplaatskaart moet de kalibreringsteller in `Card_Download` van het EF worden gereset.

— Bij de download van een werkplaatskaart mag `EF Sensor_Installation_Data` niet worden gedownload.

3.3.1 *Initialisatiesequentie*

DDP_036 De IDE moet de sequentie als volgt initiëren:

Kaart	Richting	IDE/IFD	Betekenis/Opmerkingen
	⇦	Hardware resetten	
ATR	⇨		

Het gebruik van PPS om over te schakelen op een hogere baudsnelheid is facultatief zolang de chipkaart dit ondersteunt.

3.3.2 *Sequentie voor niet-getekende gegevensbestanden*

DDP_037 De sequentie voor download van de chipkaart, IC, Card_Certificate (of CardSignCertificate) en CA_Certificate van het EF is als volgt:

Kaart	Richting	IDE/IFD	Betekenis/Opmerkingen
	⇦	**Select file**	Selecteer met bestandsidentificatiesymbolen
OK	⇨		
	⇦	**Read binary**	Indien het bestand meer gegevens bevat dan de grootte van het buffergeheugen van de lezer of van de kaart, moet het commando worden herhaald totdat het volledige bestand gelezen is.
Bestandsgegevens OK	⇨	Sla gegevens in ESM op	overeenkomstig **3.4** Opmaak gegevensopslag

Noot 1: Voor het selecteren van het Card_Certificate (of CardSignCertificate) van het EF, moet de tachograaftoepassing worden geselecteerd (selectie met AID).

Noot 2: Een bestand lezen en selecteren kan ook in één stap worden uitgevoerd met het Read Binary-commando met een kort EF-identificatiesymbool.

3.3.3 *Sequentie voor getekende gegevensbestanden*

DDP_038 De onderstaande sequentie moet worden gebruikt voor elk van de volgende bestanden die met hun handtekening moeten worden overgebracht:

Kaart	Richting	IDE/IFD	Betekenis/Opmerkingen
	⇦	**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. 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 totdat het volledige bestand is gelezen.
Bestands-gegevens OK	⇨	Sla ontvangen gegevens in ESM op	Overeenkomstig **3.4** Opmaak gegevensopslag
	⇦	**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** Opmaak gegevensopslag

Noot: Een bestand selecteren en lezen kan ook in één stap worden uitgevoerd met het Read Binary-commando met een kort EF-identificatiesymbool. In dit geval kan het EF worden geselecteerd en gelezen vóór het commando "perform hash of file" wordt toegepast.

3.3.4 *Sequentie voor het resetten van de kalibreringsteller*

DDP_039 De sequentie voor het resetten van de `NoOfCalibrationsSinceDownload`-teller in de `Card_Download` van het EF op een werkplaatskaart is de volgende:

Kaart	Richting	IDE/IFD	Betekenis/Opmerkingen
	⇦	**Select File** EF Card_Download	Selecteer met bestandsidentificatiesymbolen
OK	⇨		

Kaart	Richting	IDE/IFD	Betekenis/Opmerkingen
	⇦	**Update Binary** NoOfCalibrationsSince-Download = '00 00'	
Reset het volgnummer van kaartdownload			
OK	⇨		

Noot: Een bestand selecteren en lezen kan ook in één stap worden uitgevoerd met het Update Binary-commando met een kort EF-identificatiesymbool.

3.4. **Opmaak gegevensopslag**

3.4.1 *Inleiding*

DDP_040 De gedownloade gegevens moeten overeenkomstig de onderstaande voorwaarden worden opgeslagen:

— De gegevens moeten transparant worden opgeslagen. Dat betekent dat de volgorde van de bytes en de volgorde van de bits in de byte die vanaf de kaart worden overgebracht, tijdens de opslag gehandhaafd moeten blijven.

— Alle tijdens een downloadsessie overgebrachte bestanden van de kaart worden in één bestand in het ESM opgeslagen.

3.4.2 *Bestandsopmaak*

DDP_041 De bestandsopmaak is een aaneenschakeling van diverse TLV-objecten.

DDP_042 Het label voor een EF moet het FID plus de toevoeging "00" zijn.

DDP_043 Het label van een handtekening van een EF moet het FID van het bestand plus de toevoeging "01" zijn.

DDP_044 De lengte is een waarde van twee bytes. De waarde definieert het aantal bytes in het waardeveld. De waarde "FF FF" in het lengteveld wordt voor toekomstig gebruik gereserveerd.

DDP_045 Wanneer een bestand niet wordt gedownload, moeten geen gegevens met betrekking tot het bestand worden opgeslagen (geen label en geen nullengte).

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)	3 bytes
FID (2 bytes) || "01"	Label voor handtekening van EF (FID)	3 bytes
xx xx	Lengte van waardeveld	2 bytes

Voorbeeld van gegevens in een naar een ESM overgebracht 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`
`05 05 01`	`00 80`	Handtekening van EF `Vehicles_Used`

4. DOWNLOADEN VAN EEN TACHOGRAAFKAART VIA EEN VOERTUIGUNIT

DDP_047 De VU moet mogelijk maken de inhoud te downloaden van een bestuurderskaart die in een met de VU verbonden IDE is ingebracht

DDP_048 De IDE moet een "Transfer Data Request Card Download"-bericht naar de VU zenden om deze modus te initiëren (zie 2.2.2.9).

DDP_049 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.

DDP_050 De IDE moet de kaartgegevens van het "Positive Response Transfer Data"-bericht lezen (alle beginlabels, SID's, TREP's, tellers van subberichten en controlesommen verwijderen) en deze gegevens opslaan in een fysiek bestand zoals beschreven in punt 2.3.

DDP_051 De VU moet vervolgens, naar gelang van het geval, het bestand `Control_Activity_Data` of `Card_Download` van de bestuurderskaart bijwerken.

Aanhangsel 8

KALIBRERINGSPROTOCOL

INHOUDSOPGAVE

1. INLEIDING 283
2. TERMEN, DEFINITIES EN REFERENTIES 283
3. OVERZICHT VAN DIENSTEN 284
3.1. Beschikbare diensten 284
3.2. Antwoordcodes 285
4. COMMUNICATIEDIENSTEN 285
4.1. StartCommunication-dienst (Start overdracht) 285
4.2. StopCommunication Service 287
4.2.1 Omschrijving van het bericht 287
4.2.2 Berichtformaat 288
4.2.3 Parameterdefinitie 289
4.3. TesterPresent-dienst (Testapparaat actief) 289
4.3.1 Omschrijving van het bericht 289
4.3.2 Berichtformaat 289
5. BEHEERSDIENSTEN 291
5.1. StartDiagnosticSession-dienst (Start diagnostische sessie) 291
5.1.1 Omschrijving van het bericht 291
5.1.2 Berichtformaat 292
5.1.3 Parameterdefinitie 293
5.2. SecurityAccess-dienst (Veiligheidstoegang) 294
5.2.1 Omschrijving van het bericht 294
5.2.2 Berichtformaat — SecurityAccess — requestSeed 295
5.2.3 Berichtformaat — SecurityAccess — sendKey 296
6. GEGEVENSOVERBRENGINGSDIENSTEN 297
6.1. ReadDataByIdentifier-dienst (Lees gegevens met identificatiesymbool) 298
6.1.1 Omschrijving van het bericht 298
6.1.2 Berichtformaat 298
6.1.3 Parameterdefinitie 299
6.2. WriteDataByIdentifier service 300
6.2.1 Omschrijving van het bericht 300
6.2.2 Berichtformaat 300
6.2.3 Parameterdefinitie 302

7. CONTROLE VAN TESTIMPULSEN — INVOER-/UITVOERCONTROLE FUNCTIONELE EENHEID 302
7.1. InputOutputControlByIdentifier-dienst 302
7.1.1 Omschrijving van het bericht 302
7.1.2 Berichtformaat 303
7.1.3 Parameterdefinitie 304
8. FORMATEN VAN DATARECORDS 305
8.1. Overgebrachte parameterreeksen 305
8.2. Formaten van dataRecords 306

1. INLEIDING

In dit aanhangsel wordt beschreven hoe gegevens worden uitgewisseld tussen een voertuigunit en een testapparaat via de K-lijn die deel uitmaakt van de in aanhangsel 6 beschreven kalibreringsinterface. Voorts wordt ook de controle van de input/output-signaallijn op de kalibreringsconnector beschreven.

Het tot stand brengen van communicatie via de K-lijn wordt beschreven in punt 4 "Overdrachtsdiensten". Communicatiediensten

In dit aanhangsel wordt gebruik gemaakt van het idee van diagnostische "sessies" om het toepassingsgebied van K-lijncontrole onder verschillende omstandigheden vast te stellen. De standaardsessie is de "StandardDiagnostic-Session", waarin alle gegevens van een voertuigunit kunnen worden gelezen maar waarin geen gegevens naar een voertuigunit kunnen worden geschreven.

De selectie van de diagnostische sessie wordt beschreven in het punt 5 "Beheerdiensten".

Dit aanhangsel moet worden beschouwd als relevant voor beide generaties VU's en werkplaatskaarten, overeenkomstig de in deze verordening vastgestelde interoperabiliteitseisen.

CPR_001 Met de "ECUProgrammingSession" kunnen gegevens in de voertuigunit worden ingevoerd. Wanneer kalibreringsgegevens worden ingevoerd, moet de voertuigunit bovendien in de werkingsmodus CALIBRATION staan.

Gegevensoverdracht via K-lijn wordt beschreven in het punt 6 "Gegevensoverbrengingsdiensten". Gegevensoverbrengingsdiensten Formaten van overgebrachte gegevens worden nader beschreven in het punt 8 "Formaten van gegevensregistraties".Formaten van dataRecords

CPR_002 Met de "ECUAdjustmentSession" kan de I/O-modus van de I/O-signaallijn voor kalibrering via de K-lijninterface worden geselecteerd. De controle van de kalibrerings-I/O-signaallijn wordt beschreven in punt 7 "Controle van testimpulsen — Invoer-/uitvoercontrole functionele eenheid".

CPR_003 Overal in dit document wordt naar het testapparaat verwezen met het adres 'tt'. Hoewel er mogelijk voorkeuradressen zijn voor testapparaten, moet de VU correct reageren op elk adres van een testapparaat. Het fysieke adres van de VU is 0xEE.

2. TERMEN, DEFINITIES EN REFERENTIES

De protocollen, berichten en foutcodes zijn voornamelijk gebaseerd op een ontwerp van ISO 14229-1 (Road vehicles — Diagnostic systems — Part 1: Diagnostic services, versie 6 van 22 februari 2001).

Bytecodering en hexadecimale waarden worden voor de dienstidentificatiesymbolen, de dienstverzoeken en dienstantwoorden en de standaardparameters gebruikt.

De term „testapparaat" verwijst naar de inrichting die wordt gebruikt om programmeer-/kalibreringsgegevens in de VU in te voeren.

De termen „cliënt" en „server" verwijzen respectievelijk naar het testapparaat en de VU.

De term ECU betekent "elektronische controle-unit" en verwijst naar de VU.

Referenties:

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

Eerste editie: 1999.

Vehicles — Diagnostic.

3. OVERZICHT VAN DIENSTEN

3.1. **Beschikbare diensten**

De onderstaande tabel geeft een overzicht van de in de tachograaf beschikbare diensten; deze worden in dit document gedefinieerd.

CPR_004 De tabel geeft de diensten aan die in een actieve diagnostische sessie beschikbaar zijn.

— De **1ste kolom** vermeldt de beschikbare diensten.

— De **2de kolom** bevat het nummer van het punt in dit aanhangsel, waarin de dienst nader wordt gedefinieerd.

— De **3de kolom** kent de waarden van het dienstidentificatiesymbool toe voor verzoekberichten.

— De **4de kolom** specificeert de diensten van de **"StandardDiagnosticSession" (SD)** (standaard diagnostische sessie) die in elke VU geïmplementeerd moeten worden.

— De **5de kolom** specificeert de diensten van de **"ECUAdjustmentSession" (ECUAS)** (ECU-afstellingssessie) die geïmplementeerd moeten worden om controle van de I/O-signaallijn in het frontpaneel van de kalibreringsconnector van de VU mogelijk te maken.

— De **6de kolom** specificeert de diensten van de ECUPS (ECU-ProgrammingSession) die geïmplementeerd moeten worden om programmering van de parameters in de VU mogelijk te maken.

Tabel 1

Verzameltabel 1waarden dienstidentificatiesymbolen

			Diagnostische sessies		
Naam van de diagnostische dienst	Sectie nr.	SId Vereiste waarde	SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Dit symbool geeft aan dat deze dienst verplicht is in deze diagnostische sessie.

Geen symbool geeft aan dat deze dienst in deze diagnostische sessie niet is toegestaan.

3.2. **Antwoordcodes**

Voor elke dienst zijn antwoordcodes bepaald.

4. COMMUNICATIEDIENSTEN

Een aantal diensten zijn noodzakelijk voor het tot stand brengen en handhaven van de overdracht. Ze komen niet voor op de toepassingslaag. De beschikbare diensten worden in de onderstaande tabel beschreven:

Tabel 2

Communicatiediensten

Naam van de dienst	Beschrijving
StartCommunication	De cliënt verzoekt een overdrachtsessie met (een) server(s) te starten.
StopCommunication	De cliënt verzoekt de huidige overdrachtsessie te beëindigen.
TesterPresent	De cliënt wijst de server erop dat de verbinding nog actief is.

CPR_005 De StartCommunication Service wordt gebruikt voor het starten van een overdracht. Om een dienst uit te kunnen voeren, moet de overdracht geïnitialiseerd worden en moeten de overdrachtparameters geschikt zijn voor de gewenste modus.

4.1. **StartCommunication-dienst (Start overdracht)**

CPR_006 Na ontvangst van een StartCommunication-indicatieprimitief moet de VU controleren of de gevraagde overdrachtverbinding onder de aanwezige voorwaarden geïnitialiseerd kan worden. Geldige voorwaarden voor de initialisatie van een overdrachtverbinding worden in document ISO 14230-2 beschreven.

CPR_007 Vervolgens moet de VU alle noodzakelijke acties uitvoeren om de overdrachtverbinding te initialiseren en een StartCommunication-antwoordprimitief met de geselecteerde Positive Response-parameters zenden.

CPR_008 Indien een reeds geïnitialiseerde VU (die begonnen is aan een diagnostische sessie) een nieuw StartCommunication Request ontvangt (bijv. ten gevolge van het herstellen van fouten in het testapparaat), moet het verzoek geaccepteerd worden en moet de VU opnieuw geïnitialiseerd worden.

CPR_009 Indien de overdrachtverbinding om de een of andere reden niet geïnitialiseerd kan worden, moet de VU blijven functioneren op de manier onmiddellijk voorafgaande aan de poging om de overdrachtverbinding te initialiseren.

CPR_010 Het bericht StartCommunication Request moet fysiek geadresseerd worden.

CPR_011 De VU wordt voor diensten geïnitialiseerd via een ”snelle initialisatie”-methode.

— Aan elke activiteit gaat een bus-stilstandtijd vooraf.

— Het testapparaat zendt vervolgens een initialisatiepatroon.

— Het antwoord van de VU bevat alle noodzakelijke informatie om de overdracht tot stand te brengen.

CPR_012 Na voltooiing van de initialisatie:

— Alle overdrachtparameters worden overeenkomstig de sleutelbytes op de in tabel 4 bepaalde waarden gezet.

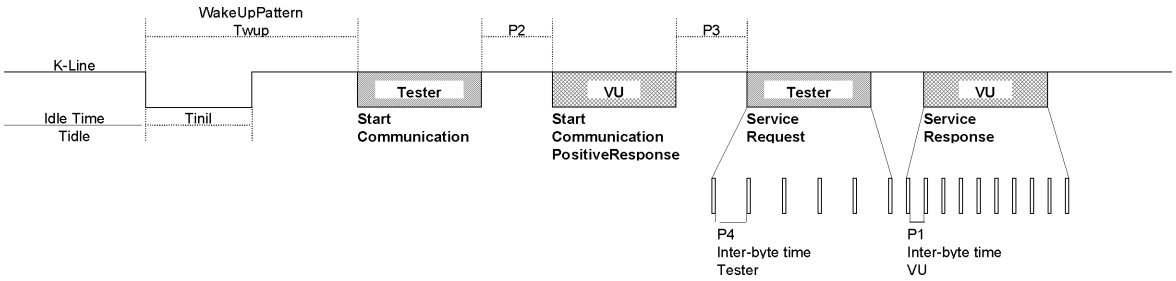
— De VU wacht op het eerste verzoek van het testapparaat.

— De VU staat in de standaard diagnostische modus, d.w.z. StandardDiagnosticSession.

— De kalibrerings-I/O-signaallijn staat in de standaardinstelling, d.w.z. geblokkeerde instelling.

CPR_014 De snelheid van de gegevensoverdracht op de K-lijn bedraagt 10 400 baud.

CPR_016 De snelle initialisatie wordt door het testapparaat gestart door het zenden van een Wake-up-patroon (Wup) op de K-lijn. Het patroon begint na de stilstandtijd op de K-lijn met een lage Tinil-tijd. Het testapparaat zendt de eerste bit van de StartCommunication-dienst na een Twup-tijd volgend op de eerste aflopende rand.



CPR_017 De timingwaarden voor snelle initialisatie en overdracht in het algemeen worden beschreven in de onderstaande tabellen. Er zijn verschillende mogelijkheden voor de stilstandtijd:

— Eerste overbrenging na inschakeling, Tidle = 300 ms.

— Na voltooiing van een StopCommunication-dienst, Tidle = P3 min.

— Na beëindiging van de overdracht door time-out P3 max, Tidle = 0.

Tabel 3

Timingwaarden voor snelle initialisatie

Parameter		Minimumwaarde	Maximumwaarde
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tabel 4

Timingwaarden voor overdracht

Timing Parameter	Parameteromschrijving	laagste waarden [ms]	hoogste waarden [ms]
		min.	max.
P1	Interbytetijd voor antwoord van de VU	0	20
P2	Tijd tussen verzoek van testapparaat en antwoord van de VU of twee antwoorden van de VU	25	250
P3	Tijd tussen einde van de antwoorden van de VU en begin van een nieuw verzoek van het testapparaat	55	5 000
P4	Interbytetijd voor verzoek van het testapparaat	5	20

CPR_018 Het berichtenformaat voor snelle initialisatie wordt omschreven in de onderstaande tabellen. (N.B.: hex staat voor hexadecimaal)

Tabel 5

StartCommunication Request-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	81	FMT
# 2	Byte van het doeladres	EE	TGT
# 3	Byte van het bronadres	tt	SRC
# 4	**StartCommunication Request Service Id**	**81**	**SCR**
# 5	Controlesom	00-FF	CS

Tabel 6

StartCommunication Positive Response-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	tt	TGT
# 3	Byte van het bronadres	EE	SRC
# 4	Additionele lengtebyte	03	LEN
# 5	**StartCommunication Positive Response Service Id**	**C1**	**SCRPR**
# 6	Sleutelbyte 1	EA	KB1
# 7	Sleutelbyte 2	8F	KB2
# 8	Controlesom	00-FF	CS

CPR_019 Er is geen negatief antwoord op het bericht StartCommunication Request. Indien er geen positief antwoordbericht moet worden verzonden, dan wordt de VU niet geïnitialiseerd. Er wordt niets verzonden en de VU blijft normaal functioneren.

4.2. **StopCommunication Service**

4.2.1 *Omschrijving van het bericht*

Het doel van de dienst van deze overdrachtslaag is het afsluiten van een overdrachtssessie.

CPR_020 Na ontvangst van een StopCommunication indicatieprimitief moet de VU controleren of de lopende condities een afsluiting van deze overdracht toestaan. In dit geval moet de VU alle noodzakelijke handelingen uitvoeren om deze overdracht af te sluiten.

CPR_021 Indien het mogelijk is de overdracht af te sluiten, moet de VU een StopCommunication-antwoordprimitief met de geselecteerde Positive Response-parameters afgeven voordat de overdracht afgesloten wordt.

CPR_022 Indien de overdracht om de een of andere reden niet kan worden afgesloten, moet de VU een StopCommunication-antwoordprimitief met de geselecteerde Negative Response-parameter afgeven.

CPR_023 Indien een time-out van P3max door de VU opgespoord wordt, moet de overdracht zonder een afgegeven antwoordprimitief worden afgesloten.

4.2.2 *Berichtformaat*

CPR_024 De berichtformaten voor de StopCommunication-primitieven worden omschreven in de onderstaande tabellen.

Tabel 7

StopCommunication Request-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	EE	TGT
# 3	Byte van het bronadres	tt	SRC
# 4	Additionele lengtebyte	01	LEN
# 5	**StopCommunication Request Service Id**	**82**	**SPR**
# 6	Controlesom	00-FF	CS

Tabel 8

StopCommunication Positive Response-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	tt	TGT
# 3	Byte van het bronadres	EE	SRC
# 4	Additionele lengtebyte	01	LEN
# 5	**StopCommunication Positive Response Service Id**	**C2**	**SPRPR**
# 6	Controlesom	00-FF	CS

Tabel 9

StopCommunication Negative Response-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	tt	TGT
# 3	Byte van het bronadres	EE	SRC
# 4	Additionele lengtebyte	03	LEN
# 5	**Negative Response Service Id**	**7F**	**NR**
# 6	StopCommunication Request Service Identification SPR	82	SPR
# 7	ResponseCode = generalReject RC_GR	10	RC_GR
# 8	Controlesom	00-FF	CS

4.2.3 *Parameterdefinitie*

Deze dienst vereist geen parameterdefinitie.

4.3. **TesterPresent-dienst (Testapparaat actief)**

4.3.1 *Omschrijving van het bericht*

De TesterPresent-dienst wordt door het testapparaat gebruikt om de server erop te wijzen dat het nog steeds aanwezig is, teneinde te voorkomen dat de server automatisch naar normaal bedrijf terugkeert en mogelijk de verbinding verbreekt. Deze dienst, die periodiek wordt verzonden, houdt de diagnostische sessie/overdracht actief door, telkens als een verzoek voor deze dienst wordt ontvangen, de P3-timer opnieuw in te stellen.

4.3.2 *Berichtformaat*

CPR_079 De berichtformaten voor de TesterPresent-primitieven worden omschreven in de onderstaande tabellen.

Tabel 10

TesterPresent Request-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	EE	TGT
# 3	Byte van het bronadres	tt	SRC
# 4	Additionele lengtebyte	02	LEN
# 5	**TesterPresent Request Service Id**	**3E**	**TP**

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 6	Subfunctie = responseRequired (antwoord vereist) = [ja	01	RESPREQ_Y
	nee]	02	RESPREQ_NO
# 7	Controlesom	00-FF	CS

CPR_080 Indien de responseRequired-parameter op "ja" wordt ingesteld, dan antwoordt de server met het volgende bericht van positief antwoord. Indien op „nee", dan zendt de server geen antwoord.

Tabel 11

TesterPresent Positive Response-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	tt	TGT
# 3	Byte van het bronadres	EE	SRC
# 4	Additionele lengtebyte	01	LEN
# 5	**TesterPresent Positive Response Service Id**	**7E**	**TPPR**
# 6	Controlesom	00-FF	CS

CPR_081 De dienst ondersteunt de volgende negatieve-antwoordcodes:

Tabel 12

TesterPresent Negative Response-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	tt	TGT
# 3	Byte van het bronadres	EE	SRC
# 4	Additionele lengtebyte	03	LEN
# 5	**Negative Response Service Id**	**7F**	**NR**
# 6	TesterPresent Request Service Identification	3E	TP

Byte-#	Parameternaam		Hex-waarde	Mnemoniek
#7	ResponseCode =	[SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
		incorrectMessageLength]	13	RC_IML
#8	Controlesom		00-FF	CS

5. BEHEERSDIENSTEN

De beschikbare diensten worden in de onderstaande tabel beschreven:

Tabel 13

Beheersdiensten

Naam van de dienst	Beschrijving
StartDiagnosticSession	De cliënt verzoekt een diagnostische sessie met een VU te starten.
SecurityAccess	De cliënt verzoekt om toegang tot functies die alleen voor bevoegde gebruikers toegankelijk zijn.

5.1. **StartDiagnosticSession-dienst (Start diagnostische sessie)**

5.1.1 *Omschrijving van het bericht*

CPR_025 De dienst StartDiagnosticSession wordt gebruikt om verschillende diagnostische sessies in de server mogelijk te maken. Een diagnostische sessie maakt een specifieke reeks diensten mogelijk volgens tabel 17. Een sessie kan specifieke diensten voor voertuigfabrikanten mogelijk maken die geen deel van dit document uitmaken. Implementatieregels moeten aan de volgende eisen voldoen:

— In de VU moet altijd precies één diagnostische sessie actief zijn.

— De VU moet bij het aanzetten altijd de StandardDiagnosticSession starten. Indien geen andere diagnostische sessie wordt gestart, moet de StandardDiagnosticSession actief blijven zolang de VU wordt aangedreven.

— Indien een diagnostische sessie die reeds actief is, door het testapparaat wordt aangevraagd, moet de VU een bericht van positief antwoord zenden.

— Telkens als het testapparaat een nieuwe diagnostische sessie aanvraagt, moet de VU eerst een StartDiagnosticSession positive response-bericht zenden voordat de nieuwe sessie in de VU actief wordt. Indien de VU de gevraagde nieuwe diagnostische sessie niet kan starten, moet deze antwoorden met een StartDiagnosticSession negative response-bericht en de lopende sessie wordt voortgezet.

CPR_026 Een diagnostische sessie kan alleen worden gestart indien overdracht tussen de cliënt en de VU tot stand gebracht is.

CPR_027 De timingparameters van tabel 4 moeten actief zijn na een succesvolle StartDiagnosticSession waarbij de diagnosticSession-parameter in het verzoekbericht ingesteld is op "StandardDiagnosticSession" indien voorheen een andere diagnostische sessie actief was.

5.1.2 *Berichtformaat*

CPR_028 De berichtformaten voor de StartDiagnosticSession-primitieven worden omschreven in de onderstaande tabellen.

Tabel 14

StartDiagnosticSession Request-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	EE	TGT
# 3	Byte van het bronadres	tt	SRC
# 4	Additionele lengtebyte	02	LEN
# 5	**StartDiagnosticSession Request Service Id**	**10**	**STDS**
# 6	DiagnosticSession = [een waarde uit tabel 17]	xx	DS_…
# 7	Controlesom	00-FF	CS

Tabel 15

StartDiagnosticSession Positive Response-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	tt	TGT
# 3	Byte van het bronadres	EE	SRC
# 4	Additionele lengtebyte	02	LEN
# 5	**# 5 StartDiagnosticSession Positive Response Service Id**	**50**	**STDSPR**
# 6	DiagnosticSession = [zelfde waarde als in Byte-# 6 tabel 14]	xx	DS_…
# 7	Controlesom	00-FF	CS

Tabel 16

StartDiagnosticSession Negative Response-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	tt	TGT

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 3	Byte van het bronadres	EE	SRC
# 4	Additionele lengtebyte	03	LEN
# 5	**Negative Response Service Id**	**7F**	**NR**
# 6	StartDiagnosticSession Request Service Id	10	STDS
# 7	ResponseCode = [subFunctionNotSupported [a]	12	RC_SFNS
	incorrectMessageLength [b]	13	RC_IML
	conditionsNotCorrect [c]	22	RC_CNC
# 8	Controlesom	00-FF	CS

[a] — de waarde opgenomen in Byte-# 6 van het verzoekbericht wordt niet ondersteund, d.w.z. niet in tabel 17,
[b] — de lengte van het ontvangen bericht is fout,
[c] — er is niet voldaan aan de criteria voor het verzoek StartDiagnosticSession.

5.1.3 *Parameterdefinitie*

CPR_029 De parameter ***diagnosticSession (DS_)*** wordt gebruikt door de StartDiagnosticSession-dienst om de specifieke werking van de server(s) te selecteren. De onderstaande diagnostische sessies worden in dit document gespecificeerd:

Tabel 17

Definitie van diagnosticSession-waarden

Hex	Beschrijving	Mnemoniek
81	**StandardDiagnosticSession** Deze diagnostische sessie maakt alle in **tabel 1 — Verzameltabel** 1, **kolom 4 "SD"** gespecificeerde diensten mogelijk. Met deze diensten kunnen gegevens van een server (VU) worden gelezen. Deze diagnostische sessie is actief nadat de initialisatie tussen cliënt (testapparaat) en server (VU) succesvol is afgesloten. Deze diagnostische sessie kan door andere in dit punt gespecificeerde diagnostische sessies overschreven worden	**SD**
85	**ECUProgrammingSession** Deze diagnostische sessie maakt alle in **tabel 1 — Verzameltabel 1**, **kolom 6 "ECUPS"** gespecificeerde diensten mogelijk. Deze diensten ondersteunen het programmeren van het geheugen van een server (VU). Deze diagnostische sessie kan door andere in dit punt gespecificeerde diagnostische sessies overschreven worden.	**ECUPS**
87	**ECUAdjustmentSession** Deze diagnostische sessie maakt alle in **tabel 1 — Verzameltabel 1**, **kolom 5 "ECUAS"** gespecificeerde diensten mogelijk. Deze diensten ondersteunen de invoer-/uitvoercontrole van een server (VU). Deze diagnostische sessie kan door andere in dit punt gespecificeerde diagnostische sessies overschreven worden.	**ECUAS**

5.2. **SecurityAccess-dienst (Veiligheidstoegang)**

Het schrijven van kalibreringsgegevens is niet mogelijk tenzij de VU in de CALIBRATION-modus staat. Naast het inbrengen van een geldige werkplaatskaart moet de juiste PIN-code worden ingevoerd voordat toegang tot de CALIBRATION-modus wordt toegestaan.

Als de VU in de CALIBRATION- of CONTROL-modus staat, is toegang tot de invoer-/uitvoerlijn van de kalibrering ook mogelijk.

De SecurityAccess-dienst verschaft een middel om de PIN-code in te voeren en om aan het testapparaat aan te geven of de VU in de CALIBRATION-modus staat.

De PIN-code kan ook door middel van alternatieve methoden worden ingevoerd.

5.2.1 *Omschrijving van het bericht*

De SecurityAccess-dienst bestaat uit een SecurityAccess "requestSeed"-bericht (aanvraag van "seed"), eventueel gevolgd door een SecurityAccess "sendKey"-bericht (verzoek om sleutel te zenden). De SecurityAccess-dienst moet na de StartDiagnosticSession-dienst worden uitgevoerd.

CPR_033 Het testapparaat moet het SecurityAccess "requestSeed"-bericht gebruiken om te controleren of de voertuigunit gereed is om een PIN-code te accepteren.

CPR_034 Indien de voertuigunit reeds in CALIBRATION-modus is, moet de unit het verzoek beantwoorden door het zenden van een "seed" van 0x0000 met gebruikmaking van de dienst SecurityAccess Positive Response.

CPR_035 Indien de voertuigunit gereed is om een PIN-code voor verificatie door een werkplaatskaart te accepteren, moet de unit het verzoek beantwoorden door het zenden van een "seed" groter dan 0x0000 met gebruikmaking van de dienst SecurityAccess Positive Response.

CPR_036 Indien de voertuigunit niet gereed is om een PIN-code van het testapparaat te accepteren, omdat de ingebrachte werkplaatskaart niet geldig is of omdat er geen werkplaatskaart ingebracht is of omdat de voertuigunit de PIN-code via een andere methode verwacht, moet de unit het verzoek beantwoorden met een Negative Response met een op conditionsNotCorrectOrRequestSequenceError ingestelde antwoordcode.

CPR_037 Het testapparaat moet dan het SecurityAccess "sendKey"-bericht gebruiken om een PIN-code naar de voertuigunit te zenden. Om de uitvoering van het kaartauthenticatieproces voldoende tijd te geven, moet de VU de negatieve antwoordcode requestCorrectlyReceived-ResponsePending (verzoek goed ontvangen — antwoord volgt) gebruiken om de tijd voor beantwoording te verlengen. De maximumtijd voor beantwoording mag evenwel niet meer dan 5 minuten bedragen. Zodra de gevraagde dienst is voltooid, moet de VU een bericht van positief antwoord zenden dan wel een bericht van negatief antwoord met een andere antwoordcode dan de eerste. De negatieve antwoordcode requestCorrectlyReceived-ResponsePending mag door de VU worden herhaald totdat de gevraagde dienst is voltooid en het definitieve antwoordbericht is gezonden.

CPR_038 De voertuigunit mag dit verzoek alleen met gebruikmaking van de dienst SecurityAccess Positive Response beantwoorden wanneer hij in CALIBRATION-modus staat.

CPR_039 In de onderstaande gevallen moet de voertuigunit dit verzoek met een Negative Response beantwoorden met de antwoordcode ingesteld op:

— subFunctionNot supported: ongeldig formaat voor de subfunctieparameter (accessType);

— conditionsNotCorrectOrRequestSequenceError: voertuigunit niet gereed om de invoer van een PIN-code te accepteren;

— invalidKey: PIN-code niet geldig en aantal controlepogingen van de PIN-code niet overschreden;

— exceededNumberOfAttempts: PIN-code niet geldig en aantal controlepogingen van de PIN-code overschreden;

— generalReject: correcte PIN-code maar wederzijdse authenticatie met werkplaatskaart mislukt.

5.2.2 *Berichtformaat — SecurityAccess — requestSeed*

CPR_040 De berichtformaten voor de SecurityAccess "requestSeed"-primitieven worden omschreven in de onderstaande tabellen.

Tabel 18

SecurityAccess REQUEST- requestSeed-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	EE	TGT
# 3	Byte van het bronadres	tt	SRC
# 4	Additionele lengtebyte	02	LEN
# 5	**SecurityAccess Request Service Id**	**27**	**SA**
# 6	AccessType — requestSeed	7D	AT_RSD
# 7	Controlesom	00-FF	CS

Tabel 19

SecurityAccess — requestSeed Positive Response-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	tt	TGT
# 3	Byte van het bronadres	EE	SRC
# 4	Additionele lengtebyte	04	LEN
# 5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
# 6	AccessType — requestSeed	7D	AT_RSD
# 7	Seed High	00-FF	SEEDH
# 8	Seed Low	00-FF	SEEDL
# 9	Controlesom	00-FF	CS

Tabel 20

SecurityAccess Negative Response-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	tt	TGT
# 3	Byte van het bronadres	EE	SRC

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 4	Additionele lengtebyte	03	LEN
# 5	**Negative Response Service Id**	**7F**	**NR**
# 6	SecurityAccess Request Service Id	27	SA
# 7	ResponseCode = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
# 8	Controlesom	00-FF	CS

5.2.3 *Berichtformaat — SecurityAccess — sendKey*

CPR_041 De berichtformaten voor de SecurityAccess "sendKey"-primitieven worden omschreven in de onderstaande tabellen.

Tabel 21

SecurityAccess Request — sendKey-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	EE	TGT
# 3	Byte van het bronadres	tt	SRC
# 4	Additionele lengtebyte	m + 2	LEN
# 5	**SecurityAccess Request Service Id**	**27**	**SA**
# 6	accessType — sendKey	7E	AT_SK
# 7 tot # m + 6	Key # 1 (High)	xx	KEY
	…	…	
	Key # m (low, m moet minimaal 4 en maximaal 8 zijn)	xx	
# m + 7	Controlesom	00-FF	CS

Tabel 22

SecurityAccess — sendKey Positive Response-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	tt	TGT
# 3	Byte van het bronadres	EE	SRC

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 4	Additionele lengtebyte	02	LEN
# 5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
# 6	accessType — sendKey	7E	AT_SK
# 7	Controlesom	00-FF	CS

Tabel 23

SecurityAccess Negative Response-bericht

Byte-#	Parameternaam		Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering		80	FMT
# 2	Byte van het doeladres		tt	TGT
# 3	Byte van het bronadres		EE	SRC
# 4	Additionele lengtebyte		03	LEN
# 5	**Negative Response Service Id**		**7F**	**NR**
# 6	SecurityAccess Request Service Id		27	SA
# 7	ResponseCode =	[generalReject	10	# 8
		subFunctionNotSupported	12	RC_SFNS
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
		invalidKey	35	RC_IK
		exceededNumberOfAttempts	36	RC_ENA
		requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
# 8	Controlesom		00-FF	CS

6. GEGEVENSOVERBRENGINGSDIENSTEN

De beschikbare diensten worden in de onderstaande tabel beschreven:

Tabel 24

Gegevensoverbrengingsdiensten

Naam van de dienst	Beschrijving
ReadDataByIdentifier	De cliënt verzoekt om overbrenging van de huidige waarde van een registratie met toegang door recordDataIdentifier.
WriteDataByIdentifier	De cliënt verzoekt een voor recordDataIdentifier toegankelijke registratie te schrijven.

6.1. **ReadDataByIdentifier-dienst (Lees gegevens met identificatiesymbool)**

6.1.1 *Omschrijving van het bericht*

CPR_050 De ReadDataByIdentifier-dienst wordt door de cliënt gebruikt om van een server om gegevensregistratiewaarden te vragen. De gegevens worden geïdentificeerd door een recordDataIdentifier. Het is de verantwoordelijkheid van de VU-fabrikant dat bij het verrichten van de dienst aan de servervoorwaarden wordt voldaan.

6.1.2 *Berichtformaat*

CPR_051 De berichtformaten voor de ReadDataByLocalIdentifier-primitieven worden omschreven in de onderstaande tabellen.

Tabel 25

ReadDataByIdentifier Request-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	EE	TGT
# 3	Byte van het bronadres	tt	SRC
# 4	Additionele lengtebyte	03	LEN
# 5	**ReadDataByIdentifier Request Service Id**	**22**	**RDBI**
# 6 en # 7	RecordDataIdentifier = [een waarde uit tabel 28]	xxxx	RDI_…
# 8	Controlesom	00-FF	CS

Tabel 26

ReadDataByIdentifier Positive Response-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	tt	TGT
# 3	Byte van het bronadres	EE	SRC
# 4	Additionele lengtebyte	m + 3	LEN
# 5	**ReadDataByIdentifier Positive Response Service Id**	**62**	**RDBIPR**
# 6 en # 7	recordDataIdentifier = [zelfde waarde als byte-nrs. 6 en 7 tabel 25 Tabel 23]	xxxx	RDI_ …
# 8 tot # m+7	dataRecord[] = [data # 1 : data # m]	xx : xx	DREC_DATA1 : DREC_DATAm
# m+8	Controlesom	00-FF	CS

Tabel 27

ReadDataByIdentifier Negative Response-bericht

Byte-#	Parameternaam		Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering		80	FMT
# 2	Byte van het doeladres		tt	TGT
# 3	Byte van het bronadres		EE	SRC
# 4	Additionele lengtebyte		03	LEN
# 5	**Negative Response Service Id**		**7F**	**NR**
# 6	ReadDataByIdentifier Request Service Id		22	RDBI
# 7	ResponseCode =	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
# 8	Controlesom		00-FF	CS

6.1.3 *Parameterdefinitie*

CPR_052 De parameter ***recordDataIdentifier (RDI_)*** in het verzoekbericht ReadDataByIdentifier identificeert een gegevensregistratie.

CPR_053 De in dit document gedefinieerde waarden van de recordDataIdentifier worden in de onderstaande tabel getoond.

De tabel recordDataIdentifier bestaat uit vier kolommen en meerdere rijen.

— De **1e kolom (Hex)** bevat de "Hex-waarde" die aan de in de 3e kolom gespecificeerde recordDataIdentifier is toegekend.

— De **2e kolom (Gegevenselement)** specificeert het gegevenselement van aanhangsel 1 waarop de recordDataIdentifier is gebaseerd (soms is transcodering nodig).

— De **3e kolom (Omschrijving)** specificeert de corresponderende recordDataIdentifier-naam.

— De **4e kolom (Mnemonisch)** specificeert de mnemonische notatie van deze recordDataIdentifier.

Tabel 28

Definitie van recordDataIdentifier-waarden

Hex	Gegevenselement	recordDataIdentifier-naam (zie formaat in punt 8.2)	Mnemoniek
F90B	`CurrentDateTime`	TimeDate	RDI_TD
F912	`HighResOdometer`	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	`K-ConstantOfRecordingEquipment`	Kfactor	RDI_KF

Hex	Gegevenselement	recordDataIdentifier-naam (zie formaat in punt 8.2)	Mnemoniek
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	Bandenmaat	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_ VRN
F190	VehicleIdentificationNumber	VIN	RDI_ VIN

CPR_054 De parameter ***dataRecord (DREC_)*** wordt gebruikt door het ReadDataByIdentifier positive response-bericht om de door de recordDataIdentifier geïdentificeerde gegevensregistratiewaarde aan de cliënt (testapparaat) te leveren. Gegevensformaten worden in punt 8 nader gespecificeerd. Aanvullende voor de gebruiker facultatieve dataRecords, met inbegrip van voor de VU specifieke invoergegevens, interne gegevens en uitvoergegevens kunnen worden geïmplementeerd, maar zijn niet in dit document gedefinieerd.

6.2. **WriteDataByIdentifier service**

6.2.1 *Omschrijving van het bericht*

CPR_056 De dienst WriteDataByIdentifier wordt door de cliënt gebruikt om gegevensregistratiewaarden naar een server te schrijven. De gegevens worden geïdentificeerd door een recordDataIdentifier. Het is de verantwoordelijkheid van de VU-fabrikant dat bij het verrichten van de dienst aan de servervoorwaarden wordt voldaan. Om de parameters van tabel 28 bij te werken moet de VU in CALIBRATION-modus staan.

6.2.2 *Berichtformaat*

CPR_057 De berichtformaten voor de WriteDataByIdentifier-primitieven worden omschreven in de onderstaande tabellen.

Tabel 29

WriteDataByIdentifier Request-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	EE	TGT
# 3	Byte van het bronadres	tt	SRC
# 4	Additionele lengtebyte	m+3	LEN
# 5	**WriteDataByIdentifier Request Service Id**	**2E**	**WDBI**
# 6 en # 7	RecordDataIdentifier = [een waarde uit tabel 28]	xxxx	RDI_ …

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 8 tot # m+7	dataRecord[] = [data # 1 : data # m]	xx : xx	DREC_DATA1 : DREC_DATAm
# m+8	Controlesom	00-FF	CS

Tabel 30

WriteDataByIdentifier Positive Response-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	tt	TGT
# 3	Byte van het bronadres	EE	SRC
# 4	Additionele lengtebyte	03	LEN
# 5	**WriteDataByIdentifier Positive Response Service Id**	**6E**	**WDBIPR**
# 6 en # 7	recordDataIdentifier = [zelfde waarde als byte-nrs. 6 en 7 tabel 29]	xxxx	RDI_ …
# 8	Controlesom	00-FF	CS

Tabel 31

WriteDataByIdentifier Negative Response-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	tt	TGT
# 3	Byte van het bronadres	EE	SRC
# 4	Additionele lengtebyte	03	LEN
# 5	**Negative Response Service Id**	**7F**	**NR**
# 6	WriteDataByIdentifier Request Service Id	2E	WDBI

Byte-#	Parameternaam		Hex-waarde	Mnemoniek
# 7	ResponseCode =	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
# 8	Controlesom		00-FF	CS

6.2.3 *Parameterdefinitie*

De parameter ***recordDataIdentifier (RDI_)*** wordt in tabel 28 gedefinieerd.

De parameter ***dataRecord (DREC_)*** wordt gebruikt door het WriteDataByIdentifier request-bericht om aan de server (VU) de gegevensregistratiewaarden te leveren die door de recordDataIdentifier zijn geïdentificeerd. Gegevensformaten worden in punt 8 nader gespecificeerd.

7. CONTROLE VAN TESTIMPULSEN — INVOER-/UITVOERCONTROLE FUNCTIONELE EENHEID

De beschikbare diensten worden in de onderstaande tabel beschreven:

Tabel 32

Invoer-/uitvoercontrole functionele eenheid

Naam van de dienst	Beschrijving
InputOutputControlByIdentifier	De cliënt verzoekt om controle van een voor de server specifieke invoer/uitvoer.

7.1. InputOutputControlByIdentifier-dienst

7.1.1 *Omschrijving van het bericht*

Er is een verbinding via de frontconnector waarmee testpulsen met gebruikmaking van een geschikt testapparaat gecontroleerd of gemonitord kunnen worden.

CPR_058 Deze kalibrerings-I/O-signaallijn kan door het K-lijncommando geconfigureerd worden met gebruikmaking van de dienst InputOutputControlByIdentifier om de vereiste invoer- of uitvoerfunctie voor de lijn te selecteren. De beschikbare instellingen van de lijn zijn:

— geblokkeerd,

— speedSignalInput, waarbij de kalibrerings-I/O-signaallijn wordt gebruikt om een snelheidssignaal (testsignaal) in te voeren dat het snelheidssignaal van de bewegingssensor vervangt, deze functie is niet beschikbaar in de CONTROL-modus,

— realTimeSpeedSignalOutputSensor, waarbij de kalibrerings-I/O-signaallijn wordt gebruikt om het snelheidssignaal van de bewegingssensor uit te voeren,

— RTCOutput, waarbij de kalibrerings-I/O-signaallijn wordt gebruikt om het UTC-kloksignaal uit te voeren, deze functie is niet beschikbaar in de CONTROL-modus.

CPR_059 De voertuigunit moet een afstellingssessie ingevoerd hebben en in CALIBRATION- of CONTROL-modus staan om de instelling van de lijn te configureren. Indien de VU in de CALIBRATION-modus staat, kunnen de vier statussen van de lijn worden geselecteerd (uitgeschakeld, speedSignalInput, realTimeSpeedSignalOutputSensor, RTCOutput). Indien de VU in de CONTROL-modus staat, kunnen slechts twee statussen van de lijn worden geselecteerd (uitgeschakeld, realTimeSpeedSignalOutputSensor). Bij het verlaten van de afstellingssessie of van de CALIBRATION- of CONTROL-modus moet de voertuigunit ervoor zorgen dat de kalibrerings-I/O-signaallijn teruggebracht wordt in de "geblokkeerde" (standaard)instelling.

CPR_060 Indien snelheidspulsen op de real-time-invoerlijn van het snelheidssignaal van de VU worden ontvangen terwijl de kalibrerings-I/O-signaallijn op invoer staat, moet de kalibrerings-I/O-signaallijn op uitvoer worden gezet of worden teruggebracht naar de geblokkeerde instelling.

CPR_061 De sequentie moet zijn:

— breng met de StartCommunication-dienst de overdracht tot stand;

— voer met de StartDiagnosticSession-dienst een afstellingssessie in en zet de VU in de CALIBRATION- of CONTROL-modus (de volgorde van deze twee opdrachten is niet belangrijk);

— wijzig de instelling van de uitvoer met de InputOutputControlByIdentifier-dienst.

7.1.2 *Berichtformaat*

CPR_062 De berichtformaten voor de InputOutputControlByIdentifier-primitieven worden omschreven in de onderstaande tabellen.

Tabel 33

InputOutputControlByIdentifier Request-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	EE	TGT
# 3	Byte van het bronadres	tt	SRC
# 4	Additionele lengtebyte	xx	LEN
# 5	**InputOutputControlByIdentifier Request Sid**	**2F**	**IOCBI**
# 6 en # 7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
# 8 of	ControlOptionRecord = [		COR_…
# 8 en # 9	InputOutputControlParameter — één waarde uit tabel 36	xx	IOCP_…
	controlState — één waarde uit tabel 37 (zie onderstaande opmerking)]	xx	CS_…
# 9 of # 10	Controlesom	00-FF	CS

Opmerking: De parameter controlState is slechts in een paar gevallen aanwezig (zie 7.1.3).

Tabel 34

InputOutputControlByIdentifier Positive Response-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	tt	TGT

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 3	Byte van het bronadres	EE	SRC
# 4	Additionele lengtebyte	xx	LEN
# 5	**inputOutputControlByIdentifier Positive Response SId**	**6F**	**IOCBIPR**
# 6 en # 7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
# 8 of	controlStatusRecord = [		CSR_
# 8 en # 9	inputOutputControlParameter (zelfde waarde als byte-# 8 tabel 33)	xx	IOCP_…
	controlState (zelfde waarde als byte-# 9 tabel 33)] (indien van toepassing)	xx	CS_…
# 9 of # 10	Controlesom	00-FF	CS

Tabel 35

InputOutputControlByIdentifier Negative Response-bericht

Byte-#	Parameternaam	Hex-waarde	Mnemoniek
# 1	Formaatbyte — fysieke adressering	80	FMT
# 2	Byte van het doeladres	tt	TGT
# 3	Byte van het bronadres	EE	SRC
# 4	Additionele lengtebyte	03	LEN
# 5	**Negative Response Service Id**	**7F**	**# 6**
# 6	inputOutputControlByIdentifier Request SId	2F	IOCBI
# 7	responseCode=[		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	conditionsNot-Correct]
	deviceControlLimitsExceeded]	7A	RC_DCLE
# 8	Controlesom	00-FF	CS

7.1.3 *Parameterdefinitie*

CPR_064 De parameter ***inputOutputControlParameter (IOCP_)*** wordt omschreven in de onderstaande tabel.

Tabel 36

Definitie van inputOutputControlParameter-waarden

Hex	Beschrijving	Mnemoniek
00	**ReturnControlToECU** Deze waarde moet aan de server (VU) aangeven dat het testapparaat niet langer controle heeft over de kalibrerings-I/O-signaallijn.	RCTECU
01	**ResetToDefault** Deze waarde moet aan de server (VU) aangeven dat gevraagd wordt de kalibrerings-I/O-signaallijn terug te stellen op de standaardinstelling.	RTD
03	**ShortTermAdjustment** Deze waarde moet aan de server (VU) aangeven dat gevraagd wordt de kalibrerings-I/O-signaallijn af te stellen op de waarde in de controlState parameter.	STA

CPR_065 De parameter ***controlState*** is alleen aanwezig wanneer de inputOutputControlParameter op ShortTermAdjustment ingesteld is en wordt in de onderstaande tabel omschreven:

Tabel 37

Definitie van controlState-waarden

Modus	Hex-waarde	Beschrijving
Uitschakelen	00	I/O-lijn is geblokkeerd (standaardinstelling)
Inschakelen	01	Kalibrerings-I/O-lijn kan worden gebruikt als speedSignalInput
Inschakelen	02	Kalibrerings-I/O-lijn kan worden gebruikt als realTimeSpeedSignalOutputSensor
Inschakelen	03	Kalibrerings-I/O-lijn kan worden gebruikt als RTCOutput

8. FORMATEN VAN DATARECORDS

Dit punt bevat nadere bijzonderheden betreffende:

— algemene regels die moeten worden toegepast op reeksen parameters die door de voertuigunit aan het testapparaat worden doorgegeven,

— formaten die moeten worden gebruikt voor gegevens die via de in punt 6 beschreven diensten voor gegevensoverbrenging worden doorgegeven.

CPR_067 Alle geïdentificeerde parameters moeten door de VU worden ondersteund.

CPR_068 Gegevens die door de VU aan het testapparaat worden doorgegeven in antwoord op een verzoekbericht, moeten van het gemeten type zijn (d.w.z. huidige waarde van de gevraagde parameter zoals gemeten of waargenomen door de VU).

8.1. **Overgebrachte parameterreeksen**

CPR_069 Tabel 38 definieert de reeksen die worden gebruikt om de geldigheid van een overgebrachte parameter te bepalen.

CPR_070 De waarden in de reeks "foutindicator" vormen een middel voor de voertuigunit om onmiddellijk aan te geven dat geldige parametrische gegevens momenteel niet beschikbaar zijn wegens een of andere fout in de tachograaf.

CPR_071 De waarden in de reeks "niet beschikbaar" vormen een middel voor de voertuigunit om een bericht over te brengen dat een parameter bevat welke in die module niet beschikbaar is of niet wordt ondersteund. De waarden in de reeks "niet gevraagd" vormen een middel voor een apparaat om een commandobericht over te brengen en de parameters te identificeren waarvoor geen antwoord van het ontvangstapparaat wordt verwacht.

CPR_072 Indien een storing in een onderdeel het onmogelijk maakt geldige gegevens voor een parameter over te brengen, moet de foutindicator, als beschreven in tabel 38, worden gebruikt in plaats van de gegevens van die parameter. Indien de gemeten of berekende gegevens echter een waarde opleveren die geldig is, maar de gedefinieerde parameterreeks overschrijdt, mag de foutindicator niet worden gebruikt. De gegevens moeten worden overgebracht met gebruikmaking van de passende minimale of maximale parameterwaarde.

Tabel 38

bereik van dataRecords

Reeksnaam	1 byte (Hex-waarde)	2 bytes (Hex-waarde)	4 bytes (Hex-waarde)	ASCII
Geldig signaal	00 tot FA	0000 tot FAFF	00000000 tot FAFFFFFF	1 tot en met 254
Parameterspecifieke indicator	FB	FB00 tot FBFF	FB000000 tot FBFFFFFF	geen
Gereserveerde reeks voor toekomstige indicatorbits	FC tot FD	FC00 tot FDFF	FC000000 tot FDFFFFFF	geen
Foutindicator	FE	FE00 tot FEFF	FE000000 tot FEFFFFFF	0
Niet beschikbaar of niet gevraagd	FF	FF00 tot FFFF	FF000000 tot FFFFFFFF	FF

CPR_073 Voor in ASCII gecodeerde parameters is het ASCII-teken "*" gereserveerd als begrenzer.

8.2. **Formaten van dataRecords**

De tabellen 39 tot en met 42 bevatten bijzonderheden over de formaten die moeten worden gebruikt via de ReadDataByIdentifier- en WriteDataByIdentifier-diensten.

CPR_074 Tabel 39 geeft de lengte, resolutie en bedrijfsreeks voor elke parameter die door zijn recordDataIdentifier is geïdentificeerd:

Tabel 39

Formaat van dataRecords

Parameternaam	Data lengte (bytes)	Resolutie	Bedrijfsreeks
TimeDate	8	Zie nadere informatie in tabel 40	
HighResolutionTotalVehicleDistance	4	5 m/bit, toename, 0 m offset	0 tot + 21 055 406 km
Kfactor	2	0,001 pulse/m/bit, toename, 0 offset	0 tot 64,255 pulsen/m
LfactorTyreCircumference	2	0,125 10^{-3} m /bit, toename, 0 offset	0 tot + 8,031 m
WvehicleCharacteristicFactor	2	0,001 pulse/m/bit, toename, 0 offset	0 tot 64,255 pulsen/m
Bandenmaat	15	ASCII	ASCII

Parameternaam	Data lengte (bytes)	Resolutie	Bedrijfsreeks
NextCalibrationDate	3	Zie nadere informatie in tabel 41	
SpeedAuthorised	2	1/256 km/h/bit, toename, 0 offset	0 tot 250,996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Zie nadere informatie in tabel 42	
VIN	17	ASCII	ASCII

CPR_075 Tabel 40 bevat bijzonderheden betreffende de formaten van de verschillende bytes van de TimeDate-parameter:

Tabel 40

Gedetailleerd formaat van TimeDate (recordDataIdentifier-waarde # F922)

Byte	Parameterdefinitie	Resolutie	Bedrijfsreeks
1	Seconden	0,25 s/bit, toename, 0 s comp.	0 tot 59,75
2	Minuten	1 min/bit, toename, 0 min comp.	0 tot 59 min
3	Uren	1 h/bit toename, 0 h comp.	0 tot 23 h
4	Maand	1 maand/bit toename, 0 maand comp.	1 tot 12 maand
5	Dag	0,25 dag/bit toename, 0 dag comp. (zie NOOT onder tabel 41)	0,25 tot 31,75 dagen
6	Jaar	1 jaar/bit toename, + 1985 jaar comp. (zie NOOT onder tabel 41)	jaar 1985 tot 2235
7	Lokale minuutcompensatie	1 min/bit, toename, – 125 min comp.	– 59 tot + 59 min
8	Lokale uurcompensatie	1 h/bit toename, – 125 h comp.	– 23 tot + 23 h

CPR_076 Tabel 41 bevat bijzonderheden betreffende de formaten van de verschillende bytes van de NextCalibrationDate-parameter.

Tabel 41

Gedetailleerd formaat van NextCalibrationDate (recordDataIdentifier-waarde # F922)

Byte	Parameterdefinitie	Resolutie	Bedrijfsreeks
1	Maand	1 maand/bit toename, 0 maand comp.	1 tot 12 maand
2	Dag	0,25 dag/bit toename, 0 dag comp. (zie NOOT hieronder)	0,25 tot 31,75 dagen
3	Jaar	1 jaar/bit toename, + 1985 jaar comp. (zie NOOT hieronder)	jaar 1985 tot 2235

NOOT betreffende het gebruik van de "Dag"-parameter:

1) Een waarde van 0 voor de datum is ongeldig. De waarden 1, 2, 3 en 4 worden gebruikt om de eerste dag van de maand aan te geven; 5, 6, 7 en 8 geven de tweede dag van de maand aan, enz. enz.

2) Deze parameter beïnvloedt of wijzigt de bovenstaande uur-parameter niet.

NOOT betreffende het gebruik van de "Jaar"-parameter:

Een waarde van 0 voor het jaar geeft het jaar 1985 aan; een waarde van 1 geeft 1986 aan, enz.

CPR_078 Tabel 42 bevat bijzonderheden betreffende de formaten van de verschillende bytes van de VehicleRegistrationNumber-parameter.

Tabel 42

Gedetailleerd formaat van VehicleRegistrationNumber (recordDataIdentifier-waarde # F97E)

Byte	Parameterdefinitie	Resolutie	Bedrijfsreeks
1	Code Page (zoals gedefinieerd in aanhangsel 1)	ASCII	01 tot 0 A
2 – 14	Vehicle Registration Number (zoals gedefinieerd in aanhangsel 1)	ASCII	ASCII

Aanhangsel 9

TYPEGOEDKEURING LIJST VAN MINIMAAL VEREISTE TESTS

INHOUDSOPGAVE

1. INLEIDING 309

2. FUNCTIETESTS VAN DE VOERTUIGUNIT 311

3. FUNCTIETESTS VAN DE BEWEGINGSSENSOR 315

4. FUNCTIETESTS VAN TACHOGRAAFKAARTEN 318

5. TESTS EXTERNE GNSS-MODULE 328

6. TESTS VAN DE APPARATUUR VOOR COMMUNICATIE OP AFSTAND 331

7. FUNCTIETESTS VAN DOCUMENTATIE 333

8. INTEROPERABILITEITSTESTS 335

1. INLEIDING

1.1. **Typegoedkeuring**

De EG-typegoedkeuring van een controleapparaat (of een component daarvan) of van een tachograafkaart is gebaseerd op:

— een **veiligheidscertificering** volgens de specificaties van de gemeenschappelijke criteria en met een veiligheidsdoelstelling die volledig voldoet aan aanhangsel 10 van deze bijlage (zoals aangevuld/gewijzigd);

— een **functiecertificering** uitgevoerd door een autoriteit van de lidstaat die certificeert dat het geteste apparaat voldoet aan de voorschriften van deze bijlage met betrekking tot uitgevoerde functies, meetnauwkeurigheid en milieukenmerken;

— een **interoperabiliteitscertificering** uitgevoerd door de bevoegde instantie die certificeert dat het controleapparaat (of de tachograafkaart) volledig interoperabel is met de vereiste modellen tachograafkaarten (of controleapparaten) (zie hoofdstuk 8 van deze bijlage).

Dit aanhangsel specificeert welke tests minimaal door een autoriteit van de lidstaat tijdens de functietests moeten worden uitgevoerd, en welke tests minimaal door de bevoegde instantie tijdens de interoperabiliteitstests moeten worden uitgevoerd. De voor het uitvoeren van de tests te volgen procedures of de soort tests worden niet nader gespecificeerd.

Aspecten in verband met de veiligheidscertificering worden niet behandeld in dit aanhangsel. Indien sommige voor de typegoedkeuring vereiste tests tijdens de veiligheidsevaluatie en het certificeringsproces uitgevoerd zijn, hoeven deze tests niet opnieuw te worden uitgevoerd. In dat geval moeten alleen de resultaten van deze veiligheidstests worden gecontroleerd. Ter informatie worden de voorschriften die naar verwachting tijdens de veiligheidscertificering worden getest (of die nauw verband houden met de tests die naar verwachting worden uitgevoerd) in dit aanhangsel met een "*" aangeduid.

De genummerde voorschriften verwijzen naar het geheel van bijlagen; de overige voorschriften verwijzen naar de andere aanhangsels. Zo verwijst PIC_001 bijvoorbeeld naar het voorschrift PIC_001 van aanhangsel 3 "Pictogrammen".

Dit aanhangsel behandelt afzonderlijk de typegoedkeuring van de bewegingssensor, de voertuigunit en de externe GNSS-module als samenstellende delen van het controleapparaat. Elk samenstellend deel krijgt een eigen typegoedkeuringscertificaat waarin de andere compatibele componenten zijn aangegeven. De functietest van de bewegingssensor (of van de externe GNSS-module) wordt uitgevoerd samen met de voertuigunit, en omgekeerd.

Er is geen interoperabiliteit vereist tussen elk model bewegingssensor (of externe GNSS-module) en elk model voertuigunit. In dit geval kan de typegoedkeuring van een bewegingssensor (of externe GNSS-module) alleen in combinatie met de typegoedkeuring van de desbetreffende voertuigunit worden verleend, en omgeke erd.

1.2. **Referentienormen**

De onderstaande referentienormen worden in dit aanhangsel gebruikt:

IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold.

IEC 60068-2-2: Basic environmental testing procedures — Part 2: tests — Tests B: Dry heat (sinusoidal).

IEC 60068-2-6: Environmental testing — Part 2: Tests — Test Fc: Vibration.

IEC 60068-2-14: Environmental testing — Part 2-14: Tests — Test N: Change of temperature.

IEC 60068-2-27: Environmental testing — Part 2: Tests — Test Ea and guidance: Shock.

IEC 60068-2-30: Environmental testing — Part 2-30: Tests — Test Db: Damp heat, cyclic (12 h + 12 h cycle).

IEC 60068-2-64: Environmental testing — Part 2-64: Tests — Test Fh: Vibration, broadband random and guidance.

IEC 60068-2-78 Environmental testing — Part 2-78: Tests — Test Cab: Damp heat, steady state.

ISO 16750-3 — Mechanical loads (2012-12).

ISO 16750-4 — Climatic loads (2010-04).

ISO 20653: Road vehicles — Degree of protection (IP code) — Protection of electrical equipment against foreign objects, water and access.

ISO 10605:2008 + Technical Corrigendum 1:2010 + AMD 1:2014 Road vehicles — Test methods for electrical disturbances from electrostatic discharge.

ISO 7637-1: 2002 + AMD 1: 2008 Road vehicles — Electrical disturbances from conduction and coupling — Part 1: Definitions and general considerations.

ISO 7637-2 Road vehicles — Electrical disturbances from conduction and coupling — Part 2: Electrical transient conduction along supply lines only.

ISO 7637-3 Road vehicles — Electrical disturbances from conduction and coupling — Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines.

ISO/IEC 7816-1 Identification cards — Integrated circuit(s) cards with contacts — Part 1: Physical characteristics.

ISO/IEC 7816-2 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts.

ISO/IEC 7816-3 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocol.

ISO/IEC 10373-1:2006 + AMD 1:2012 Identification cards — Test methods — Part 1: General characteristics.

ISO/IEC 10373-3:2010 + Technical Corrigendum 1:2013 Identification cards — Test methods — Part 3: Integrated circuit cards with contacts and related interface devices.

ISO 16844-3:2004, Cor 1:2006 Road vehicles — Tachograph systems — Part 3: Motion sensor interface (with vehicle units).

ISO 16844-4 Road vehicles — Tachograph systems — Part 4: CAN interface.

ISO 16844-6 Road vehicles — Tachograph systems — Part 6: Diagnostics

ISO 16844-7 Road vehicles — Tachograph systems — Part 7: Parameters.

ISO 534 Paper and board — Determination of thickness, density and specific volume.

UN ECE R10 Uniform provisions concerning the approval of vehicles with regard to electromagnetic compatibility (United Nation Economic Commission for Europe)

2. FUNCTIETESTS VAN DE VOERTUIGUNIT

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		03, 04, 05, 07, 382
3.2	Werkingsmodi		09 t.e.m. 11*, 132, 133
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*, 132
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, 132
3.8	Controle op de status van de bestuurders		54, 55, 132

Nr.	Test	Omschrijving	Gerelateerde voorschriften
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. 88 132
3.13	Identificatiegegevens van de apparatuur		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		134, 135, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Visuele weergave		90, 132, 149 t.e.m. 166, PIC_001, DIS_001
3.29	Afdrukken		90, 132, 167 t.e.m. 179, PIC_001, PRT_001 t.e.m. PRT_014
3.30	Waarschuwingssignalen		132, 180 t.e.m. 189, PIC_001

Nr.	Test	Omschrijving	Gerelateerde voorschriften
3.31	Doorsturen van gegevens naar externe media		90, 132, 190 t.e.m. 194
3.32	Communicatie op afstand voor gerichte wegcontroles		195 t.e.m. 197
3.33	Uitvoergegevens naar aanvullende externe apparaten		198, 199
3.34	Kalibrering		202 t.e.m. 206*, 383, 384, 388 t.e.m. 391
3.35	Kalibreringscontrole langs de weg		207 t.e.m. 209
3.36	Tijdafstelling		210 t.e.m. 212
3.37	Geen interferentie van aanvullende functies		06, 425
3.38	Interface van de bewegingssensor		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 — deel 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: tests — 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 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

Nr.	Test	Omschrijving	Gerelateerde voorschriften
4.2	Vochtigheid	Controleer of de voertuigunit bestand is tegen een cyclische vochtigheid (warmtetest) aan de hand van IEC 60068-2-30, test Db, zes cycli van 24 uur, elke temperatuur variërend van + 25 °C tot + 55 °C en een relatieve vochtigheid van 97 % bij + 25 °C en gelijk aan 93 % bij + 55 °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 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/s^2, effectieve waarde in lengterichting 11,8 m/s^2, effectieve waarde in zijwaartse richting 13,1 m/s^2, 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	219
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 12V-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

Nr.	Test	Omschrijving	Gerelateerde voorschriften
4.7	Kortsluit-beveiliging	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 ontlading	Overeenkomstig ISO 10605:2008 + technische rectificatie 1:2010 + AMD 1:2014: ± 4 kV contactontlading en ± 8 kV luchtontlading	218
5.3	Transiënte geleidings-verschijnselen in de stroomvoorziening	Voor 24V-uitvoeringen: overeenkomstig ISO 7637-2 + VN/ECE-reglement nr. 10, herz. 3: puls 1a: Vs = – 450 V, Ri = 50 ohm puls 2a: Vs = + 37 V, Ri = 2 ohm puls 2b: Vs = + 20 V, Ri = 0,05 ohm puls 3a: Vs = – 150 V, Ri = 50 ohm puls 3b: Vs = + 150 V, Ri = 50 ohm puls 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms puls 5: Vs = + 120 V, Ri = 2,2 ohm, td = 250 ms Voor 12V-uitvoeringen: overeenkomstig ISO 7637-1 + VN/ECE-reglement nr. 10, herz. 3: puls 1: Vs = – 75 V, Ri = 10 ohm puls 2a: Vs = + 37 V, Ri = 2 ohm puls 2b: Vs = + 10 V, Ri = 0,05 ohm puls 3a: Vs = – 112 V, Ri = 50 ohm puls 3b: Vs = + 75 V, Ri = 50 ohm puls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms puls 5: Vs = + 65 V, Ri = 3 ohm, td = 100 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

3. FUNCTIETESTS VAN DE BEWEGINGSSENSOR

Nr.	Test	Omschrijving	Gerelateerde voorschriften
1.	**Administratieve controle**		
1.1	Documentatie	Juistheid van de documentatie	

Nr.	Test	Omschrijving	Gerelateerde voorschriften
2	**Visuele inspectie**		
2.1	Naleving van de documentatie		
2.2	Identificatie/opschriften		225, 226
2.3	Materiaal		219 t.e.m. 223
2.4	Verzegeling		398, 401 t.e.m. 405
3	**Functietests**		
3.1	Identificatiegegevens van de sensor		95 t.e.m. 97
3.2	Koppeling bewegingssensor — voertuigunit		122*, 204
3.3	Bewegingsdetectie Juistheid van bewegingsmeting		30 t.e.m. 35
3.4	Interface van de voertuigunit		02
3.5	Controleer of de bewegingssensor bestand is tegen een constant magnetisch veld. Verifieer, als alternatief, of de bewegingssensor reageert op een constant magnetisch veld dat de bewegingsdetectie van het voertuig stoort, zodat een aangesloten VU sensorfouten kan detecteren, registreren en opslaan		217
4	**Milieutests**		
4.1	Bedrijfstemperatuur	Controleer de functionaliteit (zoals gedefinieerd in test nr. 3.3) in het temperatuurbereik [– 40 °C; + 135 °C] aan de hand van: IEC 60068-2-1, test Ad, met een testduur van 96 uur bij de laagste temperatuur To_{min}, IEC 60068-2-2, test Bd, met een testduur van 96 uur bij de hoogste temperatuur To_{max} Test overeenkomstig ISO 16750-4, punt 5.1.1.2: test bij lage temperatuur in ingeschakelde toestand (24 uur bij – 40 °C) Deze test berust op IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold; IEC 68-2-2, test Bd, met een testduur van 96 uur bij de laagste temperatuur van – 40 °C Test overeenkomstig ISO 16750-4, punt 5.1.2.2: test bij hoge temperatuur in ingeschakelde toestand (96 uur bij + 135 °C) Deze test berust op IEC 60068-2-2: Basic environmental testing procedures — Part 2: tests — Tests B: Dry heat	213

Nr.	Test	Omschrijving	Gerelateerde voorschriften
4.2	Temperatuur-wisseltest	Test overeenkomstig ISO 16750-4, punt 5.3.2: snelle temperatuurwisselingen binnen de voorgeschreven overgangsduur (20 wisselingen met een temperatuur variërend van – 40 °C tot + 135 °C, bij een verblijf gedurende 30 minuten bij de laagste en de hoogste temperatuur) IEC 60068-2-14: Environmental testing — Part 2-14: Tests — Test N: Change of temperature.	213
4.3	Vochtigheidscycli	Controleer de functionaliteit (als gedefinieerd in test nr. 3.3) aan de hand van IEC 60068-2-30, test Db, zes cycli van 24 uur, elke temperatuur variërend van + 25 °C tot + 55 ° C en een relatieve vochtigheid van 97 % bij + 25 °C en gelijk aan 93 % bij + 55 °C	214
4.4	Vibratie	ISO 16750-3: punt 4.1.2.6: test VI: bedrijfsvoertuigen, motor — versnellingsbak, vibratietest in gemengde modus, met inbegrip van a) test sinusoïdale vibraties, 20…520 Hz, 11,4 … 120 m/s², ≤ 0,5 octaaf per minuut b) test willekeurige vibraties, 10…2 000 Hz, effectieve waarde 177 m/s² 94 uur per as, inclusief temperatuurwisselingen tussen – 20 °C en + 70 °C?) Deze test berust op IEC 60068-2-80: Environmental testing — Part 2-80: Tests — Test Fi: Vibration — Mixed mode	219
4.5	Mechanische schokken	ISO 16750-3: punt 4.2.3: test VI: test van apparatuur in of op de versnellingsbak; half-sinusoïdale schok, acceleratie overeen te komen binnen een bereik van 3 000…15 000 m/s², pulsduur overeen te komen, maar kleiner dan 1 ms, aantal schokken overeen te komen Deze test berust op IEC 60068-2-27: Environmental testing — Part 2: Tests — Test Ea and guidance: Shock	219
4.6	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 64)	220, 221
4.7	Beveiliging tegen ompolen	Controleer of de bewegingssensor bestand is tegen een omkering in de stroomvoorziening	216
4.8	Kortsluitbeveiliging	Controleer of de invoer-/uitvoersignalen beveiligd zijn tegen kortsluiting in de stroomvoorziening en tegen aardsluiting	216

Nr.	Test	Omschrijving	Gerelateerde voorschriften
5	**Elektromagnetische compatibiliteit (EMC)**		
5.1	Stralingsemissies en gevoeligheid	Controleer de overeenstemming met VN/ECE-reglement nr. 10	218
5.2	Elektrostatische ontlading	Overeenkomstig ISO 10605:2008 + Technical corrigendum: 2010 + AMD 1:2014: ± 4 kV contactontlading en ± 8 kV luchtontlading	218
5.3	Transiënte geleidings-verschijnselen in datatransmissielijnen	Voor 24V-uitvoeringen: overeenkomstig ISO 7637-2 + VN/ECE-reglement nr. 10, herz. 3: puls 1a: Vs = – 450 V, Ri = 50 ohm puls 2a: Vs = + 37 V, Ri = 2 ohm puls 2b: Vs = + 20 V, Ri = 0,05 ohm puls 3a: Vs = – 150 V, Ri = 50 ohm puls 3b: Vs = + 150 V, Ri = 50 ohm puls 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms puls 5: Vs = + 120 V, Ri = 2,2 ohm, td = 250 ms Voor 12V-uitvoeringen: overeenkomstig ISO 7637-1 + VN/ECE-reglement nr. 10, herz. 3: puls 1: Vs = – 75 V, Ri = 10 ohm puls 2a: Vs = + 37 V, Ri = 2 ohm puls 2b: Vs = + 10 V, Ri = 0,05 ohm puls 3a: Vs = – 112 V, Ri = 50 ohm puls 3b: Vs = + 75 V, Ri = 50 ohm puls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms puls 5: Vs = + 65 V, Ri = 3 ohm, td = 100 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

4. FUNCTIETESTS VAN TACHOGRAAFKAARTEN

Tests overeenkomstig dit punt 4,

nr. 5 „Protocoltests”,

nr. 6 „Kaartstructuur” en

nr. 7 „Functietests”

kunnen worden uitgevoerd door de beoordelings- of certificeringsinstantie tijdens de veiligheidscertificering van voor de chipmodule op basis van gemeenschappelijke criteria (CC).

Tests nr. 2.3 en 4.2 zijn identiek. Dit zijn de mechanische tests van de combinatie voertuigcarrosserie en chipmodule. Bij vervanging van een van deze samenstellende delen (voertuigcarrosserie, chipmodule) moeten deze tests worden uitgevoerd.

Nr.	Test	Omschrijving	Gerelateerde voorschriften
1	**Administratieve controle**		
1.1	Documentatie	Juistheid van de documentatie	
2	**Kaart**		
2.1	Opdruk	Controleer of alle beveiligingskenmerken en zichtbare gegevens naar behoren en conform de regels op de kaart zijn afgedrukt [Code] Bijlage 1 C, punt 4.1 „Zichtbare gegevens”, 227 De voorkant bevat: naar gelang van de kaartsoort de vermelding „Bestuurderskaart” of „Controlekaart” of „Werkplaatskaart” of „Bedrijfskaart” in hoofdletters, gedrukt in de officiële taal/talen van de lidstaat die de kaart afgeeft. [Naam van de lidstaat] Bijlage 1 C, punt 4.1 „Zichtbare gegevens”, 229 De voorkant bevat: de vermelding van de naam van de lidstaat die de kaart afgeeft (facultatief). [Teken] Bijlage 1 C, punt 4.1 „Zichtbare gegevens”, 229 De voorkant bevat: het onderscheidingsteken van de lidstaat die de kaart afgeeft, negatief afgedrukt in een door twaalf gele sterren omringde blauwe rechthoek. [Enumeratie] Bijlage 1 C, punt 4.1 „Zichtbare gegevens”, 232 De achterkant bevat: een toelichting bij de genummerde rubrieken op de voorkant van de kaart; [Kleur] Bijlage 1 C, punt 4.1 „Zichtbare gegevens”, 234 Tachograafkaarten moeten worden gedrukt met de volgende achtergrondkleuren: — bestuurderskaart: wit, — werkplaatskaart: rood, — controlekaart: blauw, — bedrijfskaart: geel.	227 t.e.m. 229, 232, 234 t.e.m. 236

Nr.	Test	Omschrijving	Gerelateerde voorschriften
		[Beveiliging] Bijlage 1 C, punt 4.1 „Zichtbare gegevens", 235 Tachograafkaarten moeten ten minste de volgende eigenschappen hebben om de kaart te beschermen tegen vervalsing en misbruik/manipulatie: — een beveiligde achtergrond met fijne guillochepatronen en regenboogdruk, — ten minste één tweekleurige microzeefdrukregel.	
		[Opschriften] Bijlage 1 C, punt 4.1 „Zichtbare gegevens", 236 De lidstaten mogen kleuren of aanduidingen, zoals nationale symbolen of beveiligingstekens, toevoegen.	
		[Goedkeuringsmerk] Tachograafkaarten bevatten een goedkeuringsmerk. Het goedkeuringsmerk bestaat uit: — een rechthoek waarbinnen een kleine letter „e" is aangebracht, gevolgd door een onderscheidingsnummer of een onderscheidingsletter van het land waar de goedkeuring werd afgegeven, — een goedkeuringsnummer, overeenkomend met het nummer op het goedkeuringscertificaat dat is opgesteld voor de tachograafkaart, en aangebracht op een willekeurige positie vlak bij de rechthoek.	
2.2	Mechanische tests	[Kaartformaat] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810, Identification cards — Physical characteristics, [5] Dimension of card, [5.1] Card size, [5.1.1] Card dimensions and tolerances, card type ID-1 Unused card	240, 243 ISO/IEC 7810
		[Kaartranden] Tachograafkaarten moeten aan de volgende norm voldoen: ISO/IEC 7810, Identification cards — Physical characteristics, [5] Dimension of card, [5.1] Card size, [5.1.2] Card edges	

Nr.	Test	Omschrijving	Gerelateerde voorschriften
		[Kaartvorm] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810, Identification cards — Physical characteristics, [6] Card construction	
		[Kaartmateriaal] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810, Identification cards — Physical characteristics, [7] Card materials	
		[Buigstijfheid] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.1] Bending stiffness	
		[Toxiciteit] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.3] Toxicity	
		[Chemicaliënbestendigheid] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.4] Resistance to chemicals	
		[Maatvastheid] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.5] Card dimensional stability and warpage with temperature and humidity	

Nr.	Test	Omschrijving	Gerelateerde voorschriften
		[Lichtechtheid] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.6] Light	
		[Duurzaamheid] Bijlage 1 C, punt 4.4 „Milieu- en elektrotechnische specificaties”, 241 De tachograafkaarten moeten vijf jaar lang naar behoren kunnen functioneren indien de vastgestelde milieu- en elektrotechnische grenswaarden niet worden overschreden.	
		[Afpelsterkte] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.8] Peel strength	
		[Hechting of contactadhesie] De tachograafkaarten moeten voldoen aan: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.9] Adhesion or blocking	
		[Kromtrekking] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.11] Overall card warpage	
		[Hittevastheid] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.12] Resistance to heat	

Nr.	Test	Omschrijving	Gerelateerde voorschriften
		[Oppervlaktevervormingen] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.13] Surface distortions	
		[Verontreiniging] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.14] Contamination and interaction of card components	
2.3	Mechanische tests met ingebouwde chipmodule	[Buigvastheid] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810:2003/AMD 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.2] Dynamic bending stress Totaal aantal buigcycli 4 000	ISO/IEC 7810
		[Torsiesterkte] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810:2003/AMD 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.3] Dynamic torsional stress Totaal aantal torsiecycli 4 000	
3	**Module**		
3.1	Module	Module is te verstaan als de ingekapselde chip en het contactplaatje [Oppervlakteprofiel] Tachograafkaarten moeten voldoen aan: ISO/IEC 7816-1:2011, Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics [4.2] Surface profile of contacts	ISO/IEC 7816

Nr.	Test	Omschrijving	Gerelateerde voorschriften
		[Mechanische sterkte] Tachograafkaarten moeten voldoen aan: ISO/IEC 7816-1:2011, Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics [4.3] Mechanical strength (of a card and contacts)	
		[Elektrische weerstand:] Tachograafkaarten moeten voldoen aan: ISO/IEC 7816-1:2011, Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics [4.4] Electrical resistance (of contacts)	
		[Afmeting] Tachograafkaarten moeten voldoen aan: ISO/IEC 7816-2:2007, Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimension and location of the contacts [3] Dimension of the contacts	
		[Plaats] Tachograafkaarten moeten voldoen aanmoeten voldoen aan: ISO/IEC 7816-2:2007, Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimension and location of the contacts [4] Number and location of the contacts Voor modules met zes contacten vallen contacten „C4" en „C8" niet onder dit testvoorschrift.	
4	**Chip**		
4.1	Chip	[Bedrijfstemperatuur] De chip van de tachograafkaart werkt bij een omgevingstemperatuur tussen – 25 °C en + 85 °C.	241 t.e.m. 244 VN/ECE-reglement nr. 10 ISO/IEC 7810 ISO/IEC 10373

Nr.	Test	Omschrijving	Gerelateerde voorschriften
		[Temperatuur en vochtigheid] Bijlage 1 C, punt 4.4 „Milieu- en elektrotechnische specificaties", 241 Tachograafkaarten moeten naar behoren kunnen functioneren onder alle klimatologische omstandigheden die zich normaliter op het grondgebied van de Unie voordoen, en ten minste binnen het temperatuurbereik van – 25 °C tot + 70 °C met incidentele pieken tot + 85 °C; „incidenteel" betekent niet meer dan 4 uur per keer en niet meer dan 100 keer tijdens de levensduur van de kaart. Tachograafkaarten worden achtereenvolgens blootgesteld aan de volgende temperatuur en relatieve vochtigheid (RV) binnen de opgegeven tijdsduur. Na elke stap worden de tachograafkaarten getest op goede werking van de elektrische onderdelen. 1 Temperatuur van – 20 °C gedurende 2 uur 2 Temperatuur van ± 0 °C gedurende 2 uur 3 Temperatuur van + 20 °C en RV van 50 % gedurende 2 uur 4 Temperatuur van + 50 °C en RV van 50 % gedurende 2 uur 5 Temperatuur van + 70 °C en RV van 50 % gedurende 2 uur De temperatuur wordt intermitterend verhoogd tot + 85 °C, bij een RV van 50 %, gedurende 60 min. 6 Temperatuur van + 70 °C en RV van 85 % gedurende 2 uur De temperatuur wordt intermitterend verhoogd tot + 85 °C, bij een RV van 85 %, gedurende 30 min.	
		[Vochtigheid] Bijlage 1 C, punt 4.4 „Milieu- en elektrotechnische specificaties", 242 Tachograafkaarten moeten naar behoren kunnen functioneren binnen het vochtigheidsbereik van 10 % tot 90 %	
		[Elektromagnetische compatibiliteit (EMC)] Bijlage 1 C, punt 4.4 „Milieu- en elektrotechnische specificaties", 244 Tijdens de werking moeten de tachograafkaarten voldoen aan VN/ECE-reglement nr. 10 wat hun elektromagnetische compatibiliteit betreft	

Nr.	Test	Omschrijving	Gerelateerde voorschriften
		[Statische elektriciteit] Bijlage 1 C, punt 4.4 „Milieu- en elektrotechnische specificaties”, 244 Tijdens de werking moeten de tachograafkaarten beveiligd zijn tegen elektrostatische ontladingen De tachograafkaarten moeten voldoen aan: ISO/IEC 7810:2003/AMD 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.4] Static electricity [9.4.1] Contact IC cards Testspanning: 4 000 V	
		[Röntgenstralen] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810:2003/AMD 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.1] X-rays	
		[Ultraviolet licht] ISO/IEC 10373-1:2006 Identification cards — Test methods — Part 1: General characteristics [5.11] Ultraviolet light	
		[Driewieler] Tachograafkaarten moeten voldoen aan: ISO/IEC 10373-1:2006/AMD 1:2012 Identification cards — Test methods — Part 1: General characteristics, Amendment 1 [5.22] ICC — Mechanical strength: 3 wheel test for ICCs with contacts	
		[Omhulsel] Tachograafkaarten moeten voldoen aan: MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: Wrapping Test Robustness [13.2.1.32] TM-422: Mechanical Reliability: Wrapping Test	

Nr.	Test	Omschrijving	Gerelateerde voorschriften
4.2	Mechanische tests van in de kaart ingebedde chipmodule -> als onder 2.3	[Buigvastheid] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810:2003/AMD 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.2] Dynamic bending stress Totaal aantal buigcycli 4 000 [Torsiesterkte] Tachograafkaarten moeten voldoen aan: ISO/IEC 7810:2003/AMD 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.3] Dynamic torsional stress Totaal aantal torsiecycli 4 000	ISO/IEC 7810
5	**Protocoltests**		
5.1	ATR	Controleer of het antwoord op terugstellen (ATR) voldoet	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T=0	Controleer of het protocol T=0 voldoet	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Controleer of het PTS-commando (protocol voor transmissieselectie) voldoet door T=0 op T=1 te zetten	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T=1	Controleer of het protocol T=1 voldoet	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6	**Kaartstructuur**		
6.1		Ga na of de bestandsstructuur van de kaart voldoet door de kaart te controleren op de aanwezigheid van verplichte bestanden en bijbehorende toegangscondities (AC)	TCS 22 t.e.m. TCS 28 TCS_140 to TCS_179
7	**Functietests**		
7.1	Normale verwerking	Test ten minste een keer het toegestane gebruik van elk commando (test bijvoorbeeld het Update Binary-commando met CLA = '00', CLA = '0C' en met verschillende P1-, P2- en Lc-parameters) Controleer of de bewerkingen daadwerkelijk op de kaart werden uitgevoerd (bijvoorbeeld door het bestand te lezen waarop het commando werd uitgevoerd)	TCS 29 t.e.m. TCS 139

Nr.	Test	Omschrijving	Gerelateerde voorschriften
7.2	Foutmeldingen	Test voor elk commando ten minste een keer elke foutmelding (zoals gespecificeerd in aanhangsel 2) Test ten minste een keer elke algemene fout (met uitzondering van de tijdens de veiligheidscertificering gecontroleerde integriteitsfouten '**6400**')	
7.3	Codereeks en gestandaardiseerde domeinparameters		CSM_48, CSM_50
8	**Personalisatie**		
8.1	Optische personalisatie	Bijlage 1 C, punt 4.1 „Zichtbare gegevens", 230 De voorkant bevat: de gegevens die specifiek zijn voor de afgegeven kaart. Bijlage 1 C, punt 4.1 „Zichtbare gegevens", 231 De voorkant bevat: datums in de notatie „dd/mm/jjjj" of „dd.mm.jjjj" (dag, maand, jaar). Bijlage 1 C, punt 4.1 „Zichtbare gegevens", 235 Tachograafkaarten moeten ten minste de volgende eigenschappen hebben om de kaart te beschermen tegen vervalsing en misbruik/manipulatie: — bij de foto moeten de beveiligde achtergrond en de foto elkaar overlappen.	230, 231, 235

5. TESTS EXTERNE GNSS-MODULE

Nr.	Test	Omschrijving	Gerelateerde voorschriften
1	**Administratieve controle**		
1.1	Documentatie	Juistheid van de documentatie	
2	**Visuele inspectie externe GNSS-module**		
2.1	Naleving van de documentatie		
2.2	Identificatie/opschriften		224 t.e.m. 226
2.3	Materiaal		219 t.e.m. 223
3	**Functietests**		
3.1	Identificatiegegevens van de sensor		98, 99
3.2	Koppeling tussen externe GNSS-module — voertuigunit		123,205

Nr.	Test	Omschrijving	Gerelateerde voorschriften
3.3	GNSS-positie		36, 37
3.4	Interface van de voertuigunit wanneer de GNSS-ontvanger niet in de voertuigunit zit		03
3.5	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 °C) Deze test berust op IEC 60068-2-2: Basic environmental testing procedures — Part 2: tests — 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	Vochtigheid	Controleer of de voertuigunit bestand is tegen een cyclische vochtigheid (warmtetest) aan de hand van IEC 60068-2-30, test Db, zes cycli van 24 uur, elke temperatuur variërend van + 25 °C tot + 55 °C en een relatieve vochtigheid van 97 % bij + 25 °C en gelijk aan 93 % bij + 55 °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/s^2, effectieve waarde in lengterichting 11,8 m/s^2, effectieve waarde in zijwaartse richting 13,1 m/s^2, 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)	220, 221
4.5	Overspanningsbeveiliging	Controleer of de voertuigunit bestand is tegen een stroomvoorziening van: 24V-uitvoeringen: 34 V bij + 40 °C 1 uur 12V-uitvoeringen: 17 V bij + 40 °C 1 uur (ISO 16750-2, punt 4.3)	216
4.6	Beveiliging tegen ompolen	Controleer of de voertuigunit bestand is tegen een omkering in de stroomvoorziening (ISO 16750-2, punt 4.7)	216
4.7	Kortsluit-beveiliging	Controleer of de invoer-/uitvoersignalen beveiligd zijn tegen kortsluiting in de stroomvoorziening en tegen aardsluiting (ISO 16750-2, punt 4.10)	216
5	**EMC-tests**		
5.1	Stralingsemissies en gevoeligheid	Overeenkomstig VN/ECE-reglement nr. 10	218

Nr.	Test	Omschrijving	Gerelateerde voorschriften
5.2	Elektrostatische ontlading	Overeenkomstig ISO 10605:2008 + Technical Corrigendum:2010 + AMD 1:2014: ± 4 kV contactontlading en ± 8 kV luchtontlading	218
5.3	Transiënte geleidings-verschijnselen in de stroomvoorziening	Voor 24V-uitvoeringen: overeenkomstig ISO 7637-2 + VN/ECE-reglement nr. 10, herz. 3: puls 1a: Vs = – 450 V, Ri = 50 ohm puls 2a: Vs = + 37 V, Ri = 2 ohm puls 2b: Vs = + 20 V, Ri = 0,05 ohm puls 3a: Vs = – 150 V, Ri = 50 ohm puls 3b: Vs = + 150 V, Ri = 50 ohm puls 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms puls 5: Vs = + 120 V, Ri = 2,2 ohm, td = 250 ms Voor 12V-uitvoeringen: overeenkomstig ISO 7637-1 + VN/ECE-reglement nr. 10, herz. 3: puls 1: Vs = – 75 V, Ri = 10 ohm puls 2a: Vs = + 37 V, Ri = 2 ohm puls 2b: Vs = + 10 V, Ri = 0,05 ohm puls 3a: Vs = – 112 V, Ri = 50 ohm puls 3b: Vs = + 75 V, Ri = 50 ohm puls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms puls 5: Vs = + 65 V, Ri = 3 ohm, td = 100 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

6. TESTS VAN DE 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

Nr.	Test	Omschrijving	Gerelateerde voorschriften
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 — deel 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: tests — 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
4.4	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 (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 ontlading	Overeenkomstig ISO 10605:2008 + Technical corrigendum: 2010 + AMD 1:2014: ± 4 kV contactontlading en ± 8 kV luchtontlading	218
5.3	Transiënte geleidings-verschijnselen in de stroomvoorziening	Voor 24V-uitvoeringen: overeenkomstig ISO 7637-2 + VN/ECE-reglement nr. 10, herz. 3: puls 1a: Vs = – 450 V, Ri = 50 ohm puls 2a: Vs = + 37 V, Ri = 2 ohm puls 2b: Vs = + 20 V, Ri = 0,05 ohm puls 3a: Vs = – 150 V, Ri = 50 ohm puls 3b: Vs = + 150 V, Ri = 50 ohm puls 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms puls 5: Vs = + 120 V, Ri = 2,2 ohm, td = 250 ms	218

Nr.	Test	Omschrijving	Gerelateerde voorschriften
		Voor 12V-uitvoeringen: overeenkomstig ISO 7637-1 + VN/ECE-reglement nr. 10, herz. 3: puls 1: Vs = – 75 V, Ri = 10 ohm puls 2a: Vs = + 37 V, Ri = 2 ohm puls 2b: Vs = + 10 V, Ri = 0,05 ohm puls 3a: Vs = – 112 V, Ri = 50 ohm puls 3b: Vs = + 75 V, Ri = 50 ohm puls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms puls 5: Vs = + 65 V, Ri = 3 ohm, td = 100 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	

7. FUNCTIETESTS VAN DOCUMENTATIE

Nr.	Test	Omschrijving	Gerelateerde voorschriften
1	**Administratieve controle**		
1.1	Documentatie	Juistheid van de documentatie	
2	**Algemene tests**		
2.1	Aantal tekens per regel	Visuele inspectie van afdrukken	172
2.2	Minimale tekengrootte	Visuele inspectie van afdrukken en tekens	173
2.3	Ondersteunde tekensets	De printer ondersteunt de tekens zoals gespecificeerd in aanhangsel 1, hoofdstuk 4 „Tekensets”	174
2.4	Afdrukscherpte	Controle van de typekeuring van de tachograaf en visuele inspectie van afdrukken	174
2.5	Leesbaarheid en identificatie van afdrukken	Inspectie van afdrukken Aangetoond aan de hand van door de fabrikant verstrekte testverslagen en testprotocollen Het printpapier is bedrukt met alle homologatienummers van tachografen waarmee dit wordt gebruikt	175, 177, 178
2.6	Toevoeging van handgeschreven aantekeningen	Visuele inspectie: er is ruimte beschikbaar voor de handtekening van de bestuurder. Er is ruimte beschikbaar voor andere handgeschreven vermeldingen	180

Nr.	Test	Omschrijving	Gerelateerde voorschriften
2.7	Aanvullende details over papierbladen	Op de voor- en achterzijde van het blad kunnen aanvullende details en gegevens worden vermeld Dit mag geen afbreuk doen aan de leesbaarheid van de afdrukken Visuele inspectie	177, 178
3	**Opslagtests**		
3.1	Droge hitte	Voorbehandeling: 16 uur bij + 23 °C ± 2 °C en 55 % ± 3 % RV Testomgeving: 72 uur bij + 70 °C ± 2 °C Hersteltijd: 16 uur bij + 23 °C ± 2 °C en 55 % ± 3 % RV	176, 178 IEC 60068-2-2-Bb
2.2	Vochtige hitte	Voorbehandeling: 16 uur bij + 23 °C ± 2 °C en 55 % ± 3 % RV Testomgeving: 144 uur bij + 55 °C ± 2 °C en 93 % ± 3 % RV Hersteltijd: 16 uur bij + 23 °C ± 2 °C en 55 % ± 3 % RV	176, 178 IEC 60068-2-78-Cab
4	**Tests van documentatie tijdens het gebruik**		
4.1	Vochtbestendigheid ondergrond (onbedrukt papier)	Voorbehandeling: 16 uur bij + 23 °C ± 2 °C en 55 % ± 3 % RV Testomgeving: 144 uur bij + 55 °C ± 2 °C en 93 % ± 3 % RV Hersteltijd: 16 uur bij + 23 °C ± 2 °C en 55 % ± 3 % RV	176, 178 IEC 60068-2-78-Cab
4.2	Bedrukbaarheid	Voorbehandeling: 24 uur bij + 40 °C ± 2 °C en 93 % ± 3 % RV Testomgeving: afdruk gemaakt bij + 23 °C ± 2 °C Hersteltijd: 16 uur bij + 23 °C ± 2 °C en 55 % ± 3 % RV	176, 178
4.3	Hittevastheid	Voorbehandeling: 16 uur bij + 23 °C ± 2 °C en 55 % ± 3 % RV Testomgeving: 2 uur bij + 70 °C ± 2 °C, droge hitte Hersteltijd: 16 uur bij + 23 °C ± 2 °C en 55 % ± 3 % RV	176, 178 IEC 60068-2-2-Bb
4.4	Bestendigheid tegen lage temperaturen	Voorbehandeling: 16 uur bij + 23 °C ± 2 °C en 55 % ± 3 % RV Testomgeving: 24 uur bij – 20 °C ± 3 °C, droge koude Hersteltijd: 16 uur bij + 23 °C ± 2 °C en 55 % ± 3 % RV	176, 178 ISO 60068-2-1-Ab

Nr.	Test	Omschrijving	Gerelateerde voorschriften
4.5	Lichtechtheid	Voorbehandeling: 16 uur bij + 23 °C ± 2 °C en 55 % ± 3 % RV Testomgeving: 100 uur onder een verlichtingssterkte van 5 000 lux bij + 23 °C ± 2 °C en 55 % ± 3 % RV Hersteltijd: 16 uur bij + 23 °C ± 2 °C en 55 % ± 3 % RV	176, 178

Leesbaarheidscriteria voor tests 3.x en 4.x:

Ee afdruk moet leesbaar zijn indien de optische dichtheid binnen de volgende grenswaarden ligt:

gedrukte tekens: min. 1,0

ondergrond (onbedrukt papier): max. 0,2

De optische dichtheid van de gemaakte afdrukken wordt gemeten overeenkomstig DIN EN ISO 534.

De afdrukken moeten maatvast en goed leesbaar blijven

8. INTEROPERABILITEITSTESTS

Nr.	Test	Omschrijving
	9.1 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 schrijfopdrachten in zoveel mogelijk hoofdbestanden (EF's) op de kaart bevatten. Controleer door gegevens van de voertuigunit over te brengen of alle corresponderende registraties correct ingevoerd zijn. Controleer door gegevens van de kaart over te brengen of alle corresponderende registraties correct ingevoerd zijn. Controleer door middel van een dagelijkse afdruk of alle corresponderende registraties correct kunnen worden gelezen.
	9.2 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 functiescenario op de bewegingssensor uit. Het scenario heeft betrekking op een normale activiteit waarbij zoveel mogelijk voorvallen en fouten worden gegenereerd. Controleer door gegevens van de voertuigunit over te brengen of alle corresponderende registraties correct ingevoerd zijn. Controleer door gegevens van de kaart over te brengen of alle corresponderende registraties correct ingevoerd zijn. Controleer door middel van een dagelijkse afdruk of alle corresponderende registraties correct kunnen worden gelezen.

Nr.	Test	Omschrijving
9.3. Interoperabiliteitstests tussen voertuigunits en externe GNSS-modules (indien van toepassing)		
1	Wederzijdse authenticatie	Controleer of de wederzijdse authenticatie (verbindingsopbouw) tussen de voertuigunit en de externe GNSS-module normaal functioneert.
2	Activiteitstests	Voer een typisch functiescenario uit op de externe GNSS-module. Het scenario heeft betrekking op een normale activiteit waarbij zoveel mogelijk voorvallen en fouten worden gegenereerd. Controleer door gegevens van de voertuigunit over te brengen of alle corresponderende registraties correct ingevoerd zijn. Controleer door gegevens van de kaart over te brengen of alle corresponderende registraties correct ingevoerd zijn. Controleer door middel van een dagelijkse afdruk of alle corresponderende registraties correct kunnen worden gelezen.

Aanhangsel 10

BEVEILIGINGSVOORSCHRIFTEN

Dit aanhangsel beschrijft de voorschriften inzake de IT-beveiliging van de onderdelen van slimme tachografen (tachografen van de tweede generatie).

SEC_001 De volgende onderdelen van slimme tachografen worden gecertificeerd op basis van de gemeenschappelijke criteria:

— voertuigunit

— tachograafkaart

— bewegingssensor

— externe GNSS-module

SEC_002 In een overeenkomstig de gemeenschappelijke criteria opgesteld onderdeelbeveiligingsprofiel wordt voor elk onderdeel waarvoor een veiligheidscertificering vereist is, bepaald aan welke minimumeisen dat onderdeel moet voldoen op het gebied van IT-beveiliging.

SEC_003 De Europese Commissie zorgt ervoor dat de vier beveiligingsprofielen die aan deze bijlage voldoen, worden gesponsord, ontwikkeld en gevalideerd door de met IT-beveiligingscertificering belaste autoriteiten die deel uitmaken van de Joint Interpretation Working Group (JIWG), die de wederzijdse erkenning van certificaten ondersteunt onder de auspiciën van de Europese SOGIS-MRA-overeenkomst (Agreement on Mutual Recognition of Information Technology Security Evaluation Certificates), en dat deze worden geregistreerd:

— beveiligingsprofiel voertuigunit

— beveiligingsprofiel tachograafkaart

— beveiligingsprofiel bewegingssensor

— beveiligingsprofiel externe GNSS-module

Het beveiligingsprofiel voor voertuigunits regelt de gevallen waarin de VU al dan niet is ontworpen voor gebruik met een externe GNSS-module. In het laatste geval worden de beveiligingseisen voor de externe GNSS-module opgenomen in het specifieke beveiligingsprofiel.

SEC_004 Fabrikanten van onderdelen verfijnen en vervolledigen waar nodig het passende onderdeelbeveiligingsprofiel, zonder de bestaande bedreigingen, doelstellingen, procedurele middelen en specificaties van veiligheidsversterkende functies te wijzigen of te schrappen, teneinde een beveiligingsdoelstelling te ontwikkelen die als toetssteen voor de veiligheidscertificering van het onderdeel zal fungeren.

SEC_005 Tijdens het beoordelingsproces moet worden bevestigd dat de beveiligingsdoelstelling volledig conform is met het overeenkomstige beveiligingsprofiel.

SEC_006 Voor elk beveiligingsprofiel geldt betrouwbaarheidsniveau EAL4, versterkt door de betrouwbaarheidsonderdelen ATE_DPT.2 en AVA_VAN.5.

Aanhangsel 11

ALGEMENE BEVEILIGINGSMECHANISMEN

INHOUD

PREAMBULE 340

DEEL A TACHOGRAAFSYSTEEM VAN DE EERSTE GENERATIE 341

1. INLEIDING 341

1.1. Referentienormen 341

1.2. Begrippen en afkortingen 341

2. CRYPTOGRAFISCHE SYSTEMEN EN ALGORITMEN 343

2.1. Cryptografische systemen 343

2.2. Cryptografische algoritmen 343

2.2.1 RSA-algoritme 343

2.2.2 Hashalgoritme 343

2.2.3 Algoritme voor gegevenscodering 343

3. SLEUTELS EN CERTIFICATEN 343

3.1. Generering en verspreiding van sleutels 343

3.1.1 Generering en verspreiding van RSA-sleutels 343

3.1.2 RSA-testsleutels 345

3.1.3 Sleutels voor de bewegingssensor 345

3.1.4 Generering en verspreiding van TDES-sessiesleutels 345

3.2. Sleutels 345

3.3. Certificaten 345

3.3.1 Inhoud van de certificaten 346

3.3.2 Afgegeven certificaten 348

3.3.3 Certificaatverificatie en uitpakken 349

4. MECHANISME VOOR WEDERZIJDSE AUTHENTICATIE 349

5. VERTROUWELIJKHEIDS-, INTEGRITEITS- EN AUTHENTICATIEMECHANISMEN VOOR GEGEVENSOVERDRACHT VIA VU-KAARTEN 352

5.1. Beveiligde berichtenuitwisseling 352

5.2. Behandeling van fouten bij beveiligde berichtenuitwisseling (SM) 354

5.3. Algoritme voor het berekenen van cryptografische controlesommen 354

5.4. Algoritme voor het berekenen van cryptogrammen voor vertrouwelijkheids-DO's 355

6. DIGITALE HANDTEKENINGMECHANISMEN OM GEGEVENS TE DOWNLOADEN 355

6.1. Generering van de handtekening 355

6.2. Handtekeningverificatie 356

DEEL B	DIGITAAL TACHOGRAAFSYSTEEM VAN DE TWEEDE GENERATIE	357
7.	INLEIDING	357
7.1.	Referentienormen	357
7.2.	Notaties en afkortingen	357
7.3.	Definities	359
8.	CRYPTOGRAFISCHE SYSTEMEN EN ALGORITMEN	359
8.1.	Cryptografische systemen	359
8.2.	Cryptografische algoritmen	360
8.2.1	Symmetrische algoritmen	360
8.2.2	Asymmetrische algoritmen en gestandaardiseerde domeinparameters	360
8.2.3	Hashalgoritmen	361
8.2.4	Coderingssuites	361
9.	SLEUTELS EN CERTIFICATEN	361
9.1.	Asymmetrische sleutelparen en openbare-sleutelcertificaten	361
9.1.1	Algemeen	361
9.1.2	Europees niveau	362
9.1.3	Lidstaatniveau	362
9.1.4	Apparatuurniveau Voertuigunits	363
9.1.5	Apparatuurniveau: tachograafkaarten	365
9.1.6	Apparatuurniveau: externe GNSS-modules	366
9.1.7	Overzicht: vervanging van het certificaat	367
9.2.	Symmetrische sleutels	368
9.2.1	Sleutels ter beveiliging van de communicatie tussen VU en bewegingssensor	368
9.2.2	Sleutels ter beveiliging van de DSRC-communicatie	372
9.3.	Certificaten	375
9.3.1	Algemeen	375
9.3.2	Inhoud van het certificaat	375
9.3.3	Certificaataanvragen	377
10.	WEDERZIJDSE AUTHENTICATIE TUSSEN VU EN KAART, EN BEVEILIGDE BERICHTENUITWISSELING	378
10.1.	Algemeen	378
10.2.	Wederzijdse verificatie van de certificaatketen	379
10.2.1	Verificatie van de certificaatketen op kaartniveau door de VU	379
10.2.2	Verificatie van de certificaatketen op VU-niveau door de kaart	381
10.3.	VU-authenticatie	384
10.4.	Chipauthenticatie en sleutelovereenstemming tijdens de sessie	385

10.5. Beveiligde berichtenuitwisseling 387
10.5.1 Algemeen 387
10.5.2 Structuur van het beveiligde bericht 388
10.5.3 Afbreken van een sessie voor beveiligde berichtenuitwisseling 391
11. KOPPELING, WEDERZIJDSE AUTHENTICATIE EN BEVEILIGDE BERICHTENUITWISSELING TUSSEN VU EN EXTERNE GNSS-MODULE 392
11.1. Algemeen 392
11.2. Koppeling tussen VU en externe GNSS-module 393
11.3. Wederzijdse verificatie van de certificaatketen 393
11.3.1 Algemeen 393
11.3.2 Tijdens de koppeling tussen VU en externe GNSS-module 393
11.3.3 Tijdens normaal bedrijf 394
11.4. VU-authenticatie, chipauthenticatie en sleutelovereenstemming tijdens de sessie 395
11.5. Beveiligde berichtenuitwisseling 395
12. KOPPELING EN COMMUNICATIE TUSSEN VU EN BEWEGINGSSENSOR 396
12.1. Algemeen 396
12.2. Koppeling tussen VU en bewegingssensor met gebruikmaking van sleutels van verschillende generaties 396
12.3. Koppeling en communicatie tussen VU en bewegingssensor via AES 397
12.4. Koppeling tussen VU en bewegingssensor voor apparatuur van verschillende generaties 399
13. BEVEILIGING VOOR COMMUNICATIE OP AFSTAND VIA DE DSRC-INTERFACE 399
13.1. Algemeen 399
13.2. Codering van de payloadgegevens van de tachograaf en MAC-generering 400
13.3. Verificatie en decodering van de payloadgegevens van de tachograaf 401
14. ONDERTEKENING VAN GEDOWNLOADE GEGEVENS EN HANDTEKENINGVERIFICATIE 401
14.1. Algemeen 401
14.2. Generering van de handtekening 402
14.3. Handtekeningverificatie 402

PREAMBULE

Dit aanhangsel specificeert de beveiligingsmechanismen die het volgende waarborgen:

— de wederzijdse authenticatie tussen de verschillende onderdelen van het tachograafsysteem;

— de vertrouwelijkheid, integriteit, authenticiteit en/of onweerlegbaarheid van de gegevens die tussen verschillende onderdelen van het tachograafsysteem worden uitgewisseld of die op externe opslagmedia worden gedownload.

Dit aanhangsel bestaat uit twee delen: deel A specificeert de beveiligingsmechanismen voor het tachograafsysteem van de eerste generatie (digitale tachograaf); deel B specificeert de beveiligingsmechanismen voor het tachograafsysteem van de tweede generatie (slimme tachograaf).

De in deel A van dit aanhangsel gespecificeerde mechanismen zijn van toepassing indien minstens een van de bij de wederzijdse authenticatie en/of gegevensoverdracht betrokken onderdelen van het tachograafsysteem van de eerste generatie is.

De in deel B van dit aanhangsel gespecificeerde mechanismen zijn van toepassing indien de bij de wederzijdse authenticatie en/of gegevensoverdracht betrokken onderdelen van het tachograafsysteem allebei van de tweede generatie zijn.

In aanhangsel 15 wordt meer informatie verstrekt over het gebruik van onderdelen van de eerste generatie in combinatie met onderdelen van de tweede generatie.

DEEL A

TACHOGRAAFSYSTEEM VAN DE EERSTE GENERATIE

1. INLEIDING

1.1. **Referentienormen**

De onderstaande referentienormen worden in dit aanhangsel gebruikt:

SHA-1	National Institute of Standards and Technology (NIST). *FIPS Publication 180-1*: Secure Hash Standard. April 1995.
PKCS1	RSA Laboratories. PKCS 1: RSA Encryption Standard. Versie 2.0. Oktober 1998.
TDES	National Institute of Standards and Technology (NIST). *FIPS Publication 46-3*: Data Encryption Standard. Ontwerp 1999.
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998.
ISO/IEC 7816-4	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997.
ISO/IEC 7816-6	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements. First edition: 1996 + Cor 1: 1998.
ISO/IEC 7816-8	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands. First edition 1999.
ISO/IEC 9796-2	Information Technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Mechanisms using a hash function. First edition: 1997.
ISO/IEC 9798-3	Information Technology — Security techniques — Entity authentication mechanisms — Part 3: Entity authentication using a public key algorithm. Second edition 1998.
ISO 16844-3	Road vehicles — Tachograph systems — Part 3: Motion sensor interface

1.2. **Begrippen en afkortingen**

De onderstaande begrippen en afkortingen worden in dit aanhangsel gebruikt:

(K_a, K_b, K_c)	Reeks sleutels voor gebruik door het algoritme voor drievoudige gegevenscodering
CA	Certificeringsautoriteit
CAR	Referentie van de certificeringsautoriteit
CC	Cryptografische controlesom
CG	Cryptogram
CH	Koplabel (header) van het commando
CHA	Autorisatie van de certificaathouder
CHR	Referentie van de certificaathouder
D()	Decodering op basis van DES (*Data Encryption Standard*)

DE	Gegevenselement
DO	Gegevensobject
d	Particuliere RSA-sleutel, particuliere exponent
e	Openbare RSA-sleutel, openbare exponent
E()	Codering op basis van DES (*Data Encryption Standard*)
EQT	Apparatuur
Hash()	Hashwaarde als resultaat van *Hash*
Hash	Hashfunctie
KID	Sleutelidentificator
Km	TDES-sleutel. Master Key (hoofdsleutel), gedefinieerd in ISO 16844-3
Km_{VU}	TDES-sleutel ingebracht in voertuigunits
Km_{WC}	TDES-sleutel ingebracht in werkplaatskaarten
m	Berichtsymbool, een geheel getal tussen 0 en *n*-1
n	RSA-sleutels, modulus
PB	Opvulbytes (padding)
PI	Padding-indicatorbyte (voor gebruik in cryptogram ter waarborging van vertrouwelijkheid DO)
PV	Ongecodeerde waarde
s	Handtekeningsymbool, een geheel getal tussen 0 en *n*-1
SSC	Zendsequentieteller
SM	Beveiligde berichtenuitwisseling
TCBC	TDEA Cipher Block Chaining-werkingsmodus
TDEA	Algoritme voor drievoudige gegevenscodering
TLV	Waarde van de labellengte
VU	Voertuigunit
X.C	Door de certificeringsautoriteit afgegeven certificaat van gebruiker X
X.CA	Certificeringsautoriteit van gebruiker X
X.CA.PK $_{o}$ X.C	Handeling van uitpakken van een certificaat om een openbare sleutel op te halen. Het is een infix-operator; de linker operand is de openbare sleutel van de certificeringsautoriteit en de rechter operand is het door die certificeringsautoriteit afgegeven certificaat. Het resultaat is de openbare sleutel van gebruiker X wiens certificaat de rechter operand is
X.PK	Openbare RSA-sleutel van gebruiker X
X.PK[I]	RSA-codering van informatie I, met gebruikmaking van de openbare sleutel van gebruiker X
X.SK	Particuliere RSA-sleutel van gebruiker X
X.SK[I]	RSA-codering van informatie I, met gebruikmaking van de particuliere sleutel van gebruiker X
'xx'	Hexadecimale waarde
||	Samenvoegingsoperator

2. CRYPTOGRAFISCHE SYSTEMEN EN ALGORITMEN

2.1. **Cryptografische systemen**

CSM_001 Voertuigunits en tachograafkaarten gebruiken een standaard cryptografisch systeem van openbare RSA-sleutels om de onderstaande beveiligingsmechanismen te bieden:

— authenticatie tussen voertuigunits en kaarten,

— overbrenging van drievoudige DES-sessiesleutels tussen voertuigunits en tachograafkaarten,

— digitale handtekening van de gegevens die van voertuigunits of tachograafkaarten worden gedownload op externe media.

CSM_002 Voertuigunits en tachograafkaarten gebruiken een symmetrisch cryptografisch systeem van TDES-sleutels, enerzijds om een mechanisme te bieden dat de integriteit waarborgt van de tussen voertuigunits en de tachograafkaarten uitgewisselde gebruikersgegevens en anderzijds om waar nodig de vertrouwelijkheid te garanderen van de tussen voertuigunits en tachograafkaarten uitgewisselde gegevens.

2.2. **Cryptografische algoritmen**

2.2.1 *RSA-algoritme*

CSM_003 Het RSA-algoritme wordt door de onderstaande vergelijkingen volledig gedefinieerd:

$$X.SK[m] = s = m^d \bmod n$$
$$X.PK[s] = m = s^e \bmod n$$

Een uitgebreidere beschrijving van de RSA-functie is te vinden in de referentienorm [PKCS1]. De in het RSA-algoritme gebruikte openbare exponent e is een geheel getal tussen 3 en n-1 dat voldoet aan gcd(e, lcm(p-1, q-1))=1.

2.2.2 *Hashalgoritme*

CSM_004 De digitale handtekeningmechanismen gebruiken het in referentienorm [SHA-1] gedefinieerde hashalgoritme SHA-1.

2.2.3 *Algoritme voor gegevenscodering*

CSM_005 Op DES gebaseerde algoritmen worden in de Cipher Block Chaining-werkingsmodus gebruikt.

3. SLEUTELS EN CERTIFICATEN

3.1. **Generering en verspreiding van sleutels**

3.1.1 *Generering en verspreiding van RSA-sleutels*

CSM_006 RSA-sleutels worden op drie functionele hiërarchieniveaus gegenereerd:

— Europees niveau,

— lidstaatniveau,

— apparatuurniveau.

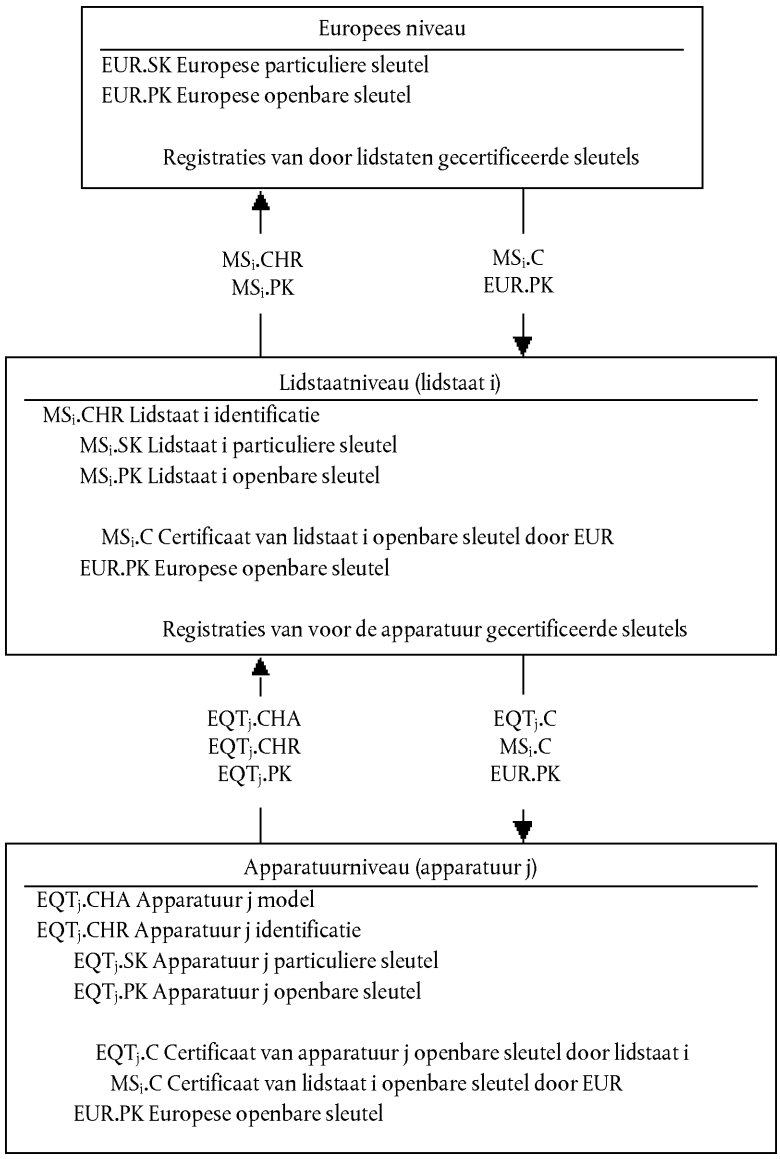
CSM_007 Op Europees niveau wordt een enkel Europees sleutelpaar (EUR.SK en EUR.PK) gegenereerd. De Europese particuliere sleutel wordt gebruikt om de openbare sleutels van de lidstaten te certificeren. Van alle gecertificeerde sleutels worden registraties bijgehouden. Deze taken worden uitgevoerd door de Europese certificeringsautoriteit in opdracht en onder verantwoordelijkheid van de Europese Commissie.

CSM_008 Op lidstaatniveau wordt een lidstaat-sleutelpaar (MS.SK en MS.PK) gegenereerd. Openbare sleutels van lidstaten worden door de Europese certificeringsautoriteit gecertificeerd. De particuliere sleutel van de lidstaat wordt gebruikt ter certificering van de openbare sleutels die in apparatuur (voertuigunit of tachograafkaart) worden ingebracht. Van alle gecertificeerde openbare sleutels worden registraties bijgehouden met de identificatie van de apparatuur waarvoor zij bedoeld zijn. Deze taken worden door de certificeringsautoriteit van de lidstaat uitgevoerd. Een lidstaat kan zijn sleutelpaar regelmatig wijzigen.

CSM_009 Op apparatuurniveau wordt een enkel sleutelpaar (EQT.SK en EQT.PK) gegenereerd en in elke apparatuur ingebracht. Openbare sleutels voor apparatuur worden door de certificeringsautoriteit van de lidstaat gecertificeerd. Deze taken kunnen door de fabrikanten en installateurs van de apparatuur of door de autoriteiten van de lidstaat worden uitgevoerd. Dit sleutelpaar dient voor de authenticatie, digitale handtekening en codering.

CSM_010 De vertrouwelijkheid van de particuliere sleutels blijft gewaarborgd tijdens de generering, eventuele overbrenging en opslag.

De gegevensstroom van dit proces wordt samengevat in het onderstaande schema:



3.1.2 *RSA-testsleutels*

CSM_011 Voor testdoeleinden van de apparatuur (inclusief interoperabiliteitstests) genereert de Europese certificeringsautoriteit een afzonderlijk Europees testsleutelpaar en ten minste twee testsleutelparen voor de lidstaten. De openbare sleutels van deze testsleutelparen worden op basis van de Europese particuliere testsleutel gecertificeerd. Voor typegoedkeuringstests van apparatuur brengen de fabrikanten testsleutels in die door een van deze testsleutels van de lidstaten gecertificeerd zijn.

3.1.3 *Sleutels voor de bewegingssensor*

Tijdens de generering, eventuele overbrenging en opslag wordt de vertrouwelijkheid van de drie hieronder beschreven drievoudige DES-sleutels op adequate wijze gewaarborgd.

Ter ondersteuning van ISO 16844-conforme tachograafonderdelen zorgen de Europese certificeringsautoriteit en de certificeringsautoriteiten van de lidstaten bovendien voor het volgende:

CSM_036 De Europese certificeringsautoriteit genereert KmVU en KmWC, twee onafhankelijke en unieke drievoudige DES-sleutels, en genereert Km als: $Km = Km_{VU}$ XOR Km_{WC}. De Europesecertificeringsautoriteit geeft deze sleutels desgevraagd door aan de certificeringsautoriteiten van de lidstaten, via adequaat beveiligde procedures.

CSM_037 De certificeringsautoriteiten van de lidstaten:

— gebruiken Km om door de fabrikanten van bewegingssensoren gevraagde gegevens van de bewegingssensor te coderen (de met Km te coderen gegevens worden gedefinieerd in ISO 16844-3);

— geven Km_{VU} via adequaat beveiligde procedures door aan de fabrikanten van voertuigunits voor gebruik in voertuigunits;

— zorgen ervoor dat Km_{WC} wordt ingebracht in alle werkplaatskaarten (`SensorInstallationSecData` in het hoofdbestand `Sensor_Installation_Data`) bij de personalisering van de kaart.

3.1.4 *Generering en verspreiding van TDES-sessiesleutels*

CSM_012 Voertuigunits en tachograafkaarten moeten als onderdeel van de wederzijdse authenticatie de vereiste gegevens genereren en uitwisselen teneinde een gemeenschappelijke drievoudige DES-sessiesleutel te ontwikkelen. Met het oog op de vertrouwelijkheid wordt deze gegevensuitwisseling beveiligd door een RSA-coderingsmechanisme.

CSM_013 Deze sleutel wordt gebruikt bij alle navolgende cryptografische bewerkingen met beveiligde berichtenuitwisseling. De geldigheid van de sleutel vervalt aan het einde van de sessie (kaartuitneming of kaartterugstelling) en/of na 240 toepassingen (een toepassing van de sleutel = een via beveiligde berichtenuitwisseling naar de kaart verzonden commando en bijbehorend antwoord).

3.2. **Sleutels**

CSM_014 RSA-sleutels hebben (ongeacht het niveau) de volgende lengte: modulus *n* 1 024 bits, openbare exponent *e* maximaal 64 bits, particuliere exponent *d* 1 024 bits.

CSM_015 Drievoudige DES-sleutels hebben de vorm (K_a, K_b, K_a), waarbij K_a en K_b onafhankelijke sleutels van 64 bits zijn. Er worden geen bits ingesteld om pariteitsfouten op te sporen.

3.3. **Certificaten**

CSM_016 Certificaten van openbare RSA-sleutels zijn van het „niet-zelfbeschrijvende" en „kaartverifieerbare" type (zie ISO/IEC 7816-8).

3.3.1 *Inhoud van de certificaten*

CSM_017 Certificaten van openbare RSA-sleutels bevatten de volgende gegevens in de onderstaande volgorde:

Gege-vens	Formaat	Bytes	Toelichting
CPI	INTEGER	1	Identificator van het certificaatprofiel ('01' voor deze versie)
CAR	OCTET STRING	8	Referentie van de certificeringsautoriteit
CHA	OCTET STRING	7	Autorisatie van de certificaathouder
EOV	TimeReal	4	Vervaldatum van het certificaat. Facultatief, 'FF' opgevuld indien niet gebruikt
CHR	OCTET STRING	8	Referentie van de certificaathouder
n	OCTET STRING	128	Openbare sleutel (modulus)
e	OCTET STRING	8	Openbare sleutel (openbare exponent)
		164	

Opmerkingen:

1. De „identificator van het certificaatprofiel" (CPI) geeft de exacte structuur van een authenticatiecertificaat aan. Dit gegeven kan worden gebruikt als interne identificator van apparatuur in een toepasselijke lijst van koplabels (headers), waarin de samenvoeging van gegevenselementen in het certificaat wordt omschreven.

   De volgende koplabels (headers) hebben betrekking op de inhoud van dit certificaat:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Toegevoegd label lijst van headers	Lengte lijst van headers	CPI-label	CPI-lengte	CAR-label	CAR-lengte	CHA-label	CHA-lengte	EOV-label	EOV-lengte	CHR-label	CHR-lengte	Label openbare sleutel (geconstrueerd)	Lengte opeenvolgende DO's	Label modulus	Lengte modulus	Label openbare exponent	Lengte openbare exponent

2. Het doel van de „referentie van de certificeringsautoriteit" (CAR) is het identificeren van de certificeringsautoriteit die het certificaat afgeeft, zodat het gegevenselement tegelijkertijd met een sleutelidentificator van de autoriteit kan worden gebruikt ter verwijzing naar de openbare sleutel van de certificeringsautoriteit (zie onderstaande sleutelidentificator voor de codering).

3. De „autorisatie van de certificaathouder" (CHA) wordt gebruikt om de rechten van de certificaathouder te identificeren. Dit gegeven bestaat uit de toepassingsidentificator van de tachograaf en het model van de apparatuur waarvoor het certificaat bedoeld is (overeenkomstig het gegevenselement `EquipmentType`, '00' voor een lidstaat).

4. Het doel van de „referentie van de certificaathouder" (CHR) is het eenduidig identificeren van de certificaathouder, zodat het gegevenselement tegelijkertijd met een sleutelidentificator van het onderwerp kan worden gebruikt ter verwijzing naar de openbare sleutel van de certificaathouder.

5. De certificaathouder of certificeringsautoriteiten worden eenduidig geïdentificeerd op basis van sleutelidentificatoren. Ze worden als volgt gecodeerd:

5.1 Apparatuur (VU of kaart):

Gegevens	Serienummer van de apparatuur	Datum	Type	Fabrikant
Lengte	4 bytes	2 bytes	1 byte	1 byte
Waarde	Geheel getal	mm yy BCD-codering	Specifiek kenmerk fabrikant	Fabrikantcode

In het geval van een VU is het mogelijk dat de fabrikant bij het aanvragen van certificaten de identificatie van de apparatuur waarin de sleutels worden ingebracht, soms wel en soms niet kent.

In het eerste geval verzendt de fabrikant de identificatie van de apparatuur met de openbare sleutel ter certificering naar de autoriteit van zijn lidstaat. Het certificaat bevat dan de identificatie van de apparatuur. De fabrikant moet garanderen dat sleutels en certificaat in de daartoe bestemde apparatuur worden ingebracht. De sleutelidentificator heeft de hierboven omschreven vorm.

In het tweede geval moet de fabrikant elke certificaataanvraag eenduidig identificeren en deze identificatie met de openbare sleutel ter certificering naar de autoriteit van zijn lidstaat verzenden. Het certificaat bevat de identificatie van de certificaataanvraag. Nadat de sleutel in de apparatuur is ingebracht, moet de fabrikant de autoriteit van zijn lidstaat op de hoogte brengen van de aan de apparatuur toegewezen sleutel (dat wil zeggen identificatie van de certificaataanvraag en identificatie van de apparatuur). De sleutelidentificator heeft de volgende vorm:

Gegevens	Serienummer certificaataanvraag	Datum	Type	Fabrikant
Lengte	4 bytes	2 bytes	1 byte	1 byte
Waarde	Geheel getal	mm yy BCD-codering	'FF'	Fabrikantcode

5.2. Certificeringsautoriteit:

Gegevens	Identificatie certificeringsautoriteit	Serienummer van de sleutel	Additionele info	Identificator
Lengte	4 bytes	1 byte	2 bytes	1 byte

Waarde	1 byte numerieke nationale code 3 bytes alfanumerieke nationale code	Geheel getal	Additionele codering (specifiek voor de certificeringsautoriteit) 'FF FF' indien niet gebruikt	'01'

Het serienummer van de sleutel dient om de verschillende sleutels van een lidstaat te onderscheiden in het geval dat de sleutel wordt gewijzigd.

6. Certificaatverificateurs weten impliciet dat de gecertificeerde openbare sleutel als RSA-sleutel van belang is voor de authenticatie, verificatie van de digitale handtekening en codering voor vertrouwelijke diensten (het certificaat bevat geen objectidentificator ter specificatie).

3.3.2 *Afgegeven certificaten*

CSM_018 Het afgegeven certificaat is een digitale handtekening met gedeeltelijke recovery van de inhoud van het certificaat overeenkomstig ISO/IEC 9796-2, uitgezonderd bijlage A.4 daarvan, waaraan de „referentie van de certificeringsautoriteit" is toegevoegd.

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, Hash(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

Met inhoud van het certificaat = Cc = C_r || C_n

106 bytes 58 bytes

Opmerkingen:

1. Dit certificaat is 194 bytes lang.

2. De door de handtekening verborgen CAR wordt ook aan de handtekening toegevoegd, zodat de openbare sleutel van de certificeringsautoriteit ter verificatie van het certificaat kan worden geselecteerd.

3. De certificaatverificateur kent impliciet het door de certificeringsautoriteit gebruikte algoritme ter ondertekening van het certificaat.

4. De volgende koplabels (headers) hebben betrekking op dit afgegeven certificaat:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Label zelfbeschrijvend certificaat (geconstrueerd)	Lengte opeenvolgende DO's	Label handtekening	Lengte handtekening	Label restant	Lengte restant	CAR-label	CAR-lengte

3.3.3 *Certificaatverificatie en uitpakken*

Certificaatverificatie en uitpakken bestaan uit het verifiëren van de handtekening overeenkomstig ISO/IEC 9796-2, het lezen van de inhoud van het certificaat en de opgenomen openbare sleutel: X.PK = X.CA.PK $_o$ X.C, en het verifiëren van de geldigheid van het certificaat.

CSM_019 Hierbij worden de volgende stappen ondernomen:

Verifieer handtekening en zoek inhoud:

— van X.C zoek Teken, C_n' en CAR': X.C = Teken || C_n' || CAR'

128 bytes 58 bytes 8 bytes

— van CAR' selecteer de vereiste openbare sleutel van de certificeringsautoriteit (indien dit nog niet met andere middelen is gedaan)

— open Teken met openbare sleutel CA: Sr' = X.CA.PK [Teken],

— controleer of Sr' begint met '6A' en of eindigt met 'BC'

— bereken C_r' en H' van: Sr' = '6A' || C_r' || H' || 'BC'

106 bytes 20 bytes

— vind inhoud van het certificaat C' = C_r' || C_n',

— controleer of *Hash*(C') = H'

Indien de controles in orde zijn, is het certificaat authentiek; de inhoud ervan is C'.

Verifieer geldigheid. Van C':

— controleer in voorkomend geval einddatum van geldigheidsduur.

Zoek en bewaar openbare sleutel, sleutelidentificator, autorisatie van de certificaathouder en vervaldatum van het certificaat van C':

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MECHANISME VOOR WEDERZIJDSE AUTHENTICATIE

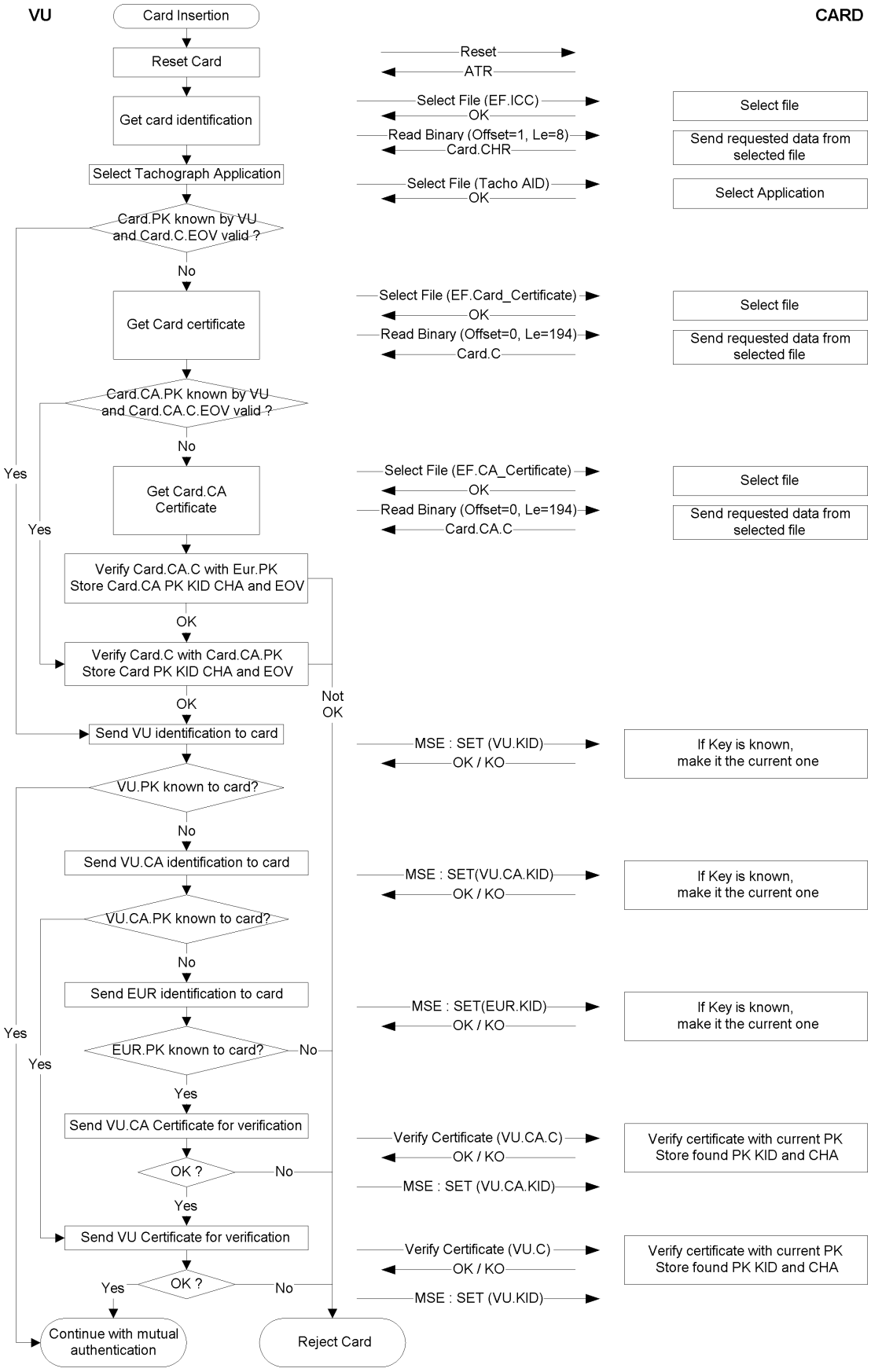
De wederzijdse authenticatie tussen kaarten en VU's is gebaseerd op het volgende principe:

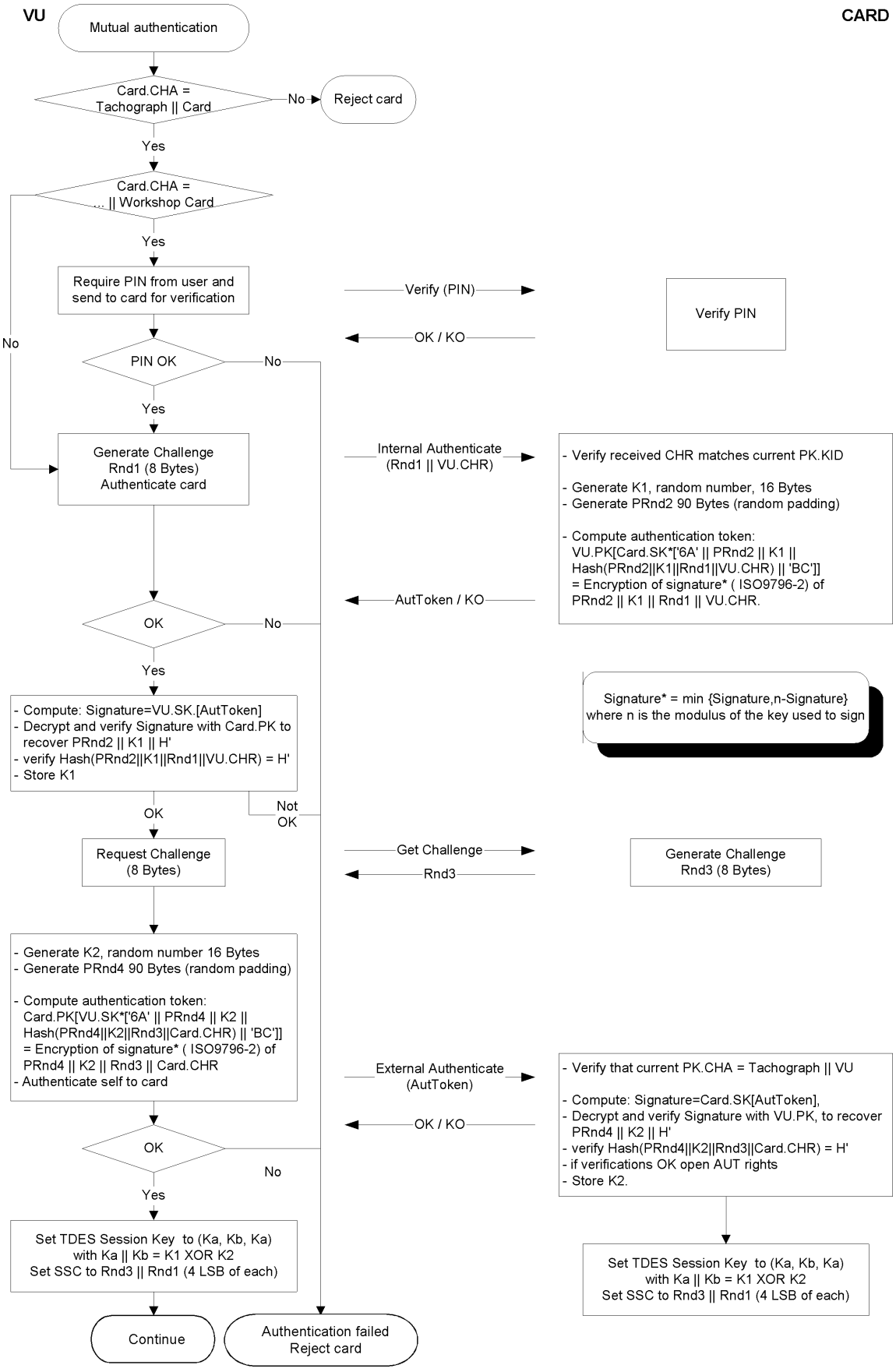
Elke partij bewijst aan de andere partij in het bezit te zijn van een geldig sleutelpaar waarvan de openbare sleutel is gecertificeerd door een certificeringsautoriteit van een lidstaat, die zelf weer is gecertificeerd door de Europese certificeringsautoriteit.

Het bewijs wordt geleverd door ondertekening met de particuliere sleutel van een willekeurig (aselect), door de andere partij gezonden nummer; de andere partij moet het verzonden willekeurige nummer bij de verificatie van deze handtekening terugvinden.

Het mechanisme wordt door de VU gestart bij kaartinbrenging. Het begint met de uitwisseling van certificaten en het uitpakken van openbare sleutels en eindigt met de instelling van een sessiesleutel.

CSM_020 Het volgende protocol wordt gebruikt (de pijlen geven commando's en uitgewisselde gegevens aan (zie aanhangsel 2)):




VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
No
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
Not OK
OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

5. VERTROUWELIJKHEIDS-, INTEGRITEITS- EN AUTHENTICATIEMECHANISMEN VOOR GEGEVENSOVERDRACHT VIA VU-KAARTEN

5.1. **Beveiligde berichtenuitwisseling**

CSM_021 De integriteit van de gegevensoverdracht via VU-kaarten wordt beschermd door beveiligde berichtenuitwisseling overeenkomstig de referentienormen [ISO/IEC 7816-4] en [ISO/IEC 7816-8].

CSM_022 Indien gegevens tijdens de overdracht moeten worden beveiligd, wordt het gegevensobject in de vorm van een cryptografische controlesom toegevoegd aan de in het commando of antwoord verzonden gegevensobjecten. De cryptografische controlesom wordt geverifieerd door de ontvanger.

CSM_023 De cryptografische controlesom van in een commando verzonden gegevens bevat de header van het commando en alle verzonden gegevensobjecten (=> CLA = '0C'; alle gegevensobjecten worden ingekapseld met labels waarin b1 = 1).

CSM_024 Indien het antwoord geen gegevensveld bevat, worden de bytes van de statusinformatie in het antwoord beveiligd door een cryptografische controlesom.

CSM_025 Cryptografische controlesommen zijn 4 bytes lang.

Bij gebruik van beveiligde berichtenuitwisseling hebben de commando's en antwoorden derhalve de volgende structuur:

De gebruikte gegevensobjecten (DO's) zijn een deelverzameling van de in ISO/IEC 7816-4 beschreven DO's voor beveiligde berichtenuitwisseling:

Label	Mnemoniek	Betekenis
'81'	T_{PV}	Ongecodeerde waarde van niet met BER-TLV gecodeerde gegevens (te beschermen door CC)
'97'	$\mathbf{T_{LE}}$	Waarde van Le in het onbeveiligde commando (te beschermen door CC)
'99'	T_{SW}	Statusinformatie (te beschermen door CC)
'8E'	T_{CC}	Cryptografische controlesom
'87'	$T_{PI\ CG}$	Padding-indicatorbyte || Cryptogram (Ongecodeerde waarde, niet met BER-TLV gecodeerd)

Gegeven een onbeveiligd commando-antwoordpaar:

Koplabel (header) commando				Inhoud commando		
CLA	INS	P1	P2	[Veld L_c]	[Gegevensveld]	[Veld L_e]
4 bytes				L bytes, aangeduid als B_1 t/m B_L		

Inhoud antwoord	Staartlabel (trailer) antwoord	
[Gegevensveld]	SW1	SW2
L_r gegevensbytes	2 bytes	

Het corresponderende beveiligde commando-antwoordpaar is:

Beveiligd commando:

Header commando (CH)				Inhoud commando										
CLA	INS	P1	P2	[Nieuw veld L_c]	[Nieuw gegevensveld]									[Nieuw veld L_e]
'OC'				Lengte van nieuw gegevensveld	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	'00'
					'81'	L_c	Gegevensveld	'97'	'01'	L_e	'8E'	'04'	CC	

In de controlesom te integreren gegevens = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = opvulbytes (80 .. 00) overeenkomstig ISO-IEC 7816-4 en ISO 9797, methode 2.

De gegevensobjecten PV en LE zijn alleen aanwezig wanneer het onbeveiligde commando corresponderende gegevens bevat.

Beveiligd antwoord:

1. Geval waarin het gegevensveld van het antwoord niet leeg is en niet hoeft te worden beveiligd ter waarborging van de vertrouwelijkheid:

Inhoud antwoord						Staartlabel (trailer) antwoord
[Nieuw gegevensveld]						Nieuwe SW1, SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	Gegevensveld	'8E'	'04'	CC	

In de controlesom te integreren gegevens = T_{PV} || L_{PV} || PV || PB

2. Geval waarin het gegevensveld van het antwoord niet leeg is en moet worden beveiligd ter waarborging van de vertrouwelijkheid:

Inhoud antwoord						Staartlabel (trailer) antwoord
[Nieuw gegevensveld]						Nieuwe SW1, SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Door CG over te dragen gegevens: niet met BER-TLV gecodeerde gegevens en opvulbytes (padding).

In de controlesom te integreren gegevens = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Geval waarin het gegevensveld van het antwoord leeg is:

Inhoud antwoord						Staartlabel (trailer) antwoord
[Nieuw gegevensveld]						Nieuwe SW1, SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	Nieuwe SW1, SW2	'8E'	'04'	CC	

In de controlesom te integreren gegevens = T_{SW} || L_{SW} || SW || PB

5.2. **Behandeling van fouten bij beveiligde berichtenuitwisseling (SM)**

CSM_026 Indien de tachograafkaart tijdens het vertalen van een commando een SM-fout ontdekt, dan moeten de statusbytes zonder SM worden teruggezonden. Overeenkomstig ISO/IEC 7816-4 worden de onderstaande statusbytes gedefinieerd om SM-fouten te melden:

'66 88': verificatie van cryptografische controlesom mislukt;

'69 87': verwachte SM-gegevensobjecten ontbreken;

'69 88': SM-gegevensobjecten onjuist.

CSM_027 Indien de tachograafkaart statusbytes zonder SM-gegevensobjecten of met een foutief SM-gegevensobject terugzendt, moet de sessie door de VU worden afgebroken.

5.3. **Algoritme voor het berekenen van cryptografische controlesommen**

CSM_028 Cryptografische controlesommen worden opgebouwd door middel van een *retail* berichtauthenticatiecode (MAC) overeenkomstig ANSI X9.19 op basis van DES (*Data Encryption Standard*):

— beginfase: het eerste checkblok y0 is E(Ka, SSC);

— volgende fase: de checkblokken y1, .., yn worden met Ka berekend;

— eindfase: de cryptografische controlesom wordt als volgt vanaf het laatste checkblok yn berekend: E(Ka, D(Kb, yn)),

waarbij E() codering met DES en D() decodering met DES betekent.

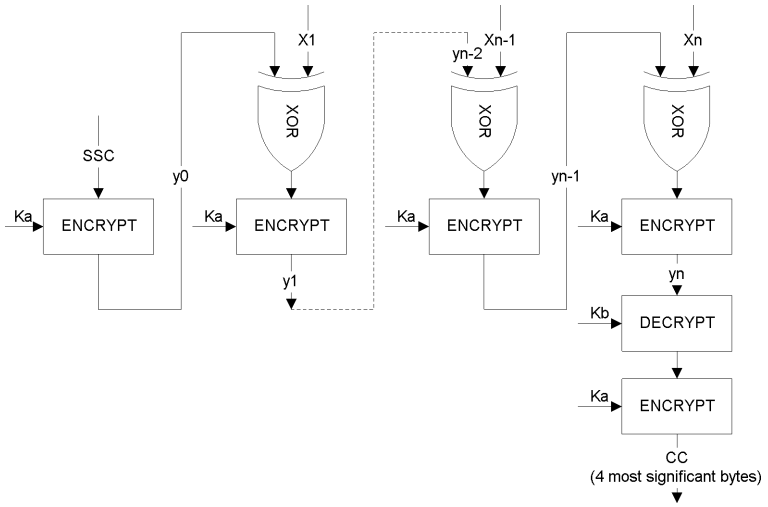
De vier meest significante bytes van de cryptografische controlesom worden overgedragen.

CSM_029 De zendsequentieteller (SSC) wordt tijdens de goedkeuringsprocedure van de sleutel (sleutelovereenstemming) geïnitieerd op:

begin SSC: Rnd3 (4 minst significante bytes) || Rnd1 (4 minst significante bytes).

CSM_030 Elke keer voordat een MAC wordt berekend, wordt de zendsequentieteller met 1 verhoogd (met andere woorden de SSC voor het eerste commando = begin SSC + 1, de SSC voor het eerste antwoord = begin SSC + 2).

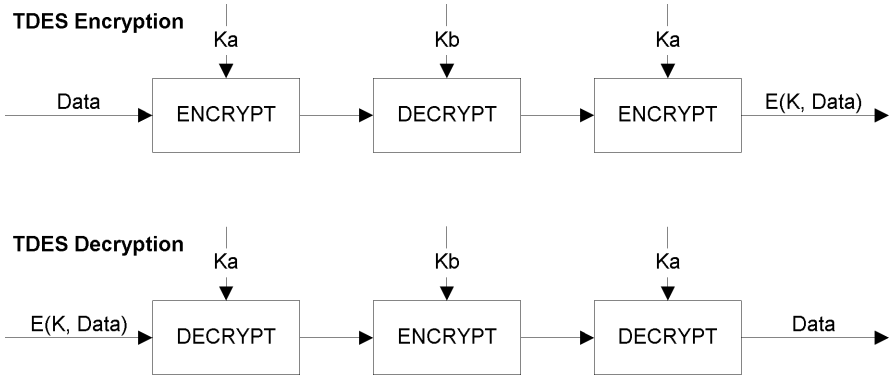
De onderstaande figuur verduidelijkt de berekening van de *retail* MAC:



5.4. Algoritme voor het berekenen van cryptogrammen voor vertrouwelijkheids-DO's

CSM_031 Cryptogrammen worden met TDEA in TCBC-werkingsmodus berekend overeenkomstig referentienorm [TDES] en [TDES-OP] en met de lege vector als beginwaardeblok.

De onderstaande figuur verduidelijkt de toepassing van sleutels in TDES:



6. DIGITALE HANDTEKENINGMECHANISMEN OM GEGEVENS TE DOWNLOADEN

CSM_032 De intelligente toepassingsgerichte apparatuur (IDE) slaat de van een apparaat (VU of kaart) tijdens een downloadsessie ontvangen gegevens op in een fysiek gegevensbestand. Dit bestand moet de certificaten MS_i.C en EQT.C bevatten. Het bestand bevat digitale handtekeningen van gegevensblokken, zoals gespecificeerd in aanhangsel 7 „Protocollen voor gegevensoverdracht".

CSM_033 Digitale handtekeningen van gedownloade gegevens gebruiken een digitaal handtekeningschema met aanhangsel zodat gedownloade gegevens desgewenst zonder decodering kunnen worden gelezen.

6.1. Generering van de handtekening

CSM_034 De gegevenshandtekening wordt door de apparatuur gegenereerd volgens het handtekeningschema met aanhangsel, zoals vastgelegd in referentienorm [PKCS1], op basis van de SHA-1-hashfunctie:

Handtekening = EQT.SK['00' || '01' || *PS* || '00' || DER(SHA-1(Gegevens))]

PS = Reeks opvulbytes (padding string) met waarde 'FF' zodat de lengte gelijk is aan 128.

DER(SHA-1(*M*)) is de codering van de identificatie van het algoritme voor de hashfunctie en de hashwaarde in een ASN.1-waarde van het type DigestInfo (kenmerkende coderingsregels):

'30'||'21'||'30'||'09'||'06'||'05'||'2B'||'0E'||'03'||'02'||'1A'||'05'||'00'||'04'||'14'||Hashwaarde.

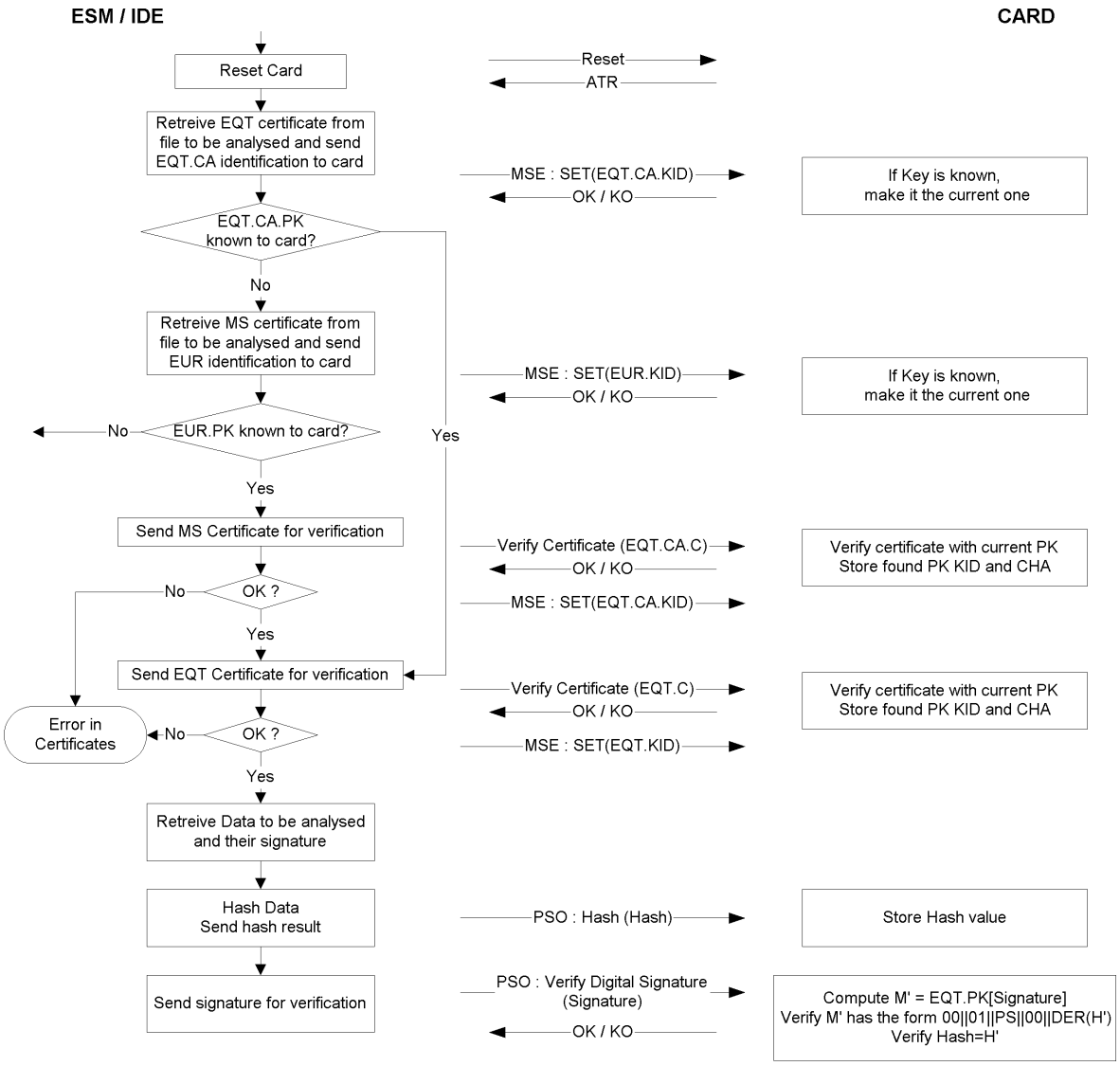
6.2. **Handtekeningverificatie**

CSM_035 De gegevenshandtekening op gedownloade gegevens wordt geverifieerd volgens het handtekeningschema met aanhangsel, zoals vastgelegd in referentienorm [PKCS1], op basis van de SHA-1-hashfunctie.

De verificateur moet de Europese openbare sleutel EUR.PK zelf kennen (en vertrouwen).

De onderstaande tabel verduidelijkt het protocol dat een IDE met ingebrachte controlekaart kan volgen om de integriteit te verifiëren van gedownloade en op externe opslagmedia (ESM) opgeslagen gegevens. De controlekaart wordt gebruikt om digitale handtekeningen te decoderen. Deze functie mag in dit geval niet in de IDE worden geïmplementeerd.

De apparatuur die de te analyseren gegevens heeft gedownload en ondertekend, wordt aangeduid met EQT.



DEEL B

TACHOGRAAFSYSTEEM VAN DE TWEEDE GENERATIE

7. INLEIDING

7.1. **Referentienormen**

De onderstaande referentienormen worden in dit aanhangsel gebruikt:

AES	National Institute of Standards and Technology (NIST), FIPS PUB 197: Advanced Encryption Standard (AES), November 26, 2001
DSS	National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013
ISO 7816-4	ISO/IEC 7816-4, Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange. Third edition 2013-04-15
ISO 7816-8	ISO/IEC 7816-8, Identification cards — Integrated circuit cards — Part 8: Commands for security operations. Second edition 2004-06-01
ISO 8825-1	ISO/IEC 8825-1, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Fourth edition, 2008-12-15
ISO 9797-1	ISO/IEC 9797-1, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher. Second edition, 2011-03-01
ISO 10116	ISO/IEC 10116, Information technology — Security techniques — Modes of operation of an *n*-bit block cipher. Third edition, 2006-02-01
ISO 16844-3	ISO/IEC 16844-3, Road vehicles — Tachograph systems — Part 3: Motion sensor interface First edition 2004, including Technical Corrigendum 1 2006
RFC 5480	Elliptic Curve Cryptography Subject Public Key Information, March 2009
RFC 5639	Elliptic Curve Cryptography (ECC) — Brainpool Standard Curves and Curve Generation, 2010
RFC 5869	HMAC-based Extract-and-Expand Key Derivation Function (HKDF), May 2010
SHS	National Institute of Standards and Technology (NIST), FIPS PUB 180-4: Secure Hash Standard, March 2012
SP 800-38B	National Institute of Standards and Technology (NIST), Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005.
TR-03111	BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 2012-06-28

7.2. **Begrippen en afkortingen**

De onderstaande begrippen en afkortingen worden in dit aanhangsel gebruikt:

AES	Advanced Encryption Standard
CA	Certificeringsautoriteit
CAR	Referentie van de certificeringsautoriteit
CBC	Cipher Block Chaining (werkingsmodus)

CH	Koplabel (header) van het commando
CHA	Autorisatie van de certificaathouder
CHR	Referentie van de certificaathouder
CV	Constante vector
DER	Kenmerkende coderingsregels
DO	Gegevensobject
DSRC	Speciale korteafstandscommunicatie
ECC	Elliptische-krommecryptografie
ECDSA	Elliptische kromme-algoritme voor digitale handtekening
ECDH	Elliptische kromme Diffie-Hellman-sleuteluitwisselingsprotocol (algoritme voor sleutelovereenstemming)
EGF	Externe GNSS-module
EQT	Apparatuur
IDE	Intelligente toepassingsgerichte apparatuur
K_M	Master Key (hoofdsleutel) van de bewegingssensor om een VU te koppelen aan een bewegingssensor
K_{M-VU}	In voertuigunits ingebrachte sleutel waarmee de VU de hoofdsleutel (Master Key) van de bewegingssensor kan afleiden indien een werkplaatskaart in de VU is ingebracht
K_{M-WC}	In werkplaatskaarten ingebrachte sleutel waarmee de VU de hoofdsleutel (Master Key) van de bewegingssensor kan afleiden indien een werkplaatskaart in de VU is ingebracht
MAC	Berichtauthenticatiecode
MoS	Bewegingssensor
MSB	Meest significante bit
PKI	Openbare-sleutelinfrastructuur
RCF	Inrichting voor communicatie op afstand
SSC	Zendsequentieteller
SM	Beveiligde berichtenuitwisseling
TDES	Standaard voor drievoudige gegevenscodering
TLV	Waarde van de labellengte
VU	Voertuigunit
X.C	Openbare-sleutelcertificaat van gebruiker X
X.CA	Certificeringsautoriteit die het certificaat van gebruiker X heeft afgegeven
X.CAR	Referentie van de certificeringsautoriteit die vermeld staat in het certificaat van gebruiker X
X.CHR	Referentie van de certificaathouder die vermeld staat in het certificaat van gebruiker X
X.PK	Openbare sleutel van gebruiker X
X.SK	Particuliere sleutel van gebruiker X
$X.PK_{eph}$	Tijdelijke openbare sleutel van gebruiker X
$X.SK_{eph}$	Tijdelijke particuliere sleutel van gebruiker X
'xx'	Hexadecimale waarde
||	Samenvoegingsoperator

7.3. **Definities**

De in dit aanhangsel gebruikte begrippen worden gedefinieerd in deel I van bijlage 1 C.

8. CRYPTOGRAFISCHE SYSTEMEN EN ALGORITMEN

8.1. **Cryptografische systemen**

CSM_38 Voertuigunits en tachograafkaarten gebruiken een op elliptische-krommecryptografie gebaseerd systeem van openbare sleutels om de volgende beveiligingsdiensten te leveren:

— wederzijdse authenticatie tussen voertuigunit en kaart;

— overeenstemming van AES-sessiesleutels tussen voertuigunit en kaart;

— waarborgen van de authenticiteit, integriteit en onweerlegbaarheid van de gegevens die van voertuigunits of tachograafkaarten worden gedownload op externe media.

CSM_39 Voertuigunits en externe GNSS-modules gebruiken een op elliptische-krommecryptografie gebaseerd systeem van openbare sleutels om de volgende beveiligingsdiensten te leveren:

— koppeling tussen voertuigunit en externe GNSS-module;

— wederzijdse authenticatie tussen voertuigunit en externe GNSS-module;

— overeenstemming van AES-sessiesleutels tussen voertuigunit en externe GNSS-module.

CSM_40 Voertuigunits en tachograafkaarten gebruiken een op AES gebaseerd symmetrisch cryptografisch systeem om de volgende beveiligingsdiensten te leveren:

— waarborgen van de authenticiteit en integriteit van de tussen voertuigunit en tachograafkaart uitgewisselde gegevens;

— waarborgen (waar nodig) van de vertrouwelijkheid van de tussen voertuigunit en tachograafkaart uitgewisselde gegevens.

CSM_41 Voertuigunits en externe GNSS-modules gebruiken een op AES gebaseerd symmetrisch cryptografisch systeem om de volgende beveiligingsdiensten te leveren:

— waarborgen van de authenticiteit en integriteit van de tussen voertuigunit en externe GNSS-module uitgewisselde gegevens.

CSM_42 Voertuigunits en bewegingssensoren gebruiken een op AES gebaseerd symmetrisch cryptografisch systeem om de volgende beveiligingsdiensten te leveren:

— koppeling tussen voertuigunit en bewegingssensor,

— wederzijdse authenticatie tussen voertuigunit en bewegingssensor;

— waarborgen van de vertrouwelijkheid van de tussen voertuigunit en bewegingssensor uitgewisselde gegevens.

CSM_43 Voertuigunits en controlekaarten gebruiken een op AES gebaseerd symmetrisch cryptografisch systeem om de volgende beveiligingsdiensten te leveren via de interface voor communicatie op afstand:

— waarborgen van de vertrouwelijkheid, authenticiteit en integriteit van de gegevens die van een voertuigunit worden overgebracht naar een controlekaart.

Opmerkingen:

— Strikt genomen worden de VU-gegevens via een inrichting voor communicatie op afstand binnen of buiten de VU overgebracht naar een door de controleambtenaar bediend systeem voor ondervraging op afstand (zie aanhangsel 14). Het systeem voor ondervraging op afstand brengt de ontvangen gegevens echter over op een controlekaart om ze te decoderen en te authenticeren. De inrichting voor communicatie op afstand en het systeem voor ondervraging op afstand zijn volledig transparant vanuit beveiligingsoogpunt.

— Voor de DSRC-interface biedt een werkplaatskaart dezelfde beveiligingsdiensten als een controlekaart. Zo kan in de werkplaats worden gecontroleerd of de VU-interface voor communicatie op afstand goed functioneert, ook wat de beveiliging betreft. Zie punt 9.2.2 voor meer informatie.

8.2. **Cryptografische algoritmen**

8.2.1 *Symmetrische algoritmen*

CSM_44 Voertuigunits, tachograafkaarten, bewegingssensoren en externe GNSS-modules ondersteunen het AES-algoritme, zoals vastgelegd in [AES], met een sleutellengte van 128, 192 en 256 bits.

8.2.2 *Asymmetrische algoritmen en gestandaardiseerde domeinparameters*

CSM_45 Voertuigunits, tachograafkaarten en externe GNSS-modules ondersteunen elliptische-krommecryptografie met een sleutelgrootte van 256, 384 en 512/521 bits.

CSM_46 Voertuigunits, tachograafkaarten en externe GNSS-modules ondersteunen het ECDSA-ondertekeningsalgoritme, zoals gespecificeerd in [DSS].

CSM_47 Voertuigunits, tachograafkaarten en externe GNSS-modules ondersteunen het ECKA-EG-algoritme voor sleutelovereenstemming, zoals gespecificeerd in [TR 03111].

CSM_48 Voertuigunits, tachograafkaarten en externe GNSS-modules ondersteunen alle gestandaardiseerde domeinparameters die hieronder in Tabel 1 worden gespecificeerd voor de elliptische-krommecryptografie.

Tabel 1

Gestandaardiseerde domeinparameters

Naam	Grootte (bits)	Referentie	Objectidentificator
NIST P-256	256	[DSS], [RFC 5480]	`secp256r1`
BrainpoolP256r1	256	[RFC 5639]	`brainpoolP256r1`
NIST P-384	384	[DSS], [RFC 5480]	`secp384r1`
BrainpoolP384r1	384	[RFC 5639]	`brainpoolP384r1`
BrainpoolP512r1	512	[RFC 5639]	`brainpoolP512r1`
NIST P-521	521	[DSS], [RFC 5480]	`secp521r1`

Opmerking: de objectidentificatoren in de laatste kolom van Tabel 1 worden gespecificeerd in [RFC 5639] wat de Brainpool-krommen betreft, en in [RFC 5480] wat de NIST-krommen betreft.

Voorbeeld 1: de objectidentificator van de Brainpool-kromme P256r1 is `{iso(1) identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8) ellipticCurve(1) versionOne(1) 7}`.

Of in puntnotatie: `1.3.36.3.3.2.8.1.1.7`.

Voorbeeld 2: de objectidentificator van de NIST-kromme P-384 is

`{iso(1) identified-organization(3) certicom(132) curve(0) 34}`.

Of in puntnotatie: `1.3.132.0.34`.

8.2.3 *Hashalgoritmen*

CSM_49 Voertuigunits en tachograafkaarten ondersteunen de in [SHS] gespecificeerde algoritmen SHA-256, SHA-384 en SHA-512.

8.2.4 *Coderingssuites*

CSM_50 Indien een symmetrisch algoritme, asymmetrisch algoritme en/of hashalgoritme worden gecombineerd om een beveiligingsprotocol te vormen, zijn de respectieve sleutellengte en hashgrootte (ongeveer) van gelijke cryptografische sterkte. De toegestane coderingssuites worden weergegeven in Tabel 2:

Tabel 2

Toegestane coderingssuites

ID coderingssuite	ECC-sleutelgrootte (bits)	AES-sleutellengte (bits)	Hashalgoritme	MAC-lengte (bytes)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Opmerking: in dit aanhangsel worden ECC-sleutels met een grootte van 512 bits en 521 bits in elk opzicht als van gelijke cryptografische sterkte beschouwd.

9. SLEUTELS EN CERTIFICATEN

9.1. **Asymmetrische sleutelparen en openbare-sleutelcertificaten**

9.1.1 *Algemeen*

Opmerking: de hier beschreven sleutels worden gebruikt voor de wederzijdse authenticatie en beveiligde berichtenuitwisseling tussen voertuigunits en tachograafkaarten en tussen voertuigunits en externe GNSS-modules. De desbetreffende procedures worden uitvoerig toegelicht in hoofdstukken 10 en 11 van dit aanhangsel.

CSM_51 In het Europese slimme tachograafsysteem worden de ECC-sleutelparen en bijbehorende certificaten op drie functionele hiërarchieniveaus gegenereerd en beheerd:

— Europees niveau,

— lidstaatniveau,

— apparatuurniveau.

CSM_52 In het volledige Europese slimme tachograafsysteem worden openbare en particuliere sleutels en certificaten gegenereerd, beheerd en uitgewisseld met gebruikmaking van gestandaardiseerde en beveiligde methoden.

9.1.2 *Europees niveau*

CSM_53 Op Europees niveau wordt een enkel Europees ECC-sleutelpaar gegenereerd, aangeduid als EUR en bestaande uit een particuliere sleutel (EUR.SK) en een openbare sleutel (EUR.PK). Dit sleutelpaar vormt de basis van de openbare-sleutelinfrastructuur (PKI) van het volledige Europese slimme tachograafsysteem. Deze taak wordt uitgevoerd door de Europese basiscertificeringsautoriteit (ERCA) in opdracht en onder verantwoordelijkheid van de Europese Commissie.

CSM_54 De ERCA gebruikt de Europese particuliere sleutel om een (zelfondertekend) basiscertificaat van de Europese openbare sleutel te ondertekenen, en deelt dit Europese basiscertificaat mee aan alle lidstaten.

CSM_55 De ERCA gebruikt de Europese particuliere sleutel om desgevraagd de openbare-sleutelcertificaten van de lidstaten te ondertekenen. De ERCA houdt registraties bij van alle ondertekende openbare-sleutelcertificaten van de lidstaten.

CSM_56 Zoals aangegeven in Figuur 1 onder 9.1.7, genereert de ERCA om de 17 jaar een nieuw Europees basissleutelpaar. Telkens wanneer de ERCA een nieuw Europees basissleutelpaar genereert, maakt zij een nieuw, zelfondertekend basiscertificaat voor de nieuwe Europese openbare sleutel. Het Europese basiscertificaat is 34 jaar en 3 maanden geldig.

Opmerking: op het ogenblik dat een nieuw basissleutelpaar wordt geïntroduceerd, genereert de ERCA ook een nieuwe hoofdsleutel voor de bewegingssensor en een nieuwe DSRC-hoofdsleutel (zie punten 9.2.1.2 en 9.2.2.2).

CSM_57 Alvorens een nieuw Europees basissleutelpaar te genereren, onderzoekt de ERCA welke cryptografische sterkte het nieuwe sleutelpaar moet hebben om gedurende de komende 34 jaar bescherming te bieden tegen inbreuken op de beveiliging. Zoals gespecificeerd in CSM_50, schakelt de ERCA indien nodig over op een coderingssuite die een grotere cryptografische sterkte heeft dan de huidige.

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 geldig. Dit wordt eveneens verduidelijkt in Figuur 1 onder 9.1.7.

Opmerking: aangezien een verbindingscertificaat de door de ERCA gegenereerde openbare sleutel van generatie *X* bevat en wordt ondertekend met de door de ERCA gegenereerde particuliere sleutel van generatie *X-1*, kan apparatuur waarvoor een sleutel van generatie *X-1* is verstrekt, vertrouwen op apparatuur die beschikt over een sleutel van generatie *X*.

CSM_59 Zodra een nieuw basissleutelcertificaat van kracht wordt, staakt de ERCA het gebruik van de particuliere sleutel van het basissleutelpaar.

CSM_60 De ERCA beschikt te allen tijde over de volgende cryptografische sleutels en certificaten:

— het huidige EUR-sleutelpaar en bijbehorend certificaat;

— alle vorige EUR-certificaten ter verificatie van de nog geldende certificaten van de certificeringsautoriteiten van de lidstaten;

— verbindingscertificaten voor EUR-certificaten van alle generaties, met uitzondering van het eerste certificaat.

9.1.3 *Lidstaatniveau*

CSM_61 Alle lidstaten die certificaten voor tachograafkaarten moeten ondertekenen, genereren een of meerdere unieke ECC-sleutelparen, aangeduid als MSCA_Card. Alle lidstaten die certificaten voor voertuigunits of externe GNSS-modules moeten ondertekenen, genereren daarnaast ook een of meerdere unieke ECC-sleutelparen, aangeduid als MSCA_VU-EGF.

CSM_62 De taak om sleutelparen op lidstaatniveau te genereren, wordt opgedragen aan de certificeringsautoriteit van de lidstaat (MSCA). Telkens wanneer de MSCA een lidstaat-sleutelpaar genereert, geeft zij de openbare sleutel door aan de ERCA om het desbetreffende, door de ERCA ondertekende lidstaatcertificaat te verkrijgen.

CSM_63 De MSCA kiest voor het lidstaat-sleutelpaar dezelfde cryptografische sterkte als die van het Europese basissleutelpaar waarmee het corresponderende lidstaatcertificaat wordt ondertekend.

CSM_64 Het sleutelpaar MSCA_VU-EGF bestaat in voorkomend geval uit een particuliere sleutel MSCA_VU-EGF.SK en een openbare sleutel MSCA_VU-EGF.PK. De MSCA gebruikt de particuliere sleutel MSCA_VU-EGF.SK uitsluitend om de openbare-sleutelcertificaten van voertuigunits en externe GNSS-modules te ondertekenen.

CSM_65 Het sleutelpaar MSCA_Card bestaat uit een particuliere sleutel (MSCA_Card.SK) en een openbare sleutel (MSCA_Card.PK). De MSCA gebruikt de particuliere sleutel MSCA_Card.SK uitsluitend om de openbare-sleutelcertificaten van tachograafkaarten te ondertekenen.

CSM_66 De MSCA houdt registraties bij van alle ondertekende certificaten van voertuigunits, externe GNSS-modules en tachograafkaarten, samen met de identificatie van de apparatuur waarvoor elk certificaat bedoeld is.

CSM_67 Het certificaat MSCA_VU-EGF is 17 jaar en 3 maanden geldig. Het certificaat MSCA_Card is 7 jaar en 1 maand geldig.

CSM_68 Zoals aangegeven in Figuur 1 onder 9.1.7, kunnen de particuliere sleutel van een sleutelpaar MSCA_VU-EGF en de particuliere sleutel van een sleutelpaar MSCA_Card gedurende twee jaar worden gebruikt.

CSM_69 De MSCA staakt het gebruik van de particuliere sleutel van het sleutelpaar MSCA_VU-EGF zodra de gebruikstermijn is verstreken. De MSCA staakt eveneens het gebruik van de particuliere sleutel van het sleutelpaar MSCA_Card zodra de gebruikstermijn is verstreken.

CSM_70 De MSCA beschikt te allen tijde over de volgende cryptografische sleutels en certificaten:

— het huidige sleutelpaar MSCA_Card en bijbehorend certificaat;

— alle vorige certificaten MSCA_Card ter verificatie van de nog geldende certificaten voor tachograafkaarten;

— het huidige EUR-certificaat ter verificatie van het huidige MSCA-certificaat;

— alle vorige EUR-certificaten ter verificatie van alle nog geldende MSCA-certificaten.

CSM_71 Voorts beschikt de MSCA, indien zij certificaten voor voertuigunits of externe GNSS-modules moet ondertekenen, over de volgende sleutels en certificaten:

— het huidige sleutelpaar MSCA_VU-EGF en bijbehorend certificaat;

— alle vorige openbare sleutels MSCA_VU-EGF ter verificatie van de nog geldende certificaten voor VU's of externe GNSS-modules.

9.1.4 *Apparatuurniveau: voertuigunits*

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 de MSCA van de lidstaat waar zij gevestigd is om het desbetreffende, door de MSCA ondertekende VU-certificaat te verkrijgen. De particuliere sleutel wordt uitsluitend door de voertuigunit gebruikt.

CSM_73 De certificaten VU_MA en VU_Sign van de voertuigunit hebben dezelfde ingangsdatum.

CSM_74 De VU-fabrikant kiest voor het VU-sleutelpaar dezelfde cryptografische sterkte als die van het MSCA-sleutelpaar waarmee het corresponderende VU-certificaat wordt ondertekend.

CSM_75 De voertuigunit gebruikt het sleutelpaar VU_MA, bestaande uit de particuliere sleutel VU_MA.SK en de openbare sleutel VU_MA.PK, uitsluitend om zich te authenticeren bij de tachograafkaarten en externe GNSS-modules, zoals gespecificeerd in punten 10.3 en 11.4 van dit aanhangsel.

CSM_76 De voertuigunit kan tijdelijke ECC-sleutelparen genereren die uitsluitend dienen voor de sleutelovereenstemming tijdens de sessie met een tachograafkaart of externe GNSS-module, zoals gespecificeerd in punten 10.4 en 11.4 van dit aanhangsel.

CSM_77 De voertuigunit gebruikt de particuliere sleutel VU_Sign.SK van het sleutelpaar VU_Sign uitsluitend om gedownloade gegevensbestanden te ondertekenen, zoals gespecificeerd in hoofdstuk 14 van dit aanhangsel. De corresponderende openbare sleutel VU_Sign.PK wordt uitsluitend gebruikt ter verificatie van de door de voertuigunit aangemaakte handtekeningen.

CSM_78 Zoals aangegeven in Figuur 1 onder 9.1.7, is het certificaat VU_MA 15 jaar en 3 maanden geldig. Het certificaat VU_Sign is eveneens 15 jaar en 3 maanden geldig.

Opmerkingen:

— Dankzij de verlengde geldigheidsduur van het certificaat VU_Sign kan de voertuigunit gedurende de eerste drie maanden na de vervaldatum van het certificaat geldige handtekeningen voor gedownloade gegevens aanmaken, zoals voorgeschreven in Verordening (EU) nr. 581/2010 van de Commissie.

— De verlengde geldigheidsduur van het certificaat VU_MA is noodzakelijk om de VU in staat te stellen zich gedurende de eerste drie maanden na de vervaldatum van het certificaat te authenticeren bij een controlekaart of bedrijfskaart en zodoende gegevens te downloaden.

CSM_79 Nadat de geldigheidsduur van het desbetreffende certificaat is verstreken, staakt de voertuigunit het gebruik van de particuliere sleutel van het VU-sleutelpaar.

CSM_80 De VU-sleutelparen (met uitzondering van tijdelijke sleutelparen) en bijbehorende VU-certificaten worden niet ter plaatse vervangen of vernieuwd nadat de voertuigunit in gebruik is genomen.

Opmerkingen:

— De tijdelijke sleutelparen vallen niet onder dit voorschrift aangezien de VU een nieuw tijdelijk sleutelpaar genereert bij elke chipauthenticatie en sleutelovereenstemming tijdens de sessie (zie punt 10.4). Tijdelijke sleutelparen hebben geen corresponderende certificaten.

— Dit voorschrift doet geen afbreuk aan de mogelijkheid om statische VU-sleutelparen te vervangen tijdens de ombouw of reparatie in een beveiligde omgeving onder het toezicht van de VU-fabrikant.

CSM_81 Bij ingebruikname bevatten voertuigunits de volgende cryptografische sleutels en certificaten:

— de particuliere sleutel VU_MA en bijbehorend certificaat;

— de particuliere sleutel VU_Sign en bijbehorend certificaat;

— het certificaat MSCA_VU-EGF met de openbare sleutel MSCA_VU-EGF.PK ter verificatie van het certificaat VU_MA en het certificaat VU_Sign;

— het EUR-certificaat met de openbare sleutel EUR.PK ter verificatie van het certificaat MSCA_VU-EGF;

— het EUR-certificaat waarvan de geldigheidsduur onmiddellijk voorafgaat aan die van het EUR-certificaat ter verificatie van het certificaat MSCA_VU-EGF (indien bestaand);

— het verbindingscertificaat tussen beide EUR-certificaten (indien bestaand).

CSM_82 Naast de in CSM_81 genoemde cryptografische sleutels en certificaten beschikken voertuigunits ook over de in deel A van dit aanhangsel gespecificeerde sleutels en certificaten ten behoeve van de interactie met tachograafkaarten van de eerste generatie.

9.1.5 *Apparatuurniveau: tachograafkaarten*

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 kaartsleutelpaar genereert, verzendt de openbare sleutel naar de MSCA van de lidstaat waar zij gevestigd is om het desbetreffende, door de MSCA ondertekende kaartcertificaat te verkrijgen. De particuliere sleutel wordt uitsluitend door de tachograafkaart gebruikt.

CSM_84 De certificaten Card_MA en Card_Sign van de bestuurders- of werkplaatskaart hebben dezelfde ingangsdatum.

CSM_85 De kaartfabrikant of -personalisator kiest voor het kaartsleutelpaar dezelfde cryptografische sterkte als die van het MSCA-sleutelpaar waarmee het corresponderende kaartcertificaat wordt ondertekend.

CSM_86 De tachograafkaart gebruikt het sleutelpaar Card_MA, bestaande uit de particuliere sleutel Card_MA.SK en de openbare sleutel Card_MA.PK, uitsluitend met het oog op de wederzijdse authenticatie en sleutelovereenstemming tijdens de sessie met voertuigunits, zoals gespecificeerd in punten 10.3 en 10.4 van dit aanhangsel.

CSM_87 De bestuurders- of werkplaatskaart gebruikt de particuliere sleutel Card_Sign.SK van het sleutelpaar Card_Sign uitsluitend om gedownloade gegevensbestanden te ondertekenen, zoals gespecificeerd in hoofdstuk 14 van dit aanhangsel. De corresponderende openbare sleutel Card_Sign.PK wordt uitsluitend gebruikt ter verificatie van de door de kaart aangemaakte handtekeningen.

CSM_88 Het certificaat Card_MA heeft de volgende geldigheidsduur:

— voor bestuurderskaarten: 5 jaar;

— voor bedrijfskaarten: 2 jaar;

— voor controlekaarten: 2 jaar;

— voor werkplaatskaarten: 1 jaar

CSM_89 Het certificaat Card_Sign heeft de volgende geldigheidsduur:

— voor bestuurderskaarten: 5 jaar en 1 maand;

— voor werkplaatskaarten: 1 jaar en 1 maand.

Opmerking: dankzij de verlengde geldigheidsduur van het certificaat Card_Sign kan de bestuurderskaart gedurende de eerste maand na de vervaldatum van het certificaat geldige handtekeningen voor gedownloade gegevens aanmaken. Dit is noodzakelijk in het licht van Verordening (EU) nr. 581/2010 van de Commissie, op grond waarvan de maximumtermijn binnen dewelke gegevens van een bestuurderskaart moeten worden gedownload, niet langer mag zijn dan 28 dagen nadat de laatste gegevens zijn geregistreerd.

CSM_90 De sleutelparen en bijbehorende certificaten van de tachograafkaart worden niet vervangen of vernieuwd na afgifte van de kaart.

CSM_91 Bij afgifte bevatten de tachograafkaarten de volgende cryptografische sleutels en certificaten:

— de particuliere sleutel Card_MA en bijbehorend certificaat;

— voor bestuurders- en werkplaatskaarten daarnaast ook de particuliere sleutel Card_Sign en bijbehorend certificaat;

— het certificaat MSCA_Card met de openbare sleutel MSCA_Card.PK ter verificatie van het certificaat Card_MA en het certificaat Card_Sign;

— het EUR-certificaat met de openbare sleutel EUR.PK ter verificatie van het certificaat MSCA_Card;

— het EUR-certificaat waarvan de geldigheidsduur onmiddellijk voorafgaat aan die van het EUR-certificaat ter verificatie van het certificaat MSCA_Card (indien bestaand);

— het verbindingscertificaat tussen beide EUR-certificaten (indien bestaand).

CSM_92 Naast de in CSM_91 genoemde cryptografische sleutels en certificaten beschikken tachograafkaarten ook over de in deel A van dit aanhangsel gespecificeerde sleutels en certificaten ten behoeve van de interactie met voertuigunits van de eerste generatie.

9.1.6 *Apparatuurniveau: externe GNSS-modules*

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 sleutelpaar EGF_MA genereert, verzendt de openbare sleutel naar de MSCA van de lidstaat waar zij gevestigd is om het desbetreffende, door de MSCA ondertekende certificaat EGF_MA te verkrijgen. De particuliere sleutel wordt uitsluitend door de externe GNSS-module gebruikt.

CSM_94 De fabrikant van de externe GNSS-module kiest voor het sleutelpaar EGF_MA dezelfde cryptografische sterkte als die van het MSCA-sleutelpaar waarmee het corresponderende certificaat EGF_MA wordt ondertekend.

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 punten 11.4 en 11.4 van dit aanhangsel.

CSM_96 Het certificaat EGF_MA is 15 jaar geldig.

CSM_97 Nadat de geldigheidsduur van het desbetreffende certificaat is verstreken, staakt de externe GNSS-module het gebruik van de particuliere sleutel van het sleutelpaar EGF_MA.

Opmerking: zoals uiteengezet in punt 11.3.3, kan de externe GNSS-module de particuliere sleutel gebruiken voor de wederzijdse authenticatie met de VU waaraan hij al gekoppeld is, zelfs wanneer de geldigheidsduur van het desbetreffende certificaat is verstreken.

CSM_98 Het sleutelpaar EGF_MA en het bijbehorende EGF-certificaat worden niet ter plaatse vervangen of vernieuwd nadat de externe GNSS-module in gebruik is genomen.

Opmerking: dit voorschrift doet geen afbreuk aan de mogelijkheid om EGF-sleutelparen te vervangen tijdens de ombouw of reparatie in een beveiligde omgeving onder het toezicht van de fabrikant van de externe GNSS-module.

CSM_99 Bij ingebruikname bevat de externe GNSS-module de volgende cryptografische sleutels en certificaten:

— de particuliere sleutel EGF_MA en bijbehorend certificaat;

— het certificaat MSCA_VU-EGF met de openbare sleutel MSCA_VU-EGF.PK ter verificatie van het certificaat EGF_MA;

— het EUR-certificaat met de openbare sleutel EUR.PK ter verificatie van het certificaat MSCA_VU-EGF;

— het EUR-certificaat waarvan de geldigheidsduur onmiddellijk voorafgaat aan die van het EUR-certificaat ter verificatie van het certificaat MSCA_VU-EGF (indien bestaand);

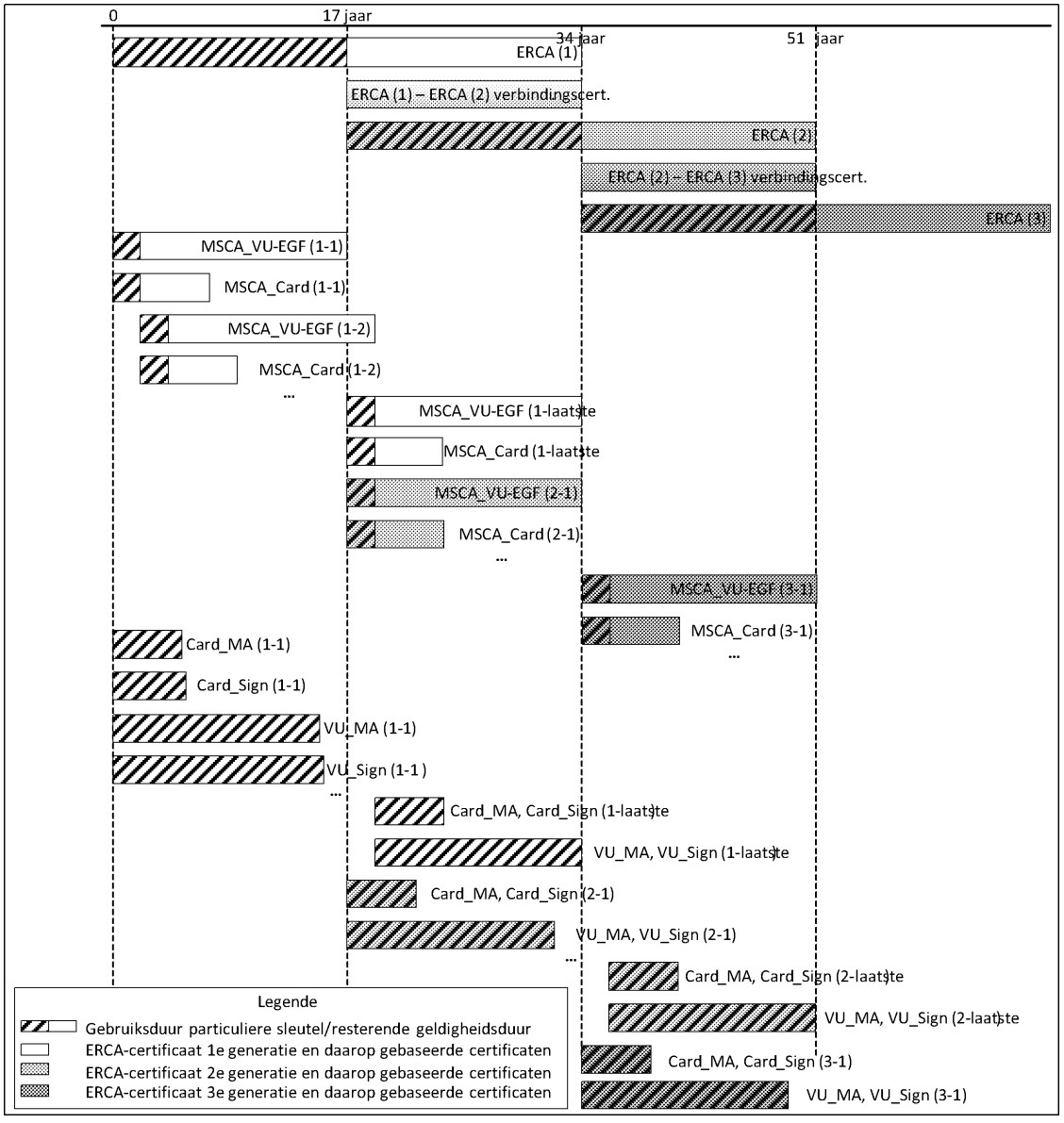
— het verbindingscertificaat tussen beide EUR-certificaten (indien bestaand).

9.1.7 *Overzicht: vervanging van het certificaat*

In Figuur 1 hieronder wordt een overzicht gegeven van de afgifte- en gebruikstermijnen voor de verschillende generaties ERCA-basiscertificaten, ERCA-verbindingscertificaten, MSCA-certificaten en apparatuurcertificaten (VU- en kaartcertificaten):

Figuur 1

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



Toelichtingen bij Figuur 1:

1. De verschillende generaties van het basiscertificaat worden aangeduid door een cijfer tussen haakjes. ERCA (1) bijvoorbeeld verwijst naar het ERCA-basiscertificaat van de eerste generatie; ERCA (2) verwijst naar het ERCA-basiscertificaat van de tweede generatie enz.

2. Andere certificaten worden aangeduid door twee cijfers tussen haakjes: het eerste cijfer geeft aan in het kader van welke generatie van het basiscertificaat het desbetreffende certificaat is afgegeven; het tweede cijfer verwijst naar de generatie van het certificaat zelf. MSCA_Card (1-1) verwijst bijvoorbeeld naar het eerste certificaat MSCA_Card dat is afgegeven in het kader van het basiscertificaat ERCA (1); MSCA_Card (2-1) verwijst naar het eerste certificaat MSCA_Card dat is afgegeven in het kader van het basiscertificaat ERCA (2); MSCA_Card (2-laatste) is het laatste certificaat MSCA_Card dat is afgegeven in het kader van het basiscertificaat ERCA (2); Card_MA (2-1) is het eerste kaartcertificaat dat met het oog op de wederzijdse authenticatie is afgegeven in het kader van het basiscertificaat ERCA (2) enz.

3. De certificaten MSCA_Card (2-1) en MSCA_Card (1-laatste) zijn bijna, maar niet exact op dezelfde datum afgegeven. MSCA_Card (2-1) is het eerste certificaat MSCA_Card in het kader van het basiscertificaat ERCA (2) en wordt iets later afgegeven dan het certificaat MSCA_Card (1-laatste), zijnde het laatste certificaat MSCA_Card dat is afgegeven in het kader van het basiscertificaat ERCA (1).

4. Uit de figuur blijkt dat de eerste VU- en kaartcertificaten die zijn afgegeven in het kader van het basiscertificaat ERCA (2), bijna twee jaar vroeger voorkomen dan de laatste VU- en kaartcertificaten die zijn afgegeven in het kader van het basiscertificaat ERCA (1). De reden hiervoor is dat de VU- en kaartcertificaten niet rechtstreeks in het kader van het ERCA-certificaat worden afgegeven, maar veeleer als onderdeel van een MSCA-certificaat. Het certificaat MSCA (2-1) wordt afgegeven direct nadat het basiscertificaat ERCA (2) geldig wordt, terwijl het certificaat MSCA (1-laatste) iets vroeger wordt afgegeven, net vóór de vervaldatum van het basiscertificaat ERCA (1). Bijgevolg hebben beide MSCA-certificaten vrijwel dezelfde geldigheidsduur, ook al behoren ze tot een verschillende generatie.

5. De aangegeven geldigheidsduur is van toepassing op bestuurderskaarten (5 jaar).

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

9.2. **Symmetrische sleutels**

9.2.1 *Sleutels ter beveiliging van de communicatie tussen VU en bewegingssensor*

9.2.1.1 *Algemeen*

Opmerking: de lezer wordt bekend verondersteld met de inhoud van [ISO 16844-3], waarin een beschrijving wordt gegeven van de interface tussen een voertuigunit en een bewegingssensor. De koppelingsprocedure tussen een VU en een bewegingssensor wordt nader toegelicht in hoofdstuk 12 van dit aanhangsel.

CSM_100 Zoals wordt verduidelijkt in Tabel 3, is een aantal symmetrische sleutels vereist, niet alleen om voertuigunits en bewegingssensoren te koppelen en wederzijds te authenticeren, maar ook om de communicatie tussen voertuigunits en bewegingssensoren te coderen. Het gaat daarbij altijd om AES-sleutels waarvan de lengte gelijk is aan die van de hoofdsleutel van de bewegingssensor, welke gerelateerd is aan de lengte van het (geplande) Europese basissleutelpaar, zoals beschreven in CSM_50.

Tabel 3

Sleutels ter beveiliging van de communicatie tussen voertuigunit en bewegingssensor

Sleutel	Symbool	Afkomstig van	Methode van genereren	Opgeslagen door
Hoofdsleutel bewegingssensor — VU-gedeelte	$K_{M\text{-}VU}$	ERCA	Aselect	ERCA, MSCA's die VU-certificaten afgeven, VU-fabrikanten, voertuigunits

Sleutel	Symbool	Afkomstig van	Methode van genereren	Opgeslagen door
Hoofdsleutel bewegingssensor — Werkplaatsgedeelte	K_{M-WC}	ERCA	Aselect	ERCA, MSCA's, kaartfabrikanten, werkplaatskaarten
Hoofdsleutel bewegingssensor	K_M	Niet afzonderlijk gegenereerd	Berekend als $K_M = K_{M-VU}$ XOR K_{M-WC}	ERCA, MSCA's die sleutels verstrekken voor bewegingssensoren (facultatief) (*)
Identificatie-sleutel	K_{ID}	Niet afzonderlijk gegenereerd	Berekend als $K_{ID} = K_M$ XOR CV, waarbij CV (constante vector) is gespecificeerd in CSM_106	ERCA, MSCA's die sleutels verstrekken voor bewegingssensoren (facultatief) (*)
Koppelings-sleutel	K_P	Fabrikanten van bewegingssensoren	Aselect	De betrokken bewegingssensor
Sessiesleutel	K_S	VU (tijdens koppeling tussen VU en bewegingssensor)	Aselect	De betrokken VU en bewegingssensor

(*) De sleutels K_M en K_{ID} worden facultatief opgeslagen aangezien ze kunnen worden afgeleid van K_{M-VU}, K_{M-WC} en CV.

CSM_101 De Europese basiscertificeringsautoriteit (ERCA) genereert K_{M-VU} en K_{M-WC}, twee aselecte en unieke AES-sleutels waarmee de hoofdsleutel van de bewegingssensor K_M kan worden berekend als K_{M-VU} XOR K_{M-WC}. De ERCA deelt de sleutels K_M, K_{M-VU} en K_{M-WC} mee aan de certificeringsautoriteiten van de lidstaten (MSCA's) die daarom verzoeken.

CSM_102 De ERCA wijst aan elke hoofdsleutel van de bewegingssensor K_M een uniek versienummer toe, dat ook geldt voor de samenstellende sleutels K_{M-VU} en K_{M-WC} en voor de bijbehorende identificatiesleutel K_{ID}. Op het ogenblik dat de ERCA de sleutels K_{M-VU} en K_{M-WC} naar de MSCA's verzendt, deelt zij ook het versienummer mee.

Opmerking: het versienummer dient om onderscheid te maken tussen de verschillende generaties van deze sleutels, zoals uiteengezet in punt 9.2.1.2.

CSM_103 De MSCA geeft de sleutel K_{M-VU}, met het bijbehorende versienummer door aan de VU-fabrikanten die daarom verzoeken. De sleutel K_{M-VU} wordt met het bijbehorende versienummer in alle geproduceerde voertuigunits ingebracht door de VU-fabrikanten.

CSM_104 De MSCA zorgt ervoor dat de sleutel K_{M-WC} met het bijbehorende versienummer wordt ingebracht in elke werkplaatskaart die onder haar verantwoordelijkheid wordt afgegeven.

Opmerkingen:

— Zie de beschrijving van het gegevenstype `SensorInstallationSecData` in aanhangsel 2.

— Zoals uiteengezet in punt 9.2.1.2, kan het nodig zijn in een en dezelfde werkplaatskaart sleutels K_{M-WC} van meerdere generaties in te brengen.

CSM_105 Naast de in CSM_104 genoemde AES-sleutel zorgt de MSCA ervoor dat de TDES-sleutel Km_{WC}, zoals gespecificeerd in voorschrift CSM_037 in deel A van dit aanhangsel, wordt ingebracht in elke werkplaatskaart die onder haar verantwoordelijkheid wordt afgegeven.

Opmerkingen:

— Op die manier kan een werkplaatskaart van de tweede generatie worden gebruikt om verbinding te maken met een VU van de eerste generatie.

— Een werkplaatskaart van de tweede generatie bevat twee verschillende toepassingen: de eerste voldoet aan deel B van dit aanhangsel en de tweede aan deel A. Deze laatste toepassing bevat de TDES-sleutel Km_{WC}.

CSM_106 De MSCA die sleutels voor bewegingssensoren verstrekt, leidt de identificatiesleutel af van de hoofdsleutel van de bewegingssensor door een exclusieve OF-bewerking („XOR") daarop uit te voeren met een constante vector (CV). De CV heeft de volgende waarde:

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

— Voor 192-bits hoofdsleutels van de bewegingssensor: CV = '72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25'

— Voor 256-bits hoofdsleutels van de bewegingssensor: CV = '1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60'

Opmerking: de constante vectoren werden als volgt gegenereerd:

Pi_10 = eerste 10 bytes van het decimale gedeelte van de wiskundige constante π = '24 3F 6A 88 85 A3 08 D3 13 19'

CV_128-bits = eerste 16 bytes van SHA-256(Pi_10)

CV_192-bits = eerste 24 bytes van SHA-384(Pi_10)

CV_256-bits = eerste 32 bytes van SHA-512(Pi_10)

CSM_107 Fabrikanten van bewegingssensoren genereren voor elke bewegingssensor een aselecte en unieke koppelingssleutel K_P, en verzenden elke koppelingssleutel naar de 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.

Opmerking: zoals uiteengezet in punt 9.2.1.2, kan het zijn dat de fabrikant van bewegingssensoren voor een en dezelfde bewegingssensor meerdere unieke koppelingssleutels moet genereren.

CSM_108 De fabrikant van bewegingssensoren genereert een uniek serienummer voor elke bewegingssensor en verzendt alle serienummers naar de 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.

CSM_109 Om te voldoen aan de voorschriften CSM_107 en CSM_108, gebruikt de MSCA het AES-algoritme in CBS(Cipher Block Chaining)-werkingsmodus, zoals vastgelegd in [ISO 10116], met een interleave-parameter *m* = 1 en een initialisatievector IV = '00' {16}, dat wil zeggen 16 bytes met een binaire nul. Zo nodig past de MSCA de in [ISO 9797-1] vastgelegde paddingmethode 2 toe om de gegevens op te vullen.

CSM_110 De fabrikant van bewegingssensoren slaat de gecodeerde koppelingssleutel en het gecodeerde serienummer op in de desbetreffende bewegingssensor, samen met de corresponderende ongecodeerde tekstwaarden en het versienummer van de voor de codering gebruikte sleutels K_M en K_{ID}.

Opmerking: zoals uiteengezet in punt 9.2.1.2, kan het zijn dat de fabrikant van bewegingssensoren in een en dezelfde bewegingssensor meerdere gecodeerde koppelingssleutels en serienummers moet inbrengen.

CSM_111 Naast het op AES gebaseerde cryptografisch materiaal, zoals gespecificeerd in CSM_110, kan een fabrikant van bewegingssensoren ook in elke bewegingssensor het op TDES gebaseerde cryptografisch materiaal opslaan dat nader wordt omschreven in voorschrift CSM_037 in deel A van dit aanhangsel.

Opmerking: deze werkwijze maakt het mogelijk een verbinding tot stand te brengen tussen een bewegingssensor van de tweede generatie en een VU van de eerste generatie.

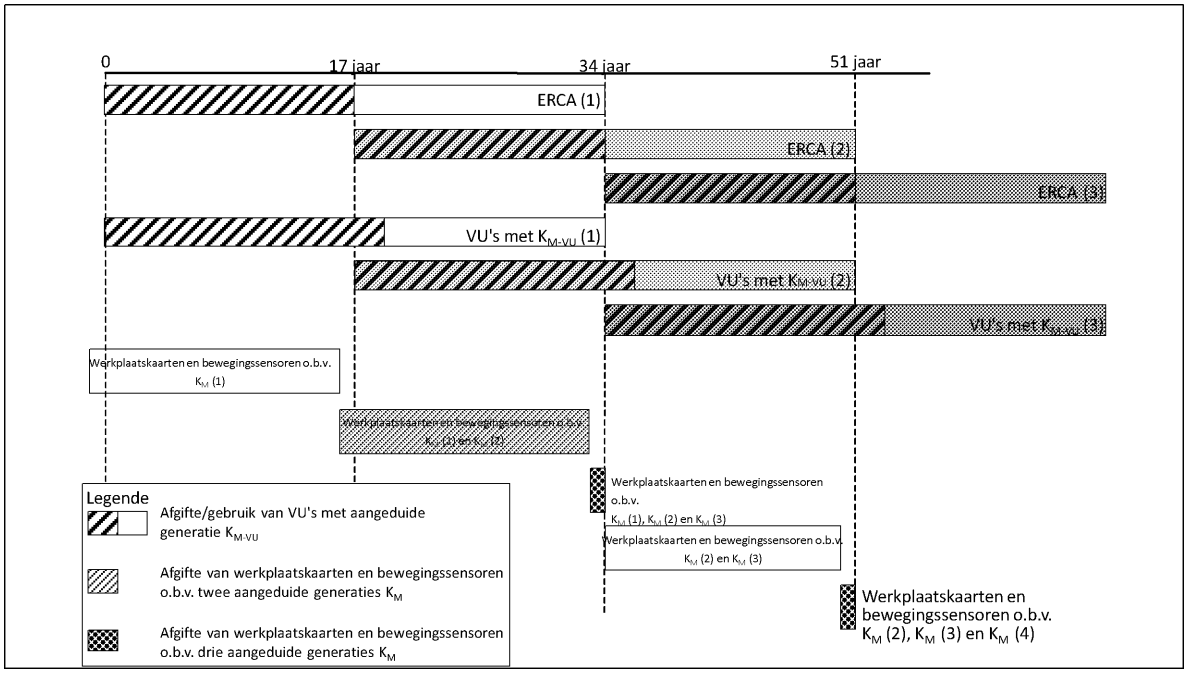
CSM_112 De lengte van de sessiesleutel K_S die door een VU wordt gegenereerd tijdens de koppeling met een bewegingssensor, is gerelateerd aan de lengte van de bijbehorende sleutel K_{M-VU}, zoals beschreven in CSM_50.

9.2.1.2 *Vervanging van de hoofdsleutel van de bewegingssensor in apparatuur van de tweede generatie*

CSM_113 Elke hoofdsleutel van de bewegingssensor is samen met alle bijbehorende sleutels (zie Tabel 3) gerelateerd aan het ERCA-basissleutelpaar van een specifieke generatie. Bijgevolg worden deze sleutels om de 17 jaar vervangen. De geldigheidsduur van elke generatie hoofdsleutels van bewegingssensoren gaat in één jaar voordat het bijbehorende ERCA-basissleutelpaar van kracht wordt, en eindigt op het ogenblik dat dit ERCA-basissleutelpaar vervalt. Dit wordt verduidelijkt in Figuur 2.

Figuur 2

Afgifte en gebruik van verschillende generaties hoofdsleutels van bewegingssensoren in voertuigunits, bewegingssensoren en werkplaatskaarten



CSM_114 Ten minste één jaar voordat een nieuw Europees basissleutelpaar wordt gegenereerd, zoals beschreven in CSM_56, genereert de ERCA een nieuwe hoofdsleutel van de bewegingssensor K_M door nieuwe sleutels K_{M-VU} en K_{M-WC} aan te maken. Overeenkomstig CSM_50 is de lengte van de hoofdsleutel van de bewegingssensor gerelateerd aan de verwachte cryptografische sterkte van het nieuwe Europese basissleutelpaar. De ERCA deelt de nieuwe sleutels K_M, K_{M-VU} en K_{M-WC} met het bijbehorende versienummer mee aan de MSCA's die daarom verzoeken.

CSM_115 Zoals verduidelijkt in Figuur 2, zorgt de MSCA ervoor dat alle geldige generaties van de sleutels K_{M-WC} samen met de bijbehorende versienummers worden opgeslagen in elke werkplaatskaart die onder haar verantwoordelijkheid wordt afgegeven.

Opmerking: dit betekent dat in het laatste jaar van de geldigheidsduur van een ERCA-certificaat werkplaatskaarten worden afgegeven met sleutels K_{M-WC} van drie verschillende generaties, zoals verduidelijkt in Figuur 2.

CSM_116 Voor de in CSM_107 en CSM_108 hierboven toegelichte procedure geldt het volgende: Elke koppelingssleutel K_P die de MSCA van een fabrikant van bewegingssensoren ontvangt, wordt afzonderlijk gecodeerd voor elke geldige generatie hoofdsleutel van de bewegingssensor K_M. Elk serienummer dat de MSCA van een fabrikant van bewegingssensoren ontvangt, wordt eveneens afzonderlijk gecodeerd voor elke geldige generatie identificatiesleutel K_{ID}. De fabrikant van bewegingssensoren slaat alle gecodeerde koppelingssleutels en serienummers op in de desbetreffende bewegingssensor, samen met de corresponderende ongecodeerde tekstwaarden en het (de) versienummer(s) van de voor de codering gebruikte sleutels K_M en K_{ID}.

Opmerking: dit betekent dat in het laatste jaar van de geldigheidsduur van een ERCA-certificaat bewegingssensoren worden afgegeven met gecodeerde gegevens die berusten op sleutels K_M van drie verschillende generaties, zoals verduidelijkt in Figuur 2.

CSM_117 Voor de in CSM_107 hierboven toegelichte procedure geldt het volgende: Aangezien de lengte van de koppelingssleutel K_P gerelateerd is aan de lengte van de sleutel K_M (zie CSM_100), kan het zijn dat de fabrikant van bewegingssensoren voor een en dezelfde bewegingssensor tot drie verschillende koppelingssleutels (van uiteenlopende lengte) moet genereren in het geval dat de sleutels K_M van opeenvolgende generaties een verschillende lengte hebben. In dit geval verzendt de fabrikant elke koppelingssleutel naar de MSCA. De MSCA zorgt ervoor dat elke koppelingssleutel wordt gecodeerd met de hoofdsleutel van de bewegingssensor van de juiste generatie, dat wil zeggen die welke dezelfde lengte heeft.

Opmerking: indien de fabrikant van bewegingssensoren ervoor kiest een op TDES gebaseerde koppelingssleutel te gebruiken voor een bewegingssensor van de tweede generatie (zie CSM_111), meldt hij de MSCA dat deze koppelingssleutel moet worden gecodeerd met de op TDES gebaseerde hoofdsleutel van de bewegingssensor. Een TDES-sleutel kan immers dezelfde lengte hebben als een AES-sleutel, zodat de MSCA niet alleen op de sleutellengte kan afgaan.

CSM_118 VU-fabrikanten brengen in elke voertuigunit de sleutel K_{M-VU} van een enkele generatie in, samen met het bijbehorende versienummer. De sleutel K_{M-VU} van deze generatie is gerelateerd aan het ERCA-certificaat waarop de VU-certificaten gebaseerd zijn.

Opmerkingen:

— Een voertuigunit die berust op een ERCA-certificaat van generatie *X*, bevat alleen de sleutel K_{M-VU} van de generatie *X*, zelfs indien deze wordt verstrekt nadat de geldigheidsduur van het ERCA-certificaat van de generatie *X + 1* is ingegaan. Dit wordt verduidelijkt in Figuur 2.

— Een VU van generatie *X* kan niet worden gekoppeld aan een bewegingssensor van generatie *X-1*.

— Aangezien werkplaatskaarten één jaar geldig zijn, hebben de voorschriften CSM_113 tot en met CSM_118 tot gevolg dat alle werkplaatskaarten de nieuwe sleutel K_{M-WC} bevatten op het ogenblik dat de eerste VU met de nieuwe sleutel K_{M-VU} in gebruik wordt genomen. Bijgevolg kan deze VU altijd de nieuwe sleutel K_M berekenen. Bovendien bevatten de meeste nieuwe bewegingssensoren tegen dan ook gecodeerde gegevens die gebaseerd zijn op de nieuwe sleutel K_M.

9.2.2 *Sleutels ter beveiliging van de DSRC-communicatie*

9.2.2.1 *Algemeen*

CSM_119 De authenticiteit en vertrouwelijkheid van gegevens die via een DSRC-interface voor communicatie op afstand worden overgebracht van een voertuigunit naar een controleautoriteit, worden gewaarborgd door een reeks VU-specifieke AES-sleutels die zijn afgeleid van een enkele DSRC-hoofdsleutel, KM_{DSRC}.

CSM_120 De DSRC-hoofdsleutel KM_{DSRC} is een AES-sleutel die op beveiligde wijze wordt gegenereerd, opgeslagen en verspreid door de ERCA. De sleutellengte bedraagt 128, 192 of 256 bits en is gerelateerd aan de lengte van het Europese basissleutelpaar, zoals beschreven in CSM_50.

CSM_121 De ERCA geeft de DSRC-hoofdsleutel op beveiligde wijze door aan de MSCA's die daarom verzoeken, zodat zij VU-specifieke DSRC-sleutels daarvan kunnen afleiden, alsook om ervoor te zorgen dat de DSRC-hoofdsleutel wordt ingebracht in alle controle- en werkplaatskaarten die onder hun verantwoordelijkheid worden afgegeven.

CSM_122 De ERCA wijst aan elke DSRC-hoofdsleutel een uniek versienummer toe. Op het ogenblik dat de ERCA de DSRC-hoofdsleutel verzendt naar de MSCA's, deelt zij ook het versienummer mee.

Opmerking: het versienummer dient om onderscheid te maken tussen de verschillende generaties van de DSRC-hoofdsleutel, zoals uiteengezet in punt 9.2.2.2.

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`. Voor de codering worden de kenmerkende coderingsregels (DER) toegepast overeenkomstig [ISO 8825-1].

CSM_124 Bij ontvangst van een verzoek om VU-specifieke DSRC-sleutels, leidt de MSCA twee AES-sleutels voor de voertuigunit af, K_VU_{DSRC}_ENC en K_VU_{DSRC}_MAC genoemd. Deze VU-specifieke sleutels hebben dezelfde lengte als de DSRC-hoofdsleutel. De MSCA gebruikt de in [RFC 5869] vastgelegde sleutelafleidingsfunctie (KDF). De hashfunctie die nodig is om de HMAC-hashfunctie te concretiseren, is gerelateerd aan de lengte van de DSRC-hoofdsleutel, zoals uiteengezet in CSM_50. De in [RFC 5869] vastgelegde sleutelafleidingsfunctie (KDF) wordt als volgt gebruikt:

Stap 1 (Extractie):

— *PRK* = HMAC-Hash (*salt, IKM*), waarbij *salt* een lege string ' ' is en *IKM* gelijk is aan KM_{DSRC}.

Stap 2 (Expansie):

— *OKM* = *T(1)*, waarbij

T(1) = HMAC-Hash (*PRK, T(0)* || *info* || '01') met

— *T(0)* = een lege string (' ')

— *info* = VU-serienummer, zoals gespecificeerd in CSM_123

— K_VU_{DSRC}_ENC = eerste *L* bytes van *OKM* en

K_VU_{DSRC}_MAC = laatste *L* bytes van *OKM*

waarbij *L* de vereiste lengte is van K_VU_{DSRC}_ENC en K_VU_{DSRC}_MAC in bytes.

CSM_125 De MSCA geeft de sleutels K_VU_{DSRC}_ENC en K_VU_{DSRC}_MAC op beveiligde wijze door aan de VU-fabrikant, zodat die ze kan inbrengen in de voertuigunit waarvoor ze bedoeld zijn.

CSM_126 Bij afgifte zijn de sleutels K_VU_{DSRC}_ENC en K_VU_{DSRC}_MAC opgeslagen in het beveiligde geheugen van de voertuigunit ter waarborging van de integriteit, authenticiteit en vertrouwelijkheid van de gegevens die worden verzonden via de interface voor communicatie op afstand. De voertuigunit slaat ook het versienummer op van de DSRC-hoofdsleutel waarmee deze VU-specifieke sleutels worden afgeleid.

CSM_127 Bij afgifte is de DSRC-hoofdsleutel KM_{DSRC} opgeslagen in het beveiligde geheugen van de controle- en werkplaatskaarten ter verificatie van de integriteit en authenticiteit van de gegevens die de VU via de interface voor communicatie op afstand verzendt, alsook om deze gegevens te decoderen. Ook het versienummer van de DSRC-hoofdsleutel wordt in controle- en werkplaatskaarten opgeslagen.

Opmerking: zoals uiteengezet in punt 9.2.2.2, kan het nodig zijn in een en dezelfde controle- of werkplaatskaart een DSRC-hoofdsleutel KM_{DSRC} van verschillende generaties in te brengen.

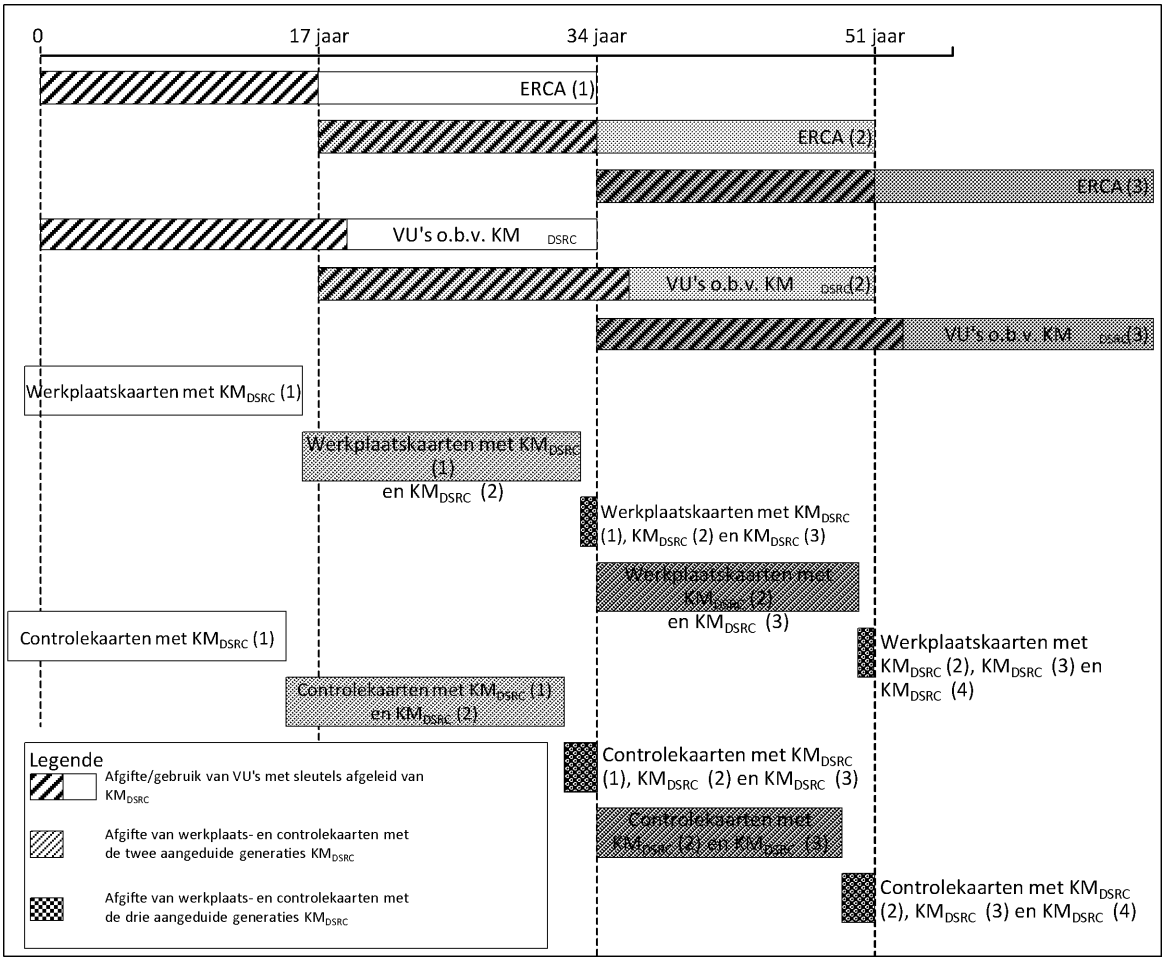
CSM_128 De MSCA houdt registraties bij van alle door haar gegenereerde VU-specifieke DSRC-sleutels, van het bijbehorende versienummer alsook van de identificatie van de VU waarvoor elke sleutelreeks bedoeld is.

9.2.2.2 *Vervanging van de DSRC-hoofdsleutel*

CSM_129 Elke DSRC-hoofdsleutel is verbonden aan het ERCA-basissleutelpaar van een specifieke generatie. Bijgevolg wordt de DSRC-hoofdsleutel om de 17 jaar vervangen door de ERCA. De geldigheidsduur van de DSRC-hoofdsleutel van elke generatie gaat in twee jaar voordat het bijbehorende ERCA-basissleutelpaar van kracht wordt, en eindigt op het ogenblik dat dit ERCA-basissleutelpaar vervalt. Dit wordt verduidelijkt in Figuur 3.

Figuur 3

Afgifte en gebruik van de DSRC-hoofdsleutel van verschillende generaties in voertuigunits, controle- en werkplaatskaarten



CSM_130 Ten minste twee jaar voordat een nieuw Europees basissleutelpaar wordt gegenereerd, zoals beschreven in CSM_56, genereert de ERCA een nieuwe DSRC-hoofdsleutel. Overeenkomstig CSM_50 is de lengte van de DSRC-hoofdsleutel gerelateerd aan de verwachte cryptografische sterkte van het nieuwe Europese basissleutelpaar. De ERCA deelt de nieuwe DSRC-hoofdsleutel met het bijbehorende versienummer mee aan de MSCA's die daarom verzoeken.

CSM_131 Zoals wordt verduidelijkt in Figuur 3, zorgt de MSCA ervoor dat alle geldige generaties van de sleutel KM_{DSRC} samen met de bijbehorende versienummers worden opgeslagen in elke controlekaart die onder haar verantwoordelijkheid wordt afgegeven.

Opmerking: dit betekent dat in de laatste twee jaar van de geldigheidsduur van een ERCA-certificaat controlekaarten worden afgegeven met een sleutel KM_{DSRC} van drie verschillende generaties, zoals aangegeven in Figuur 3.

CSM_132 Zoals verduidelijkt in Figuur 3, zorgt de MSCA ervoor dat alle generaties van de sleutel KM_{DSRC} die ten minste één jaar geldig zijn geweest en nog steeds geldig zijn, samen met de bijbehorende versienummers worden opgeslagen in elke werkplaatskaart die onder haar verantwoordelijkheid wordt afgegeven.

Opmerking: dit betekent dat in het laatste jaar van de geldigheidsduur van een ERCA-certificaat werkplaatskaarten worden afgegeven met een sleutel KM_{DSRC} van drie verschillende generaties, zoals verduidelijkt in Figuur 3.

CSM_133 VU-fabrikanten brengen in elke voertuigunit een enkele reeks VU-specifieke DSRC-sleutels in, samen met het bijbehorende versienummer. Deze sleutelreeks wordt afgeleid van de sleutel KM_{DSRC} van de generatie van het ERCA-certificaat waarop de VU-certificaten gebaseerd zijn.

Opmerkingen:

— een voertuigunit die gebaseerd is op een ERCA-certificaat van generatie *X*, bevat bijgevolg alleen de sleutels K_VU_{DSRC}_ENC en K_VU_{DSRC}_MAC van de generatie *X*, zelfs indien deze wordt verstrekt nadat de geldigheidsduur van het ERCA-certificaat van de generatie *X + 1* is ingegaan. Dit wordt verduidelijkt in Figuur 3.

— Aangezien werkplaatskaarten één jaar en controlekaarten twee jaar geldig zijn, hebben de voorschriften CSM_131 tot en met CSM_133 tot gevolg dat alle werkplaats- en controlekaarten de nieuwe DSRC-hoofdsleutel bevatten op het ogenblik dat de eerste VU met op die hoofdsleutel gebaseerde VU-specifieke sleutels in gebruik wordt genomen.

9.3. **Certificaten**

9.3.1 *Algemeen*

CSM_134 Alle certificaten in het Europese slimme tachograafsysteem zijn zelfbeschrijvend en kaartverifieerbaar overeenkomstig [ISO 7816-4] en [ISO 7816-8].

CSM_135 De kenmerkende coderingsregels (DER) overeenkomstig [ISO 8825-1] worden toegepast om de ASN.1-gegevensstructuren en (toepassingsspecifieke) gegevensobjecten in certificaten te coderen.

Opmerking: door deze codering wordt de waarde van de labellengte (TLV) als volgt gestructureerd:

Label: het label wordt ingevoerd in 1 of 2 bytes en geeft de inhoud aan.

Lengte: de lengte wordt ingevoerd als niet-getekend geheel getal in 1, 2 of 3 bytes, wat een maximumlengte van 65 535 bytes geeft. Er worden zo weinig mogelijk bytes gebruikt.

Waarde: de waarde wordt ingevoerd in nul of meer bytes.

9.3.2 *Inhoud van het certificaat*

CSM_136 Alle certificaten zijn opgebouwd volgens de in Tabel 4 aangegeven structuur van het certificaatprofiel.

Tabel 4

Certificaatprofiel versie 1

Veld	Veld-ID	Label	Lengte (bytes)	ASN.1-gegevenstype (zie aanhangsel 1)
ECC-certificaat	C	'7F 21'	var	
ECC-certificeringsinstantie	B	'7F 4E'	var	

Veld	Veld-ID	Label	Lengte (bytes)	ASN.1-gegevenstype (zie aanhangsel 1)
Identificator van het certificaatprofiel	CPI	'5F 29'	'01'	`INTEGER(0..255)`
Referentie van de certificeringsautoriteit	CAR	'42'	'08'	`KeyIdentifier`
Autorisatie van de certificaathouder	CHA	'5F 4C'	'07'	`CertificateHolder Authorisation`
Openbare sleutel	PK	'7F 49'	var	
Domeinparameters	DP	'06'	var	`OBJECT IDENTIFIER`
Openbaar punt	PP	'86'	var	`OCTET STRING`
Referentie van de certificaathouder	CHR	'5F 20'	'08'	`KeyIdentifier`
Ingangsdatum van het certificaat	CEfD	'5F 25'	'04'	`TimeReal`
Vervaldatum van het certificaat	CExD	'5F 24'	'04'	`TimeReal`
Handtekening van het ECC-certificaat	S	'5F 37'	var	`OCTET STRING`

Opmerking: verderop in dit aanhangsel wordt de veld-ID gebruikt om te verwijzen naar afzonderlijke velden van een certificaat; zo is X.CAR bijvoorbeeld de referentie van de certificeringsautoriteit (CAR) die vermeld staat in het certificaat van gebruiker X.

9.3.2.1 Identificator van het certificaatprofiel (CPI)

CSM_137 Deze identificator geeft aan welk certificaatprofiel wordt gebruikt. Versie 1, zoals gespecificeerd in Tabel 4, wordt geïdentificeerd door de waarde '00'.

9.3.2.2 Referentie van de certificeringsautoriteit (CAR)

CSM_138 Deze referentie bepaalt welke openbare sleutel wordt gebruikt ter verificatie van de handtekening van het certificaat. De referentie van de certificeringsautoriteit is bijgevolg gelijk aan de referentie van de certificaathouder in het certificaat van de betrokken certificeringsautoriteit.

CSM_139 Het ERCA-basiscertificaat is zelfondertekend, wat betekent dat de referentie van de certificeringsautoriteit gelijk is aan de referentie van de certificaathouder in het certificaat.

CSM_140 Voor een ERCA-verbindingscertificaat is de referentie van de certificaathouder (CHR) gelijk aan die van het nieuwe ERCA-basiscertificaat. Voor een verbindingscertificaat is de referentie van de certificeringsautoriteit gelijk aan de CHR van het vorige ERCA-basiscertificaat.

9.3.2.3 Autorisatie van de certificaathouder (CHA)

CSM_141 De autorisatie van de certificaathouder dient om het certificaattype te identificeren. De CHA bestaat uit de zes meest significante bytes van de toepassingsidentificator (AID) van de tachograaf, samengevoegd met het model van de apparatuur waarvoor het certificaat bedoeld is.

9.3.2.4 Openbare sleutel (PK)

De openbare sleutel bevat twee gegevenselementen: de gestandaardiseerde domeinparameters (DP) die men moet gebruiken met de openbare sleutel van het certificaat, en de waarde van het openbare punt (PP).

CSM_142 Het gegevenselement „DP" bevat een van de in Tabel 1 gespecificeerde objectidentificatoren als verwijzing naar een reeks gestandaardiseerde domeinparameters.

CSM_143 Het gegevenselement „PP" bevat het openbare punt. Zoals gespecificeerd in [TR-03111], worden openbare punten op elliptische krommen omgezet in bytereeksen (octet strings). Het niet-gecomprimeerde coderingsformaat wordt gebruikt. Om een punt van de elliptische kromme te herstellen uit het gecodeerde formaat, worden altijd de in [TR-03111] omschreven validaties uitgevoerd.

9.3.2.5 Referentie van de certificaathouder (CHR)

CSM_144 Dit is een identificator van de openbare sleutel in het certificaat. De CHR dient om in andere certificaten naar deze openbare sleutel te verwijzen.

CSM_145 Voor certificaten van tachograafkaarten en externe GNSS-modules heeft de referentie van de certificaathouder het in aanhangsel 1 gespecificeerde gegevenstype `ExtendedSerialNumber`.

CSM_146 In het geval van een certificaataanvraag voor voertuigunits is het mogelijk dat de fabrikant het fabrikantspecifieke serienummer van de VU waarvoor dit certificaat en de bijbehorende particuliere sleutel bedoeld zijn, soms wel en soms niet kent. In het eerste geval heeft de referentie van de certificaathouder het in aanhangsel 1 gespecificeerde gegevenstype `ExtendedSerialNumber`. In het tweede geval heeft de referentie van de certificaathouder het in aanhangsel 1 gespecificeerde gegevenstype `CertificateRequestID`.

CSM_147 Voor de ERCA- en MSCA-certificaten heeft de referentie van de certificaathouder het in aanhangsel 1 gespecificeerde gegevenstype `CertificationAuthorityKID`.

9.3.2.6 Ingangsdatum van het certificaat (CEfD)

CSM_148 Dit veld bevat de begindatum en -tijd van de geldigheidsduur van het certificaat. De ingangsdatum van het certificaat is de datum waarop het certificaat is gegenereerd.

9.3.2.7 Vervaldatum van het certificaat (CExD)

CSM_149 Dit veld bevat de einddatum en -tijd van de geldigheidsduur van het certificaat.

9.3.2.8 Handtekening van het certificaat (S)

CSM_150 De handtekening van het certificaat wordt in *overlay* geplaatst op het inhoudelijk gecodeerde deel van het certificaat, en bevat het label en de lengte daarvan. Het ondertekeningsalgoritme is ECDSA, zoals gespecificeerd in [DSS]. Daarbij wordt het hashalgoritme toegepast dat gerelateerd is aan het sleutelgrootte van de ondertekeningsautoriteit, zoals gespecificeerd in CSM_50. Het handtekeningformaat is ongecodeerd, zoals gespecificeerd in [TR-03111].

9.3.3 *Certificaataanvragen*

CSM_151 De certificaataanvrager verzendt de volgende gegevens naar de certificeringsautoriteit:

— de identificator van het certificaatprofiel (CPI) voor het gewenste certificaat;

— de referentie van de certificeringsautoriteit (CAR) waarmee het certificaat naar verwachting wordt ondertekend;

— de te ondertekenen openbare sleutel (PK).

CSM_152 Naast de in CSM_151 vermelde gegevens stuurt de MSCA in een certificaataanvraag de volgende gegevens naar de ERCA zodat die de referentie van de certificaathouder van het nieuwe MSCA-certificaat kan aanmaken:

— de numerieke nationale code van de certificeringsautoriteit (gegevenstype `NationNumeric`, zoals vastgelegd in aanhangsel 1);

— de alfanumerieke nationale code van de certificeringsautoriteit (gegevenstype `NationAlpha`, zoals vastgelegd in aanhangsel 1);

— het serienummer van 1 byte om de verschillende sleutels van de certificeringsautoriteit te onderscheiden in het geval dat sleutels worden gewijzigd;

— het veld van 2 bytes met aanvullende codering (specifiek voor de certificeringsautoriteit).

CSM_153 Naast de in CSM_151 vermelde gegevens verzendt de apparatuurfabrikant in een certificaat-aanvraag de volgende gegevens naar de MSCA zodat die de referentie van de certificaathouder van het nieuwe apparatuurcertificaat kan aanmaken:

— de fabrikantspecifieke identificator van het model van de apparatuur;

— 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.

CSM_154 In het geval van een certificaataanvraag voor een VU is het mogelijk dat de fabrikant het fabrikant-specifieke serienummer van de VU waarvoor dit certificaat en de bijbehorende particuliere sleutel bedoeld zijn, soms wel en soms niet kent. In het eerste geval verzendt de VU-fabrikant het serienummer naar de MSCA. In het tweede geval moet de fabrikant elke certificaataanvraag eenduidig identificeren en het serienummer daarvan verzenden naar de MSCA. Het resulterende certificaat bevat dan het serienummer van de certificaataanvraag. Na het inbrengen van het certificaat in een specifieke VU brengt de fabrikant de MSCA op de hoogte van de link tussen het serienummer van de certificaataanvraag en de VU-identificatie.

10. WEDERZIJDSE AUTHENTICATIE TUSSEN VU EN KAART, EN BEVEILIGDE BERICHTENUITWISSELING

10.1. **Algemeen**

CSM_155 De beveiligde communicatie op hoog niveau tussen een voertuigunit en tachograaf verloopt in de volgende stappen:

— Stap 1: elke partij bewijst aan de andere partij in het bezit te zijn van een geldig openbare-sleutelcertificaat dat is ondertekend door de certificeringsautoriteit van de lidstaat (MSCA). Het openbare-sleutelcertificaat van de MSCA moet op zijn beurt zijn ondertekend door de Europese basiscertificeringsautoriteit (ERCA). Deze stap wordt verificatie van de certificaatketen genoemd en wordt uitvoerig toegelicht in punt 10.2.

— Stap 2: de voertuigunit (VU) bewijst aan de kaart in het bezit te zijn van de particuliere sleutel die overeenstemt met de openbare sleutel in het aangeboden certificaat. Het bewijs wordt geleverd door ondertekening met een willekeurig, door de kaart verzonden nummer. De kaart moet dit nummer bij de verificatie van de handtekening terugvinden. Bij een succesvolle verificatie wordt de VU geauthenticeerd. Deze stap wordt VU-authenticatie genoemd en wordt uitvoerig toegelicht in punt 10.3.

— Stap 3: beide partijen berekenen zelfstandig twee AES-sessiesleutels met behulp van een asymmetrisch algoritme voor sleutelovereenstemming. Met een van beide sessiesleutels maakt de kaart een berichtauthenticatiecode (MAC) aan voor sommige door de VU verzonden gegevens. De VU verifieert de MAC. Bij een succesvolle verificatie wordt de kaart geauthenticeerd. Deze stap wordt kaartauthenticatie genoemd en wordt uitvoerig toegelicht in punt 10.4.

— Stap 4: de VU en de kaart gebruiken de overeengekomen sessiesleutels om de vertrouwelijkheid, integriteit en authenticiteit van alle uitgewisselde berichten te waarborgen. Deze stap wordt beveiligde berichtenuitwisseling (SM) genoemd en wordt uitvoerig toegelicht in punt 10.5.

CSM_156 Het in CSM_155 beschreven mechanisme wordt door de VU gestart bij kaartinbrenging in een van de lezers.

10.2. **Wederzijdse verificatie van de certificaatketen**

10.2.1 *Verificatie van de certificaatketen op kaartniveau door de VU*

CSM_157 Voertuigunits verifiëren de certificaatketen van een tachograafkaart volgens het stroomschema in Figuur 4.

Toelichtingen bij Figuur 4:

— De kaartcertificaten en openbare sleutels in deze figuur dienen voor de wederzijdse authenticatie. In punt 9.1.5 worden deze aangeduid als Card_MA.

— De openbare sleutels en certificaten Card.CA in deze figuur dienen om kaartcertificaten te ondertekenen en worden aangegeven in de CAR van het kaartcertificaat. In punt 9.1.3 worden deze aangeduid als MSCA_Card.

— Het certificaat Card.CA.EUR in deze figuur is het Europese basiscertificaat dat vermeld staat in de referentie van de certificeringsautoriteit (CAR) van het certificaat Card.CA.

— Het certificaat Card.Link in deze figuur is het verbindingscertificaat van de kaart (indien aanwezig). Zoals verduidelijkt in punt 9.1.2, is dit een verbindingscertificaat voor een nieuw Europees basissleutelpaar dat door de ERCA is aangemaakt en dat met de vorige Europese particuliere sleutel is ondertekend.

— Het certificaat Card.Link.EUR is het Europese basiscertificaat dat vermeld staat in de referentie van de certificeringsautoriteit (CAR) van het certificaat Card.Link.

CSM_158 Zoals blijkt uit Figuur 4, begint de verificatie van de certificaatketen op kaartniveau bij kaartinbrenging. De VU leest de referentie van de kaarthouder (`cardExtendedSerialNumber`) in het hoofdbestand van de chipkaart (EF ICC). De VU controleert of de kaart bekend is, met andere woorden of de certificaatketen van de kaart in het verleden met succes is geverifieerd en voor toekomstig gebruik werd opgeslagen. Indien dat het geval is en het kaartcertificaat nog geldig is, wordt de procedure voortgezet met de verificatie van de certificaatketen op VU-niveau. Zo niet, leest de VU achtereenvolgens op de kaart het certificaat MSCA_Card ter verificatie van het kaartcertificaat, het Card.CA.EUR-certificaat ter verificatie van het certificaat MSCA_Card, en in voorkomend geval het verbindingscertificaat, totdat een bekend of verifieerbaar certificaat wordt gevonden. Indien een bekend certificaat wordt gevonden, gebruikt de VU dit ter verificatie van de onderliggende kaartcertificaten die op de kaart werden gelezen. Bij een succesvolle verificatie wordt de procedure voortgezet met de verificatie van de certificaatketen op VU-niveau. Zo niet, wordt de kaart genegeerd door de VU.

Opmerking: de VU kan het certificaat Card.CA.EUR op drie manieren kennen:

— het certificaat Card.CA.EUR is hetzelfde certificaat als het EUR-certificaat van de VU zelf;

— het certificaat Card.CA.EUR gaat het EUR-certificaat van de VU zelf vooraf en is bij afgifte al in de VU opgeslagen (zie CSM_81);

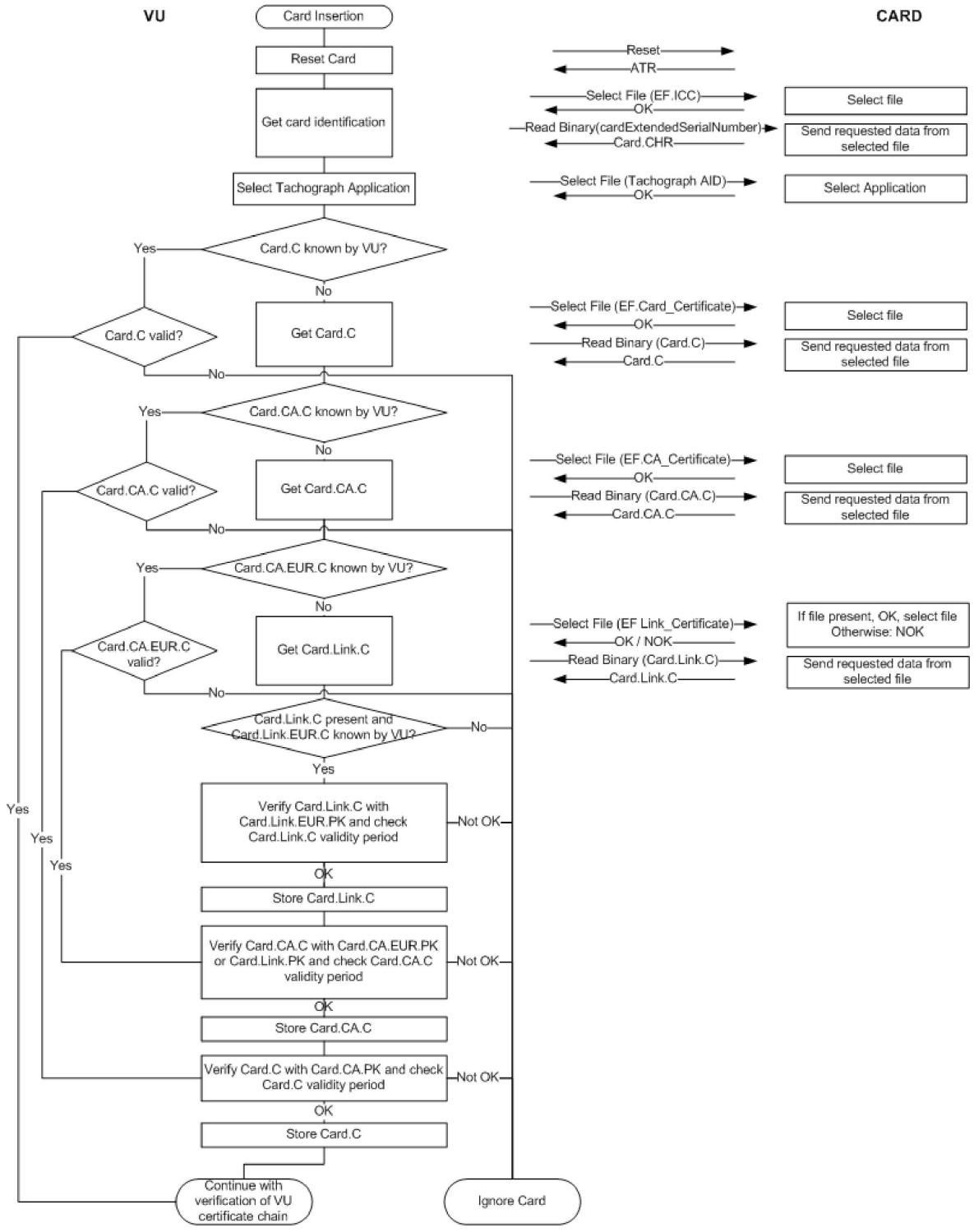
— het certificaat Card.CA.EUR volgt op het EUR-certificaat van de VU zelf en de VU heeft in het verleden een verbindingscertificaat van een andere tachograafkaart ontvangen, geverifieerd en voor toekomstig gebruik opgeslagen.

CSM_159 Zoals aangegeven in Figuur 4, kan de VU na verificatie van de authenticiteit en geldigheid van een tot dan toe niet bekend certificaat, dit certificaat voor toekomstig gebruik opslaan. Op die manier hoeft de VU de authenticiteit van dit certificaat niet opnieuw te verifiëren wanneer het nogmaals wordt aangeboden. Zoals gespecificeerd in punt 9.3.2, kan de VU in plaats van het volledige certificaat alleen het inhoudelijk deel van het certificaat opslaan.

CSM_160 De VU verifieert de temporele geldigheid van elk certificaat dat op de kaart wordt gelezen of dat in het VU-geheugen is opgeslagen. Vervallen certificaten worden verworpen. Om de temporele geldigheid van een door de kaart aangeboden certificaat te verifiëren, gebruikt de VU zijn interne klok.

Figuur 4

Stroomschema ter verificatie van de certificaatketen op kaartniveau door de VU

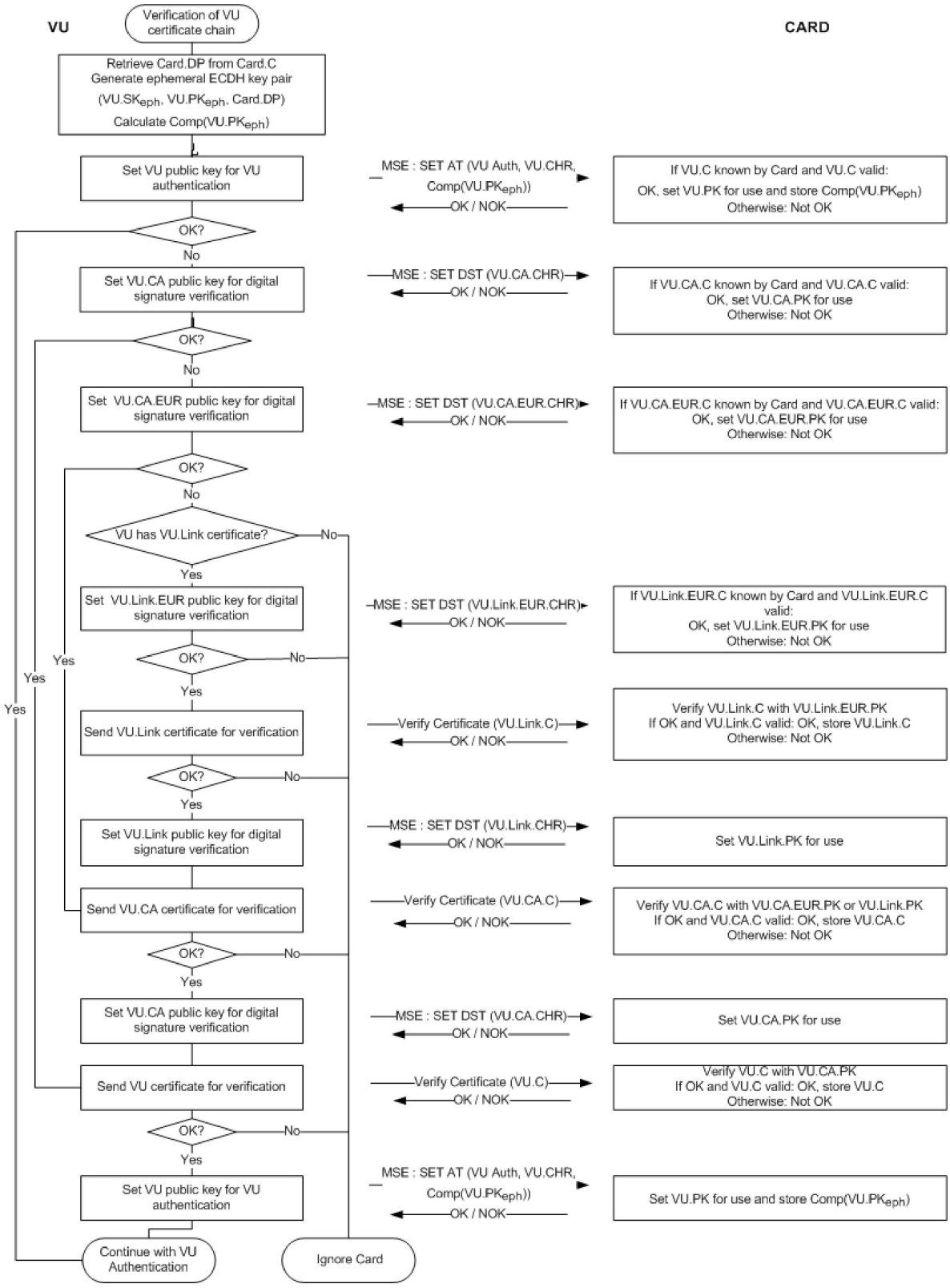


10.2.2 *Verificatie van de certificaatketen op VU-niveau door de kaart*

CSM_161 Tachograafkaarten verifiëren de certificaatketen van een voertuigunit (VU) volgens het stroomschema in Figuur 5.

Figuur 5

Stroomschema ter verificatie van de certificaatketen op VU-niveau door de kaart



Toelichtingen bij Figuur 5:

— De VU-certificaten en openbare sleutels in deze figuur dienen voor de wederzijdse authenticatie. In punt 9.1.4 worden deze aangeduid als VU_MA.

— De openbare sleutels en certificaten VU.CA in deze figuur dienen om certificaten van voertuigunits en externe GNSS-modules te ondertekenen. In punt 9.1.3 worden deze aangeduid als MSCA_VU-EGF.

— Het certificaat VU.CA.EUR in deze figuur is het Europese basiscertificaat dat vermeld staat in de referentie van de certificeringsautoriteit (CAR) van het certificaat VU.CA.

— Het certificaat VU.Link in deze figuur is het verbindingscertificaat van de VU (indien aanwezig). Zoals verduidelijkt in punt 9.1.2, is dit een verbindingscertificaat voor een nieuw Europees basissleutelpaar dat door de ERCA is aangemaakt en dat met de vorige Europese particuliere sleutel is ondertekend.

— Het certificaat VU.Link.EUR is het Europese basiscertificaat dat vermeld staat in de referentie van de certificeringsautoriteit (CAR) van het certificaat VU.Link.

CSM_162 Zoals blijkt uit Figuur 5, begint de verificatie van de certificaatketen van de VU op het ogenblik dat de VU probeert zijn eigen openbare sleutel in te stellen voor gebruik in de tachograafkaart. Als de VU daarin slaagt, betekent dit dat de kaart de certificaatketen van de VU in het verleden met succes heeft geverifieerd en het VU-certificaat voor toekomstig gebruik heeft opgeslagen. In dit geval wordt het VU-certificaat voor gebruik ingesteld en wordt de procedure voortgezet met de VU-authenticatie. Indien de kaart het VU-certificaat niet kent, biedt de VU achtereenvolgens het certificaat VU.CA aan ter verificatie van het VU-certificaat, het EUR-certificaat ter verificatie van het certificaat VU.CA, en in voorkomend geval het verbindingscertificaat ter verificatie van het EUR-certificaat, om een door de kaart gekend certificaat te vinden. Indien een dergelijk certificaat wordt gevonden, gebruikt de kaart dit ter verificatie van de onderliggende VU-certificaten die werden aangeboden. Bij een succesvolle verificatie stelt de VU de openbare sleutel in voor gebruik in de tachograafkaart. Zo niet, wordt de kaart genegeerd door de VU.

Opmerking: de kaart kan het certificaat VU.CA.EUR op drie manieren kennen:

— het certificaat VU.CA.EUR is hetzelfde certificaat als het EUR-certificaat van de kaart zelf;

— het certificaat VU.CA.EUR gaat het EUR-certificaat van de kaart zelf vooraf en is bij afgifte al in de kaart opgeslagen (zie CSM_91);

— het certificaat VU.CA.EUR volgt op het EUR-certificaat van de kaart zelf en de kaart heeft in het verleden een verbindingscertificaat van een andere voertuigunit ontvangen, geverifieerd en voor toekomstig gebruik opgeslagen.

CSM_163 De VU gebruikt het MSE: Set AT-commando om de openbare sleutel in te stellen voor gebruik in de tachograafkaart. Zoals gespecificeerd in aanhangsel 2, geeft dit commando aan welk cryptografisch mechanisme met de ingestelde sleutel wordt gebruikt. Dit mechanisme is, zoals gespecificeerd in CSM_50, de VU-authenticatie met behulp van het ECDSA-algoritme, in combinatie met het hashalgoritme dat gerelateerd is aan de grootte van het sleutelpaar VU_MA van de VU.

CSM_164 Het MSE: Set AT-commando geeft ook aan welk tijdelijk sleutelpaar de VU gebruikt voor de sleutelovereenstemming tijdens de sessie (zie punt 10.4). Bijgevolg genereert de VU een tijdelijk ECC-sleutelpaar alvorens het MSE:Set AT-commando te verzenden. Om het tijdelijke sleutelpaar te genereren, gebruikt de VU de gestandaardiseerde domeinparameters die in het kaartcertificaat vermeld staan. Het tijdelijke sleutelpaar wordt aangeduid als ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). De VU neemt de x-coördinaat van het met het ECDH-algoritme bepaalde tijdelijke openbare punt als sleutelidentificatie. Dit is de gecomprimeerde voorstelling van de openbare sleutel, aangeduid als $Comp(VU.PK_{eph})$.

CSM_165 Indien 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 $Comp(VU.PK_{eph})$ 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 $Comp(VU.PK_{eph})$ op.

CSM_166 De kaart verifieert de temporele geldigheid van elk certificaat dat door de VU wordt aangeboden of waarnaar de VU verwijst in het kaartgeheugen. Vervallen certificaten worden verworpen.

CSM_167 Om de temporele geldigheid van een door de VU aangeboden certificaat te verifiëren, slaat elke tachograafkaart bepaalde gegevens met betrekking tot de huidige tijd (hierna „lopende tijd") intern op. Deze gegevens kunnen niet rechtstreeks door een VU worden geactualiseerd. Bij afgifte wordt de lopende tijd van de kaart ingesteld op de ingangsdatum van het certificaat Card_MA van de kaart. De kaart actualiseert de lopende tijd indien de ingangsdatum van een authentiek certificaat dat door de VU als „geldige tijdbron" wordt aangeboden, recenter is dan de tijdaanduiding van de kaart. In dit geval stelt de kaart de lopende tijd in op basis van de ingangsdatum van dat certificaat. De kaart accepteert uitsluitend de volgende certificaten als geldige tijdbron:

— ERCA-verbindingscertificaten van de tweede generatie;

— MSCA-certificaten van de tweede generatie;

— VU-certificaten van de tweede generatie die zijn afgegeven door dezelfde lidstaat als het (de) kaartcertifica(a)t(en) zelf.

Opmerking: het laatste voorschrift houdt in dat de referentie van de certificeringsautoriteit (CAR) van het VU-certificaat, dat wil zeggen het certificaat MSCA_VU-EGF, herkenbaar is voor de kaart. Deze referentie verschilt van de CAR van het kaartcertificaat zelf, namelijk het certificaat MSCA_Card.

CSM_168 Zoals aangegeven in Figuur 5, kan de kaart na verificatie van de authenticiteit en geldigheid van een tot dan toe niet bekend certificaat, dit certificaat voor toekomstig gebruik opslaan. Op die manier hoeft de kaart de authenticiteit van dit certificaat niet opnieuw te verifiëren wanneer het nogmaals wordt aangeboden. Zoals uiteengezet in punt 9.3.2, kan de kaart in plaats van het volledige certificaat alleen het inhoudelijk deel van het certificaat opslaan.

10.3. **VU-authenticatie**

CSM_169 Voertuigunits en kaarten gaan te werk volgens het stroomschema in Figuur 6 om de VU te authenticeren bij de kaart. Door de VU te authenticeren, kan de tachograafkaart zeker stellen dat de VU authentiek is. Daartoe gebruikt de VU zijn particuliere sleutel om een door de kaart afgegeven identiteit („challenge") te ondertekenen.

CSM_170 Naast de door de kaart afgegeven identiteit vermeldt de VU in de handtekening de in het kaartcertificaat vermelde referentie van de kaarthouder.

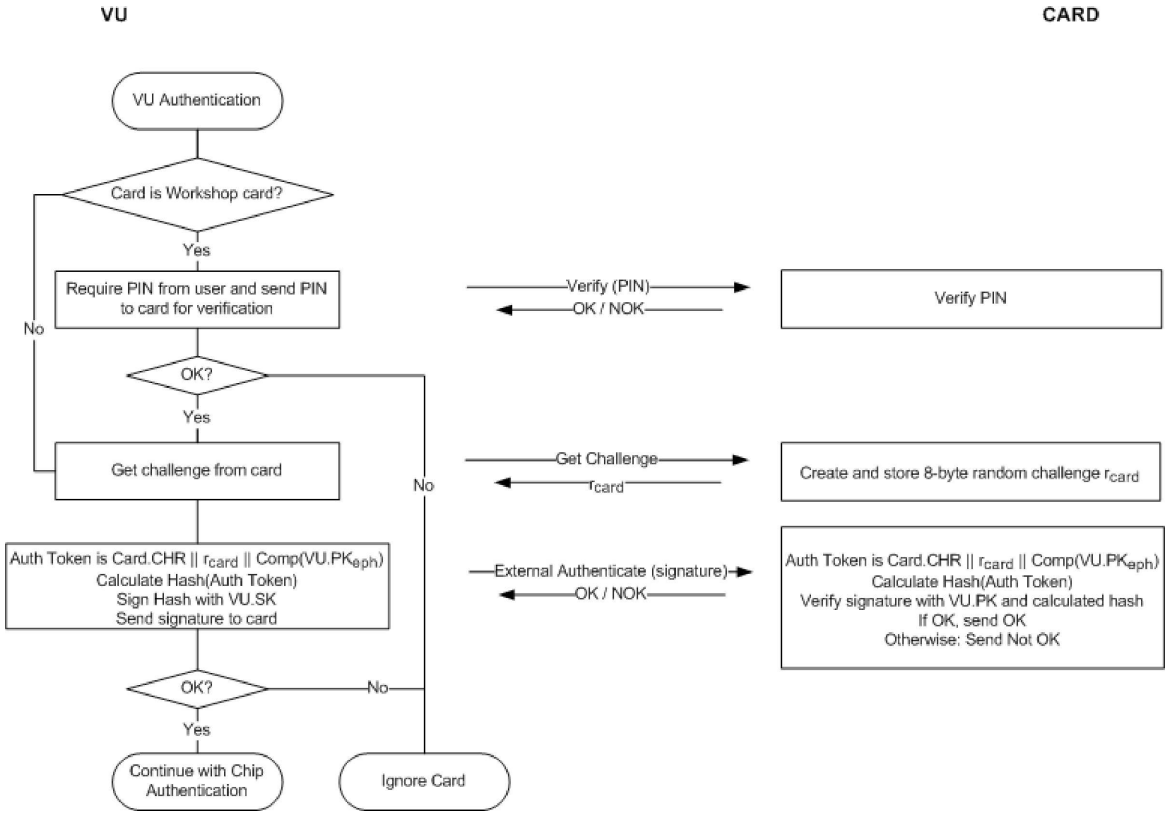
Opmerking: hiermee wordt gewaarborgd dat de kaart waarbij de VU zich authenticeert dezelfde kaart is waarvan de certificaatketen eerder door de VU werd geverifieerd.

CSM_171 De VU vermeldt in de handtekening ook de identificator van de tijdelijke openbare sleutel Comp ($VU.PK_{eph}$), waarmee de VU de beveiligde berichtenuitwisseling (SM) tot stand brengt tijdens de in punt 10.4 uiteengezette procedure voor chipauthenticatie.

Opmerking: hiermee wordt gewaarborgd dat de VU waarmee de kaart tijdens een SM-sessie communiceert dezelfde VU is die eerder door de kaart werd geauthenticeerd.

Figuur 6

Stroomschema van de VU-authenticatie



CSM_172 Indien de VU tijdens de VU-authenticatie meerdere GET CHALLENGE-commando's verzendt, zendt de kaart telkens een nieuwe aselecte identiteit („challenge") van 8 bytes terug, terwijl alleen de laatste identiteit wordt opgeslagen.

CSM_173 Voor de VU-authenticatie gebruikt de VU het ondertekeningsalgoritme ECDSA, zoals gespecificeerd in [DSS]. Daarbij wordt het hashalgoritme toegepast dat gerelateerd is aan het grootte van het sleutelpaar VU_MA van de VU, zoals gespecificeerd in CSM_50. Het handtekeningformaat is ongecodeerd, zoals gespecificeerd in [TR-03111]. De VU verzendt de resulterende handtekening naar de kaart.

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 r_{card} en de identificator van de tijdelijke openbare sleutel van de VU Comp ($VU.PK_{eph}$);

— berekent de kaart de hashwaarde voor het authenticatietoken met behulp van het hashalgoritme dat gerelateerd is aan de grootte van het sleutelpaar VU_MA van de VU, zoals gespecificeerd in CSM_50,

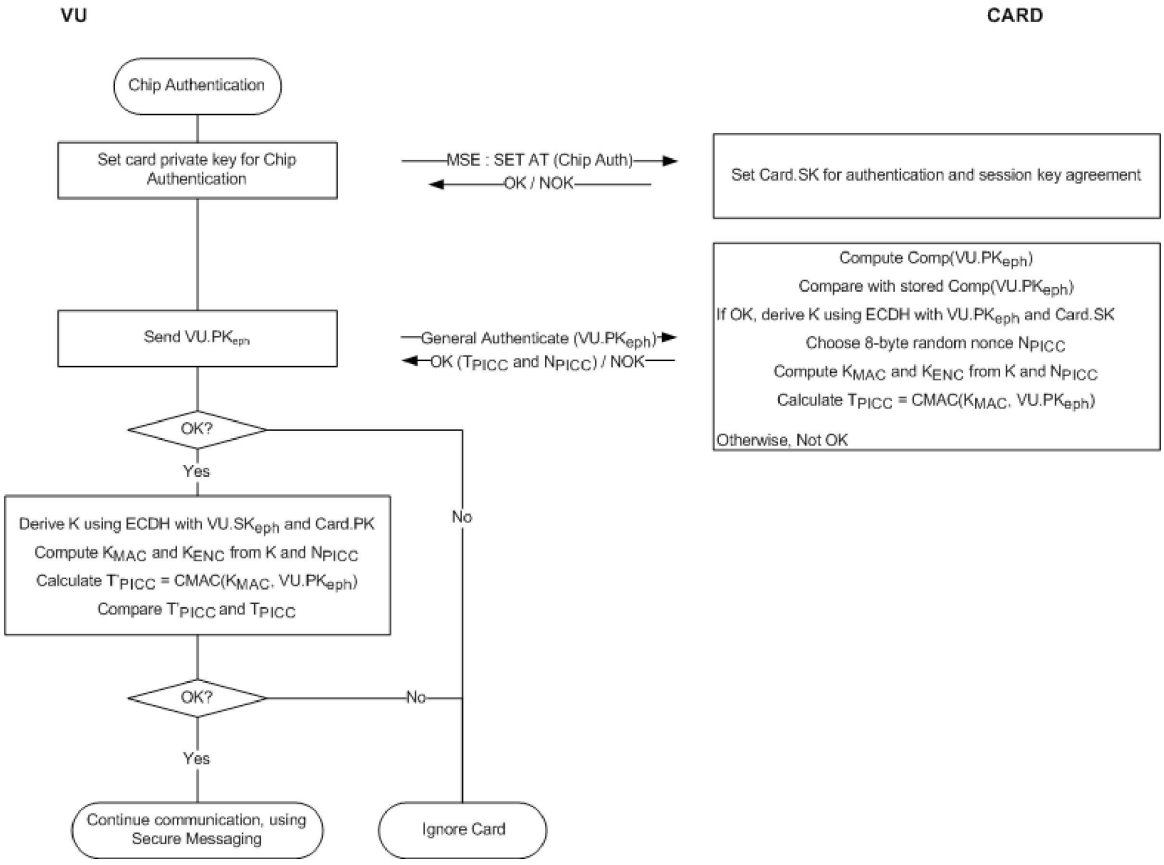
— verifieert de kaart de handtekening van de VU met behulp van het ECDSA-algoritme, in combinatie met de sleutel VU.PK en de berekende hashwaarde.

10.4. Chipauthenticatie en sleutelovereenstemming tijdens de sessie

CSM_175 Voertuigunits en kaarten gaan te werk volgens het stroomschema in **Figuur 7** om de kaart te authenticeren bij de VU. Door de chipkaart te authenticeren, kan de voertuigunit zeker stellen dat de kaart authentiek is.

Figuur 7

Chipauthenticatie en sleutelovereenstemming tijdens de sessie



CSM_176 De voertuigunit (VU) en de kaart voeren de volgende stappen uit:

1. De VU start de procedure voor chipauthenticatie door het MSE: Set AT-commando te verzenden ter aankondiging van de 'chipauthenticatie met behulp van het ECDH-algoritme, met als resultaat een AES-sessiesleutel waarvan de lengte gerelateerd is aan de grootte van het sleutelpaar Card_MA van de kaart, zoals gespecificeerd in CSM_50'. De VU bepaalt op basis van het kaartcertificaat de grootte van het sleutelpaar van de kaart.

2. De VU verzendt het openbare punt $VU.PK_{eph}$ van zijn tijdelijke sleutelpaar naar de kaart. Zoals uiteengezet in CSM_164, heeft de VU dit tijdelijkere sleutelpaar gegenereerd alvorens de certificaatketen op VU-niveau te verifiëren. De VU verzendt de identificator van de tijdelijke openbare sleutel $Comp(VU.PK_{eph})$ naar de kaart, en de kaart slaat deze op.

3. De kaart berekent $Comp(VU.PK_{eph})$ op basis van $VU.PK_{eph}$ en vergelijkt het resultaat met de opgeslagen waarde van $Comp(VU.PK_{eph})$.

4. Met behulp van het ECDH-algoritme, gecombineerd met de statische particuliere sleutel van de kaart en de tijdelijke openbare sleutel van de VU, berekent de kaart een geheime sleutel K.

5. De kaart kiest een *nonce* (willekeurig getal) van 8 bytes N_{PICC} om twee AES-sessiesleutels K_{MAC} en K_{ENC} af te leiden van de geheime sleutel K (zie CSM_179).

6. Met behulp van K_{MAC} berekent de kaart een authenticatietoken voor de identificator van de tijdelijke openbare sleutel van de VU: $T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})$. De kaart verzendt N_{PICC} en T_{PICC} naar de voertuigunit.

7. Met behulp van het ECDH-algoritme, gecombineerd met de statische openbare sleutel van de kaart en de tijdelijke particuliere sleutel van de VU, berekent de VU dezelfde geheime sleutel K als de kaart al eerder heeft gedaan in stap 4.

8. De VU leidt de sessiesleutels K_{MAC} en K_{ENC} af van K en N_{PICC} (zie CSM_179).

9. De VU verifieert het authenticatietoken T_{PICC}.

CSM_177 In stap 3 hierboven berekent de kaart Comp(VU.PKeph) als x-coördinaat van het openbare punt in VU.PKeph.

CSM_178 In stappen 4 en 7 hierboven passen de kaart en de voertuigunit het ECKA-EG-algoritme toe, zoals vastgelegd in [TR-03111].

CSM_179 In stappen 5 en 8 hierboven passen de kaart en de voertuigunit de sleutelafleidingsfunctie (KDF) voor de in [TR-03111] vastgelegde AES-sessiesleutels toe, met de volgende preciseringen en aanpassingen:

— De teller heeft de waarde '00 00 00 01' voor K_{ENC} en '00 00 00 02' voor K_{MAC}.

— De facultatieve nonce *r* wordt gebruikt en is gelijk aan N_{PICC}.

— Om de 128-bits AES-sleutels af te leiden, wordt het hashalgoritme SHA-256 gebruikt.

— Om de 192-bits AES-sleutels af te leiden, wordt het hashalgoritme SHA-384 gebruikt.

— Om de 256-bits AES-sleutels af te leiden, wordt het hashalgoritme SHA-512 gebruikt.

De lengte van de sessiesleutels (dat wil zeggen de lengte vanaf welke de hashwaarde wordt afgekapt) is gerelateerd aan de grootte van het sleutelpaar Card_MA, zoals gespecificeerd in CSM_50.

CSM_180 In stappen 6 en 9 hierboven passen de kaart en de voertuigunit het AES-algoritme toe in CMAC (*Cipher-based Message Authentication Code*)-modus, zoals gespecificeerd in [SP 800-38B]. De lengte van T_{PICC} is gerelateerd aan de lengte van de AES-sessiesleutels, zoals gespecificeerd in CSM_50.

10.5. **Beveiligde berichtenuitwisseling**

10.5.1 *Algemeen*

CSM_181 Nadat de chip met succes is geauthenticeerd, worden alle commando's en antwoorden die de voertuigunit en tachograafkaart met elkaar uitwisselen beschermd door beveiligde berichtenuitwisseling (SM) tot op het ogenblik dat de sessie wordt beëindigd.

CSM_182 Tenzij wanneer gegevens worden gelezen in een bestand met toegangsconditie SM-R-ENC-MAC-G2 (zie aanhangsel 2, hoofdstuk 4), vindt de beveiligde berichtenuitwisseling plaats in alleen-authenticeren-modus. In deze modus wordt aan alle commando's en antwoorden een cryptografische controlesom (ook berichtauthenticatiecode of MAC genoemd) toegevoegd om de authenticiteit en integriteit te waarborgen.

CSM_183 Bij het lezen van gegevens in een bestand met toegangsconditie SM-R-ENC-MAC-G2, wordt de beveiligde berichtenuitwisseling gebruikt in eerst-coderen-dan-authenticeren-modus. Dit betekent dat de antwoordgegevens eerst worden gecodeerd om de vertrouwelijkheid van het bericht te waarborgen en dat daarna een MAC voor de geformatteerde gecodeerde gegevens wordt berekend om de authenticiteit en integriteit te waarborgen.

CSM_184 De beveiligde berichtenuitwisseling gebruikt het AES-algoritme, zoals vastgelegd in [AES], met de sessiesleutels K_{MAC} en K_{ENC} die werden overeengekomen tijdens de chipauthenticatie.

CSM_185 Een niet-getekend geheel getal wordt gebruikt als zendsequentieteller (SSC) om replay-aanvallen tegen te gaan. De grootte van de SSC is gelijk aan de AES-blokgrootte, namelijk 128 bits. De SSC heeft het formaat „MSB-first" (meest significante bits eerst). Bij het starten van de beveiligde berichtenuitwisseling wordt de zendsequentieteller geïnitialiseerd op nul (dat wil zeggen '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00'). Voordat een APDU-commando of -antwoord wordt gegenereerd, wordt de SSC telkens met 1 verhoogd. Aangezien de SSC aan het begin van een SM-sessie op '0' staat, is de waarde van de SSC in het eerste commando gelijk aan '1'. Voor het eerste antwoord is de waarde van de SSC gelijk aan '2'.

CSM_186 Om het bericht te coderen, wordt K_{ENC} gebruikt met het AES-algoritme in de CBC(Cipher Block Chaining)-werkingsmodus, zoals vastgelegd in [ISO 10116], met een interleave-parameter m = 1 en een initialisatievector IV = E(K_{ENC}, SSC), dat wil zeggen de huidige waarde van de zendsequentieteller (SCC), gecodeerd met K_{ENC}.

CSM_187 Om het bericht te authenticeren, wordt K_{MAC} gebruikt met het AES-algoritme in CMAC-modus, zoals gespecificeerd in [SP 800-38B]. De lengte van de berichtauthenticatiecode (MAC) is gerelateerd aan de lengte van de AES-sessiesleutels, zoals gespecificeerd in CSM_50. De zendsequentieteller wordt in de MAC opgenomen door die te laten voorafgaan aan het te authenticeren datagram.

10.5.2 *Structuur van het beveiligde bericht*

CSM_188 De beveiligde berichtenuitwisseling (SM) gebruikt uitsluitend de in Tabel 5 opgesomde SM-gegevensobjecten (zie [ISO 7816-4]). In elk bericht worden deze gegevensobjecten gebruikt in de volgorde die wordt aangegeven in deze tabel.

Tabel 5

Gegevensobjecten voor beveiligde berichtenuitwisseling (SM DO's)

Naam gegevensobject	Label	Aanwezigheid (V)erplicht, (C)onditioneel of (N)iet toegestaan in	
		Commando's	Antwoorden
Ongecodeerde waarde van niet met BER-TLV gecodeerde gegevens	'81'	C	C
Ongecodeerde waarde van met BER-TLV gecodeerde gegevens, exclusief SM-gegevensobjecten	'B3'	C	C
Paddingindicator gevolgd door cryptogram, ongecodeerde waarde van niet met BER-TLV gecodeerde gegevens	'87'	C	C
Beschermde lengtebyte (Le)	'97'	C	N
Verwerkingsstatus	'99'	N	V
Cryptografische controlesom	'8E'	V	V

Opmerking: Zoals gespecificeerd in aanhangsel 2, kunnen tachograafkaarten het READ BINARY- en UPDATE BINARY-commando ondersteunen met een oneven instructiebyte (INS) (respectievelijk 'B1' en 'D7'). Deze varianten van commando zijn nodig om bestanden met 32 768 bytes of meer te lezen en te actualiseren. Indien geen dergelijke variant wordt gebruikt, wordt een gegevensobject met label 'B3' gebruikt in plaats van een gegevensobject met label '81'. Zie aanhangsel 2 voor meer informatie.

CSM_189 Alle SM-gegevensobjecten worden gecodeerd met DER TLV, zoals gespecificeerd in [ISO 8825-1]. Door deze codering wordt de waarde van de labellengte (TLV) als volgt gestructureerd:

Label: het label wordt ingevoerd in 1 of 2 bytes en geeft de inhoud aan.

Lengte: de lengte wordt ingevoerd als niet-getekend geheel getal in 1, 2 of 3 bytes, wat een maximumlengte van 65 535 bytes geeft. Er worden zo weinig mogelijk bytes gebruikt.

Waarde: de waarde wordt ingevoerd in nul of meer bytes.

CSM_190 Door beveiligde berichtenuitwisseling beschermde APDU's worden als volgt aangemaakt:

— Het koplabel (header) van het commando wordt opgenomen in de MAC-berekening. Bijgevolg wordt de waarde '0C' wordt gebruikt voor de bytecategorie CLA.

— Zoals gespecificeerd in aanhangsel 2, zijn alle instructiebytes (INS) even, met als mogelijke uitzondering oneven instructiebytes voor de READ BINARY- en UPDATE BINARY-commando's.

— De werkelijke waarde van Lc wordt gewijzigd in Lc' na toepassing van de beveiligde berichtenuitwisseling.

— Het gegevensveld bestaat uit gegevensobjecten voor beveiligde berichtenuitwisseling (SM DO's).

— In het beveiligde APDU-commando wordt de nieuwe lengtebyte (Le) ingesteld op '00'. Indien nodig wordt een gegevensobject '97' toegevoegd aan het gegevensveld om de oorspronkelijke waarde van Le door te geven.

CSM_191 Elk te coderen gegevensobject wordt opgevuld overeenkomstig [ISO 7816-4] met behulp van de paddingindicator '01'. Om de MAC te berekenen, wordt elk gegevensobject in de APDU ook afzonderlijk 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:

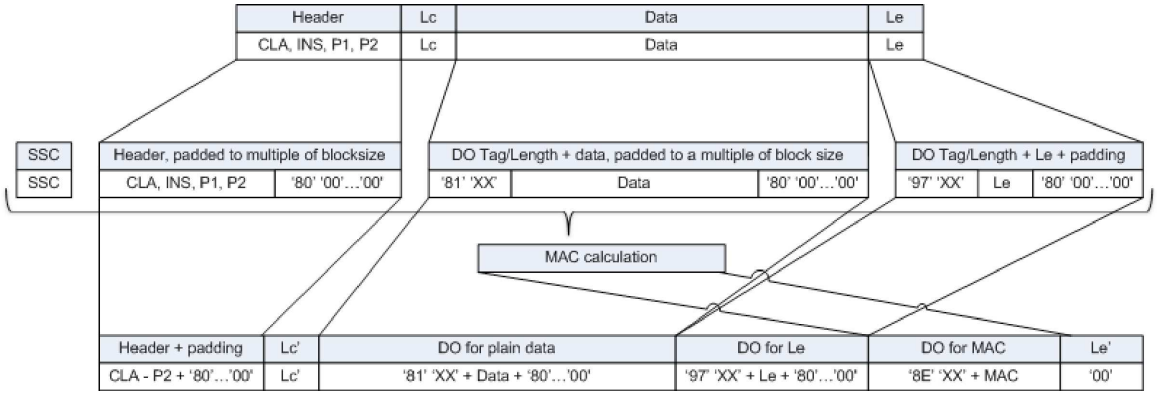
Geval 1 of 3:	DO '99' || DO '8E' || SW1SW2
Geval 2 of 4 (even instructiebyte INS) met codering:	DO '81' || DO '99' || DO '8E' || SW1SW2
Geval 2 of 4 (even instructiebyte INS) zonder codering:	DO '87' || DO '99' || DO '8E' || SW1SW2
Geval 2 of 4 (oneven instructiebyte INS) zonder codering:	DO 'B3' || 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 2/geval 4, en Figuur 10 toont een gecodeerd en geauthenticeerd APDU-antwoord in geval 2/geval 4.

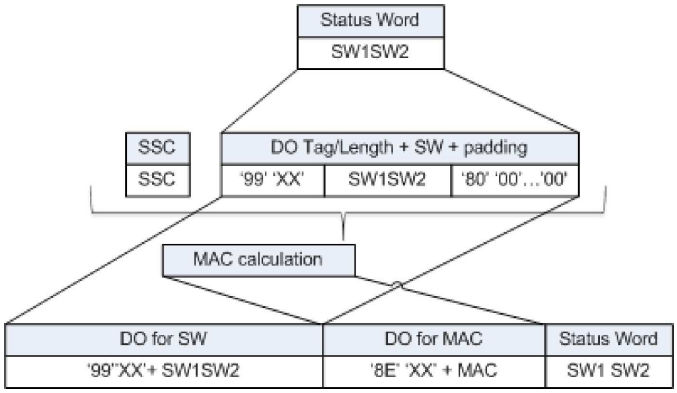
Figuur 8

Transformatie van een geauthenticeerd APDU-commando in geval 4



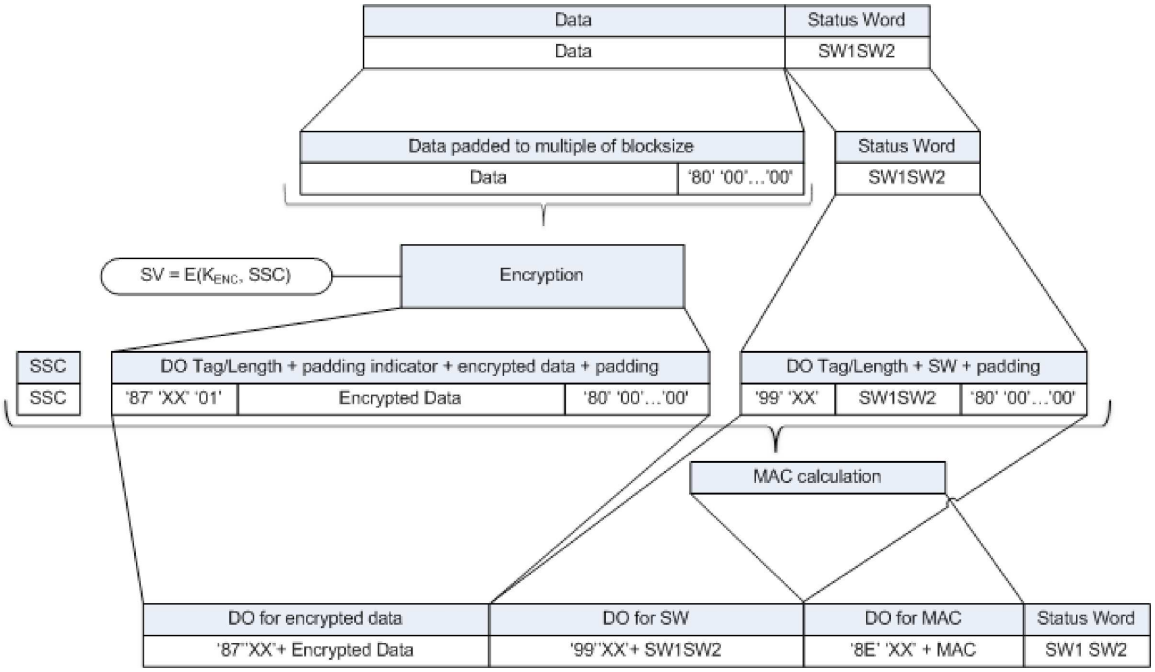
Figuur 9

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



10.5.3 *Afbreken van een sessie voor beveiligde berichtenuitwisseling*

CSM_192 De voertuigunit breekt een actieve sessie voor beveiligde berichtenuitwisseling (SM-sessie) enkel en alleen af indien een van de volgende omstandigheden zich voordoet:

— de VU ontvangt een ongecodeerd APDU-antwoord;

— de VU stelt een SM-fout in een APDU-antwoord 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, onjuiste TLV-structuur of paddingindicator in label '87' verschilt van '01';

— de kaart zendt een statusbyte terug om te melden dat een SM-fout werd vastgesteld (zie CSM_194);

— het maximumaantal commando's en bijbehorende antwoorden van de huidige sessie is bereikt. Dit maximumaantal wordt voor de VU vastgelegd door de fabrikant, rekening houdend met de beveiligingseisen van de gebruikte hardware, en bedraagt 240 SM-commando's en bijbehorende antwoorden per sessie.

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 selecteert een toepassing op de kaart;

— de VU start de VU-authenticatieprocedure,

— het maximumaantal commando's en bijbehorende antwoorden van de huidige sessie is bereikt. Dit maximumaantal 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.

CSM_194 De tachograafkaart behandelt SM-fouten als volgt:

— Indien sommige in een APDU-commando verwachte SM-gegevensobjecten ontbreken, gegevensobjecten niet in de juiste volgorde staan of onbekende gegevensobjecten aanwezig zijn, zendt de tachograafkaart de statusbytes '69 87' terug.

— Indien een APDU-commando een onjuist SM-gegevensobject bevat, zendt de tachograafkaart de statusbytes '69 88' terug.

In dit geval worden de statusbytes teruggezonden zonder SM.

CSM_195 Indien een SM-sessie tussen de VU en tachograafkaart wordt afgebroken, voeren de VU en tachograafkaart de volgende acties uit:

— de opgeslagen sessiesleutels worden veilig vernietigd;

— er wordt onmiddellijk een nieuwe SM-sessie tot stand gebracht, zoals beschreven in punten 10.2 tot en met 10.5.

CSM_196 Indien de VU om welke reden dan ook beslist de wederzijdse authenticatie voor een ingebrachte kaart opnieuw te starten, begint de procedure opnieuw met de verificatie van de certificaatketen op kaartniveau, zoals uiteengezet in punt 10.2. Vervolgens wordt de procedure voortgezet zoals beschreven in punten 10.2 tot en met 10.5.

11. KOPPELING, WEDERZIJDSE AUTHENTICATIE EN BEVEILIGDE BERICHTENUITWISSELING TUSSEN VU EN EXTERNE GNSS-MODULE

11.1. **Algemeen**

CSM_197 De GNSS-module die de VU gebruikt om zijn positie te bepalen, kan zich zowel binnen de VU bevinden (in de VU-systeemkast ingebouwd en niet demonteerbaar) als daarbuiten, in de vorm van een externe module. In het eerste geval is het niet nodig de interne communicatie tussen de GNSS-module en de VU te standaardiseren, en zijn de in dit hoofdstuk vastgelegde voorschriften niet van toepassing. In het tweede geval moet de communicatie tussen de VU en de externe GNSS-module worden gestandaardiseerd en beschermd op de in dit hoofdstuk beschreven wijze.

CSM_198 De beveiligde communicatie tussen een voertuigunit en externe GNSS-module vindt op dezelfde wijze plaats als tussen een voertuigunit en tachograafkaart, met dit verschil dat de externe GNSS-module (EGF) de rol van de kaart overneemt. De externe GNSS-module moet voldoen aan alle in hoofdstuk 10 vermelde voorschriften voor tachograafkaarten, onverminderd de in dit hoofdstuk genoemde afwijkingen, verduidelijkingen en aanvullingen. In het bijzonder de wederzijdse verificatie van de certificaatketen, de VU-authenticatie en chipauthenticatie moeten worden uitgevoerd zoals beschreven in punten 11.3 en 11.4.

CSM_199 Anders dan bij de communicatie tussen een voertuigunit en tachograafkaart, moeten de voertuigunit en externe GNSS-module eenmaal worden gekoppeld in de werkplaats voordat ze op GNSS gebaseerde gegevens kunnen uitwisselen tijdens normaal bedrijf. Het koppelingsproces wordt nader toegelicht in punt 11.2.

CSM_200 Voor de communicatie tussen een voertuigunit en externe GNSS-module worden op [ISO 7816-4] en [ISO 7816-8] gebaseerde APDU-commando's en -antwoorden gebruikt. De exacte structuur daarvan wordt gedefinieerd in aanhangsel 2 van deze bijlage.

11.2. **Koppeling tussen VU en externe GNSS-module**

CSM_201 De voertuigunit en de externe GNSS-module worden in de werkplaats gekoppeld. Zodra de voertuigunit en de externe GNSS-module gekoppeld zijn, kunnen ze met elkaar communiceren tijdens normaal bedrijf.

CSM_202 Het is alleen mogelijk een voertuigunit en externe GNSS-module te koppelen indien de voertuigunit in kalibreringsmodus staat. De koppelingsprocedure wordt gestart door de voertuigunit.

CSM_203 In de werkplaats kan een voertuigunit te allen tijde aan een andere of opnieuw aan dezelfde externe GNSS-module worden gekoppeld. Bij het opnieuw koppelen wordt het bestaande certificaat EGF_MA in het geheugen van de VU veilig vernietigd, en slaat de VU het certificaat EGF_MA op van de externe GNSS-module waaraan hij wordt gekoppeld.

CSM_204 In de werkplaats kan een externe GNSS-module te allen tijde aan een andere of opnieuw aan dezelfde voertuigunit worden gekoppeld. Bij het opnieuw koppelen wordt het bestaande certificaat VU_MA in het geheugen van de externe GNSS-module veilig vernietigd, en slaat de module het certificaat VU_MA op van de VU waaraan hij wordt gekoppeld.

11.3. **Wederzijdse verificatie van de certificaatketen**

11.3.1 *Algemeen*

CSM_205 De wederzijdse verificatie van de certificaatketen tussen een VU en externe GNSS-module vindt uitsluitend plaats op het ogenblik dat de VU en de externe GNSS-module in de werkplaats worden gekoppeld. Tijdens normaal bedrijf van een gekoppelde VU en externe GNSS-module worden geen certificaten geverifieerd. In plaats daarvan worden de certificaten die tijdens de koppelingsprocedure zijn opgeslagen als vertrouwde certificaten beschouwd door de VU en de externe GNSS-module, nadat ze op temporele geldigheid zijn gecontroleerd. Andere certificaten wordt niet vertrouwd ter bescherming van de communicatie tussen de VU en de externe GNSS-module tijdens normaal bedrijf.

11.3.2 *Tijdens de koppeling tussen VU en externe GNSS-module*

CSM_206 Tijdens de koppeling met een externe GNSS-module gaat de voertuigunit te werk volgens het stroomschema in Figuur 4 (zie punt 10.2.1) om de certificaatketen van de externe GNSS-module te verifiëren.

Toelichtingen bij Figuur 4 in deze context:

— De communicatiecontrole valt buiten het toepassingsgebied van dit aanhangsel. Een externe GNSS-module is echter geen smartcard, waardoor de VU wellicht geen terugstelcommando (reset) zal verzenden om de communicatie te initiëren en evenmin een antwoord op terugstellen (ATR) zal ontvangen.

— De kaartcertificaten en openbare sleutels in deze figuur worden opgevat als die van de externe GNSS-module ten behoeve van de wederzijdse authenticatie. In punt 9.1.6 worden deze aangeduid als EGF_MA.

— De openbare sleutels en certificaten Card.CA in deze figuur worden opgevat als die van de MSCA ter ondertekening van de certificaten van de externe GNSS-module. In punt 9.1.3 worden deze aangeduid als MSCA_VU-EGF.

— Het certificaat Card.CA.EUR in deze figuur wordt opgevat als het Europese basiscertificaat dat vermeld staat in de referentie van de certificeringsautoriteit (CAR) van het certificaat MSCA_VU-EGF.

— Het certificaat Card.Link in deze figuur wordt opgevat als het verbindingscertificaat van de externe GNSS-module (indien aanwezig). Zoals verduidelijkt in punt 9.1.2, is dit een verbindingscertificaat voor een nieuw Europees basissleutelpaar dat door de ERCA is aangemaakt en dat met de vorige Europese particuliere sleutel is ondertekend.

— Het certificaat Card.Link.EUR is het Europese basiscertificaat dat vermeld staat in de referentie van de certificeringsautoriteit (CAR) van het certificaat Card.Link.

— In plaats van `cardExtendedSerialNumber` leest de VU `sensorGNSSserialNumber` in het hoofdbestand van de chipkaart (EF ICC).

— De VU selecteert hier niet de toepassingsidentificator (AID) van de tachograaf, maar die van de externe GNSS-module (EGF AID).

— De instructie 'Ignore Card' wordt opgevat als 'Ignore EGF'.

CSM_207 Na verificatie van het certificaat EGF_MA slaat de voertuigunit dit certificaat op voor gebruik tijdens normaal bedrijf (zie punt 11.3.3).

CSM_208 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.

Toelichtingen bij Figuur 5 in deze context:

— De VU genereert een nieuw tijdelijk sleutelpaar op basis van de domeinparameters in het certificaat van de externe GNSS-module.

— De VU-certificaten en openbare sleutels in deze figuur dienen voor de wederzijdse authenticatie. In punt 9.1.4 worden deze aangeduid als VU_MA.

— De openbare sleutels en certificaten VU.CA in deze figuur dienen om certificaten van voertuigunits en externe GNSS-modules te ondertekenen. In punt 9.1.3 worden deze aangeduid als MSCA_VU-EGF.

— Het certificaat VU.CA.EUR in deze figuur is het Europese basiscertificaat dat vermeld staat in de referentie van de certificeringsautoriteit (CAR) van het certificaat VU.CA.

— Het certificaat VU.Link in deze figuur is het verbindingscertificaat van de VU (indien aanwezig). Zoals verduidelijkt in punt 9.1.2, is dit een verbindingscertificaat voor een nieuw Europees basissleutelpaar dat door de ERCA is aangemaakt en dat met de vorige Europese particuliere sleutel is ondertekend.

— Het certificaat VU.Link.EUR is het Europese basiscertificaat dat vermeld staat in de referentie van de certificeringsautoriteit (CAR) van het certificaat VU.Link.

CSM_209 In afwijking van het voorschrift CSM_167 gebruikt de externe GNSS-module de eigen tijdaanduiding om de temporele geldigheid van een aangeboden certificaat te verifiëren.

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).

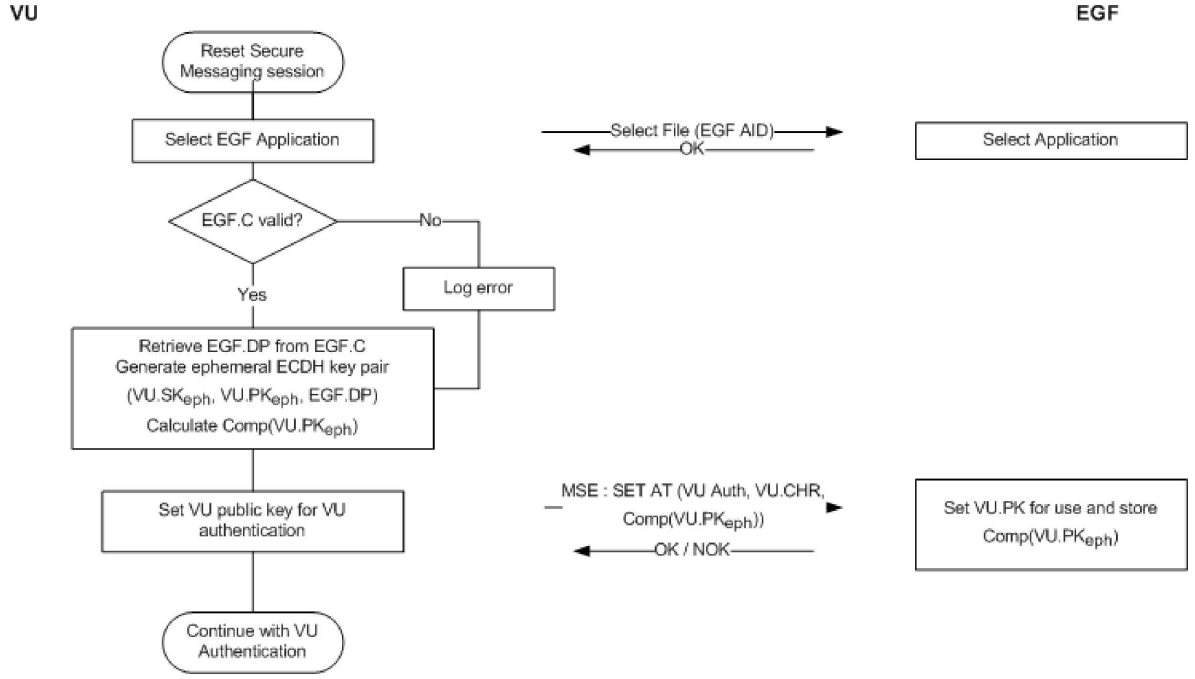
11.3.3 *Tijdens normaal bedrijf*

CSM_211 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 de opgeslagen certificaten EGF_MA en VU_MA 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.

Het stroomschema in Figuur 11 omvat in wezen de eerste stappen die terug te vinden zijn in Figuur 4 en Figuur 5. Zoals gezegd, is een externe GNSS-module echter geen smartcard, waardoor de VU ook hier wellicht geen terugstelcommando (reset) zal verzenden om de communicatie te initiëren en evenmin een antwoord op terugstellen (ATR) zal ontvangen. Dit valt hoe dan ook buiten het toepassingsgebied van dit aanhangsel.

Figuur 11

Wederzijdse verificatie van de temporele geldigheid van het certificaat tijdens normaal bedrijf van VU en externe GNSS-module



CSM_212 Zoals blijkt uit Figuur 11, registreert de voertuigunit een fout indien het certificaat EGF_MA niet langer geldig is. De wederzijdse authenticatie, sleutelovereenstemming en latere communicatie via beveiligde berichtenuitwisseling verlopen echter op de gebruikelijke wijze.

11.4. VU-authenticatie, chipauthenticatie en sleutelovereenstemming tijdens de sessie

CSM_213 De VU-authenticatie, chipauthenticatie en sleutelovereenstemming tijdens de sessie tussen een VU en externe GNSS-module vinden plaats tijdens de koppelingsprocedure en telkens wanneer een nieuwe sessie voor beveiligde berichtenuitwisseling (SM-sessie) tot stand wordt gebracht tijdens normaal bedrijf. De VU en de externe GNSS-module voeren de in punten 10.3 en 10.4 beschreven procedures uit. Alle in deze punten vastgestelde voorschriften zijn van toepassing.

11.5. Beveiligde berichtenuitwisseling

CSM_214 Nadat de chip met succes is geauthenticeerd en tot op het ogenblik dat de sessie wordt beëindigd, worden alle commando's en antwoorden die de voertuigunit en externe GNSS-module met elkaar uitwisselen beschermd door beveiligde berichtenuitwisseling in alleen-authenticeren-modus. Alle in punt 10.5 vastgestelde voorschriften zijn van toepassing.

CSM_215 Indien de beveiligde berichtenuitwisseling tussen een VU en externe GNSS-module wordt afgebroken, brengt de VU onmiddellijk een nieuwe SM-sessie tot stand, zoals uiteengezet in punten 11.3.3 en 11.4.

12. KOPPELING EN COMMUNICATIE TUSSEN VU EN BEWEGINGSSENSOR

12.1. **Algemeen**

CSM_216 Tijdens de koppelingsprocedure en tijdens normaal bedrijf communiceren de voertuigunit en bewegingssensor met elkaar overeenkomstig het in [ISO 16844-3] gespecificeerde interfaceprotocol, onverminderd de wijzigingen die nader worden omschreven in dit hoofdstuk en in punt 9.2.1.

Opmerking: de lezer wordt bekend verondersteld met de inhoud van [ISO 16844-3].

12.2. **Koppeling tussen VU en bewegingssensor met gebruikmaking van sleutels van verschillende generaties**

Zoals uiteengezet in punt 9.2.1, wordt de hoofdsleutel van de bewegingssensor met alle bijbehorende sleutels regelmatig vervangen. Het gevolg hiervan is dat op werkplaatskaarten tot drie aan de bewegingssensor gerelateerde AES-sleutels $K_{M\text{-}WC}$ (van opeenvolgende generaties) kunnen voorkomen. Ook bewegingssensoren kunnen tot drie verschillende op AES gebaseerde gegevenscoderingen bevatten (die berusten op opeenvolgende generaties van de hoofdsleutel van de bewegingssensor K_M). De voertuigunit bevat slechts één aan de bewegingssensor gerelateerde sleutel $K_{M\text{-}VU}$.

CSM_217 Een VU van de tweede generatie en een bewegingssensor van de tweede generatie worden als volgt gekoppeld (zie ook tabel 6 in [ISO 16844-3]):

1. De werkplaatskaart van de tweede generatie wordt ingebracht in de VU en de VU wordt verbonden met de bewegingssensor.

2. De VU leest alle beschikbare sleutels $K_{M\text{-}WC}$ op de werkplaatskaart, controleert het versienummer van de sleutels en kiest de sleutel die overeenstemt met het versienummer van de sleutel $K_{M\text{-}VU}$ van de VU. Indien de werkplaatskaart geen overeenstemmende sleutel $K_{M\text{-}WC}$ bevat, wordt de koppelingsprocedure afgebroken door de VU en krijgt de werkplaatskaarthouder een foutmelding te zien.

3. Zoals gespecificeerd in punt 9.2.1, berekent de VU de hoofdsleutel van de bewegingssensor K_M op basis van de sleutels $K_{M\text{-}VU}$ en $K_{M\text{-}WC}$ en de identificatiesleutel K_{ID} op basis van de sleutel K_M.

4. De VU geeft de bewegingssensor opdracht om de koppelingsprocedure te starten, zoals beschreven in [ISO 16844-3], en codeert het van de bewegingssensor ontvangen serienummer met de identificatiesleutel K_{ID}. De VU zendt het gecodeerde serienummer terug naar de bewegingssensor.

5. De bewegingssensor vergelijkt het gecodeerde serienummer achtereenvolgens met de intern opgeslagen gecodeerde versies van het serienummer. Indien een overeenstemmend serienummer wordt gevonden, wordt de VU geauthenticeerd. De bewegingssensor registreert de generatie van de door de VU gebruikte sleutel K_{ID} en zendt de overeenstemmende gecodeerde versie van de koppelingssleutel terug, dat wil zeggen de gecodeerde sleutel die werd aangemaakt met de sleutel K_M van dezelfde generatie.

6. De VU decodeert de koppelingssleutel met K_M, genereert een sessiesleutel K_S, codeert die met de koppelingssleutel en zendt het resultaat terug naar de bewegingssensor. De bewegingssensor decodeert de sessiesleutel K_S.

7. De VU verzamelt de koppelingsinformatie zoals aangegeven in [ISO 16844-3] en codeert die met de koppelingssleutel. Vervolgens zendt de VU het resultaat terug naar de bewegingssensor. De bewegingssensor decodeert de koppelingsinformatie.

8. De bewegingssensor codeert de ontvangen koppelingsinformatie met de ontvangen sessiesleutel K_S en zendt deze terug naar de VU. De VU controleert of de koppelingsinformatie identiek is aan de informatie die in de vorige stap naar de bewegingssensor werd verzonden. Indien het gaat om dezelfde informatie, bewijst dit dat de bewegingssensor dezelfde sessiesleutel K_S heeft gebruikt als de VU en bijgevolg in stap 5 de koppelingssleutel heeft teruggezonden nadat die met de sleutel K_M van de juiste generatie werd gecodeerd. Bijgevolg wordt de bewegingssensor geauthenticeerd.

Stappen 2 en 5 verschillen van de standaardprocedure in [ISO 16844-3]; de overige stappen komen overeen met de standaardprocedure.

Voorbeeld: Stel dat de koppelingsprocedure wordt uitgevoerd in het eerste jaar van geldigheid van het certificaat ERCA (3); zie Figuur 2 in punt 9.2.1.2. Stel verder dat

— de bewegingssensor in gebruik werd genomen in het laatste jaar van geldigheid van het certificaat ERCA (1). De bewegingssensor bevat bijgevolg de volgende sleutels en gegevens:

  — $N_s[1]$: het serienummer van de bewegingssensor, gecodeerd met de identificatiesleutel K_{ID} van de eerste generatie;

  — $N_s[2]$: het serienummer van de bewegingssensor, gecodeerd met de identificatiesleutel K_{ID} van de tweede generatie;

  — $N_s[3]$: het serienummer van de bewegingssensor, gecodeerd met de identificatiesleutel K_{ID} van de derde generatie;

  — $K_P[1]$: de koppelingssleutel van de eerste generatie ([1]), gecodeerd met de sleutel K_M van de eerste generatie;

  — $K_P[2]$: de koppelingssleutel van de tweede generatie, gecodeerd met de sleutel K_M van de tweede generatie;

  — $K_P[3]$: de koppelingssleutel van de derde generatie, gecodeerd met de sleutel K_M van de derde generatie.

— Stel dat de werkplaatskaart werd afgegeven in het eerste jaar van geldigheid van het certificaat ERCA (3). Deze kaart bevat bijgevolg de sleutel $K_{M\text{-}WC}$ van de tweede en de derde generatie.

— Stel dat de VU van de tweede generatie is en de sleutel $K_{M\text{-}VU}$ van de tweede generatie bevat.

In dit geval verlopen stappen 2 tot en met 5 als volgt:

— Stap 2: de VU leest de sleutel $K_{M\text{-}WC}$ van de tweede en de derde generatie op de werkplaatskaart, en controleert de versienummers ervan.

— Stap 3: de VU combineert de sleutel $K_{M\text{-}WC}$ van de tweede generatie met zijn sleutel $K_{M\text{-}VU}$ om K_M en K_{ID} af te leiden.

— Stap 4: de VU codeert het van de bewegingssensor ontvangen serienummer met de identificatiesleutel K_{ID}.

— Stap 5: de bewegingssensor vergelijkt de ontvangen gegevens met $N_s[1]$ en vindt geen overeenkomst. Daarna vergelijkt de bewegingssensor de gegevens met $N_s[2]$ en vindt een overeenkomst. De bewegingssensor maakt hieruit op dat de VU van de tweede generatie is en zendt bijgevolg $K_P[2]$ terug.

12.3. **Koppeling en communicatie tussen VU en bewegingssensor via AES**

CSM_218 Zoals gespecificeerd in Tabel 3 onder 9.2.1, zijn alle sleutels die worden gebruikt voor de koppeling van een voertuigunit (van de tweede generatie) en een bewegingssensor en voor de latere communicatie, AES-sleutels en geen TDES-sleutels met dubbele lengte zoals gespecificeerd in [ISO 16844-3]. Deze AES-sleutels kunnen 128, 192 of 256 bits lang zijn. Aangezien de AES-blokgrootte 16 bytes bedraagt, moet de lengte van een gecodeerd bericht een veelvoud zijn van 16 bytes, tegenover 8 bytes voor TDES-sleutels. Bovendien worden sommige van die berichten gebruikt om AES-sleutels over te brengen met een lengte van 128, 192 of 256 bits. Bijgevolg wordt het in tabel 5 van [ISO 16844-3] vermelde aantal gegevensbytes per instructie aangepast zoals aangegeven in Tabel 6:

Tabel 6

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

Instructie	Type	Gegevens-beschrijving	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	Authenticatie-gegevens + bestandsnummer	8	8	16	16	16

([1]) Zoals uiteengezet in CSM_117, kunnen de koppelingssleutels van de eerste, tweede en derde generatie betrekking hebben op dezelfde sleutel dan wel op drie verschillende sleutels met een onderling afwijkende lengte.

Instructie	Type	Gegevens-beschrijving	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
11	Antwoord	Authenticatie-gegevens + bestandsinhoud	16 of 32, afhankelijk van bestand	16 of 32, afhankelijk van bestand	16 / 32	16 / 32	16 / 32
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	Authenticatie-gegevens	8	8	16	16	16
80	Antwoord	Tellerwaarde bewegingssensor + authenticatie-gegevens	8	8	16	16	16

CSM_219 De koppelingsinformatie die wordt verzonden in instructies 43 (verzoek VU) en 50 (antwoord bewegingssensor), wordt verzameld zoals gespecificeerd in punt 7.6.10 van [ISO 16844-3], met dit verschil dat in het coderingsschema van de koppelingsgegevens het AES-algoritme wordt toegepast in plaats van het TDES-algoritme, waardoor twee AES-coderingen ontstaan, en dat de in CSM_220 vermelde padding wordt gebruikt ter aanpassing aan de AES-blokgrootte. De voor deze codering gebruikte sleutel K'_P wordt als volgt gegenereerd:

— Indien de koppelingssleutel K_P 16 bytes lang is: $K'_P = K_P \text{ XOR } (N_s||N_s)$

— Indien de koppelingssleutel K_P 24 bytes lang is: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s)$

— Indien de koppelingssleutel K_P 32 bytes lang is: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s||N_s)$

waarbij N_s het serienummer van 8 bytes van de bewegingssensor is.

CSM_220 Indien de ongecodeerde gegevenslengte (bij gebruik van AES-sleutels) geen veelvoud van 16 bytes is, wordt de in [ISO 9797-1] vastgelegde paddingmethode 2 toegepast.

Opmerking: in [ISO 16844-3] is het aantal ongecodeerde gegevensbytes altijd een veelvoud van 8, zodat bij gebruik van TDES geen padding nodig is. De definitie van gegevens en berichten in [ISO 16844-3] wordt niet gewijzigd door dit onderdeel van dit aanhangsel, waardoor padding noodzakelijk is.

CSM_221 Voor instructie 11 en indien men meerdere gegevensblokken moet coderen, wordt de CBC(Cipher Block Chaining)-werkingsmodus toegepast, zoals vastgelegd in [ISO 10116], met een interleave-parameter *m* = 1. Hierbij wordt de volgende initialisatievector (IV) gebruikt:

— Voor instructie 11: het authenticatieblok van 8 bytes zoals gespecificeerd in punt 7.6.3.3 van [ISO 16844-3], opgevuld volgens de in [ISO 9797-1] vastgelegde paddingmethode 2; zie ook punten 7.6.5 en 7.6.6 van [ISO 16844-3].

— Voor alle andere instructies waarin meer dan 16 bytes worden overgebracht, zoals gespecificeerd in Tabel 6: '00' {16}, dat wil zeggen 16 bytes met een binaire nul.

Opmerking: zoals verduidelijkt in punten 7.6.5 en 7.6.6 van [ISO 16844-3], in het geval dat de bewegingssensor gegevensbestanden codeert om die op te nemen in instructie 11, wordt het authenticatieblok:

— gebruikt als de initialisatievector om de gegevensbestanden in CBC-modus te coderen;

— gecodeerd en als eerste blok opgenomen in de naar de VU verzonden gegevens.

12.4. **Koppeling tussen VU en bewegingssensor voor apparatuur van verschillende generaties**

CSM_222 Zoals uiteengezet in punt 9.2.1, kan een bewegingssensor van de tweede generatie de op TDES gebaseerde codering van de koppelingsgegevens bevatten (zoals vastgelegd in deel A van dit aanhangsel). Hierdoor kan de bewegingssensor worden gekoppeld aan een VU van de eerste generatie. In dit geval moet men de VU van de eerste generatie en de bewegingssensor van de tweede generatie koppelen zoals beschreven in deel A van dit aanhangsel en in [ISO 16844-3]. Voor de koppelingsprocedure kan een werkplaatskaart van de eerste of van de tweede generatie worden gebruikt.

Opmerkingen:

— Het is niet mogelijk een VU van de tweede generatie te koppelen aan een bewegingssensor van de eerste generatie.

— Het is niet mogelijk een werkplaatskaart van de eerste generatie te gebruiken om een VU van de tweede generatie te koppelen aan een bewegingssensor.

13. BEVEILIGING VOOR COMMUNICATIE OP AFSTAND VIA DE DSRC-INTERFACE

13.1. **Algemeen**

Zoals gespecificeerd in aanhangsel 14, genereert een VU regelmatig gegevens over de tachograafcontrole op afstand (RTM), en verzendt die naar de (interne of externe) inrichting voor communicatie op afstand (RCF). De inrichting voor communicatie op afstand dient deze gegevens naar het systeem voor ondervraging op afstand te verzenden via de in aanhangsel 14 beschreven DSRC-interface. In aanhangsel 1 worden de RTM-gegevens gespecificeerd als samenvoeging van:

gecodeerde payloadgegevens van de tachograaf de codering van de ongecodeerde payloadgegevens van de tachograaf;

DSRC-beveiligingsgegevens zie onderstaande beschrijving.

Het formaat van de ongecodeerde payloadgegevens van de tachograaf wordt gespecificeerd in aanhangsel 1 en nader toegelicht in aanhangsel 14. In dit gedeelte wordt een beschrijving gegeven van de structuur van de DSRC-beveiligingsgegevens; de formele specificaties zijn terug te vinden in aanhangsel 1.

CSM_223 De ongecodeerde `tachographPayload`-gegevens die de VU doorgeeft aan een inrichting voor communicatie op afstand (indien de RCF zich buiten de VU bevindt) of aan een systeem voor ondervraging op afstand via de DSRC-interface (indien de RCF zich in de VU bevindt), worden beveiligd in eerst-coderen-dan-authenticeren-modus. Dit betekent dat de payloadgegevens van de tachograaf eerst worden gecodeerd om de vertrouwelijkheid van het bericht te waarborgen, waarna een berichtauthenticatiecode (MAC) wordt berekend om de authenticiteit en integriteit van de gegevens te waarborgen.

CSM_224 De DSRC-beveiligingsgegevens bestaan uit de samenvoeging van de volgende gegevenselementen in de hieronder aangegeven volgorde (zie ook Figuur 12):

Lopende datum/tijd	de huidige datum en tijd van de VU (gegevenstype `TimeReal`)
Teller	een teller van 3 bytes (zie CSM_225)

Serienummer van de VU	het serienummer van de VU (gegevenstype `VuSerialNumber`)
Versienummer van DSRC-hoofdsleutel	het versienummer van 1 byte van de DSRC-hoofdsleutel waarvan de VU-specifieke DSRC-sleutels zijn afgeleid (zie punt 9.2.2)
MAC	de berichtauthenticatiecode, berekend op basis van alle vorige bytes in de RTM-gegevens.

CSM_225 De teller van 3 bytes in de DSRC-beveiligingsgegevens heeft het formaat „MSB-first" (meest significante bits eerst). Wanneer de VU voor het eerst na ingebruikname een reeks RTM-gegevens berekent, wordt de teller op nul gezet. Alvorens een nieuwe reeks RTM-gegevens te berekenen, verhoogt de VU de waarde van de teller telkens met 1.

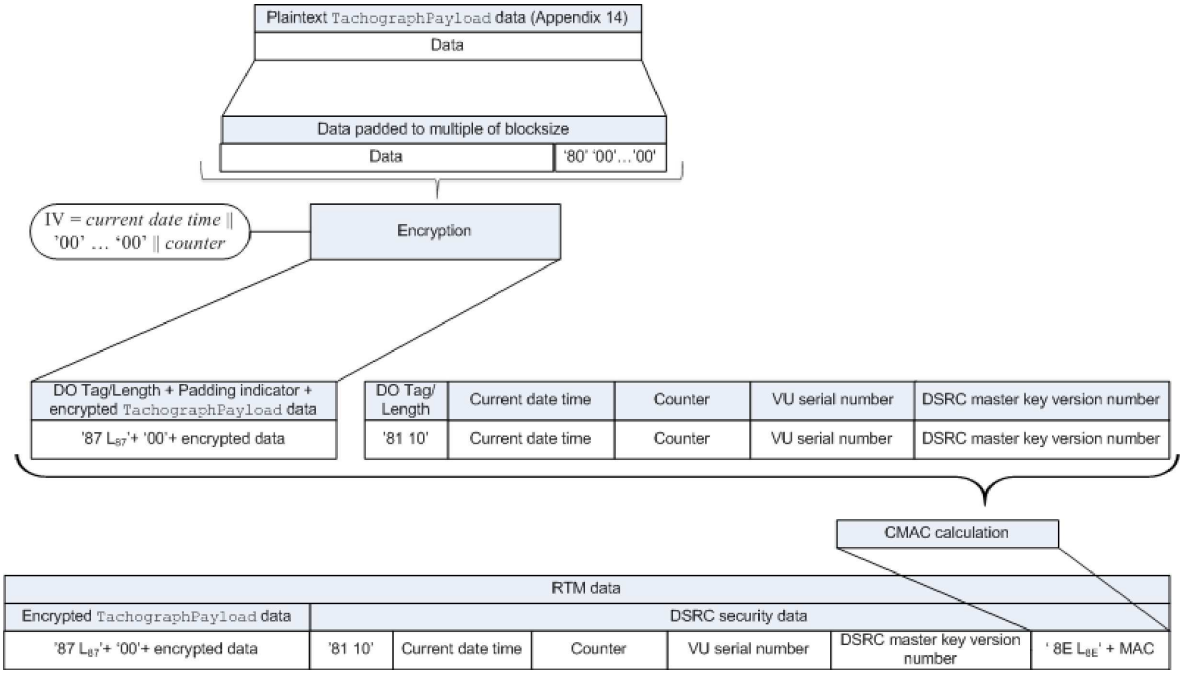
13.2. Codering van de payloadgegevens van de tachograaf en MAC-generering

CSM_226 Stel een ongecodeerd gegevenselement met gegevenstype `TachographPayload`, zoals beschreven in aanhangsel 14. De VU codeert deze gegevens zoals aangegeven in Figuur 12. De DSRC-coderingssleutel $K_VU_{DSRC}_ENC$ van de VU (zie punt 9.2.2) wordt gebruikt met het AES-algoritme in de CBC(Cipher Block Chaining)-werkingsmodus, zoals vastgelegd in [ISO 10116], met een interleave-parameter $m = 1$. De initialisatievector is gelijk aan *IV = lopende datum/tijd || '00 00 00 00 00 00 00 00' || teller,* met *lopende datum/tijd* en *teller* zoals gespecificeerd in CSM_224. De te coderen gegevens worden opgevuld volgens de in [ISO 9797-1] vastgelegde paddingmethode 2.

CSM_227 De VU berekent de berichtauthenticatiecode (MAC) in de DSRC-beveiligingsgegevens zoals verduidelijkt in Figuur 12. De MAC wordt berekend voor alle vorige bytes in de RTM-gegevens, tot en met het versienummer van de DSRC-hoofdsleutel, met inbegrip van de labels en rekening houdend met de lengte van de gegevensobjecten. De VU gebruikt deze DSRC-sleutel om de authenticiteit te waarborgen met $K_VU_{DSRC}_MAC$ (zie punt 9.2.2) en past daarbij het AES-algoritme toe in CMAC-modus, zoals gespecificeerd in [SP 800-38B]. De lengte van de berichtauthenticatiecode (MAC) is gerelateerd aan de lengte van de VU-specifieke DSRC-sleutels, zoals gespecificeerd in CSM_50.

Figuur 12

Codering van de payloadgegevens van de tachograaf en MAC-generering



13.3. **Verificatie en decodering van de payloadgegevens van de tachograaf**

CSM_228 Bij ontvangst van RTM-gegevens van een VU brengt het systeem voor ondervraging op afstand alle RTM-gegevens over op een controlekaart in het gegevensveld van een PROCESS DSRC MESSAGE-commando, zoals beschreven in aanhangsel 2. Daarna gebeurt het volgende:

1. De controlekaart inspecteert het versienummer van de DSRC-hoofdsleutel in de DSRC-beveiligingsgegevens. Indien de controlekaart de opgegeven DSRC-hoofdsleutel niet kent, zendt deze een fout terug, zoals gespecificeerd in aanhangsel 2, en wordt de procedure afgebroken.

2. De controlekaart gebruikt de opgegeven DSRC-hoofdsleutel in combinatie met het VU-serienummer 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.

3. De controlekaart gebruikt de sleutel K_VU_{DSRC}_MAC om de berichtauthenticatiecode (MAC) in de DSRC-beveiligingsgegevens te verifiëren, zoals gespecificeerd in CSM_227. Indien de MAC onjuist is, zendt de controlekaart een fout terug, zoals gespecificeerd in aanhangsel 2, en wordt de procedure afgebroken.

4. De controlekaart gebruikt de sleutel K_VU_{DSRC}_ENC om de gecodeerde payloadgegevens van de tachograaf te decoderen, zoals gespecificeerd in CSM_226. De controlekaart verwijdert de padding en zendt de gedecodeerde payloadgegevens van de tachograaf terug naar het systeem voor ondervraging op afstand.

CSM_229 Om replay-aanvallen tegen te gaan, controleert het systeem voor ondervraging op afstand of de RTM-gegevens up-to-date zijn door zeker te stellen dat de tijdstempel (*lopende datum/tijd*) van de DSRC-beveiligingsgegevens niet te veel afwijkt van zijn eigen tijdaanduiding.

Opmerkingen:

— het systeem voor ondervraging op afstand moet daartoe beschikken over een nauwkeurige en betrouwbare tijdbron.

— Aangezien de VU overeenkomstig aanhangsel 14 om de 60 seconden een nieuwe reeks RTM-gegevens moet berekenen, en de interne klok van de VU 1 minuut van de werkelijke tijd mag afwijken, wordt een grenswaarde van 2 minuten toegepast om te bepalen of de RTM-gegevens up-to-date zijn. De vereiste mate van actueel-zijn hangt ook af van de nauwkeurigheid van de klok van het systeem voor ondervraging op afstand.

CSM_230 Wanneer in de werkplaats wordt gecontroleerd of de DSRC-functie van een VU goed functioneert, worden alle van de VU ontvangen RTM-gegevens overgebracht op een werkplaatskaart in het gegevensveld van een PROCESS DSRC MESSAGE-commando, zoals beschreven in aanhangsel 2. De werkplaatskaart voert alle in CSM_228 gespecificeerde controles en acties uit.

14. ONDERTEKENING VAN GEDOWNLOADE GEGEVENS EN HANDTEKENINGVERIFICATIE

14.1. **Algemeen**

CSM_231 De gegevens die de intelligente toepassingsgerichte apparatuur (IDE) van een VU of kaart ontvangt tijdens een downloadsessie, worden opgeslagen in een fysiek gegevensbestand. De gegevens kunnen ook op een extern opslagmedium (ESM) worden bewaard. Dit bestand bevat digitale handtekeningen van gegevensblokken, zoals gespecificeerd in aanhangsel 7. Dit bestand bevat eveneens de volgende certificaten (zie punt 9.1):

— Indien gegevens worden gedownload van een VU:

  — het certificaat VU_Sign,

  — het certificaat MSCA_VU-EGF met de openbare sleutel ter verificatie van het certificaat VU_Sign.

— Indien gegevens worden gedownload van een kaart:

— het certificaat Card_Sign,

— het certificaat MSCA_Card met de openbare sleutel ter verificatie van het certificaat Card_Sign.

CSM_232 Daarnaast beschikt de IDE over de volgende certificaten.

— Bij handtekeningverificatie met behulp van een controlekaart, zoals verduidelijkt in Figuur 13: het verbindingscertificaat tussen het laatste EUR-certificaat en het in voorkomend geval onmiddellijk daaraan voorafgaande EUR-certificaat.

— Bij handtekeningverificatie door de IDE zelf: alle geldige Europese basiscertificaten.

Opmerking: de methode die de IDE gebruikt om deze certificaten te lezen, wordt niet nader gespecificeerd in dit aanhangsel.

14.2. **Generering van de handtekening**

CSM_233 Om voor de gedownloade gegevens digitale handtekeningen aan te maken, wordt het ondertekeningsalgoritme ECDSA gebruikt, zoals gespecificeerd in [DSS]. Daarbij wordt het hashalgoritme toegepast dat gerelateerd is aan het sleutelgrootte van de VU of de kaart, zoals gespecificeerd in CSM_50. Het handtekeningformaat is ongecodeerd, zoals gespecificeerd in [TR-03111].

14.3. **Handtekeningverificatie**

CSM_234 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. 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.

Toelichtingen bij Figuur 13:

— De apparatuur die de te analyseren gegevens heeft ondertekend, wordt aangeduid als EQT.

— De openbare sleutels en certificaten van de apparatuur (EQT) in deze figuur dienen om de certificaten VU_Sign of Card-Sign te ondertekenen.

— De openbare sleutels en certificaten EQT.CA in deze figuur dienen in voorkomend geval om de VU- of kaartcertificaten te ondertekenen.

— Het certificaat EQT.CA.EUR in deze figuur is het Europese basiscertificaat dat vermeld staat in de referentie van de certificeringsautoriteit (CAR) van het certificaat EQT.CA.

— Het certificaat EQT.Link in deze figuur is het verbindingscertificaat van de apparatuur (EQT), indien aanwezig. Zoals verduidelijkt in punt 9.1.2, is dit een verbindingscertificaat voor een nieuw Europees basissleutelpaar dat door de ERCA is aangemaakt en dat met de vorige Europese particuliere sleutel is ondertekend.

— Het certificaat EQT.Link.EUR is het Europese basiscertificaat dat vermeld staat in de referentie van de certificeringsautoriteit (CAR) van het certificaat EQT.Link.

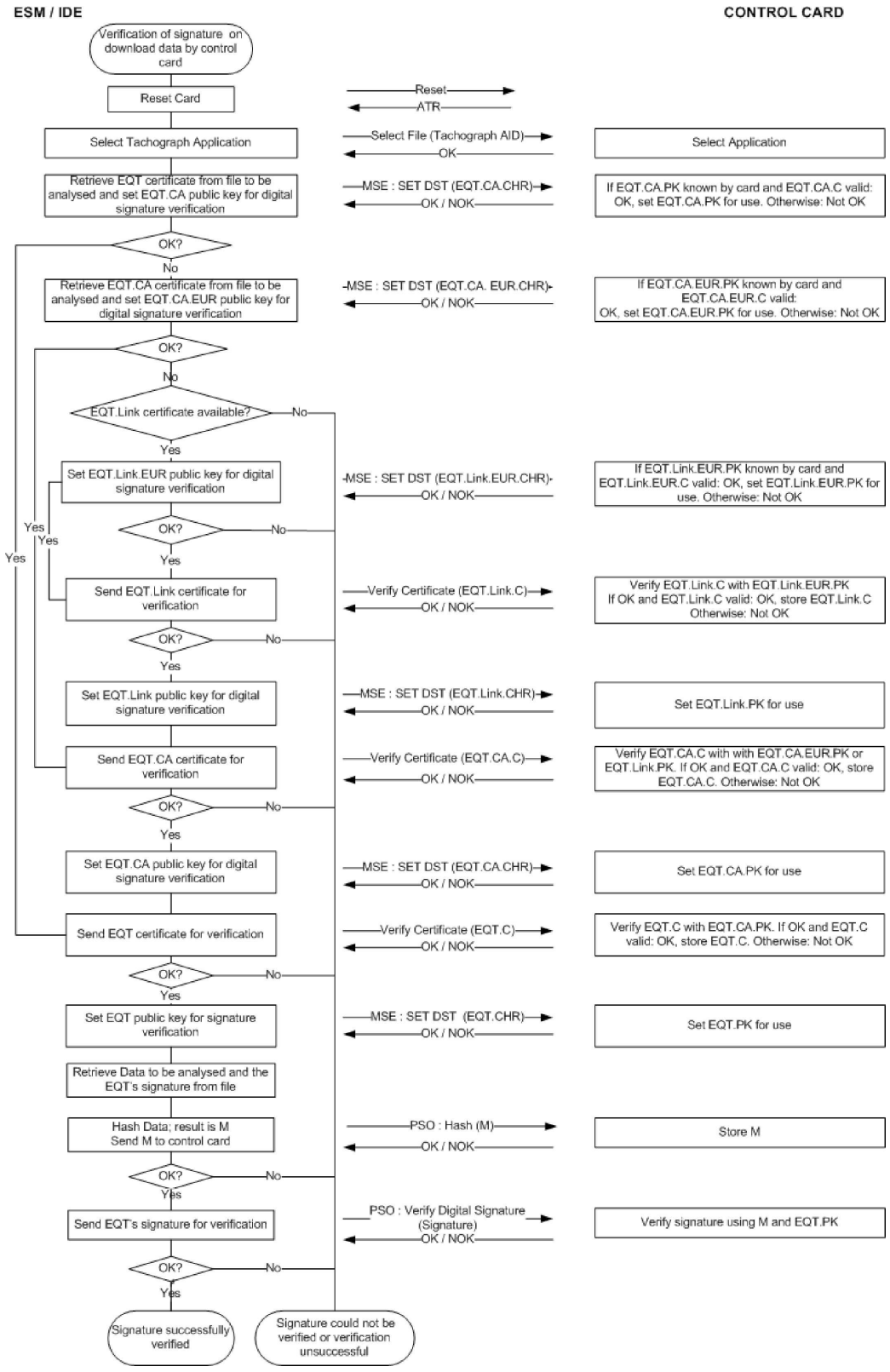
CSM_235 De hashwaarde M die naar de controlekaart in het PSO:Hash-commando wordt verzonden, wordt door de IDE berekend met behulp van het hashalgoritme dat gerelateerd is aan de sleutelgrootte van de VU of de kaart waarvan de gegevens worden gedownload, zoals gespecificeerd in CSM_50.

CSM_236 Ter verificatie van de handtekening van de apparatuur (EQT) volgt de controlekaart het in [DSS] vastgestelde handtekeningschema.

Opmerking: in dit aanhangsel wordt niet nader gespecificeerd welke acties men moet uitvoeren indien de handtekening van een gedownload gegevensbestand niet kan worden geverifieerd of indien de verificatie niet succesvol is.

Figuur 13

Stroomschema ter verificatie van de handtekening van een gedownload gegevensbestand



Aanhangsel 12

PLAATSBEPALING OP BASIS VAN WERELDWIJD SATELLIETNAVIGATIESYSTEEM (GNSS)

INHOUDSOPGAVE

1. INLEIDING 405

1.1. Toepassingsgebied 405

1.2. Acroniemen en notaties 405

2. SPECIFICATIE VAN DE GNSS-ONTVANGER 406

3. NMEA-ZINNEN 406

4. VOERTUIGUNIT MET EXTERNE GNSS-MODULE 408

4.1. Configuratie 408

4.1.1 Belangrijkste onderdelen en interfaces 408

4.1.2 Status van de externe GNSS-module aan het eind van de productie 408

4.2. Communicatie tussen de externe GNSS-module en de voertuigunit 409

4.2.1 Communicatieprotocol 409

4.2.2 Beveiligde GNSS-gegevensoverdracht 411

4.2.3 Structuur van het Read Record-commando 412

4.3. Koppeling, wederzijdse authenticatie en sleutelovereenstemming tijdens de sessie tussen de externe GNSS-module en de voertuigunit 413

4.4. Behandeling van fouten 413

4.4.1 Fout in communicatie met de externe GNSS-module 413

4.4.2 Aantasting van de fysieke integriteit van de externe GNSS-module 413

4.4.3 Afwezigheid van positie-informatie van de GNSS-ontvanger 413

4.4.4 Geldigheidsduur certificaat van de externe GNSS-module verstreken 414

5. VOERTUIGUNIT ZONDER EXTERNE GNSS-MODULE 414

5.1. Configuratie 414

5.2. Behandeling van fouten 414

5.2.1 Afwezigheid van positie-informatie van de GNSS-ontvanger 414

6. TEGENSTRIJDIGE GNSS-TIJDGEGEVENS 414

7. TEGENSTRIJDIGE BEWEGINGSGEGEVENS 415

1. INLEIDING

Dit aanhangsel bevat de technische voorschriften voor de door de voertuigunit gebruikte GNSS-gegevens, met inbegrip van de protocollen die moeten worden toegepast om een veilige en correcte overdracht van plaatsbepalingsinformatie te waarborgen.

Deze voorschriften vinden hun grondslag in de volgende belangrijke artikelen van deze Verordening (EU) nr. 165/2014: artikel 8 „Registratie van de positie van het voertuig op bepaalde momenten tijdens de dagelijkse werktijd", artikel 10 „Interface met intelligente vervoerssystemen" en artikel 11 „Gedetailleerde bepalingen voor de slimme tachograaf".

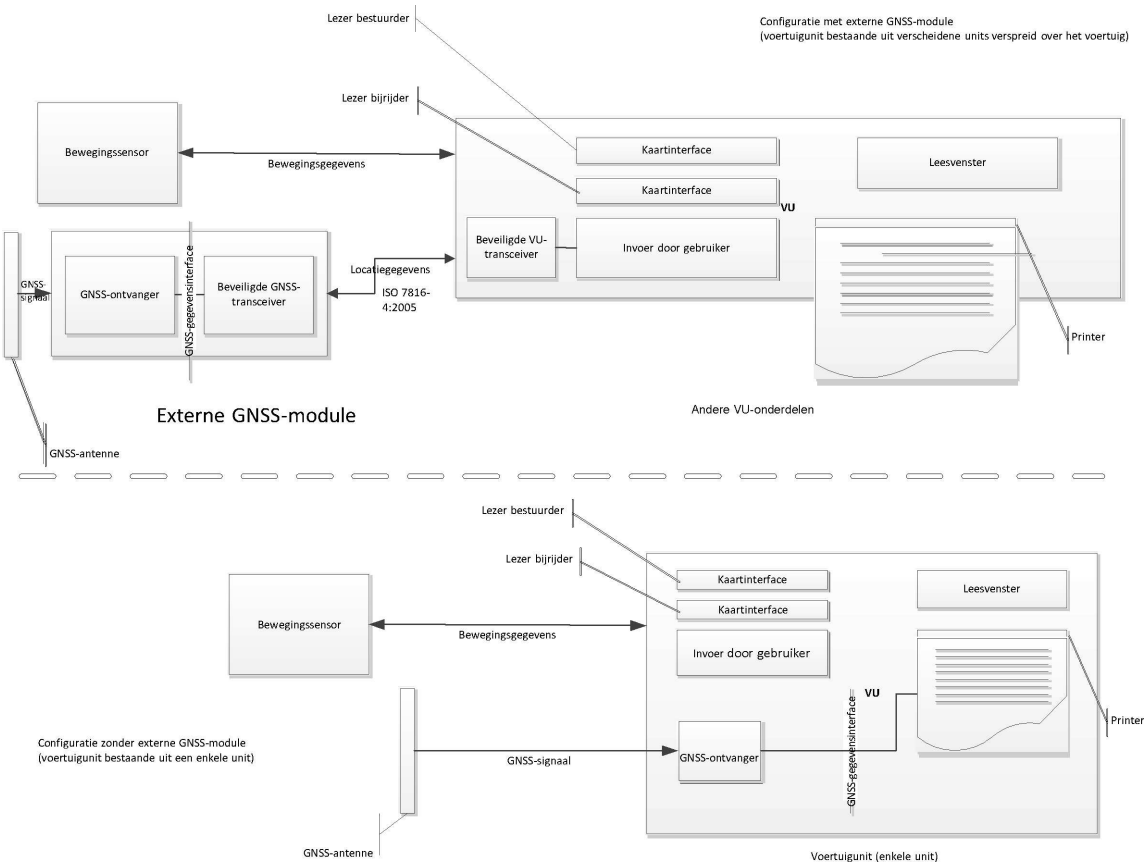
1.1. **Toepassingsgebied**

GNS_1 Ter ondersteuning van de uitvoering van artikel 8 verzamelt de voertuigunit (VU) locatiegegevens van ten minste één GNSS.

Zoals wordt verduidelijkt in Figuur 1, kan de voertuigunit al dan niet met een externe GNSS-module uitgerust zijn:

Figuur 1

Configuratiemogelijkheden voor de GNSS-ontvanger



1.2. **Acroniemen en notaties**

De onderstaande acroniemen worden in dit aanhangsel gebruikt:

DOP Dilution of Precision (verzwakking van nauwkeurigheid)

EGF Externe GNSS-module

EGNOS European Geostationary Navigation Overlay Service (Europees overlaysysteem voor geostationaire navigatie)

GNSS Global Navigation Satellite System (wereldwijd satellietnavigatiesysteem)

GSA GPS DOP en actieve satellieten

HDOP Horizontal Dilution of Precision (verzwakking van horizontale nauwkeurigheid)

ICD Interfacebesturingsdocument

NMEA National Marine Electronics Association

PDOP Position Dilution of Precision (verzwakking van positienauwkeurigheid)

RMC Recommended Minimum Specific (aanbevolen minimale specifieke [GNSS-gegevens])

SIS Signal in Space (ruimtesignaal)

VDOP Vertical Dilution of Precision (verzwakking van verticale nauwkeurigheid)

VU Voertuigunit

2. SPECIFICATIE VAN DE GNSS-ONTVANGER

Ongeacht de configuratie van de slimme tachograaf, met of zonder externe GNSS-module, is het verstrekken van nauwkeurige en betrouwbare plaatsbepalingsinformatie een essentieel onderdeel van de effectieve werking van de slimme tachograaf. Het systeem moet dan ook compatibel zijn met de door de Galileo- en Egnos-programma's geboden diensten, zoals uiteengezet in Verordening (EU) nr. 1285/2013 van het Europees Parlement en de Raad [1]. Het in het kader van het Galileo-programma ontwikkelde systeem is een onafhankelijk wereldwijd satellietnavigatiesysteem en het in het kader van het Egnos-programma ingestelde systeem is een regionaal satellietnavigatiesysteem dat de kwaliteit van het signaal van het global positioning system verbetert.

GNS_2 De fabrikanten zien erop toe dat de GNSS-ontvangers in de slimme tachografen compatibel zijn met de plaatsbepalingsdiensten van de systemen Galileo en Egnos. De fabrikanten kunnen voorts ook kiezen voor compatibiliteit met andere satellietnavigatiesystemen.

GNS_3 De GNSS-ontvanger ondersteunt authenticatie van de open dienst die wordt aangeboden door het in het kader van het Galileo-programma ingestelde systeem, zodra dit beschikbaar is en door de fabrikanten van GNSS-ontvangers wordt ondersteund. Voor slimme tachografen die op de markt zijn gebracht vóór aan de bovenstaande voorwaarden is voldaan en die de authenticatie van de open dienst van Galileo niet ondersteunen, is retrofitting niet vereist.

3. NMEA-ZINNEN

In dit gedeelte wordt een beschrijving gegeven van de NMEA-zinnen die voor de werking van de slimme tachograaf worden gebruikt. Dit gedeelte geldt voor de configuratie van de slimme tachograaf, zowel met als zonder externe GNSS-module.

GNS_4 De locatiegegevens berusten op de aanbevolen minimale specifieke (RMC) GNSS-gegevens van de NMEA-zin, bestaande uit de positie-informatie (breedte- en lengtegraad), de UTC-tijd (gecoördineerde wereldtijd) in het formaat hhmmss.ss, de in knopen uitgedrukte snelheid over de grond (SOG) alsook op extra waarden.

De RMC-zin heeft de volgende notatie (vanaf NMEA-standaard V4.1):

[1] Verordening (EU) nr. 1285/2013 van het Europees Parlement en de Raad van 11 december 2013 betreffende de uitvoering en exploitatie van de Europese satellietnavigatiesystemen en tot intrekking van Verordening (EG) nr. 876/2002 van de Raad en Verordening (EG) nr. 683/2008 van het Europees Parlement en de Raad (PB L 347 van 20.12.2013, blz. 1).

Figuur 2

Opbouw van de RMC-zin

1) Time (UTC)
2) Status, A = Valid position, V = Warning
3) Latitude
4) N or S
5) Longitude
6) E or W
7) Speed over ground in knots
8) Track made good, degrees true
9) Date, ddmmyy
10) Magnetic Variation, degrees
11) E or W
12) Checksum

De status geeft aan of het GNSS-signaal beschikbaar is. Zolang de statuswaarde verschilt van „A", kunnen de ontvangen gegevens (bijvoorbeeld de tijd of breedte-/lengtegraad) niet worden gebruikt om de voertuigpositie te registreren in de VU.

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 (breedtegraad voor veld 3 en lengtegraad voor veld 5). 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).

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.

De GNSS-systeemidentificatie staat voor GPS, Glonass, Galileo, Beidou of Satellite-Based Augmentation System (SBAS — satellietaugmentatiesysteem).

Figuur 3

Opbouw van de GSA-zin

1) Selectiemodus
2) Modus
3) Identificatie van eerste satelliet voor positiebepaling
4) Identificatie van tweede satelliet voor positiebepaling
...
14) Identificatie van twaalfde satelliet voor positiebepaling
15) PDOP in meter
16) HDOP in meter
17) VDOP in meter
18) GNSS-systeemidentificatie
19) Controlesom

De modus (veld 2) geeft het volgende aan: geen positiebepaling („fix") beschikbaar (modus = 1), tweedimensionale (2D) positiebepaling beschikbaar (modus = 2) of driedimensionale (3D) positiebepaling (modus = 3) beschikbaar.

GNS_6 De GSA-zin wordt opgeslagen onder recordnummer '06'.

GNS_7 De maximumgrootte van de NMEA-zinnen (bijvoorbeeld RMC-zinnen, GSA-zinnen e.d.) om het formaat van het Read Record-commando aan te passen, bedraagt 85 bytes (zie Tabel 1).

4. VOERTUIGUNIT MET EXTERNE GNSS-MODULE

4.1. **Configuratie**

4.1.1 *Belangrijkste onderdelen en interfaces*

In deze configuratie maakt de GNSS-ontvanger deel uit van de externe GNSS-module.

GNS_8 De externe GNSS-module moet van stroom worden voorzien via een specifieke voertuiginterface.

GNS_9 De externe GNSS-module bestaat uit de volgende onderdelen (zie Figuur 4):

a) Een commerciële GNSS-ontvanger die de positiegegevens verstrekt via de GNSS-gegevensinterface. De GNSS-gegevensinterface kan bijvoorbeeld vallen onder NMEA-standaard V4.10, waarbij de GNSS-ontvanger functioneert als zender en NMEA-zinnen verstuurt naar de beveiligde GNSS-transceiver. De zendfrequentie bedraagt 1 Hz voor de vooraf gedefinieerde reeks NMEA-zinnen, die ten minste de RMC- en GSA-zinnen moeten bevatten. De keuze van de GNSS-gegevensinterface wordt overgelaten aan de fabrikant van de externe GNSS-module.

b) Een zendontvanger (beveiligde GNSS-transceiver) die voldoet aan de norm ISO/IEC 7816-4:2013 (zie 4.2.1) om te communiceren met de voertuigunit en ondersteuning te bieden aan de GNSS-gegevens-interface met de GNSS-ontvanger. De transceiver heeft een geheugen om de identificatiegegevens van de GNSS-ontvanger en de externe GNSS-module op te slaan.

c) Een behuizing (systeemkast) voor de GNSS-ontvanger en de beveiligde GNSS-transceiver, uitgerust met een functie om manipulatie te detecteren. In de functie om manipulatie te detecteren worden de beveiligingsmaatregelen toegepast die zijn voorgeschreven in het beschermingsprofiel van de slimme tachograaf.

d) Een op het voertuig gemonteerde GNSS-antenne die via de systeemkast verbonden is met de GNSS-ontvanger.

GNS_10 De externe GNSS-module is ten minste uitgerust met de volgende externe interfaces:

a) de interface met de op het voertuig gemonteerde GNSS-antenne, voor zover een externe antenne wordt gebruikt;

b) de interface met de voertuigunit.

GNS_11 De beveiligde VU-transceiver is het andere eindpunt van het communicatiesysteem met de beveiligde GNSS-transceiver; deze moet voldoen aan ISO/IEC 7816-4:2013 wat de verbinding met de externe GNSS-module betreft.

GNS_12 Voor de fysieke communicatielaag met de externe GNSS-module ondersteunt de voertuigunit ISO/IEC 7816-12:2005 of andere normen die ISO/IEC 7816-4:2013 ondersteunen (zie 4.2.1).

4.1.2 *Status van de externe GNSS-module aan het eind van de productie*

GNS_13 Bij het verlaten van de fabriek slaat de externe GNSS-module de volgende waarden op in het niet-vluchtige geheugen van de beveiligde GNSS-transceiver:

— het sleutelpaar EGF_MA met bijbehorend certificaat;

— het certificaat MSCA_VU-EGF met de openbare sleutel MSCA_VU-EGF.PK ter verificatie van het certificaat EGF_MA;

— het EUR-certificaat met de openbare sleutel EUR.PK ter verificatie van het certificaat MSCA_VU-EGF;

— het EUR-certificaat waarvan de geldigheidsduur onmiddellijk voorafgaat aan die van het EUR-certificaat ter verificatie van het certificaat MSCA_VU-EGF (indien bestaand);

— het verbindingscertificaat dat beide EUR-certificaten met elkaar in verband brengt (indien bestaand);

— het verlengde serienummer van de externe GNSS-module;

— de identificator van het besturingssysteem (OS — Operating System) van de GNSS-module;

— het typegoedkeuringsnummer van de externe GNSS-module;

— de identificator van de beveiligingscomponent van de externe GNSS-module.

4.2. **Communicatie tussen de externe GNSS-module en de voertuigunit**

4.2.1 *Communicatieprotocol*

GNS_14 Het communicatieprotocol tussen de externe GNSS-module en de voertuigunit ondersteunt drie functies:

1. de verzameling en verspreiding van GNSS-gegevens (bijvoorbeeld positie, tijd en snelheid);

2. de verzameling van de configuratiegegevens van de externe GNSS-module;

3. het beheerprotocol ter ondersteuning van de koppeling, wederzijdse authenticatie en sleutelovereenstemming tijdens de sessie tussen de externe GNSS-module en de VU.

GNS_15 Het communicatieprotocol is gebaseerd op de norm ISO/IEC 7816-4:2013, waarbij de beveiligde VU-transceiver de rol van *master* en de beveiligde GNSS-transceiver die van *slave* vervult. De fysieke verbinding tussen de externe GNSS-module en de voertuigunit is gebaseerd op ISO/IEC 7816-12:2005 of andere normen die ISO/IEC 7816-4:2013 ondersteunen.

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

GNS_17 Het communicatieprotocol van ISO 7816 (zowel *-4:2013 als *-12:2005) tussen de externe GNSS-module en de VU wordt ingesteld op T = 1.

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 toepassingsidentificator 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 identificator gelijk is aan '2F2F', zoals beschreven in Tabel 1.

GNS_19 De beveiligde GNSS-transceiver slaat de gegevens van de GNSS-ontvanger en de configuratie op in het hoofdbestand EF.EGF. Dit is een lineair recordbestand met variabele lengte en met als identificator '2F2F' in hexadecimale notatie.

GNS_20 De beveiligde GNSS-transceiver slaat de gegevens op in een geheugen dat ten minste 20 miljoen lees-/schrijfcycli kan 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 vier GSA-zinnen voor de vier satellietsystemen en het satellietaugmentatiesysteem (SBAS).

GNS_21 De bestandsstructuur wordt verduidelijkt in Tabel 1. De toegangscondities (ALW, NEV, SM-MAC) zijn te vinden in aanhangsel 2, punt 3.5.

Tabel 1

Bestandsstructuur

		Toegangscondities (AC)		
Bestand	Bestandsidentificatie	Lezen	Bijwerken	Gecodeerd
MF	3F00			
EF.ICC	0002	ALW	NEV (door VU)	Neen
DF GNSS-module	0501	ALW	NEV	Neen
EF EGF_MA_Certificate	C100	ALW	NEV	Neen
EF CA_Certificate	C108	ALW	NEV	Neen
EF Link_Certificate	C109	ALW	NEV	Neen
EF.EGF	2F2F	SM-MAC	NEV (door VU)	Neen

Bestand/gegevenselement	Record-nummer	Grootte (in bytes)		Standaard-waarden
		Min.	Max.	
MF		552.	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF GNSS-module		*612*	*1 023*	
EF EGF_MA_Certificate		*204*	*341*	
EGFCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF.EGF				
NMEA RMC-zin	‘01’	85	85	
Eerste NMEA GSA-zin	‘02’	85	85	
Tweede NMEA GSA-zin	‘03’	85	85	

Bestand/gegevenselement	Record-nummer	Grootte (in bytes)		Standaard-waarden
		Min.	Max.	
Derde NMEA GSA-zin	'04'	85	85	
Vierde NMEA GSA-zin	'05'	85	85	
Vijfde NMEA GSA-zin	'06'	85	85	
Verlengd serienummer van de externe GNSS-module, in aanhangsel 1 gedefinieerd als SensorGNSSSerialNumber	'07'	8	8	
Identificator van het besturingssysteem van de beveiligde GNSS-transceiver, in aanhangsel 1 gedefinieerd als SensorOSIdentifier	'08'	2	2	
Typegoedkeuringsnummer van de externe GNSS-module, in aanhangsel 1 gedefinieerd als SensorExternalGNSSApprovalNumber	'09'	16	16	
Identificatiesymbool van de beveiligingscomponent van de externe GNSS-module, in aanhangsel 1 gedefinieerd als SensorExternalGNSSSCIdentifier	'10'	8	8	
RFU — Gereserveerd voor toekomstig gebruik	'11' t/m 'FD'			

4.2.2 *Beveiligde GNSS-gegevensoverdracht*

GNS_22 De beveiligde overdracht van GNSS-positiegegevens kan alleen plaatsvinden onder de volgende voorwaarden:

1. Het koppelingsproces is voltooid zoals beschreven in aanhangsel 11 „Algemene veiligheidsmechanismen".

2. De periodieke wederzijdse authenticatie en sleutelovereenstemming tijdens de sessie tussen de VU en de externe GNSS-module (zie beschrijving in aanhangsel 11 „Algemene veiligheidsmechanismen") werden met voldoende regelmaat uitgevoerd.

GNS_23 Tenzij de koppeling of wederzijdse authenticatie en sleutelovereenstemming tijdens de sessie plaatsvindt, vraagt de VU iedere T seconden — waarbij T een waarde is kleiner dan of gelijk aan 10 — de positie-informatie op van de externe GNSS-module. Dit proces verloopt als volgt:

1. De VU vraagt locatiegegevens op van de externe GNSS-module, samen met de DOP-waarden (mate van onnauwkeurigheid, gebaseerd op de GSA NMEA-zin). De beveiligde VU-transceiver gebruikt de Select- en Read Record-commando's van de norm ISO/IEC 7816-4:2013 voor beveiligde berichtenuitwisseling in alleen-authenticeren-modus, zoals beschreven in punt 11.5 van aanhangsel 11; de bestandsidentificator is '2F2F' en het recordnummer is '01' voor de NMEA RMC-zin en '02', '03', '04', '05', '06' voor de NMEA GSA-zin.

2. De laatste ontvangen locatiegegevens worden in het hoofdbestand (EF) opgeslagen met de identificator '2F2F'. De in Tabel 1 omschreven records worden opgeslagen in de beveiligde GNSS-transceiver naarmate die via de GNSS-interface NMEA-gegevens met een frequentie van ten minste 1 Hz ontvangt van de GNSS-ontvanger.

3. De beveiligde GNSS-transceiver verstuurt het antwoord naar de beveiligde VU-transceiver en gebruikt daarvoor het APDU-antwoordbericht met beveiligde berichtenuitwisseling in alleen-authenticeren-modus, zoals toegelicht in punt 11.5 van aanhangsel 11.

4. De beveiligde VU-transceiver controleert de authenticiteit en integriteit van het ontvangen antwoord. Bij een positieve uitkomst worden de locatiegegevens via de GNSS-interface overgebracht naar de verwerkingseenheid van de VU.

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 gemiddelde waarde voor de beschikbare satellietsystemen berekend (voor zover positiebepaling mogelijk is).

6. De verwerkingseenheid van de VU slaat de ontvangen en verwerkte informatie, zoals breedtegraad, lengtegraad, tijd en snelheid, op in het in aanhangsel 1 „Data Dictionary" vastgestelde formaat als geografische coördinaten samen met de HDOP-waarde, berekend als minimum van de voor de beschikbare GNSS-systemen verzamelde HDOP-waarden.

4.2.3 *Structuur van het Read Record-commando*

In dit gedeelte wordt een uitvoerige beschrijving gegeven van de structuur van het Read Record-commando. Daarbij komt ook de beveiligde berichtenuitwisseling (in alleen-authenticeren-modus) aan bod, zoals beschreven in aanhangsel 11 „Algemene beveiligingsmechanismen".

GNS_24 Het commando ondersteunt de beveiligde berichtenuitwisseling in alleen-authenticeren-modus (zie aanhangsel 11).

GNS_25 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'0Ch'	Beveiligde berichtenuitwisseling gevraagd
INS	1	'B2h'	Record lezen
P1	1	'XXh'	Recordnummer ('00' verwijst naar de huidige record)
P2	1	'04h'	Record lezen waarvan het nummer in P1 staat
Le	1	'XXh'	Lengte van verwachte gegevens. Aantal te lezen bytes

GNS_26 De in P1 aangeduide record wordt de geldige record.

Byte	Lengte	Waarde	Omschrijving
#1-#X	X	'XX..XXh'	Gelezen gegevens
SW	2.	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de beveiligde GNSS-transceiver '**9000**' terug.

— Indien het huidige bestand niet recordgeoriënteerd is, zendt de beveiligde GNSS-transceiver '**6981**' terug.

— Indien het commando wordt gebruikt met P1 = '00' terwijl er geen geldig hoofdbestand (EF) is, zendt de beveiligde GNSS-transceiver '**6986**' terug (commando niet toegestaan).

— Indien de record niet wordt gevonden, zendt de beveiligde GNSS-transceiver '**6A83**' terug.

— Indien manipulatie werd vastgesteld, zendt de externe GNSS-module de statuswoorden '**6690**' terug.

GNS_27 De beveiligde GNSS-transceiver ondersteunt de volgende commando's van tachografen van de tweede generatie:

Commando	Verwijzing
Select (Selecteer)	Aanhangsel 2, punt 3.5.1
Read Binary (Lees binair getal)	Aanhangsel 2, punt 3.5.2
Get Challenge (Vraag naar identiteit)	Aanhangsel 2, punt 3.5.4
PSO: Verify Certificate (Verifieer certificaat)	Aanhangsel 2, punt 3.5.7
External Authenticate (Externe authenticatie)	Aanhangsel 2, punt 3.5.9
General Authenticate (Algemene authenticatie)	Aanhangsel 2, punt 3-5-2010
MSE:SET	Aanhangsel 2, punt 3-5-2011

4.3. **Koppeling, wederzijdse authenticatie en sleutelovereenstemming tijdens de sessie tussen de externe GNSS-module en de voertuigunit**

In hoofdstuk 11 van aanhangsel 11 „Algemene veiligheidsmechanismen" wordt een beschrijving gegeven van de koppeling, wederzijdse authenticatie en sleutelovereenstemming tijdens de sessie tussen de externe GNSS-module en de voertuigunit.

4.4. **Behandeling van fouten**

In dit gedeelte wordt uiteengezet hoe mogelijke fouttoestanden van de externe GNSS-module worden behandeld en geregistreerd in de VU.

4.4.1 *Fout in communicatie met de externe GNSS-module*

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 '53'H *External GNSS communication fault* (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.

4.4.2 *Aantasting van de fysieke integriteit van de externe GNSS-module*

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 '*55'H Tamper detection of GNSS* (Manipulatie GNSS gedetecteerd).

4.4.3 *Afwezigheid van positie-informatie van de GNSS-ontvanger*

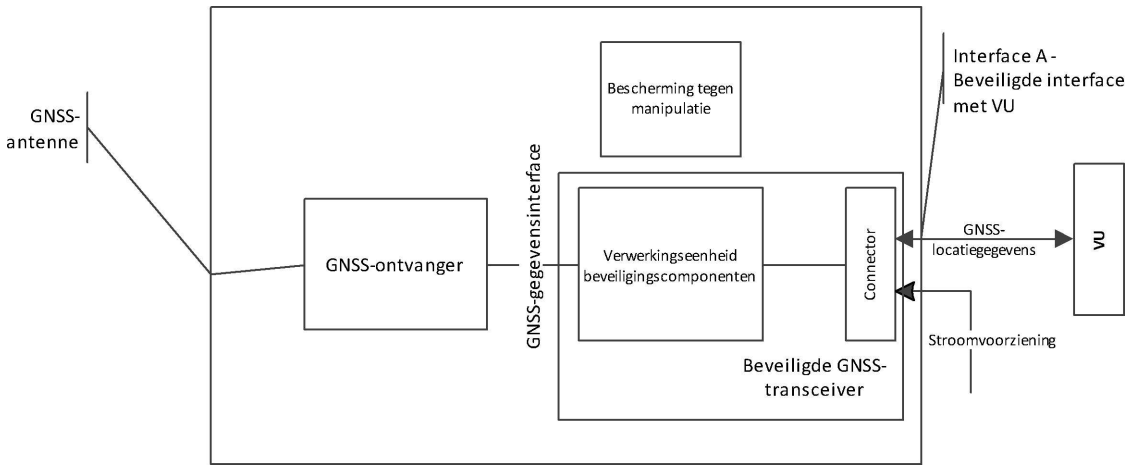
GNS_30 Indien gedurende ten minste drie aaneengesloten uren geen gegevens van de GNSS-ontvanger worden ontvangen, genereert de beveiligde GNSS-transceiver een antwoordbericht op het Read Record-commando waarvan het recordnummer gelijk is aan '01' en met een gegevensveld van 12 bytes, allemaal ingesteld 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 '52'H *External GNSS receiver fault (Fout externe 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.

4.4.4 *Geldigheidsduur certificaat van de externe GNSS-module verstreken*

GNS_31 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 controleapparaatfout van het type EventFaultType met de enum-waarde *'56'H 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.

Figuur 4

Overzicht van de externe GNSS-module



5. VOERTUIGUNIT ZONDER EXTERNE GNSS-MODULE

5.1. Configuratie

In deze configuratie bevindt de GNSS-ontvanger zich binnen de voertuigunit, zoals omschreven in Figuur 1.

GNS_32 De GNSS-ontvanger functioneert als zender en verstuurt NMEA-zinnen naar de verwerkingseenheid van de VU, die functioneert als ontvanger. De zendfrequentie bedraagt 1/10 Hz of meer voor de vooraf gedefinieerde reeks NMEA-zinnen, die ten minste de RMC- en GSA-zinnen moeten bevatten.

GNS_33 Een op het voertuig gemonteerde externe GNSS-antenne of een ingebouwde GNSS-antenne wordt aangesloten op de VU.

5.2. Behandeling van fouten

5.2.1 *Afwezigheid van positie-informatie van de GNSS-ontvanger*

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 '51'H *Internal GNSS receiver fault (Fout ingebouwde 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.

6. TEGENSTRIJDIGE GNSS-TIJDGEGEVENS

Indien een verschil van meer dan één minuut wordt vastgesteld tussen de door de tijdmetingsfunctie 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 *'0B'H Time conflict (GNSS versus VU internal clock) (Tegenstrijdige tijdgegevens tussen GNSS en interne klok VU)*. Dit voorval wordt geregistreerd samen met de waarde van de interne klok van de voertuigunit, en gaat gepaard met een automatische tijdafstelling. Nadat een voorval van tegenstrijdige tijdgegevens werd gestart, voert de VU de eerstvolgende twaalf uren geen controle op tijdverschillen uit. Dit voorval wordt niet gestart indien de GNSS-ontvanger gedurende de afgelopen dertig dagen geen geldig GNSS-signaal heeft kunnen detecteren. Zodra echter opnieuw positie-informatie van de GNSS-ontvanger beschikbaar is, wordt de automatische tijdafstelling uitgevoerd.

7. TEGENSTRIJDIGE BEWEGINGSGEGEVENS

GNS_35 Indien de berekeningsinformatie van de bewegingssensor wordt tegengesproken door die van de interne GNSS-ontvanger of van de externe GNSS-module, start en registreert de VU een voorval van tegenstrijdige bewegingsgegevens (zie voorschrift 84 in deze bijlage) waarvan de tijdaanduiding gelijk is aan de huidige tijd. Tegenstrijdige bewegingsgegevens worden opgespoord op basis van de mediaan van de verschillen in de door deze bronnen gemeten snelheid, zoals hieronder gespecificeerd:

— Maximaal één keer per 10 seconden wordt de absolute waarde berekend van het verschil tussen de via GNSS geraamde voertuigsnelheid en de door de bewegingssensor geraamde voertuigsnelheid.

— De mediaan wordt berekend op basis van alle waarden binnen een tijdvenster dat de voertuigbeweging over de laatste vijf minuten bestrijkt.

— De mediaan wordt berekend als gemiddelde van 80 % van de betreffende snelheidswaarden, na eliminatie van de hoogste absolute waarden.

Het voorval van tegenstrijdige bewegingsgegevens wordt gestart indien de mediaan van de snelheidsverschillen gedurende vijf ononderbroken minuten groter is dan 10 km/h. Er mag facultatief gebruik worden gemaakt van andere onafhankelijke bronnen van bewegingsinformatie, met het doel (pogingen tot) manipulatie van de tachograaf op een meer betrouwbare wijze te detecteren. (*Opmerking:* door de mediaan over de laatste vijf minuten te berekenen, wordt het risico van uitschieters en tijdelijk afwijkende meetwaarden tegengegaan). Dit voorval wordt niet gestart in de volgende omstandigheden: a) tijdens vervoer per veerboot/trein, b) indien geen positie-informatie van de GNSS-ontvanger beschikbaar is en c) in kalibreringsmodus.

Aanhangsel 13

ITS-INTERFACE

INHOUD

1. INLEIDING 416

2. TOEPASSINGSGEBIED 416

2.1. Acroniemen, definities en notaties 417

3. REFERENTIEVERORDENINGEN EN -NORMEN 418

4. WERKINGSBEGINSELEN VAN DE INTERFACE 418

4.1. Eerste vereisten voor gegevensoverdracht via de ITS-interface 418

4.1.1 Via de ITS-interface beschikbaar gestelde gegevens 418

4.1.2 Gegevensinhoud 418

4.1.3 ITS-toepassingen 418

4.2. Communicatietechnologie 419

4.3. Pincodeverificatie 419

4.4. Berichtformaat 421

4.5. Toestemming van de bestuurder 425

4.6. Standaardgegevens opvragen 426

4.7. Persoonsgegevens opvragen 426

4.8. Fout- en voorvalgegevens opvragen 426

1. INLEIDING

In dit aanhangsel worden de ontwerpspecificaties en toepasselijke procedures uiteengezet ter implementatie van de interface met intelligente vervoerssystemen (ITS), zoals voorgeschreven in artikel 10 van Verordening (EU) nr. 165/2014 (tachograafverordening).

Deze verordening bepaalt dat de tachografen van voertuigen mogen worden uitgerust met een gestandaardiseerde interface die het gebruik in operationele modus van de door de tachograaf geregistreerde of verstrekte gegevens door een extern apparaat mogelijk maakt, mits aan de volgende voorwaarden is voldaan:

a) de interface doet geen afbreuk aan de authenticiteit en de integriteit van de gegevens van de tachograaf;

b) de interface voldoet aan de gedetailleerde bepalingen in artikel 11 van de tachograafverordening;

c) het externe apparaat dat is aangesloten op de interface krijgt alleen toegang tot de persoonsgegevens, inclusief positioneringsgegevens, na verifieerbare toestemming van de bestuurder op wie de gegevens betrekking hebben.

2. TOEPASSINGSGEBIED

Dit aanhangsel beoogt nader te omschrijven hoe toepassingen die zich op externe apparaten bevinden, via een Bluetooth®-verbinding gegevens van een tachograaf kunnen verkrijgen.

In bijlage 1 bij dit aanhangsel staat een beschrijving van de gegevens die via deze interface beschikbaar zijn. Deze interface verhindert niet de implementatie van andere interfaces (bijvoorbeeld via de CAN-bus) om de gegevens van de voertuigunit (VU) naar de verwerkingseenheden van andere voertuigen te verzenden.

Dit aanhangsel bevat specificaties met betrekking tot:

— de gegevens die beschikbaar zijn via de ITS-interface;

— het Bluetooth®-profiel dat wordt gebruikt om de gegevens over te brengen;

— de opvraag- en downloadprocedures en de volgorde van bewerkingen;

— het koppelingsmechanisme tussen de tachograaf en het externe apparaat;

— het toestemmingsmechanisme waarover de bestuurder beschikt.

Voor alle duidelijkheid: deze bijlage 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 tachograafverordening 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 gegevensinhoud (die elders in de tachograafverordening worden gespecificeerd [aanhangsel 10 „Algemene beveiligingsmechanismen"]);

— de door de ITS-interface gebruikte Bluetooth®-protocollen.

2.1. **Acroniemen, definities en notaties**

In dit aanhangsel worden de volgende acroniemen en definities gebruikt in de daarachter vermelde betekenis:

communicatie	uitwisseling van informatie/gegevens tussen een hoofdunit (dat wil zeggen de tachograaf) en een externe unit via de ITS-interface met gebruikmaking van Bluetooth®;
gegevens	de in bijlage 1 gespecificeerde datasets;
tachograafverordening	Verordening (EU) nr. 165/2014 van het Europees Parlement en van de Raad van 4 februari 2014 betreffende tachografen in het wegvervoer, tot intrekking van Verordening (EEG) nr. 3821/85 van de Raad betreffende het controleapparaat in het wegvervoer en tot wijziging van Verordening (EG) nr. 561/2006 van het Europees Parlement en de Raad tot harmonisatie van bepaalde voorschriften van sociale aard voor het wegvervoer;
BR	Basissnelheid
EDR	Verhoogde gegevenssnelheid
GNSS	Wereldwijd satellietnavigatiesysteem
IRK	Sleutel ter vaststelling van de identiteit
ITS	Intelligent vervoerssysteem
LE	Lage energie
PIN	Persoonlijk identificatienummer (pincode)
PUC	Persoonlijke ontgrendelingscode
SID	Identificator van de dienst
SPP	Serieel poortprofiel
SSP	Secure Simple Pairing
TRTP	Overdrachtparameter verzoek
TREP	Overdrachtparameter antwoord
VU	Voertuigunit

3. REFERENTIEVERORDENINGEN EN -NORMEN

De in dit aanhangsel vastgestelde specificatie verwijst naar en wordt geregeld door de hierna genoemde verordeningen en normen of gedeelten daarvan. In de bepalingen van dit aanhangsel wordt uitdrukkelijk aangegeven welke normen of clausules daarvan toepassing vinden. In geval van tegenstrijdigheid prevaleren de bepalingen in dit aanhangsel.

In dit aanhangsel wordt verwezen naar de volgende verordeningen en normen:

— Verordening (EU) nr. 165/2014 van het Europees Parlement en van de Raad van 4 februari 2014 betreffende tachografen in het wegvervoer, tot intrekking van Verordening (EEG) nr. 3821/85 van de Raad betreffende het controleapparaat in het wegvervoer en tot wijziging van Verordening (EG) nr. 561/2006 van het Europees Parlement en de Raad tot harmonisatie van bepaalde voorschriften van sociale aard voor het wegvervoer

— Verordening (EG) nr. 561/2006 van het Europees Parlement en de Raad van 15 maart 2006 tot harmonisatie van bepaalde voorschriften van sociale aard voor het wegvervoer, tot wijziging van Verordeningen (EEG) nr. 3821/85 en (EG) nr. 2135/98 van de Raad en tot intrekking van Verordening (EEG) nr. 3820/85 van de Raad

— ISO 16844 — 4: Road vehicles — Tachograph systems — Part 4: CAN interface

— ISO 16844 — 7: Road vehicles — Tachograph systems — Part 7: Parameters

— Bluetooth® — Serial Port Profile — V1.2

— Bluetooth®– Core Version 4.2

— NMEA 0183 V4.1-protocol

4. WERKINGSBEGINSELEN VAN DE INTERFACE

4.1. **Eerste vereisten voor gegevensoverdracht via de ITS-interface**

De VU dient de gegevens die in de VU moeten worden opgeslagen, te actualiseren en bij te houden zonder tussenkomst van de ITS-interface. De daartoe gebruikte middelen hangen af van het interne ontwerp van de VU, zoals elders gespecificeerd in de tachograafverordening, en worden niet nader gespecificeerd in dit aanhangsel.

4.1.1 *Via de ITS-interface beschikbaar gestelde gegevens*

De VU dient de via de ITS-interface beschikbaar gestelde gegevens te actualiseren met een regelmaat die in de VU-procedures wordt vastgesteld, zonder tussenkomst van de ITS-interface. De VU-gegevens worden gebruikt als uitgangspunt voor het samenstellen en actualiseren van de gegevens. De daartoe gebruikte middelen worden elders in de tachograafverordening gespecificeerd; bij gebrek aan ter zake dienende specificaties hangen deze middelen af van het productontwerp en worden zij niet nader omschreven in dit aanhangsel.

4.1.2 *Gegevensinhoud*

De gegevensinhoud wordt nader omschreven in bijlage 1 bij dit aanhangsel.

4.1.3 *ITS-toepassingen*

De via de ITS-interface beschikbaar gestelde gegevens worden gebruikt door ITS-toepassingen, bijvoorbeeld om de activiteiten van de bestuurder optimaal te beheren met inachtneming van de tachograafverordening, om eventuele fouten in de tachograaf op te sporen of om de GNSS-gegevens te gebruiken. De specificatie van deze toepassingen valt buiten het toepassingsgebied van dit aanhangsel.

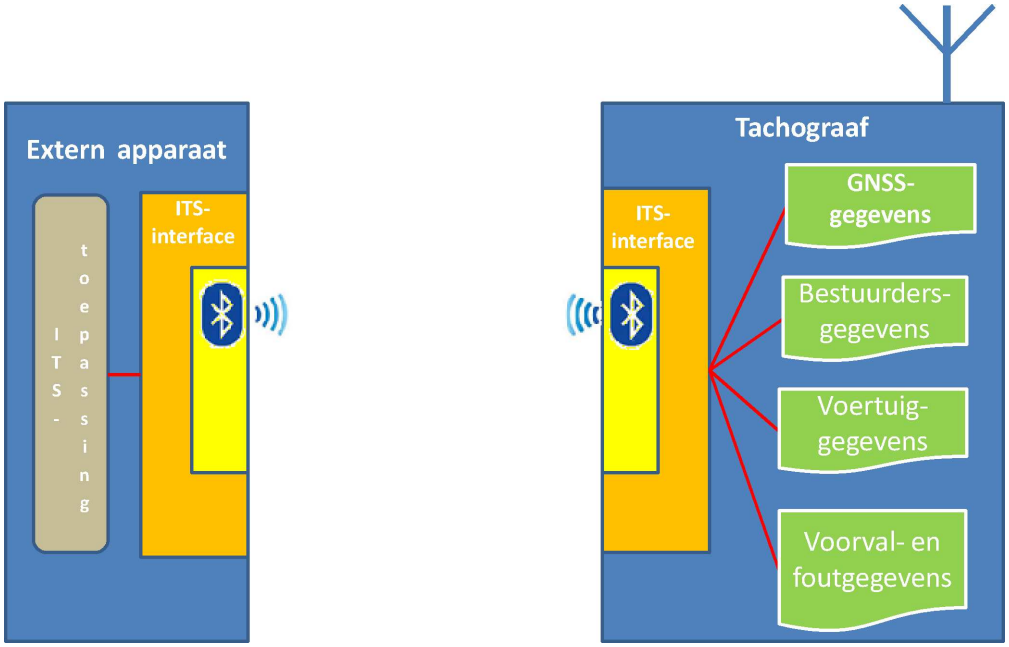
4.2. **Communicatietechnologie**

De gegevens worden door middel van de ITS-interface uitgewisseld via een compatibele Bluetooth®-interface van versie 4.2 of hoger. Bluetooth® werkt in een licentievrije frequentieband voor industriële, wetenschappelijk en medische doeleinden (ISM-band) van 2,4 tot en met 2,485 GHz. Bluetooth® 4.2 biedt niet alleen verbeterde mechanismen voor informatiebeveiliging en privacybescherming, maar verhoogt ook de snelheid en betrouwbaarheid van de gegevensoverdracht. Ten behoeve van deze specificatie wordt Bluetooth® klasse 2-radioapparatuur gebruikt met een bereik tot 10 m. Meer informatie over Bluetooth® 4.2 is te vinden op www.Bluetooth.1?>www.Bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676 (https://www.Bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

De communicatie wordt tot stand gebracht door middel van de communicatieapparatuur na voltooiing van een koppelingsprocedure met een goedgekeurd apparaat. Bluetooth® gebruikt een master-slavemodel om te controleren wanneer en waar apparaten gegevens kunnen verzenden. Bijgevolg vervult de tachograaf de rol van *master* en het externe apparaat die van *slave*.

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 10 „Algemene beveiligingsmechanismen”.

De communicatie verloopt in principe zoals aangegeven in de onderstaande figuur:



Het seriële poortprofiel (SPP) van Bluetooth® wordt gebruikt om gegevens van de VU over te brengen naar het externe apparaat.

4.3. **Pincodeverificatie**

Om veiligheidsredenen moet de VU een systeem voor pincodeverificatie toepassen 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.

Na het invoeren van de juiste pincode wordt het apparaat op de witte lijst geplaatst. De witte lijst bevat ten minste 64 apparaten die aan de specifieke VU werden gekoppeld.

Na drie opeenvolgende mislukte pogingen om de juiste pincode in te voeren, wordt het apparaat tijdelijk op de zwarte lijst geplaatst. Zolang het apparaat op de zwarte lijst staat, wordt elke toegangspoging geweigerd. Na nogmaals drie opeenvolgende mislukte pogingen om de juiste pincode in te voeren, wordt het apparaat voor langere tijd geblokkeerd (zie tabel 1). Zodra de juiste pincode wordt ingevoerd, worden de blokkeringstijd en het aantal pogingen opnieuw ingesteld. In figuur 1 van bijlage 2 staat een overzicht van de blokkeringstijd als functie van het aantal mislukte invoerpogingen van de pincode.

Tabel 1

Blokkeringstijd als functie van het aantal mislukte invoerpogingen van de pincode

Aantal mislukte invoerpogingen	Blokkeringstijd
3	30 seconden
6	5 minuten
9	1 uur
12	24 uur
15	Voor onbepaalde tijd

Na vijftien (vijf keer drie) opeenvolgende mislukte pogingen om de juiste pincode in te voeren, wordt de ITS-unit voor onbepaalde tijd op de zwarte lijst geplaatst. Deze blokkering voor onbepaalde tijd kan uitsluitend worden opgeheven door de correcte PUC-code in te voeren.

Deze achtcijferige PUC-code wordt door de fabrikant geleverd bij de VU. Na tien opeenvolgende mislukte pogingen om de juiste PUC-code in te voeren, wordt de ITS-unit voorgoed op de zwarte lijst geplaatst.

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.

Bovendien blijven alle apparaten op de witte lijst staan totdat de gebruiker ze handmatig verwijdert (bijvoorbeeld via de mens-machine-interface van de VU of op een andere wijze). Dit maakt het mogelijk om bij verlies of diefstal ITS-units uit de witte lijst te verwijderen. Elke ITS-unit die zich langer dan vierentwintig uur buiten het bereik van de Bluetooth®-verbinding bevindt, wordt automatisch uit de witte lijst van de VU verwijderd en moet opnieuw de juiste pincode invoeren om verbinding te maken.

Het formaat van de tussen de VU-interface en de VU uitgewisselde berichten is niet vastgelegd, maar wordt overgelaten aan de fabrikant. Niettemin moet de fabrikant ervoor zorgen dat het formaat voor de berichtenuitwisseling tussen de ITS-unit en de VU-interface in acht wordt genomen (zie ASN.1-specificaties).

Bijgevolg mag aan een verzoek om gegevensoverdracht pas gevolg worden gegeven nadat de verzender eenduidig is geïdentificeerd. Deze procedure wordt verduidelijkt in figuur 2 van bijlage 2. Elke verbindingspoging van een apparaat dat op de zwarte lijst staat, wordt automatisch geweigerd; voor apparaten die noch op de zwarte lijst, noch op de witte lijst zijn geplaatst, moet een juiste pincode worden ingevoerd voordat het verzoek om gegevensoverdracht wordt verzonden.

4.4. **Berichtformaat**

Alle tussen de ITS-unit en de VU-interface uitgewisselde berichten zijn opgemaakt volgens een uit drie delen bestaande structuur: een koptitel ("header") bestaande uit een doelbyte (TGT), een bronbyte (SRC) en mogelijk een lengtebyte (LEN);

het gegevensveld bestaande uit een identificatiebyte van de dienst (SID) en een variabel aantal gegevensbytes (ten hoogste 255);

de controlesombyte (CS), zijnde de 1-bits somserie module 256 van alle bytes van het bericht exclusief de CS zelf.

Het bericht staat in de bytevolgorde "Big Endian".

Tabel 2

Algemeen berichtformaat

Header			Gegevensveld					Controlesom
TGT	SRC	LEN	SID	TRTP	CC	CM	DATA	CS
3 bytes			Max. 255 bytes					1 byte

Header

TGT- en SRC-byte: de identificatie (ID) van het doelapparaat (TGT) en het bronapparaat (SRC) van het bericht. De ID van de VU-interface is standaard ingesteld op "EE". Deze ID kan niet worden gewijzigd. De ITS-unit gebruikt de standaardidentificatie "A0" voor het eerste bericht van de communicatiesessie. De VU-interface wijst dan een unieke ID toe aan de ITS-unit en geeft deze ID door aan de ITS-unit voor toekomstige berichten tijdens de sessie.

De lengtebyte (LEN) houdt uitsluitend rekening met het "DATA"-onderdeel van het gegevensveld (zie tabel 2); de eerste vier bytes zijn impliciet.

De VU-interface bevestigt de authenticiteit van de verzender van het bericht door de eigen lijst van ID's te vergelijken met de Bluetooth®-gegevens. Daarbij wordt nagegaan of de ITS-unit die voor de opgegeven ID in de lijst staat, zich binnen het bereik van de Bluetooth®-verbinding bevindt.

Gegevensveld

Naast de identificator van de dienst (SID) bevat het gegevensveld ook andere parameters: een overdrachtparameterbyte (TRTP) en tellerbytes.

Indien de lengte van de over te brengen gegevens de beschikbare ruimte van één bericht overschrijdt, 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 overbrenging 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 overbrenging voortijdig beëindigen.

Indien de tellers CC en CM niet worden gebruikt, wordt de waarde ervan ingesteld op "0xFF".

Zo wordt bijvoorbeeld het volgende bericht:

HEADER	SID	TRTP	CC	CM	DATA	CS
3 bytes	Langer dan 255 bytes					1 byte

overgebracht als:

HEADER	SID	TRTP	01	n	DATA	CS
3 bytes	255 bytes					1 byte

HEADER	SID	TRTP	02	n	DATA	CS
3 bytes	255 bytes					1 byte

…

HEADER	SID	TRTP	N	N	DATA	CS
3 bytes	Max. 255 bytes					1 byte

In tabel 3 staan de berichten die de VU en de ITS-unit met elkaar kunnen uitwisselen. De inhoud van elke parameter wordt in hexadecimale notatie voorgesteld. Duidelijkheidshalve worden de tellers CC en CM in deze tabel niet getoond (zie hierboven voor het volledige formaat).

Tabel 3

Gedetailleerde berichtinhoud

Bericht	Header			DATA			Controlesom
	TGT	SRC	LEN	SID	TRTP	DATA	
RequestPIN	*ITSID*	EE	00	01	FF		
SendITSID	*ITSID*	EE	01	02	FF	*ITSID*	
SendPIN	EE	*ITSID*	04	03	FF	4*INTEGER (0..9)	
PairingResult	*ITSID*	EE	01	04	FF	BOOLEAN (T/F)	
SendPUC	EE	*ITSID*	08	05	FF	8*INTEGER (0..9)	
BanLiftingResult	*ITSID*	EE	01	06	FF	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FF	Tijd	
RequestData							
standardTachData	EE	*ITSID*	01	08	01		
personalTachData	EE	*ITSID*	01	08	02		
gnssData	EE	*ITSID*	01	08	03		
standardEventData	EE	*ITSID*	01	08	04		
personalEventData	EE	*ITSID*	01	08	05		
standardFaultData	EE	*ITSID*	01	08	06		
manufacturerData	EE	*ITSID*	01	08	07		

Bericht	Header			DATA			Controlesom
	TGT	SRC	LEN	SID	TRTP	DATA	
ResquestAccepted	*ITSID*	EE	Len	09	TREP	Gegevens	
DataUnavailable							
Geen gegevens	*ITSID*	EE	02	0A	TREP	10	
Persoonsgegevens niet gedeeld	*ITSID*	EE	02	0A	TREP	11	
NegativeAnswer							
Algemene verwerping	*ITSID*	EE	02	0B	SID Req	10	
Dienst niet ondersteund	*ITSID*	EE	02	0B	SID Req	11	
Subfunctie niet ondersteund	*ITSID*	EE	02	0B	SID Req	12	
Onjuiste berichtlengte	*ITSID*	EE	02	0B	SID Req	13	
Voorwaarden niet correct of verzoeksequentiefout	*ITSID*	EE	02	0B	SID Req	22	
Verzoek buiten bereik	*ITSID*	EE	02	0B	SID Req	31	
Antwoord in behandeling	*ITSID*	EE	02	0B	SID Req	78	
ITSID komt niet overeen	*ITSID*	EE	02	0B	SID Req	FC	
ITSID niet gevonden	*ITSID*	EE	02	0B	SID Req	FB	

RequestPIN (SID 01)

Dit bericht wordt door de VU-interface verstrekt als antwoord op een verzoek om gegevensoverdracht van een ITS-unit die noch op de zwarte lijst, noch op de witte lijst is geplaatst.

SendITSID (SID 02)

Dit bericht wordt door de VU-interface verstrekt telkens wanneer een nieuw apparaat een verzoek verzendt. Dit apparaat gebruikt de standaardidentificatie "A0" voordat het een unieke ID voor de communicatiesessie toegewezen krijgt.

SendPIN (SID 03)

Dit bericht wordt door de ITS-unit verstrekt om op de witte lijst te worden geplaatst door de VU-interface. De inhoud van dit bericht is een geheel getal ("INTEGER") met vier cijfers tussen 0 en 9.

PairingResult (SID 04)

Dit bericht wordt door de VU-interface verstrekt om de ITS-unit op de hoogte te brengen van het resultaat van de pincodeverificatie. De inhoud van dit bericht is een Booleaanse operator ("BOOLEAN") met de waarde "True" (waar) voor een juiste pincode en de waarde "False" (onwaar) in het tegenovergestelde geval.

SendPUC (SID 05)

Dit bericht wordt door de ITS-unit verstrekt ter opheffing van een blokkering die het gevolg is van de plaatsing op de zwarte lijst door de VU-interface. De inhoud van dit bericht is een geheel getal ("INTEGER") met acht cijfers tussen 0 en 9.

BanLiftingResult (SID 06)

Dit bericht wordt door de VU-interface verstrekt om de ITS-unit te melden of de juiste PUC-code werd opgegeven ter opheffing van de blokkering. De inhoud van dit bericht is een Booleaanse operator ("BOOLEAN") met de waarde "T(rue)" (waar) voor een correcte PUC-code en de waarde "F(alse)" (onwaar) in het tegenovergestelde geval.

RequestRejected (SID 07)

Dit bericht wordt door de VU-interface verstrekt als antwoord op elk bericht van een op de zwarte lijst geplaatste ITS-unit, met uitzondering van het bericht "SendPUC". In het bericht staat hoelang de ITS-unit nog op de zwarte lijst is geplaatst (resterende blokkeringstijd), volgens het in bijlage 3 vastgestelde tijdreeksformaat "Time".

RequestData (SID 08)

Dit bericht voor gegevenstoegang wordt verstrekt door de ITS-unit. Een overdrachtparameter verzoek (TRTP) van één byte geeft het type van de opgevraagde gegevens aan. Er zijn verschillende gegevenstypen:

— standardTachData (TRTP 01): beschikbare tachograafgegevens die als niet-persoonsgebonden worden aangemerkt.

— personalTachData (TRTP 02): beschikbare tachograafgegevens die als persoonsgebonden worden aangemerkt.

— gnssData (TRTP 03): GNSS-gegevens, die altijd als persoonsgebonden worden aangemerkt.

— standardEventData (TRTP 04): geregistreerde voorvalgegevens die als niet-persoonsgebonden worden aangemerkt.

— personalEventData (TRTP 05): geregistreerde voorvalgegevens die als persoonsgebonden worden aangemerkt.

— standardFaultData (TRTP 06): geregistreerde foutgegevens die als niet-persoonsgebonden worden aangemerkt.

— manufacturerData (TRTP 07): door de fabrikant beschikbaar gestelde gegevens.

Zie bijlage 3 van dit aanhangsel voor meer informatie over de inhoud van elk gegevenstype.

Zie aanhangsel 12 voor meer informatie over het formaat en de inhoud van GNSS-gegevens.

Zie bijlagen I B en I C voor meer informatie over voorval- en foutgegevens.

ResquestAccepted (SID 09)

Dit bericht wordt door de VU-interface verstrekt indien een bericht "RequestData" van de ITS-unit werd geaccepteerd. Dit bericht bevat een overdrachtparameter antwoord (TREP) van één byte, die correspondeert met de overdrachtparameter verzoek (TRTP) van het bijbehorende bericht "RequestData", alsook alle gegevens van het opgevraagde type.

DataUnavailable (SID 0A)

Dit bericht wordt door de VU-interface verstrekt indien de opgevraagde gegevens om een bepaalde reden niet beschikbaar zijn voor verzending naar een op de witte lijst geplaatste ITS-unit. Dit bericht bevat een overdrachtparameter antwoord (TREP) van één byte, die correspondeert met de overdrachtparameter verzoek (TRTP) van de opgevraagde gegevens, en een in tabel 3 gespecificeerde foutcode van één byte. De onderstaande codes zijn beschikbaar:

— Geen gegevens beschikbaar (10): de VU-interface heeft om niet nader bepaalde redenen geen toegang tot de VU-gegevens.

— Persoonsgegevens niet gedeeld (11): de ITS-unit probeert persoonsgegevens op te halen terwijl die niet worden gedeeld.

NegativeAnswer (SID 0B)

Deze berichten worden door de VU-interface verstrekt indien het verzoek niet kan worden afgehandeld om een andere reden dan de niet-beschikbaarheid van de gegevens. Deze berichten zijn doorgaans — maar niet altijd — het gevolg van een ongeldig formaat van het verzoek (lengte, SID, ITSID enz.). De overdrachtparameter verzoek (TRTP) in het gegevensveld bevat de SID van het verzoek. Het gegevensveld bevat de code die de reden van het negatieve antwoord specificeert. De onderstaande codes zijn beschikbaar:

— Algemene verwerping (code 10)

— De actie kan niet worden uitgevoerd om een reden die niet wordt genoemd hieronder, noch in punt (vul het nummer van het punt in *DataUnavailable* in).

— Dienst niet ondersteund (code 11)

— De SID van het verzoek wordt niet herkend.

— Subfunctie niet ondersteund (code 12)

— De overdrachtparameter verzoek (TRTP) wordt niet herkend, bijvoorbeeld omdat die ontbreekt of ongeldig is.

— Onjuiste berichtlengte (code 13)

— De lengte van het ontvangen bericht is onjuist (de LEN-byte stemt niet overeen met de werkelijke berichtlengte).

— Voorwaarden niet correct of verzoeksequentiefout (code 22)

— De gevraagde dienst is niet actief of de sequentie van verzoekberichten is niet correct.

— Verzoek buiten bereik (code 33)

— De parameterrecord van het verzoek (gegevensveld) is niet geldig.

— Antwoord in behandeling (code 78)

— De verzochte actie kan niet op tijd worden beëindigd en de VU is niet klaar om een ander verzoek te accepteren.

— *ITSID* komt niet overeen (code FB)

— Uit de vergelijking met de Bluetooth®-informatie blijkt dat de SRC *ITSID* niet overeenkomt met het aangesloten apparaat.

— *ITSID* niet gevonden (code FC)

— Geen enkel apparaat is verbonden aan de SRC *ITSID*.

De regels 1 tot en met 72 (**FormatMessageModule**) van de ASN.1-code in bijlage 3 specificeren het berichtformaat, zoals verduidelijkt in tabel 3. De berichtinhoud wordt hieronder nader toegelicht.

4.5. **Toestemming van de bestuurder**

Alle beschikbare gegevens worden als standaardgegevens dan wel als persoonsgegevens aangemerkt. Er wordt alleen toegang verschaft tot persoonsgegevens indien de bestuurder daarin heeft toegestemd door te verklaren dat zijn via de tachograaf beschikbare persoonsgegevens buiten het communicatienetwerk van het voertuig mogen worden gebruikt door derde toepassingen.

Die toestemming wordt verleend op het ogenblik dat een voor de voertuigunit onbekende bestuurders- of werkplaatskaart voor het eerst wordt ingebracht en de kaarthouder wordt gevraagd erin toe te stemmen dat zijn aan de tachograaf gerelateerde persoonsgegevens toegankelijk worden gemaakt via de facultatieve ITS-interface (zie ook bijlage I C, punt 3.6.2).

De status van de toestemming (actief/inactief) wordt geregistreerd in het geheugen van de tachograaf.

Indien er meerdere bestuurders zijn, worden alleen de persoonsgegevens van de bestuurders die hierin hebben toegestemd, gedeeld met de ITS-interface. Indien er bijvoorbeeld twee bestuurders in het voertuig aanwezig zijn en alleen de eerste bestuurder heeft erin toegestemd dat zijn persoonsgegevens worden gedeeld, worden de persoonsgegevens van de tweede bestuurder niet gedeeld.

4.6. **Standaardgegevens opvragen**

In figuur 3 van bijlage 2 staat een stroomschema van een geldig verzoek dat door de ITS-unit wordt verzonden om toegang te krijgen tot standaardgegevens. Aangezien de ITS-unit op de witte lijst staat en geen persoonsgegevens opvraagt, is geen verdere controle nodig. In dit stroomschema wordt ervan uitgegaan dat de gepaste procedure, zoals verduidelijkt in figuur 2 van bijlage 2, is nageleefd. Dit stroomschema is te vergelijken met het grijs gearceerde vak "REQUEST TREATMENT" in figuur 2.

Van de beschikbare gegevens worden als standaardgegevens aangemerkt:

— standardTachData (TRTP 01)

— StandardEventData (TRTP 04)

— standardFaultData (TRTP 06)

4.7. **Persoonsgegevens opvragen**

In figuur 4 van bijlage 2 staat het stroomschema voor de behandeling van een verzoek om persoonsgegevens. Zoals eerder aangegeven, worden persoonsgegevens uitsluitend via de VU-interface verzonden indien de bestuurder uitdrukkelijk daarin heeft toegestemd (zie ook punt 4.5). Zo niet, moet het verzoek automatisch worden verworpen.

Van de beschikbare gegevens worden als persoonsgegevens aangemerkt:

— personalTachData (TRTP 02)

— gnssData (TRTP 03)

— personalEventData (TRTP 05)

— manufacturerData (TRTP 07)

4.8. **Fout- en voorvalgegevens opvragen**

De ITS-units kunnen voorvalgegevens opvragen in de vorm van een lijst van alle onverwachte voorvallen. Deze gegevens worden als standaardgegevens dan wel als persoonsgegevens aangemerkt (zie bijlage 3). De inhoud van elk voorval stemt overeen met de documentatie in bijlage 1 van dit aanhangsel.

BIJLAGE 1

LIJST VAN VIA DE ITS-INTERFACE BESCHIKBARE GEGEVENS

Data	Source	Data classification (personal/ not personal)
VehicleIdentificationNumber	Vehicle Unit	**not personal**
CalibrationDate	Vehicle Unit	**not personal**
TachographVehicleSpeed speed instant t	Vehicle Unit	personal
Driver1WorkingState Selector driver	Vehicle Unit	personal
Driver2WorkingState	Vehicle Unit	personal
DriveRecognize Speed Threshold detected	Vehicle Unit	**not personal**
Driver1TimeRelatedStates Weekly day time	Driver Card	personal
Driver2TimeRelatedStates	Driver Card	personal
DriverCardDriver1	Vehicle Unit	**not personal**
DriverCardDriver2	Vehicle Unit	**not personal**
OverSpeed	Vehicle Unit	personal
TimeDate	Vehicle Unit	**not personal**
HighResolutionTotalVehicleDistance	Vehicle Unit	**not personal**
ServiceComponentIdentification	Vehicle Unit	**not personal**
ServiceDelayCalendarTimeBased	Vehicle Unit	**not personal**
Driver1Identification	Driver Card	personal
Driver2Identification	Driver Card	personal
NextCalibrationDate	Vehicle Unit	**not personal**
Driver1ContinuousDrivingTime	Driver Card	personal
Driver2ContinuousDrivingTime	Driver Card	personal
Driver1CumulativeBreakTime	Driver Card	personal
Driver2CumulativeBreakTime	Driver Card	personal
Driver1CurrentDurationOfSelectedActivity	Driver Card	personal
Driver2CurrentDurationOfSelectedActivity	Driver Card	personal

Data	Source	Data classification (personal/ not personal)
SpeedAuthorised	Vehicle Unit	**not personal**
TachographCardSlot1	Driver Card	**not personal**
TachographCardSlot2	Driver Card	**not personal**
Driver1Name	Driver Card	personal
Driver2Name	Driver Card	personal
OutOfScopeCondition	Vehicle Unit	**not personal**
ModeOfOperation	Vehicle Unit	**not personal**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Driver Card	personal
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Driver Card	personal
EngineSpeed	Vehicle Unit	personal
RegisteringMemberState	Vehicle Unit	**not personal**
VehicleRegistrationNumber	Vehicle Unit	**not personal**
Driver1EndOfLastDailyRestPeriod	Driver Card	personal
Driver2EndOfLastDailyRestPeriod	Driver Card	personal
Driver1EndOfLastWeeklyRestPeriod	Driver Card	personal
Driver2EndOfLastWeeklyRestPeriod	Driver Card	personal
Driver1EndOfSecondLastWeeklyRestPeriod	Driver Card	personal
Driver2EndOfSecondLastWeeklyRestPeriod	Driver Card	personal
Driver1CurrentDailyDrivingTime	Driver Card	personal
Driver2CurrentDailyDrivingTime	Driver Card	personal
Driver1CurrentWeeklyDrivingTime	Driver Card	personal
Driver2CurrentWeeklyDrivingTime	Driver Card	personal
Driver1TimeLeftUntilNewDailyRestPeriod	Driver Card	personal
Driver2TimeLeftUntilNewDailyRestPeriod	Driver Card	personal
Driver1CardExpiryDate	Driver Card	personal

Data	Source	Data classification (personal/ not personal)
Driver2CardExpiryDate	Driver Card	personal
Driver1CardNextMandatoryDownloadDate	Driver Card	personal
Driver2CardNextMandatoryDownloadDate	Driver Card	personal
TachographNextMandatoryDownloadDate	Vehicle Unit	**not personal**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Driver Card	personal
Driver2TimeLeftUntilNewWeeklyRestPeriod	Driver Card	personal
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Driver Card	personal
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Driver Card	personal
Driver1CumulativeUninterruptedRestTime	Driver Card	personal
Driver2CumulativeUninterruptedRestTime	Driver Card	personal
Driver1MinimumDailyRest	Driver Card	personal
Driver2MinimumDailyRest	Driver Card	personal
Driver1MinimumWeeklyRest	Driver Card	personal
Driver2MinimumWeeklyRest	Driver Card	personal
Driver1MaximumDailyPeriod	Driver Card	personal
Driver2MaximumDailyPeriod	Driver Card	personal
Driver1MaximumDailyDrivingTime	Driver Card	personal
Driver2MaximumDailyDrivingTime	Driver Card	personal
Driver1NumberOfUsedReducedDailyRestPeriods	Driver Card	personal
Driver2NumberOfUsedReducedDailyRestPeriods	Driver Card	personal
Driver1RemainingCurrentDrivingTime	Driver Card	personal
Driver2RemainingCurrentDrivingTime	Driver Card	personal
GNSS position	Vehicle Unit	personal

2. GNSS-GEGEVENS DIE CONTINU BESCHIKBAAR ZIJN MET TOESTEMMING VAN DE BESTUURDER

Zie Aanhangsel 12 „GNSS”.

3. VOORVALGEGEVENS DIE BESCHIKBAAR ZIJN ZONDER TOESTEMMING VAN DE BESTUURDER

Voorval	Opslagregels	Te registreren gegevens per voorval
Inbrengen van een ongeldige kaart	— de 10 meest recente voorvallen	— datum en tijd van het voorval — kaartsoort, kaartnummer, lidstaat van afgifte en generatie van de kaart die het voorval veroorzaakt — aantal vergelijkbare voorvallen op die dag
Kaartconflict	— de 10 meest recente voorvallen	— datum en tijd van het begin van het voorval — datum en tijd van het einde van het voorval — kaartsoort, kaartnummer, lidstaat van afgifte en generatie van de twee kaarten die het conflict veroorzaken
Laatste kaartsessie niet correct afgesloten	— de 10 meest recente voorvallen	— datum en tijd van kaartinbrenging — kaartsoort, kaartnummer, lidstaat van afgifte en generatie van de kaart die het voorval veroorzaakt — laatste sessiegegevens zoals af te lezen van de kaart: — datum en tijd van kaartinbrenging — kentekennummer van het voertuig, lidstaat van registratie en generatie van de VU
Onderbreking in de stroomvoorziening (2)	— 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 tijd van het begin van het voorval — datum en tijd van het einde van het voorval — kaartsoort, kaartnummer, lidstaat van afgifte en generatie van de kaart die bij het begin en/of einde van het voorval is ingebracht — aantal vergelijkbare voorvallen op die dag
Fout in communicatie met de inrichting voor communicatie op afstand	— 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 tijd van het begin van het voorval — datum en tijd van het einde van het voorval — kaartsoort, kaartnummer, lidstaat van afgifte en generatie van de kaart die bij het begin en/of einde van het voorval is ingebracht — aantal vergelijkbare voorvallen op die dag
Afwezigheid van positie-informatie van de GNSS-ontvanger	— 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 tijd van het begin van het voorval — datum en tijd van het einde van het voorval — kaartsoort, kaartnummer, lidstaat van afgifte en generatie van de kaart die bij het begin en/of einde van het voorval is ingebracht — aantal vergelijkbare voorvallen op die dag
Fout in de bewegingsgegevens	— 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 tijd van het begin van het voorval — datum en tijd van het einde van het voorval — kaartsoort, kaartnummer, lidstaat van afgifte en generatie van de kaart die bij het begin en/of einde van het voorval is ingebracht — aantal vergelijkbare voorvallen op die dag

Voorval	Opslagregels	Te registreren gegevens per voorval
Tegenstrijdige bewegingsgegevens	— 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 tijd van het begin van het voorval — datum en tijd van het einde van het voorval — kaartsoort, kaartnummer, lidstaat van afgifte en generatie van de kaart die bij het begin en/of einde van het voorval is ingebracht — aantal vergelijkbare voorvallen op die dag
Poging tot inbreuk op de beveiliging	de 10 meest recente voorvallen per soort voorval	— datum en tijd van het begin van het voorval — datum en tijd van het einde van het voorval (indien relevant) — kaartsoort, kaartnummer, lidstaat van afgifte en generatie van de kaart die bij het begin en/of einde van het voorval is ingebracht — soort voorval
Tegenstrijdige tijdgegevens	— 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	— door het controleapparaat geregistreerde datum en tijd — door het GNSS-systeem geregistreerde datum en tijd — kaartsoort, kaartnummer, lidstaat van afgifte en generatie van de kaart die bij het begin en/of einde van het voorval is ingebracht — aantal vergelijkbare voorvallen op die dag

4. VOORVALGEGEVENS DIE BESCHIKBAAR ZIJN MET TOESTEMMING VAN DE BESTUURDER

Voorval	Opslagregels	Te registreren gegevens per voorval
Rijden zonder geschikte kaart	— 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 tijd van het begin van het voorval — datum en tijd van het einde van het voorval — kaartsoort, kaartnummer, lidstaat van afgifte en generatie van de kaart die bij het begin en/of einde van het voorval is ingebracht — aantal vergelijkbare voorvallen op die dag
Kaartinbrenging tijdens het rijden	— het laatste voorval op elk van de laatste 10 dagen waarop een dergelijk voorval is opgetreden	— datum en tijd van het voorval — kaartsoort, kaartnummer, lidstaat van afgifte en generatie van de kaart die het voorval veroorzaakt — aantal vergelijkbare voorvallen op die dag
Snelheidsoverschrijding (1)	— het ernstigste voorval op elk van de laatste 10 dagen waarop een dergelijk voorval is opgetreden (d. w.z. het voorval met de hoogste gemiddelde snelheid) — de 5 ernstigste voorvallen gedurende de afgelopen 365 dagen — het eerste voorval dat is opgetreden na de laatste kalibrering	— datum en tijd van het begin van het voorval — datum en tijd van het einde van het voorval — tijdens het voorval gemeten maximumsnelheid — tijdens het voorval gemeten rekenkundige maximumsnelheid — kaartsoort, kaartnummer, lidstaat van afgifte en generatie van de bestuurderskaart (indien van toepassing) — aantal vergelijkbare voorvallen op die dag

5. FOUTGEGEVENS DIE BESCHIKBAAR ZIJN ZONDER TOESTEMMING VAN DE BESTUURDER

Fout	Opslagregels	Te registreren gegevens per fout
Kaartfout	— de 10 meest recente bestuurderskaartfouten	— datum en tijd van het begin van de fout — datum en tijd van het einde van de fout — kaartsoort, kaartnummer, lidstaat van afgifte en generatie van de kaart die de fout veroorzaakt
Controleapparaatfouten	— de 10 meest recente fouten van iedere soort — de eerste fout na de laatste kalibrering	— datum en tijd van het begin van de fout — datum en tijd van het einde van de fout — soort fout — kaartsoort, kaartnummer, lidstaat van afgifte en generatie van de kaart die bij het begin en/of einde van de fout is ingebracht

Deze fout wordt veroorzaakt door de onderstaande storingen, echter niet in de kalibreringsmodus:

— Interne fout in de VU

— Printerfout

— Displayfout

— Downloadfout

— Sensorfout

— Fout in de GNSS-ontvanger of externe GNSS-module

— Fout in de inrichting voor communicatie op afstand

6. FABRIKANTSPECIFIEKE VOORVALLEN EN FOUTEN ZONDER TOESTEMMING VAN DE BESTUURDER

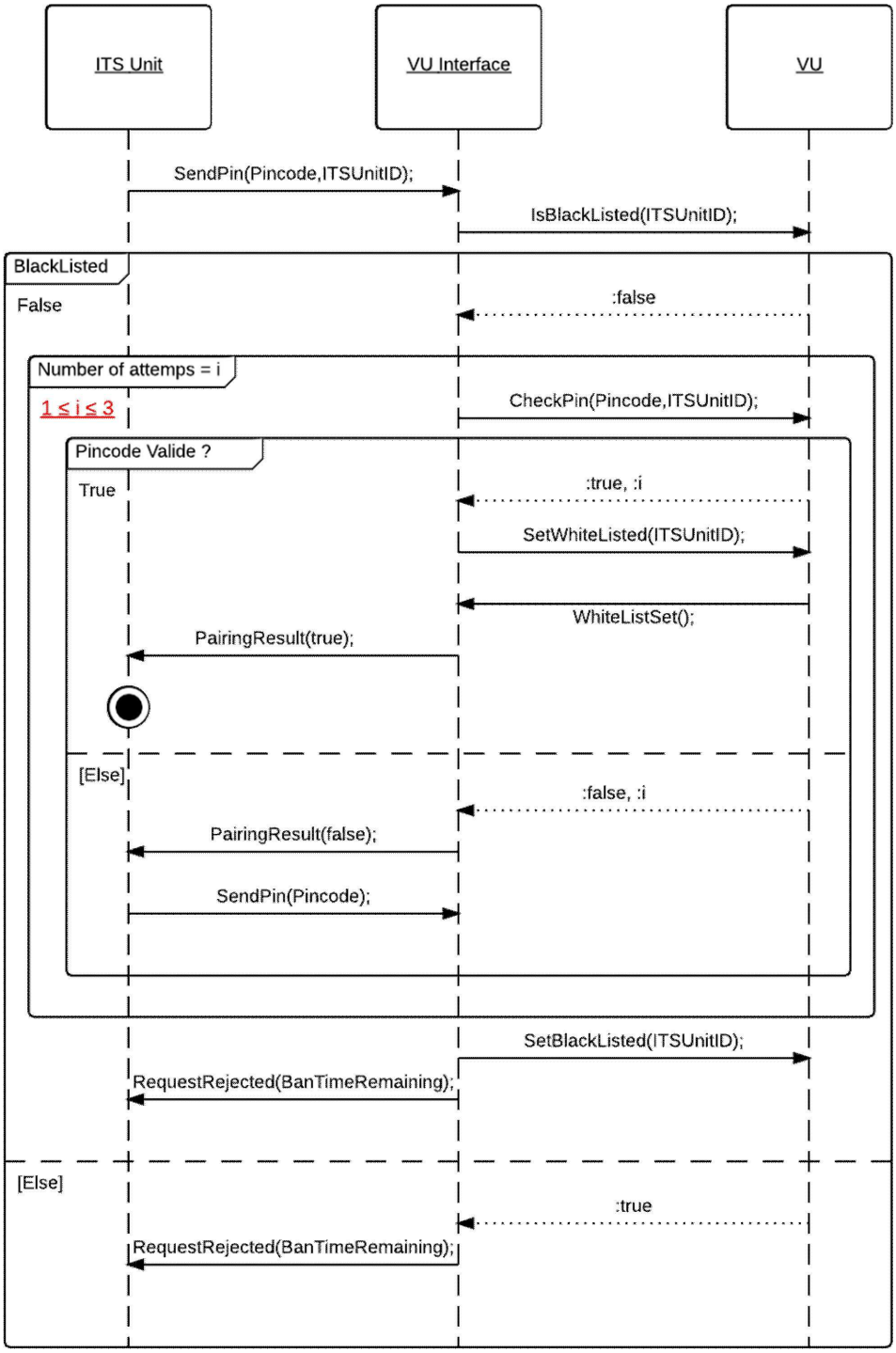
Voorval of fout	Opslagregels	Te registreren gegevens per voorval
Nog te bepalen door de fabrikant	Nog te bepalen door de fabrikant	Nog te bepalen door de fabrikant

BIJLAGE 2

STROOMSCHEMA'S VOOR DE BERICHTENUITWISSELING MET DE ITS-UNIT

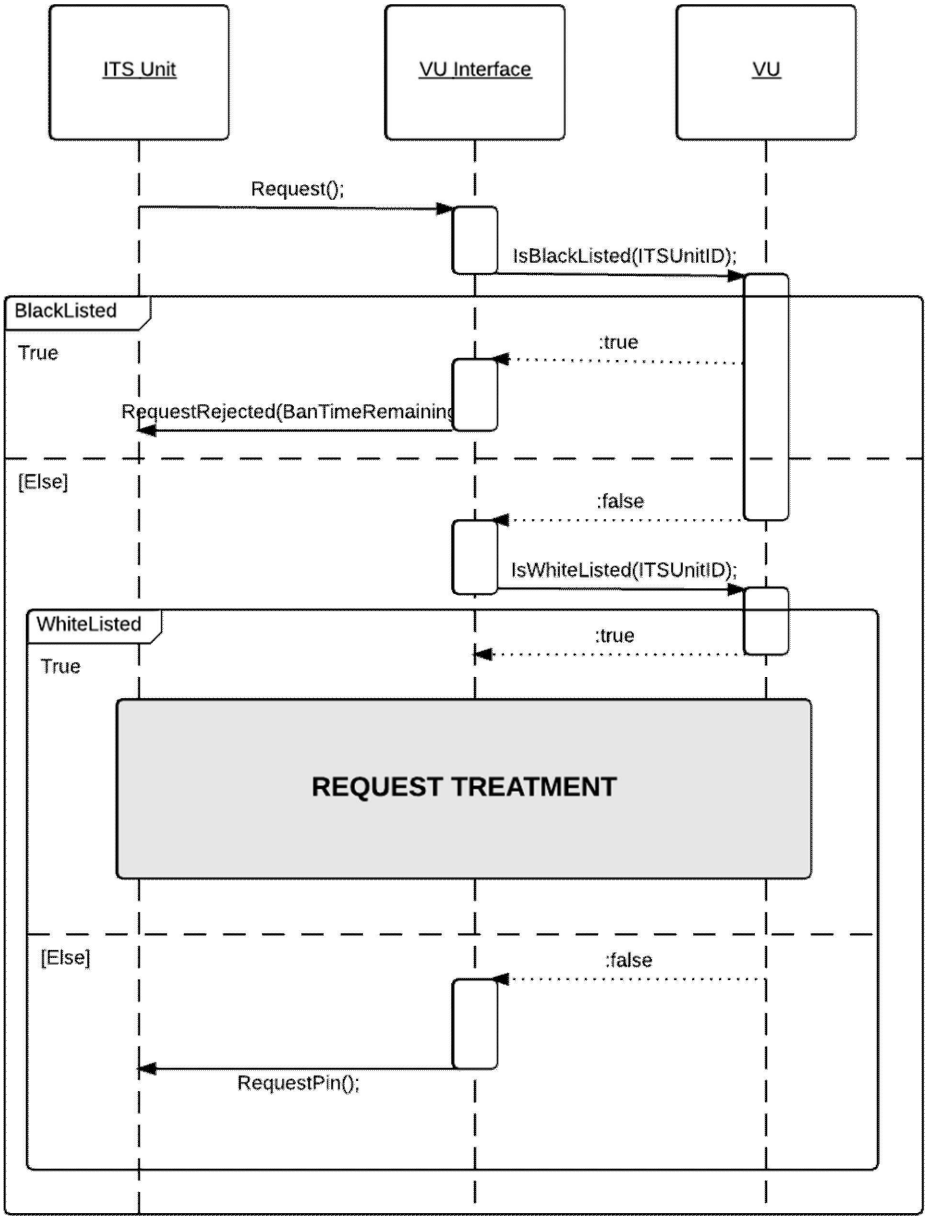
Figuur 1

Stroomschema voor een poging tot validatie van de pincode



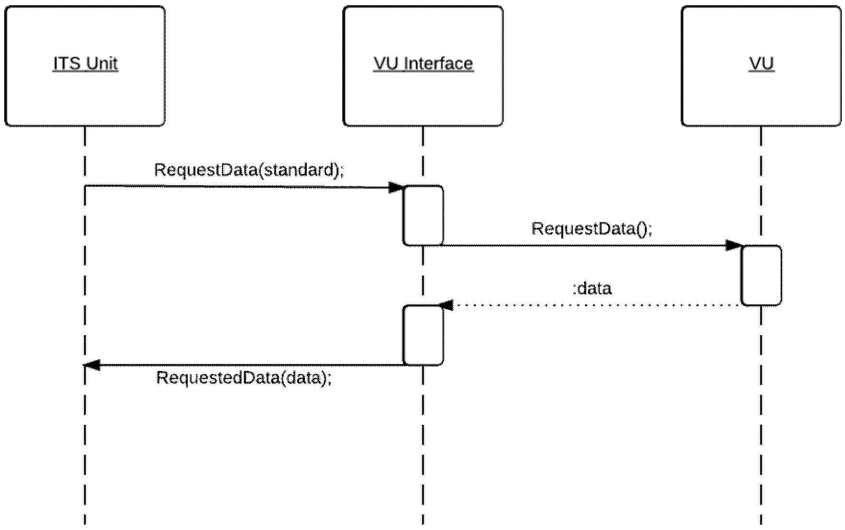
Figuur 2

Stroomschema voor de autorisatiecontrole van de ITS-unit



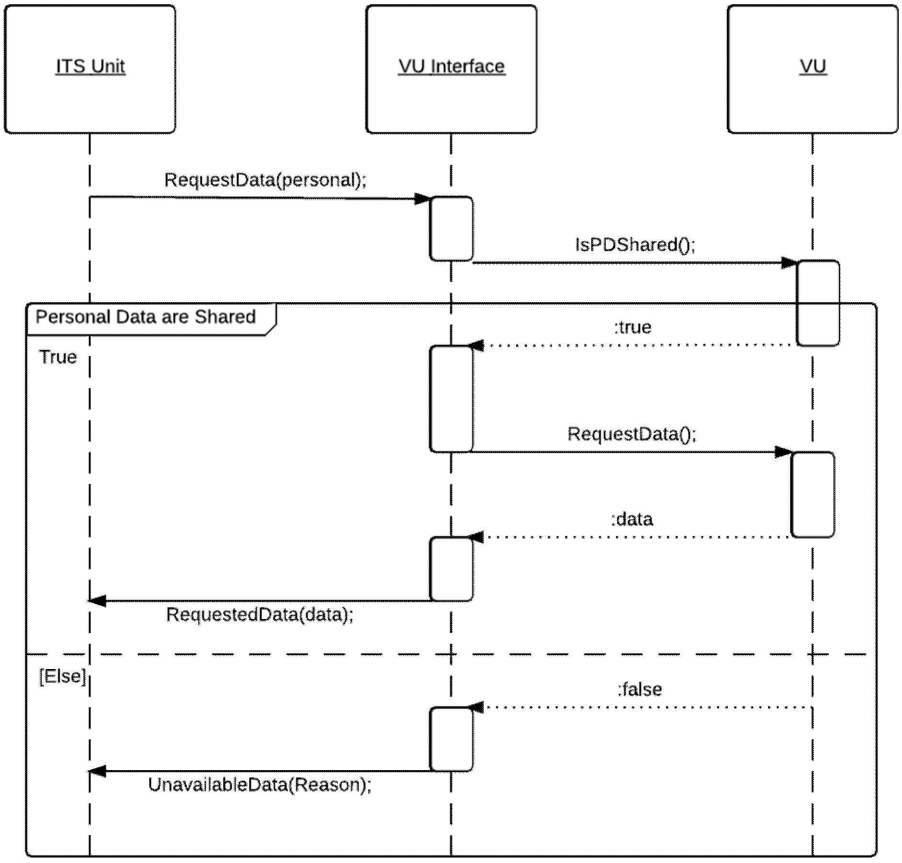
Figuur 3

Stroomschema voor de behandeling van een verzoek om overdracht van als niet-persoonsgebonden aangemerkte gegevens (na invoer van juiste pincode)



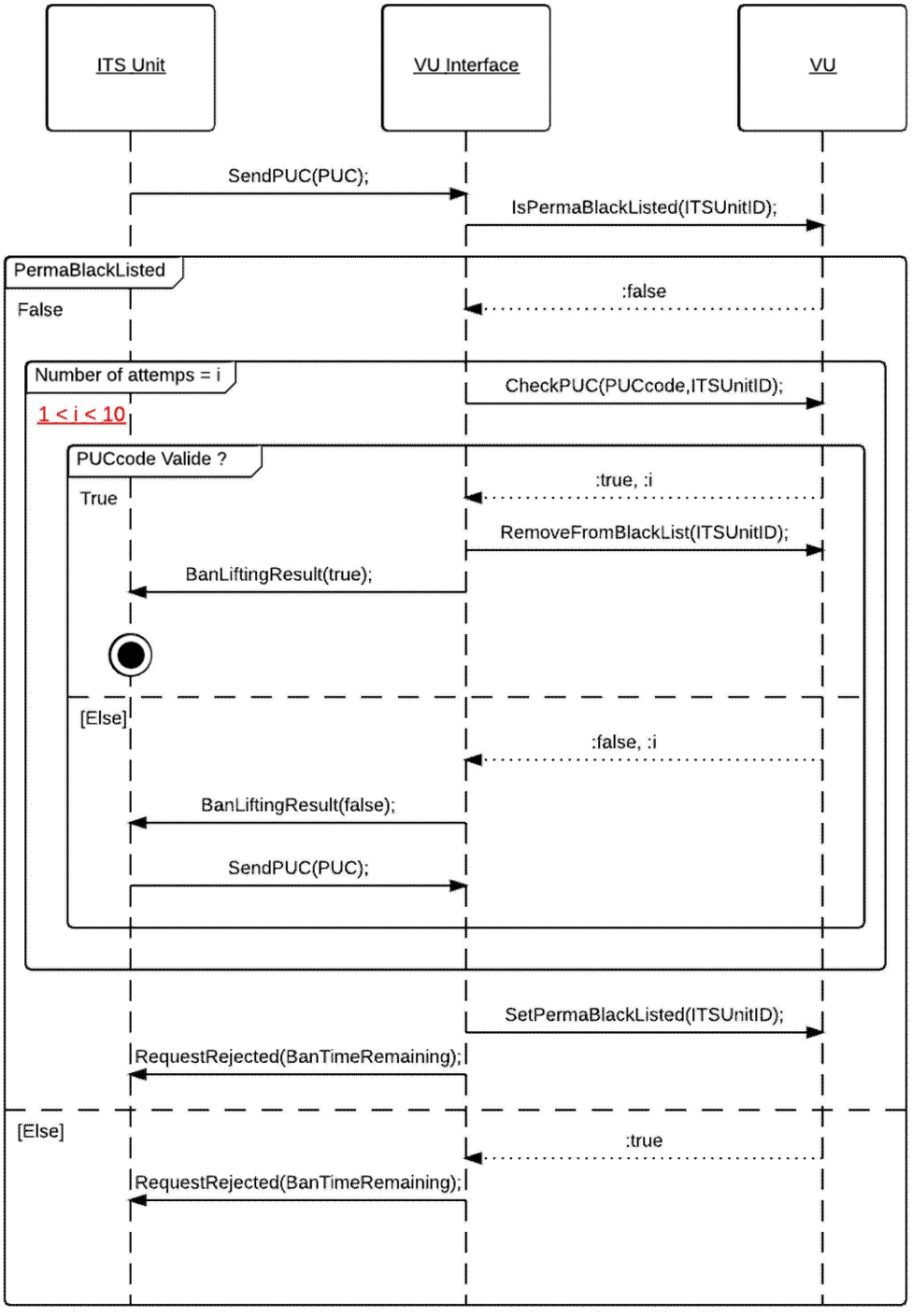
Figuur 4

Stroomschema voor de behandeling van een verzoek om overdracht van als persoonsgebonden aangemerkte gegevens (na invoer van juiste pincode)



Figuur 5

Stroomschema voor een poging tot validatie van de PUC-code



BIJLAGE 3

ASN.1 SPECIFICATIONS

```
FormatMessageModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ;
IMPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
        BanLiftingResult FROM PINPUCDataFieldsModule
        RequestAccepted,RequestData, DataUnavailable FROM
        RequestDataFieldsModule
        SendITSID, NegativeAnswer FROM OtherDataFieldsModule;

      CompleteMessage ::=SEQUENCE{
            header Header,
            data DataField,
            checksum Checksum
      }

      ----------------
      --HEADER TYPES--
      ----------------


      Header::=SEQUENCE{
            tgt IDList,
            src IDList,
            len BIT STRING (1..255)
      }

      vuID BIT STRING ::= 'EE'H
      IDList ::=CHOICE{
            vu BIT STRING (vuID),
            itsUnits SEQUENCE OF BIT STRING,
                  --Default hex Value:A0, redefined after first message exchange--
                  --Each ID will be linked to the Bluetooth ID of the device--
            ...
      }

      --------------------
      --DATAFIELDS TYPES--
      --------------------
      DataField ::=SEQUENCE{
            sid BIT STRING,
            trtp BIT STRING,
            subMBytes SubMessageBytes,
            dataField Content,
            ...
      }

      SubMessageBytes ::= SEQUENCE{
            currentSubM BIT STRING,
            totalSubM BIT STRING
      }

      Content ::= CHOICE{
            requestPIN RequestPIN,
            sendITSID SendITSID,
            sendPin SendPIN,
```

```
55                pairRslt PairingResult,
56                sendPUC SendPUC,
57                banlift BanLiftingResult,
58                requestRejected RequestRejected,
59                requestData RequestData,
60                requestOK RequestAccepted,
61                dataUnavailable DataUnavailable,
62                negAns NegativeAnswer
63          }
64
65          ------------------
66          --CHECKSUM TYPES--
67          ------------------
68
69          Checksum ::= SEQUENCE{
70                --SHA2 checksum
71          }
72    END
73
```

```
PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult;
IMPORTS ;

	----------
	---Utils--
	----------

	PUC ::= SEQUENCE (SIZE(8)) OF
	INTEGER (SIZE(0..9))

	PIN ::=	SEQUENCE (SIZE(4)) OF
		INTEGER (SIZE(0..9))

	--------------------------
	--Messages From ITS Unit--
	--------------------------

	SendPIN {PIN:pin} ::= SEQUENCE {
		sid BIT STRING ('03'H),
		pin PIN (pin)
	}

	SendPUC {PUC:puc} ::= SEQUENCE {
		sid BIT STRING ('05'H),
		puc PUC (puc)
	}
	--------------------
	--Messages From VU--
	--------------------

	PairingResult ::= SEQUENCE{
		sid BIT STRING ('04'H),
		result BOOLEAN
	}

	RequestPIN {MType:receivedRequest}::= SEQUENCE{
		sid BIT STRING ('01'H)
	}

	RequestRejected ::= SEQUENCE{
		sid BIT STRING ('07'H),
		banTimeRemaining GeneralizedTime, --PermaBan == 1k years-- }

	BanLiftingResult ::= SEQUENCE{
		sid BIT STRING ('06'H),
		result BOOLEAN
	}
END
```

```
RequestDataFields DEFINITIONS AUTOMATIC TAGS ::= BEGIN
	EXPORTS RequestAccepted,RequestData, DataUnavailable ;
	IMPORTS StandardEvent, PersonalEvent, StandardFault FROM EventsModule;

	------------------
	---From ITS Unit--
	------------------
	RequestData ::= SEQUENCE{
		sid BIT STRING ('08'H),
		requestedData DataTypeCode,
		...
	}

	-----------
	--From VU--
	-----------
	RequestAccepted ::=SEQUENCE{
		sid BIT STRING ('09'H),
		trtp DataTypeCode,
		dataSheet CHOICE{
			standardData StandardTachDataContent,
			personalData PersonalTachDataContent,
			gnss GNSSDataContent,
			standardEvent StandardEventContent,
			personalEvent PersonalEventContent,
			standardFault StandardFaultContent,
			manufacturerdata ManufacturerDataContent,
			...
		}
	}

	DataTypeCode ::=CHOICE{
		standardTachData BIT STRING ('01'H),
		personalTachData BIT STRING ('02'H),
		gnssData BIT STRING ('03'H),
		standardEventData BIT STRING ('04'H),
		personalEventData BIT STRING ('05'H),
		standardFaultData BIT STRING ('06'H),
		manufacturerData BIT STRING ('07'H),
		...
	}

	DataUnavailable ::=SEQUENCE{
		sid BIT STRING ('0A'H),
		trtp DataTypeCode,
		reason UnavailableDataCodes
	}

	UnavailableDataCodes ::= CHOICE{
		noDataAvailable BIT STRING ('10'H),
		personalDataNotShared BIT STRING ('11'H),
		...
	}
	----------------------------
	--Complete Tachograph Data--
	----------------------------
	--The format of the data was taken from the ISO16844-7 norm, more information
available in this ISO document—

```

```
Time ::= SEQUENCE{
	seconds INTEGER (0..59.75), --increment: 0.25s--
	minutes INTEGER (0..59), --increment: 1min--
	hours INTEGER (0..23), --increment: 1h--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	month INTEGER (1..12), --increment: 1month--
	year INTEGER (1985..2235), --increment: 1year--
	locMinOffset INTEGER (-59..59), --increment: 1min--
	locHouroffset INTEGER (-23..23)--increment: 1h--
}

Date ::= SEQUENCE{
	month INTEGER (1..12), --increment: 1month--
	day INTEGER (0.25.. 31.75), --increment: 0.25d--
	year INTEGER (1985..2235) --increment: 1year--
}

DriverName ::=SEQUENCE{
	codePageSurname UTF8String, --See ISO/IEC 8859--
	surname UTF8String,
	codePageFirstname UTF8String, --See ISO/IEC 8859--
	firstname UTF8String,
}

--------------------
--Message Content--
--------------------

StandardTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardTachData),
	personal BOOLEAN (FALSE),
	data StandardTachyDataSheet,
}

PersonalTachDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalTachData),
	personal BOOLEAN (TRUE),
	data PersonalTachyDataSheet
}

GNSSDataContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&gnssData),
	personal BOOLEAN (TRUE),
	data GNSSDataSheet
}

StandardEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&standardEventData),
	personal BOOLEAN (FALSE),
	data StandardEventDataSheet
}

PersonalEventContent ::= SEQUENCE{
	trtp DataTypeCode (DataTypeCode.&personalEventData),
	personal BOOLEAN (TRUE),
	data PersonalEventDataSheet
}

StandardFaultContent ::= SEQUENCE{
```

```
243                 trtp DataTypeCode (DataTypeCode.&standardFaultData),
244                 personal BOOLEAN (FALSE),
245                 data StandardFault
246           }
247
248           ManufacturerDataContent ::= SEQUENCE{
249                 trtp DataTypeCode (DataTypeCode.&manufacturerData),
250                 personal BOOLEAN (TRUE),
251                 ...
252           }
253
254           ---------------
255           --DATA SHEETS--
256           ---------------
257
258           --Data sheet format follows ISO 16844-7.--
259           StandardTachyDataSheet ::= SEQUENCE{
260                 vin UTF8String (SIZE(17)),
261                 calibrationDate Date,
262                 driveRecognize INTEGER (2 UNION 12),
263                 driverCardDriver1 INTEGER (2 UNION 12),
264                 driverCardDriver2 INTEGER (2 UNION 12),
265                 timeDate Time,
266                 highResolutionTotalVehicleDistance INTEGER (0..21055406), --increment:
267     5m--
268                 serviceComponentIdentification INTEGER (0..255),
269                 serviceDelayCalendarTimeBased INTEGER (-125..125), --increment: 1week-
270     -
271                 nextCalibrationDate Date,
272                 speedAuthorised INTEGER (0..250.996), --increment 1/256km/h--
273                 tachographCardSlot1 INTEGER (0..4...), --Maximum 250--
274                 tachographCardSlot2 INTEGER (0..4...), --Maximum 250--
275                 outOfScopeCondition INTEGER(2 UNION 12),
276                 modeOfOperation INTEGER (0..4...), --Maximum 250--
277                 registeringMemberState UTF8String,
278           vehicleRegistrationNumber SEQUENCE {
279                       codePageVRN INTEGER (0..255),
280                       vrn OCTET STRING (SIZE(13)),
281                 },
282                 tachographNextMandatoryDownloadDate Date,
283                 ...
284           }
285
286           PersonalTachyDataSheet ::= SEQUENCE{
287                 tachographVehicleSpeed INTEGER (0..250.996), --increment 1/256km/h--
288                 driver1WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
289     UNION 1012...),
290                 driver2WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
291     UNION 1012...),
292
293                 driver1TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
294     1002 UNION
295                                                   1012 UNION 1102 UNION 1112 UNION
296     10002 UNION 10012 UNION
297                                                   10102 UNION 10112 UNION 11002 UNION
298     11012...),
299                 driver2TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
300     1002 UNION
```

```
                                                    1012 UNION 1102 UNION 1112 UNION
10002 UNION 10012 UNION
                                                    10102 UNION 10112 UNION 11002 UNION
11012...),

             overSpeed INTEGER (2 UNION 12),
             driver1Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
             driver2Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
             driver1ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
             driver2ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
             driver1CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
             driver2CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
             driver1Name DriverName,
             driver2Name DriverName,
             driver1CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
             driver2CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
             engineSpeed INTEGER(0..8031.875), --increment: 0,125r/min--
             driver1EndOfLastDailyRestPeriod Time,
             driver2EndOfLastDailyRestPeriod Time,
             driver1EndOfLastWeeklyRestPeriod Time,
             driver2EndOfLastWeeklyRestPeriod Time,
             driver1EndOfSecondLastWeeklyRestPeriod Time,
             driver2EndOfSecondLastWeeklyRestPeriod Time,
             driver1CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
             driver2CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
             driver1CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
             driver2CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
             driver1TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver2TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver1CardExpiryDate Date,
             driver2CardExpiryDate Date,
             driver1CardNextMandatoryDownloadDate Date,
             driver2CardNextMandatoryDownloadDate Date,
             driver1TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver2TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
             driver1NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),
             driver2NumberOfTimes9hDailyDrivingTimesExceeced INTEGER (0..13),
             driver1CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
             driver2CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
             driver1MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
             driver2MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
             driver1MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
             driver2MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
```

```
360                driver1MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
361                driver2MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
362                driver1MaximumDailyDrivingTime INTEGER (910 UNION 1010),
363                driver2MaximumDailyDrivingTime INTEGER (910 UNION 1010),
364                driver1NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
365                driver2NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
366                driver1RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
367   1min--
368                driver2RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
369   1min--
370                ...
371          }
372
373          GNSSDataSheet ::=  SEQUENCE {
374          gnssPosition GeoCoordinates
375                --See Appendix 1 for definition of GeoCoordinates--
376          }
377
378          StandardEventDataSheet ::= SEQUENCE{
379                events SEQUENCE OF StandardEvent
380          }
381
382          PersonalEventDataSheet ::= SEQUENCE{
383                events SEQUENCE OF PersonalEvent
384          }
385   END
386
387   EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
388          EXPORTS ALL;
389          IMPORTS NationAlpha FROM Appendix1; --See Appendix 1 for more information
390   about NationAlpha--
391
392                SecurityBreachEvent ::=SEQUENCE{
393                      --See Annex 1B for more information--
394                }
395
396                RecordingEquipmentFaultType ::= SEQUENCE{
397                      --See Annex 1B for more information--
398                }
399
400                StandardEvent::= CHOICE{
401                      insertionInvalidCard InsertionOfANonValidCard,
402                      cardConflict CardConflict,
403                      timeOverlap TimeOverlap,
404                      previousSessionNotClosed LastCardSessionNotCorrectlyClosed,
405                      overSpeeding OverSpeeding,
406                      powerSupplyInterruption PowerSupplyInterruption,
407                      comErrorWithRemoteFacility
408   CommunicationErrorWithTheRemoteCommunicationFacility,
409                      absenceGNSSPosition
410   AbsenceOfPositionInformationFromGNSSReceiver,
411                      positionDataError PositionDataError,
412                      motionDataError MotionDataError,
413                      vehicleMotionConflict VehicleMotionConflict,
414                      securityBreachAttempt SecurityBreachAttempt,
415                      timeConflict TimeConflict,
416                      ...
417                }
418
```

```
PersonalEvent ::= CHOICE{
	lackOfAppropriateCard DrivingWithoutAnAppropriateCard,
	cardInsertionWhileDriving CardInsertionWhileDriving,
	overSpeeding OverSpeeding,
	...
}

StandardFault ::= CHOICE{
	cardFault CardFault,
	recordingEquipementFault RecordingEquipmentFault,
...
}

---------------
--EVENTS LIST--
---------------

InsertionOfANonValidCard::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

CardConflict ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER
}

TimeOverlap ::=SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberSimilarEvent INTEGER
}

DrivingWithoutAnAppropriateCard ::= SEQUENCE{
	beginDate GeneralizedTime,
	endDate GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
	issuingMemberState SEQUENCE OF NationAlpha,
	cardsGeneration SEQUENCE OF INTEGER,
	numberOfSimilarEvent INTEGER
}

CardInsertionWhileDriving ::= SEQUENCE{
	date GeneralizedTime,
	carsdType SEQUENCE OF UTF8String,
	cardsNumber SEQUENCE OF INTEGER,
```

```
478                     issuingMemberState SEQUENCE OF NationAlpha,
479                     numberOfSimilarEvents INTEGER
480             }
481
482             LastCardSessionNotCorrectlyClosed ::=SEQUENCE{
483                     beginDate GeneralizedTime,
484                     endDate GeneralizedTime,
485                     carsdType SEQUENCE OF UTF8String,
486                     cardsNumber SEQUENCE OF INTEGER,
487                     issuingMemberState SEQUENCE OF NationAlpha,
488                     cardsGeneration SEQUENCE OF INTEGER,
489                     oldSession SEQUENCE{
490                             beginDate GeneralizedTime,
491                             endDate GeneralizedTime,
492                             vrn UTF8String,
493                             issuingMemberState NationAlpha,
494                             cardsGeneration INTEGER,
495                     }
496             }
497
498             OverSpeeding ::=SEQUENCE{
499                     beginDate GeneralizedTime,
500                     endDate GeneralizedTime,
501                     maximumSpeed INTEGER,
502                     averageSpeed INTEGER,
503                     cardType UTF8String,
504                     cardNumber INTEGER,
505                     issuingMemberState NationAlpha,
506                     cardGeneration INTEGER,
507                     numberOfSimilarEvents INTEGER
508             }
509
510             PowerSupplyInterruption ::=SEQUENCE{
511                     beginDate GeneralizedTime,
512                     endDate GeneralizedTime,
513                     carsdType SEQUENCE OF UTF8String,
514                     cardsNumber SEQUENCE OF INTEGER,
515                     issuingMemberState SEQUENCE OF NationAlpha,
516                     cardsGeneration SEQUENCE OF INTEGER,
517                     numberOfSimilarEvent INTEGER
518             }
519
520             CommunicationErrorWithTheRemoteCommunicationFacility ::=SEQUENCE{
521                     beginDate GeneralizedTime,
522                     endDate GeneralizedTime,
523                     carsdType SEQUENCE OF UTF8String,
524                     cardsNumber SEQUENCE OF INTEGER,
525                     issuingMemberState SEQUENCE OF NationAlpha,
526                     cardsGeneration SEQUENCE OF INTEGER,
527                     numberOfSimilarEvent INTEGER
528             }
529
530             AbsenceOfPositionInformationFromGNSSReceiver ::= SEQUENCE{
531                     beginDate GeneralizedTime,
532                     endDate GeneralizedTime,
533                     carsdType SEQUENCE OF UTF8String,
534                     cardsNumber SEQUENCE OF INTEGER,
535                     issuingMemberState SEQUENCE OF NationAlpha,
536                     cardsGeneration SEQUENCE OF INTEGER,
```

```
		numberOfSimilarEvent INTEGER
	}

	PositionDataError ::= SEQUENCE{
		beginDate GeneralizedTime,
		endDate GeneralizedTime,
		carsdType SEQUENCE OF UTF8String,
		cardsNumber SEQUENCE OF INTEGER,
		issuingMemberState SEQUENCE OF NationAlpha,
		cardsGeneration SEQUENCE OF INTEGER,
		numberOfSimilarEvent INTEGER
	}

	MotionDataError ::= SEQUENCE{
		beginDate GeneralizedTime,
		endDate GeneralizedTime,
		carsdType SEQUENCE OF UTF8String,
		cardsNumber SEQUENCE OF INTEGER,
		issuingMemberState SEQUENCE OF NationAlpha,
		cardsGeneration SEQUENCE OF INTEGER,
		numberOfSimilarEvent INTEGER
	}

	VehicleMotionConflict ::= SEQUENCE{
		beginDate GeneralizedTime,
		endDate GeneralizedTime,
		carsdType SEQUENCE OF UTF8String,
		cardsNumber SEQUENCE OF INTEGER,
		issuingMemberState SEQUENCE OF NationAlpha,
		cardsGeneration SEQUENCE OF INTEGER,
		numberOfSimilarEvent INTEGER
	}

	SecurityBreachAttempt ::= SEQUENCE{
		beginDate GeneralizedTime,
		endDate GeneralizedTime OPTIONAL,
		carsdType SEQUENCE OF UTF8String,
		cardsNumber SEQUENCE OF INTEGER,
		issuingMemberState SEQUENCE OF NationAlpha,
		numberOfSimilarEvent INTEGER,
		typeOfEvent SecurityBreachEvent
	}


	TimeConflict ::= SEQUENCE{
		beginDate GeneralizedTime,
		endDate GeneralizedTime,
		carsdType SEQUENCE OF UTF8String,
		cardsNumber SEQUENCE OF INTEGER,
		issuingMemberState SEQUENCE OF NationAlpha,
		cardsGeneration SEQUENCE OF INTEGER,
		numberOfSimilarEvent INTEGER
	}

	---------------
	--FAULTS LIST--
	---------------

	CardFault ::= SEQUENCE{
```

```
596                     beginDate GeneralizedTime,
597                     endDate GeneralizedTime,
598                     carsdType SEQUENCE OF UTF8String,
599                     cardsNumber SEQUENCE OF INTEGER,
600                     issuingMemberState SEQUENCE OF NationAlpha,
601                     cardsGeneration SEQUENCE OF INTEGER,
602             }
603
604             RecordingEquipmentFault ::= SEQUENCE{
605                     beginDate GeneralizedTime,
606                     endDate GeneralizedTime,
607                     faultType RecordingEquipmentFaultType,
608                     carsdType SEQUENCE OF UTF8String,
609                     cardsNumber SEQUENCE OF INTEGER,
610                     issuingMemberState SEQUENCE OF NationAlpha,
611                     cardsGeneration SEQUENCE OF INTEGER,
612             }
613 END
```

Aanhangsel 14

FUNCTIE VOOR COMMUNICATIE OP AFSTAND

INHOUDSOPGAVE

1 INLEIDING 450

2 TOEPASSINGSGEBIED 451

3 ACRONIEMEN, DEFINITIES EN NOTATIES 452

4 OPERATIONELE SCENARIO'S 454

4.1 Overzicht 454

4.1.1 Eerste vereisten voor gegevensoverdracht via 5,8 GHz DSRC-interfaces 454

4.1.2 Profiel 1a: via een in de hand gehouden of tijdelijk langs de weg opgestelde REDCR 455

4.1.3 Profiel 1b: via een in het voertuig gemonteerde en van daaruit gerichte REDCR 456

4.2 Beveiliging/integriteit 456

5 ONTWERP EN PROTOCOLLEN VOOR COMMUNICATIE OP AFSTAND 456

5.1 Ontwerp 456

5.2 Workflow 459

5.2.1 Operaties 459

5.2.2 Interpretatie van de via de DSRC-interface ontvangen gegevens 461

5.3 Fysieke DSRC-interfaceparameters voor communicatie op afstand 461

5.3.1 Beperkingen met betrekking tot de gebruikslocatie 461

5.3.2 Downlink- en uplinkparameters 461

5.3.3 Antenneontwerp 466

5.4 DSRC-protocolvereisten voor RTM 466

5.4.1 Overzicht 466

5.4.2 Commando's 469

5.4.3 Volgorde van ondervragingscommando's 469

5.4.4 Gegevensstructuren 470

5.4.5 Elementen van RtmData, uitgevoerde acties en definities 472

5.4.6 Mechanisme voor gegevensoverdracht 476

5.4.7 Gedetailleerde beschrijving van transacties via DSRC-interfaces 476

5.4.8 Beschrijving van de testtransactie via DSRC-interfaces 486

5.5 Naleving van Richtlijn (EU) 2015/71 490

5.5.1 Overzicht 490

5.5.2 Commando's 490

5.5.3 Volgorde van ondervragingscommando's 490

5.5.4 Gegevensstructuren 490

5.5.5 ASN.1-module voor de OWS-transactie via DSRC-interface 491

5.5.6 Elementen van OwsData, uitgevoerde acties en definities 492

5.5.7 Mechanisme voor gegevensoverdracht 492

5.6 Gegevensoverdracht tussen DSRC-VU en VU 492

5.6.1 Fysieke verbinding en interfaces 492

5.6.2 Toepassingsprotocol 493

5.7 Behandeling van fouten 494

5.7.1 Registratie en doorgifte van de gegevens in de DSRC-VU 494

5.7.2 Fouten in de draadloze communicatie 494

6 TESTS BIJ INBEDRIJFSTELLING EN PERIODIEKE CONTROLE VAN DE FUNCTIE VOOR COMMUNICATIE OP AFSTAND 496

6.1 Algemeen 496

6.2 Echo-commando 496

6.3 Tests om de beveiligde gegevensinhoud te bevestigen 496

1 INLEIDING

In dit aanhangsel worden de ontwerpspecificaties en de toepasselijke procedures uiteengezet om de functie voor communicatie op afstand uit te voeren zoals voorgeschreven in artikel 9 van Verordening (EU) nr. 165/2014 (tachograafverordening).

DSC_1 Op grond van Verordening (EU) nr. 165/2014 wordt de tachograaf uitgerust met een functie voor communicatie op afstand waarmee de personeelsleden van de bevoegde controleautoriteiten tachograafinformatie van voorbijrijdende voertuigen kunnen lezen met behulp van apparatuur voor ondervraging op afstand (lezer voor communicatie over vroegtijdige detectie op afstand [REDCR]), in het bijzonder draadloze ondervragingssystemen die gebruikmaken van DSRC-interfaces in de frequentieband van 5,8 GHz en die voldoen aan de voorschriften van het Europees Comité voor normalisatie (CEN).

Het is van belang in te zien dat deze functie uitsluitend dient als voorfilter om de voertuigen te selecteren voor nadere controle, en niet bedoeld is ter vervanging van de formele controleprocedure waarin Verordening (EU) nr. 165/2014 voorziet. Punt 9 van de considerans van de tachograafverordening bepaalt inderdaad dat communicatie op afstand tussen de tachograaf en de controleautoriteiten alleen beoogt gerichte wegcontroles te vergemakkelijken.

DSC_2 De gegevens worden uitgewisseld via communicatie op afstand, waarbij de transmissie langs draadloze weg plaatsvindt via een 5,8 GHz DSRC-systeem dat in overeenstemming is met dit aanhangsel en dat werd getoetst aan de desbetreffende parameters van EN 300 674-1, {Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On-Board Units (OBU)}.

DSC_3 De communicatieverbinding wordt uitsluitend tot stand gebracht door toedoen van het apparaat van de controleautoriteiten, met gebruikmaking van een conform radiocommunicatiemiddel (lezer voor communicatie over vroegtijdige detectie op afstand (REDCR)).

DSC_4 De gegevens worden beveiligd om de integriteit te waarborgen.

DSC_5 Toegang tot de uitgewisselde gegevens wordt beperkt tot voor controle bevoegde autoriteiten die gemachtigd zijn inbreuken op Verordening (EG) nr. 561/2006 en Verordening (EU) nr. 165/2014 te controleren, en tot werkplaatsen voor zover het noodzakelijk is te controleren of de tachograaf goed functioneert.

DSC_6 Tijdens de communicatie op afstand worden uitsluitend gegevens uitgewisseld die nodig zijn voor gerichte wegcontrole van voertuigen met een tachograaf ten aanzien waarvan het vermoeden van manipulatie of misbruik bestaat.

DSC_7 De gegevensintegriteit en -beveiliging worden gewaarborgd door de gegevens in de voertuigunit (VU) te versleutelen en door uitsluitend versleutelde payload- en beveiligingsgegevens (zie punt 5.4.4) door te geven via het draadloze 5,8 GHz DSRC-systeem voor communicatie op afstand. Dit betekent dat alleen daartoe gemachtigde personen van de bevoegde controleautoriteiten in staat zijn de via de communicatie op afstand uitgewisselde gegevens te begrijpen en de authenticiteit daarvan te controleren. Zie aanhangsel 11 „Algemene beveiligingsmechanismen".

DSC_8 De gegevens bevatten een tijdaanduiding die aangeeft wanneer ze voor het laatst werden geactualiseerd.

DSC_9 Uitsluitend de bevoegde controleautoriteiten en de partijen met wie zij deze informatie delen, zijn op de hoogte van de beveiligingsgegevens, en hebben de controle over de inhoud daarvan. Deze inhoud valt buiten de werkingssfeer van de in dit aanhangsel vervatte bepalingen met betrekking tot communicatie op afstand. Niettemin wordt ervoor gezorgd dat bij elke overdracht van payloadgegevens ook beveiligingsgegevens worden meegezonden.

DSC_10 Dezelfde architectuur en apparatuur moeten het mogelijk maken andere gegevens (bijvoorbeeld van een weegsysteem aan boord van het voertuig) te verzamelen met toepassing van de hierin vervatte architectuurvoorschriften.

DSC_11 Voor alle duidelijkheid: overeenkomstig artikel 7 van Verordening (EU) nr. 165/2014 worden via communicatie op afstand geen gegevens over de identiteit van de bestuurder uitgewisseld.

2 TOEPASSINGSGEBIED

In dit aanhangsel wordt gespecificeerd hoe personeelsleden van de bevoegde controleautoriteiten een specifiek 5,8 GHz DSRC-systeem voor draadloze communicatie op afstand gebruiken met het doel gegevens te verzamelen ter identificatie van een bepaald voertuig dat mogelijkerwijs inbreuk maakt op Verordening (EU) nr. 165/2014 en dat daarom moet worden tegengehouden voor nadere controle.

Overeenkomstig artikel 9 van Verordening (EU) nr. 165/2014 moeten de verzamelde gegevens beperkt blijven tot, of betrekking hebben op gegevens ter identificatie van eventuele inbreuken op de tachograafverordening.

In dit geval is de voor de communicatie beschikbare tijd beperkt omdat gerichte gegevens over korte afstand moeten worden uitgewisseld. Bovendien 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 vrachtvoertuigen als bedoeld in Richtlijn (EU) 2015/719). Dit kan, naar keuze van de bevoegde controleautoriteiten, geschieden in de vorm van aparte of opeenvolgende verrichtingen.

Dit aanhangsel bevat specificaties met betrekking tot:

— de voor de communicatie op afstand te gebruiken apparatuur, procedures en -protocollen;

— de normen en verordeningen waaraan de radioapparatuur dient te voldoen;

— de aanbiedingsvorm van de gegevens aan de communicatieapparatuur;

— de opvraag- en downloadprocedures en de bewerkingsvolgorde;

— de over te brengen gegevens;

— de mogelijke interpretatie van de via communicatie op afstand overgebrachte gegevens;

— de bepalingen met betrekking tot beveiligingsgegevens in het kader van de communicatie op afstand;

— de beschikbaarstelling van de gegevens aan de bevoegde controleautoriteiten;

— de wijze waarop de lezer voor communicatie over vroegtijdige detectie op afstand (REDCR) uiteenlopende gegevens over het vrachtvervoer en voertuigenpark kan opvragen.

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

— het verzamelen van gegevens met het oog op de werking en het beheer in de VU (dit hangt af van het productontwerp tenzij anders is bepaald in Verordening (EU) nr. 165/2014);

— de aanbiedingsvorm van de verzamelde gegevens aan de personeelsleden van de bevoegde controleautoriteiten, noch de criteria die deze autoriteiten toepassen om te beslissen welke voertuigen worden tegengehouden (dit hangt af van het productontwerp, tenzij anders is bepaald in Verordening (EU) nr. 165/2014 of in beleidsbeslissingen van de bevoegde controleautoriteiten). Voor alle duidelijkheid: de functie voor communicatie op afstand beoogt uitsluitend de gegevens beschikbaar te stellen aan de bevoegde controleautoriteiten zodat zij zelf met kennis van zaken een beslissing kunnen nemen;

— de bepalingen inzake gegevensbeveiliging (zoals codering) met betrekking tot de gegevensinhoud (die worden gespecificeerd aanhangsel 11 „Algemene beveiligingsmechanismen”);

— bijzonderheden over andere gegevens die losstaan van de tachograafcontrole op afstand (RTM) en die met behulp van dezelfde architectuur en apparatuur kunnen worden verkregen;

— bijzonderheden over de wisselwerking en het beheer tussen de VU en de DSRC-VU, noch over de interne werking van de DSRC-VU (tenzij om de door een REDCR opgevraagde gegevens te verstrekken).

3 ACRONIEMEN, DEFINITIES EN NOTATIES

In dit aanhangsel worden de volgende acroniemen en begrippen gebruikt in de daarachter vermelde betekenis:

antenne: elektrisch apparaat dat wisselstroom omzet in radiofrequente energie (zendantenne) en omgekeerd (ontvangantenne), in combinatie met een radiozender of radio-ontvanger. Bij gebruik als zendantenne voert een radiozender radiofrequente wisselstroom toe aan de antenneklemmen en straalt de antenne deze radiofrequente energie uit in de vorm van elektromagnetische golven (radiogolven). Bij gebruik als ontvangantenne onttrekt de antenne een bepaalde hoeveelheid energie aan een elektromagnetische golf om op de antenneklemmen wisselstroom op te wekken; deze wisselstroom wordt aangelegd op een ontvanger om het signaal te versterken;

communicatie: uitwisseling van informatie/gegevens op master-slavebasis tussen een DSRC-REDCR en DSRC-VU, zoals uiteengezet in punt 5, met het doel gerichte gegevens te verkrijgen;

gegevens: beveiligde gegevens in een vastgelegd formaat (zie punt 5.4.4), die door de DSRC-REDCR worden opgevraagd en door de DSRC-VU aan de DSRC-REDCR worden verstrekt via een 5,8 GHz DSRC-interface als bedoeld in punt 5 hieronder;

tachograafverordening: Verordening (EU) nr. 165/2014 van het Europees Parlement en van de Raad van 4 februari 2014 betreffende tachografen in het wegvervoer, tot intrekking van Verordening (EEG) nr. 3821/85 van de Raad betreffende het controleapparaat in het wegvervoer en tot wijziging van Verordening (EG) nr. 561/2006 van het Europees Parlement en de Raad tot harmonisatie van bepaalde voorschriften van sociale aard voor het wegvervoer;

AID Toepassingsidentificator

BLE Bluetooth Low Energy

BST Dienstrooster radiobaken

CIWD	Inbrengen van de kaart tijdens het rijden
CRC	Cyclische redundantiecontrole
DSC (n)	Identificator van een voorschrift voor een specifieke DSRC-inrichting
DSRC	Speciale korteafstandscommunicatie
DSRC-REDCR	DSRC-lezer voor communicatie over vroegtijdige detectie op afstand
DSRC-VU	DSRC-voertuigunit. Dit is de „apparatuur voor vroegtijdige detectie op afstand" als gedefinieerd in bijlage 1 C.
DWVC	Rijden zonder geldige kaart
EID	Elementidentificator
LLC	Logische verbindingsbesturing
LPDU	LLC-protocol gegevensunit
OWS	Weegsysteem aan boord van een voertuig
PDU	Protocol gegevensunit
REDCR	Lezer voor communicatie over vroegtijdige detectie op afstand. Dit is de „apparatuur voor communicatie over vroegtijdige detectie op afstand" als gedefinieerd in bijlage 1 C.
RTM	Tachograafcontrole op afstand
SM-REDCR	Beveiligingsmodule van de lezer voor communicatie over vroegtijdige detectie op afstand
TARV	Telematics Applications for Regulated Vehicles (ISO 15638-normenreeks)
VU	Voertuigunit
VUPM	Payloadgeheugen van de voertuigunit
VUSM	Beveiligingsmodule van de voertuigunit
VST	Dienstrooster voertuig
WIM	Wegen terwijl het voertuig aan het rijden is
WOB	Wegen aan boord van het voertuig

De in dit aanhangsel vastgestelde specificatie verwijst naar en wordt geregeld door de hierna genoemde verordeningen en normen of gedeelten daarvan. In dit aanhangsel zijn de relevante normen of de relevante bepalingen van normen gespecificeerd. In geval van tegenspraak prevaleert dit aanhangsel. Indien er zich tegenstrijdigheden voordoen waarvoor een duidelijke specificatie in dit aanhangsel ontbreekt, prevaleert aanbeveling 70-03 van het Europees Comité voor radiocommunicatie (ERC) (na toetsing aan de desbetreffende parameters van EN 300 674-1), in afnemende volgorde van voorkeur gevolgd door EN 12795, EN 12253, EN 12834 en EN 13372, punten 6.2, 6.3, 6.4 en 7.1.

In dit aanhangsel wordt verwezen naar de volgende verordeningen en normen:

[1] Verordening (EU) nr. 165/2014 van het Europees Parlement en van de Raad van 4 februari 2014 betreffende tachografen in het wegvervoer, tot intrekking van Verordening (EEG) nr. 3821/85 van de Raad betreffende het controleapparaat in het wegvervoer en tot wijziging van Verordening (EG) nr. 561/2006 van het Europees Parlement en de Raad tot harmonisatie van bepaalde voorschriften van sociale aard voor het wegvervoer

[2] Verordening (EG) nr. 561/2006 van het Europees Parlement en de Raad van 15 maart 2006 tot harmonisatie van bepaalde voorschriften van sociale aard voor het wegvervoer, tot wijziging van Verordeningen (EEG) nr. 3821/85 en (EG) nr. 2135/98 van de Raad en tot intrekking van Verordening (EEG) nr. 3820/85 van de Raad (Voor de EER relevante tekst)

[3] ERC 70-03 CEPT: ECC Recommendation 70-03: Relating to the Use of Short Range Devices (SRD)

[4] ISO 15638 Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV)

[5] EN 300 674-1 Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5.8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On-Board Units (OBU).

[6] EN 12253 Road transport and traffic telematics — Dedicated short-range communication — Physical layer using microwave at 5.8 GHz.

[7] EN 12795 Road transport and traffic telematics — Dedicated short-range communication — Data link layer: medium access and logical link control.

[8] EN 12834 Road transport and traffic telematics — Dedicated short-range communication — Application layer.

[9] EN 13372 Road transport and traffic telematics — Dedicated short-range communication — Profiles for RTTT applications

[10] ISO 14906 Electronic fee collection — Application interface definition for dedicated short- range communication

4 OPERATIONELE SCENARIO'S

4.1 **Overzicht**

De tachograafverordening voorziet in specifieke, duidelijk afgebakende scenario's waarin gebruik dient te worden gemaakt van communicatie op afstand.

De ondersteunde scenario's zijn:

„Communication Profile 1: Roadside inspection using a short range wireless communication Remote Early Detection Communication Reader instigating a physical roadside inspection (master-:-slave)

Reader Profile 1a: via a hand aimed or temporary roadside mounted and aimed Remote Early Detection Communication

Reader Profile 1b: via a vehicle mounted and directed Remote Early Detection Communication Reader."

4.1.1 *Eerste vereisten voor gegevensoverdracht via 5,8 GHz DSRC-interfaces*

OPMERKING: voor een beter begrip van het kader waarin deze eerste vereisten worden toegepast, wordt verwezen naar figuur 14.3 hieronder.

4.1.1.1 In de VU bewaarde gegevens

DSC_12 De VU dient de gegevens die in de VU moeten worden opgeslagen, om de 60 seconden te actualiseren en bij te houden zonder tussenkomst van de DSRC-functie voor communicatie op afstand. De daartoe gebruikte middelen hangen af van het interne ontwerp van de VU, zoals gespecificeerd in de tachograafverordening, bijlage 1 C, punt 3.19 „Communicatie op afstand voor gerichte wegcontroles", en worden niet behandeld in dit aanhangsel.

4.1.1.2 Aan de DSRC-VU verstrekte gegevens

DSC_13 De VU dient de DSRC-gerelateerde tachograafgegevens bij te werken telkens wanneer de in de VU opgeslagen gegevens worden geactualiseerd met de in punt 4.1.1.1 (DSC_12) bepaalde regelmaat, zonder tussenkomst van de DSRC-functie voor communicatie op afstand.

DSC_14 De VU-gegevens dienen als uitgangspunt voor het samenstellen en actualiseren van de tachograafgegevens. De daartoe gebruikte middelen worden gespecificeerd in de tachograafverordening, bijlage 1 C, punt 3.19 „Communicatie op afstand voor gerichte wegcontroles". Bij gebrek aan ter zake dienende specificaties hangen deze middelen af van het productontwerp en worden zij niet behandeld in dit aanhangsel. Zie punt 5.6 voor meer informatie over het ontwerp van de communicatieverbinding tussen de DSRC-VU en de VU.

4.1.1.3 Gegevensinhoud

DSC_15 De gegevens zijn inhoudelijk zodanig opgemaakt dat ze na decodering kunnen worden gestructureerd en beschikbaar gesteld in de vorm die en het formaat dat is vastgelegd in punt 5.4.4 „Gegevensstructuren" van dit aanhangsel.

4.1.1.4 Aanbiedingsvorm van de gegevens

DSC_16 De gegevens die met de in punt 4.1.1.1 bepaalde regelmaat zijn geactualiseerd, worden op voorhand versleuteld en als beveiligde gegevens aangeboden aan de DSRC-VU om daar tijdelijk te worden opgeslagen als huidige versie van de gegevens. De VUSM brengt deze gegevens over naar de VUPM via de DSRC-functie. De VUSM en VUPM zijn functionele voorzieningen en niet noodzakelijk fysieke inrichtingen. De uitvoeringsvorm van deze functionele voorzieningen hangt af van het productontwerp tenzij anders is bepaald in de tachograafverordening.

4.1.1.5 Beveiligingsgegevens

DSC_17 Beveiligingsgegevens (*securityData*), met inbegrip van de gegevens die de REDCR nodig heeft om de tachograafgegevens te decoderen, worden verstrekt op de in aanhangsel 11 „Algemene beveiligingsmechanismen" vastgelegde wijze, en aangeboden in de vorm van gegevens die tijdelijk in de DSRC-VU worden opgeslagen als huidige versie van *securityData*, in het in punt 5.4.4 van dit aanhangsel omschreven formaat.

4.1.1.6 Voor overdracht via de DSRC-interface beschikbare VUPM-gegevens

DSC_18 In punt 5.4.4 wordt in het kader van de integrale specificaties van de ASN.1-module vastgelegd welke gegevens altijd beschikbaar moeten zijn in de VUPM voor onmiddellijke overdracht op verzoek van de REDCR.

Algemeen overzicht van communicatieprofiel 1

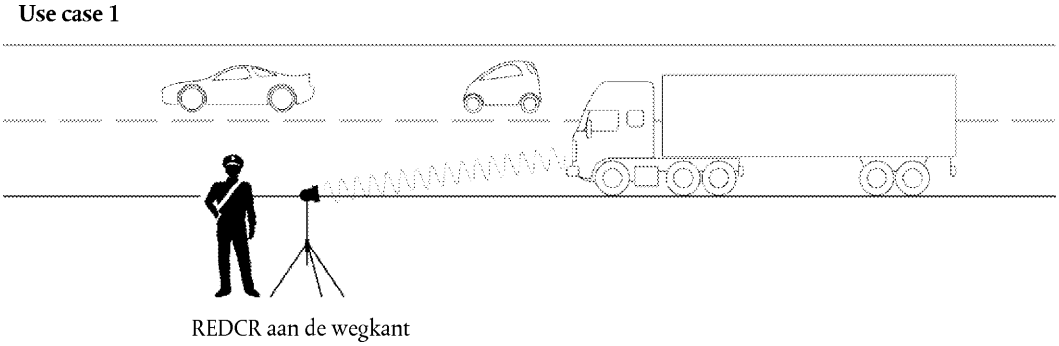
Dit profiel is van toepassing indien een personeelslid van de bevoegde controleautoriteiten („controleambtenaar") gebruikmaakt van een DSRC-REDCR (5,8 GHz DSRC-interfaces die functioneren overeenkomstig ERC-aanbeveling 70-03 en die zijn getoetst aan de desbetreffende parameters van EN 300 674-1 zoals omschreven in punt 5) teneinde op afstand een voertuig te identificeren dat mogelijkerwijs inbreuk maakt op de tachograafverordening. Zodra dit voertuig is geïdentificeerd, beslist de controleambtenaar op basis van de opgevraagde gegevens of het voertuig moet worden tegengehouden.

4.1.2 *Profiel 1a: via een in de hand gehouden of tijdelijk langs de weg opgestelde REDCR*

De controleambtenaar staat in dit geval aan de wegkant en richt een in de hand gehouden, op een statief gemonteerde of soortgelijke draagbare REDCR naar het midden van de voorruit van het gecontroleerde voertuig. Voor de ondervraging wordt gebruikgemaakt van 5,8 GHz DSRC-interfaces die functioneren overeenkomstig ERC-aanbeveling 70-03 en die zijn getoetst aan de desbetreffende parameters van EN 300 674-1 zoals omschreven in punt 5. Zie figuur 14.1 (praktijkgeval 1).

Figuur 14.1

Ondervraging aan de wegkant via 5,8 GHz DSRC-interfaces

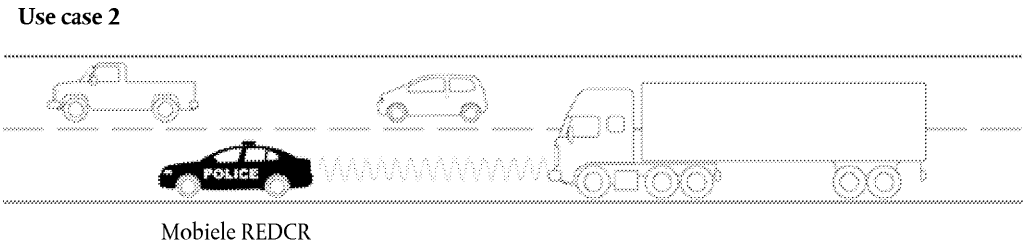


4.1.3 *Profiel 1b: via een in het voertuig gemonteerde en van daaruit gerichte REDCR*

De controleambtenaar zit in dit geval in een rijdend voertuig en richt van daaruit een in de hand gehouden, draagbare REDCR naar het midden van de voorruit van het gecontroleerde voertuig. De REDCR kan ook in of op het voertuig van de controleambtenaar gemonteerd zijn. In dit geval wordt de REDCR naar het midden van de voorruit van het gecontroleerde voertuig gericht indien het voertuig van de controleambtenaar zich in een bepaalde positie bevindt (bijvoorbeeld voorligger) ten opzichte van het gecontroleerde voertuig (achterligger). Voor de ondervraging wordt gebruikgemaakt van 5,8 GHz DSRC-interfaces die functioneren overeenkomstig ERC-aanbeveling 70-03 en die zijn getoetst aan de desbetreffende parameters van EN 300 674-1 zoals omschreven in punt 5. Zie figuur 14.2 (praktijkgeval 2)

Figuur 14.2

Ondervraging vanuit het voertuig via 5,8 GHz DSRC-interfaces



4.2 **Beveiliging/integriteit**

Teneinde de authenticiteit en integriteit van de via communicatie op afstand gedownloade gegevens te kunnen verifiëren, worden de beveiligde gegevens geverifieerd en gedecodeerd overeenkomstig aanhangsel 11 „Algemene beveiligingsmechanismen”.

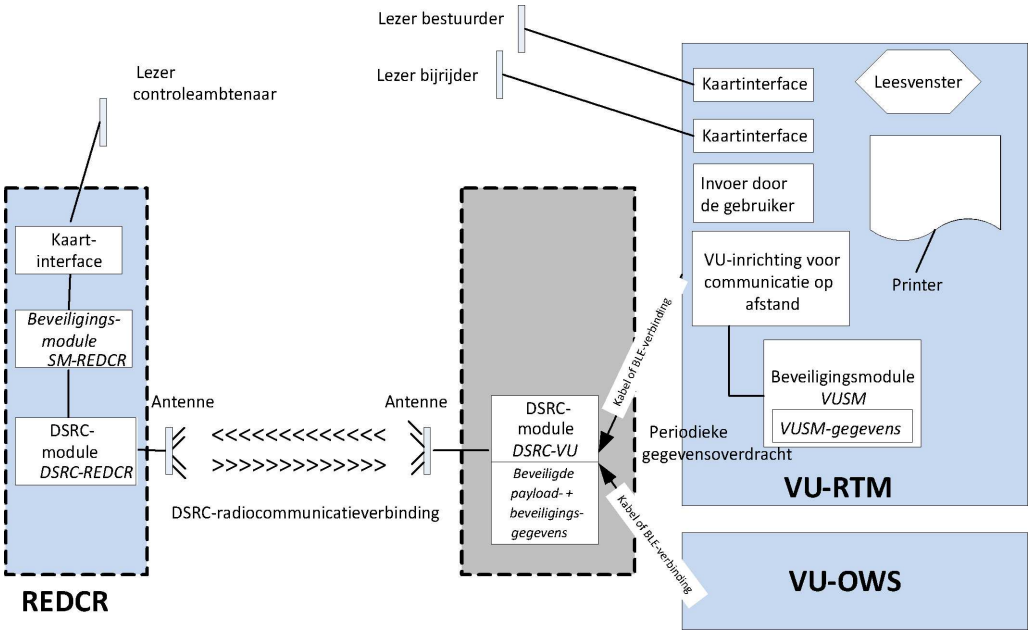
5 ONTWERP EN PROTOCOLLEN VOOR COMMUNICATIE OP AFSTAND

5.1 **Ontwerp**

Het ontwerp van de functie voor communicatie op afstand in de slimme tachograaf wordt verduidelijkt in figuur 14.3.

Figuur 14.3

Ontwerp van de functie voor communicatie op afstand



DSC_19 Hieronder wordt een overzicht gegeven van de functies die zich in de VU bevinden.

— VUSM (beveiligingsmodule van de VU): deze functie in de VU beveiligt de gegevens die de DSRC-VU via communicatie op afstand doorgeeft aan de controleambtenaar.

— De beveiligde gegevens worden opgeslagen in het geheugen van de VUSM. De in het geheugen van de DSRC-VU bijgehouden RTM-gegevens (met inbegrip van de verderop in dit aanhangsel bepaalde payload- en beveiligingsgegevens) worden door de VU gecodeerd en gecompleteerd met de in punt 4.1.1.1 (DSC_12) bepaalde regelmaat. De werking van de beveiligingsmodule wordt nader omschreven in aanhangsel 11 „Algemene beveiligingsmechanismen" en valt buiten het toepassingsgebied van dit aanhangsel. Niettemin moet de beveiligingsmodule, telkens wanneer de VUSM-gegevens veranderen, aangepaste gegevens verstrekken aan de VU-inrichting voor communicatie op afstand.

— De communicatie tussen de VU en de DSRC-VU vindt plaats via een kabel- of draadverbinding dan wel langs draadloze weg, via een BLE(Bluetooth Low Energy)-verbinding. De DSRC-VU kan geïntegreerd zijn in de antenne op de voorruit van het voertuig, in de VU ingebouwd zijn of zich ergens daartussen bevinden.

— De DSRC-VU moet beschikken over een betrouwbare, ononderbroken stroomvoorziening. De daartoe gebruikte middelen worden in de ontwerpfase vastgesteld.

— De DSRC-VU heeft een niet-vluchtig geheugen zodat de gegevens in de DSRC-VU bewaard blijven zelfs wanneer de ontsteking van het voertuig uitgeschakeld is.

— Indien de VU en de DSRC-VU via een BLE-verbinding met elkaar communiceren en de DSRC-VU via een niet-oplaadbare batterij van stroom wordt voorzien, moet deze stroombron bij elke periodieke controle van de DSRC-VU worden vervangen. De fabrikant van de DSRC-VU dient ervoor te zorgen dat de stroomvoorziening gewaarborgd blijft tussen twee periodieke controles. Daarbij moeten de gegevens op normale wijze en zonder enige storing of onderbreking toegankelijk blijven voor een REDCR.

— VUPM (payloadgeheugen van de VU) voor tachograafcontrole op afstand (RTM): via deze functie in de VU worden de gegevens verstrekt en geactualiseerd. De gegevensinhoud („TachographPayload") wordt hieronder gedefinieerd in punten 5.4.4 en 5.4.5, en wordt geactualiseerd met de in punt 4.1.1.1 (DSC_12) bepaalde regelmaat.

— DSRC-VU: deze functie is geïntegreerd in of aangesloten op de antenne en communiceert met de VU via een kabel- of draadverbinding dan wel langs draadloze weg, via een BLE-verbinding. Deze functie houdt de huidige gegevens (VUPM-gegevens) bij en beheert het antwoord op een ondervraging via de 5,8 GHz DSRC-interface. Het loskoppelen van de DSRC-interface of het anderszins belemmeren of verhinderen van de werking daarvan tijdens normaal bedrijf van het voertuig wordt aangemerkt als inbreuk op de tachograafverordening.

— SM-REDCR (beveiligingsmodule van de REDCR): deze functie wordt gebruikt om de gegevens afkomstig van de VU te decoderen en op integriteit te controleren. De daartoe gebruikte middelen worden niet nader omschreven in dit aanhangsel, maar vastgelegd in aanhangsel 11 „Algemene beveiligingsmechanismen".

— DSRC-REDCR: deze functie bevat een 5,8 GHz zendontvangapparaat („transceiver") met bijbehorende firmware en software voor het beheer van de communicatie op afstand met de DSRC-VU overeenkomstig dit aanhangsel.

— De DSRC-REDCR ondervraagt de DSRC-VU van het gecontroleerde voertuig en ontvangt de gegevens (de huidige VUPM-gegevens van het gecontroleerde voertuig) via de DSRC-interface, verwerkt die en slaat ze op in de SM-REDCR.

— 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 (meestal in of nabij het midden van de voorruit van het voertuig). Voor lichte voertuigen (bestelwagens e.d.) kan de antenne aan de bovenzijde van de voorruit worden gemonteerd.

— Tegenover of bij de antenne mogen er zich geen metalen voorwerpen bevinden (zoals badges, stickers, reflectiewerende folie (kleurstrips), zonnekleppen, wisserarmen van de voorruit in ruststand e.d.) die de communicatie kunnen storen.

— De antenne wordt zodanig gemonteerd dat de referentieas ervan ongeveer evenwijdig aan het wegdek loopt.

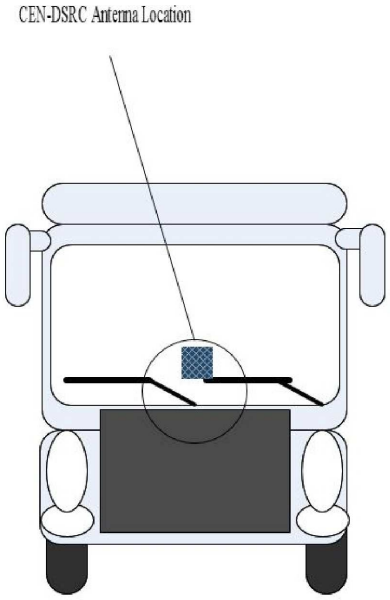
DSC_20 De antenne en de functie voor communicatie op afstand werken overeenkomstig ERC-aanbeveling 70-03 en zijn getoetst aan de desbetreffende parameters van EN 300 674-1 zoals omschreven in punt 5. In de antenne en de functie voor communicatie op afstand kunnen ontstoringstechnieken worden toegepast om interferentie van andere draadloze apparaten tegen te gaan, zoals omschreven in rapport 228 van het Comité voor elektronische communicatie (ECC), bijvoorbeeld door gebruik te maken van ontstoringsfilters voor de CEN DSRC 5,8 GHz communicatie.

DSC_21 De antenne wordt hetzij rechtstreeks aangesloten op de DSRC-VU in de module op of nabij de voorruit, hetzij via een specifieke kabel die niet onrechtmatig kan worden losgekoppeld. Het loskoppelen van de antenne of het anderszins belemmeren of verhinderen van de werking daarvan wordt beschouwd als een inbreuk op de tachograafverordening. Het opzettelijk maskeren/afschermen van de antenne of het anderszins nadelig beïnvloeden van de operationele prestaties daarvan wordt beschouwd als een inbreuk op de tachograafverordening.

DSC_22 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 gemonteerd zoals omschreven in DSC_19 en verduidelijkt in figuur 14.4 (ovale lijn), en biedt op efficiënte wijze ondersteuning aan de in punten 4.1.2 en 4.1.3 toegelichte praktijkgevallen.

Figuur 14.4

Montage van de 5,8 GHz DSRC-antenne op de voorruit van gereglementeerde voertuigen



De vormfactor van de REDCR en bijbehorende antenne kan variëren afhankelijk van de opstellingswijze van de lezer (op statief, in de hand gehouden, in het voertuig gemonteerd enz.) en de werkmethode van de controleambtenaar.

Via een weergave- en/of meldfunctie wordt de controleambtenaar op de hoogte gebracht van de resultaten van de communicatie op afstand. De resultaten kunnen beschikbaar worden gesteld door weergave in een leesvenster, in de vorm van een afdruk, via een akoestisch waarschuwingssignaal of een combinatie daarvan. De uitvoeringsvorm van deze weergave- en/of meldfunctie hangt af van vereisten van de controleambtenaren, en wordt niet behandeld in dit aanhangsel.

DSC_23 Het ontwerp en de vormfactor van de REDCR hangen af van de commerciële vormgeving, van de werking overeenkomstig ERC-aanbeveling 70-03 alsook van de in punt 5.3.2 van dit aanhangsel gespecificeerde ontwerp- en prestatie-eigenschappen. Zo wordt marktdeelnemers zoveel mogelijk marge geboden om apparatuur te ontwerpen en te leveren die afgestemd is op de specifieke ondervragingsscenario's van de bevoegde controleautoriteiten.

DSC_24 Het ontwerp en de vormfactor van de DSRC-VU alsook de opstellingswijze daarvan (binnen of buiten de VU) hangen af van de commerciële vormgeving, van de werking overeenkomstig ERC-aanbeveling 70-03 alsmede van de in dit voorschrift (punt 5.1) en de in punt 5.3.2 van dit aanhangsel gespecificeerde ontwerp- en prestatie-eigenschappen.

DSC_25 Niettemin moet de DSRC-VU redelijkerwijs in staat zijn gegevens van andere slimme voertuigapparatuur, zoals weegsystemen aan boord van het voertuig, te ontvangen via op een open industrienorm gebaseerde verbindingen en protocollen. Als voorwaarde daarbij geldt dat deze gegevens worden geïdentificeerd door unieke en bekende toepassingsidentificatoren/bestandsnamen, dat de gebruiksinstructies voor deze protocollen beschikbaar worden gesteld aan de Europese Commissie en tevens kosteloos verkrijgbaar zijn voor de betrokken apparatuurfabrikanten.

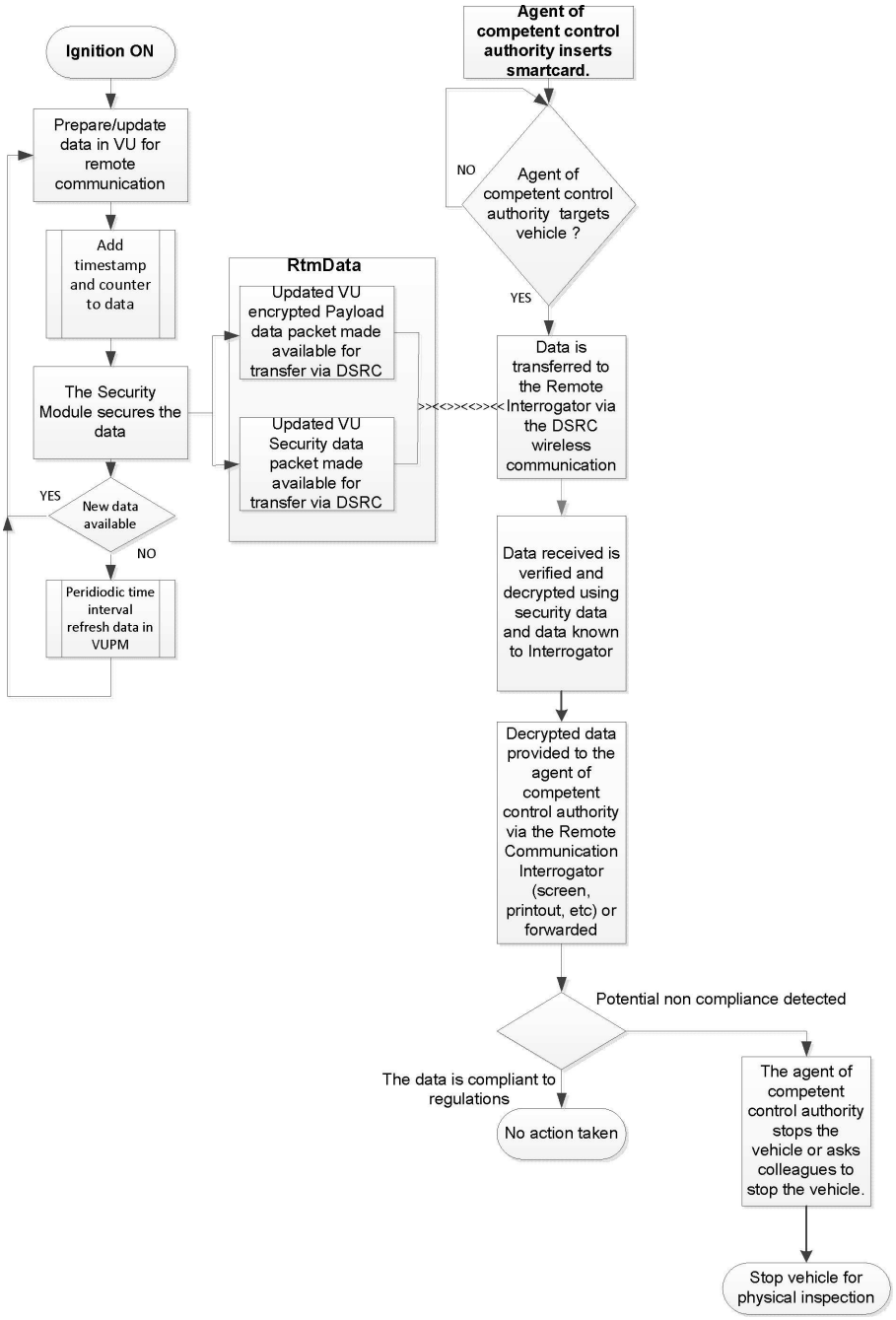
5.2 **Workflow**

5.2.1 *Operaties*

De operationele workflow wordt verduidelijkt in figuur 14.5.

Figuur 14.5

Workflow van de functie voor communicatie op afstand



Hieronder wordt een stapsgewijze beschrijving gegeven van deze workflow.

a. Wanneer het voertuig in gebruik is (contact aangezet), verstrekt de tachograaf gegevens aan de VU-functie. De VU-functie maakt de gegevens gereed voor communicatie op afstand door ze te coderen, en actualiseert de VUPM-gegevens die worden bijgehouden in het geheugen van de DSRC-VU (zoals omschreven in punten 4.1.1.1 en 4.1.1.2). De verzamelde gegevens worden opgemaakt volgens het in punten 5.4.4 en 5.4.5 hieronder vastgestelde formaat.

b. Telkens wanneer de gegevens worden geactualiseerd, wordt de tijdaanduiding van de beveiligingsgegevens bijgewerkt.

c. De VUSM-functie beveiligt de gegevens volgens de in aanhangsel 11 vastgestelde procedures.

d. Telkens wanneer de gegevens worden geactualiseerd (zie punten 4.1.1.1 en 4.1.1.2), worden ze overgebracht naar de DSRC-VU en worden eventueel bestaande gegevens overschreven. Op die manier zijn de huidige gegevens altijd up-to-date in het geval dat het voertuig wordt ondervraagd door een REDCR. De gegevens die de VU aan de DSRC-VU verstrekt, zijn identificeerbaar aan de hand van de bestandsnaam *RTMData* of de toepassingsidentificator (AID) en de attribuutidentificator.

e. Indien een controleambtenaar de gegevens van een voertuig wil verzamelen voor controledoeleinden, plaatst hij zijn smartcard in de REDCR om de functie voor communicatie op afstand te activeren en om de SM-REDCR in staat te stellen een authenticiteitscontrole uit te voeren en de gegevens te decoderen.

f. De controleambtenaar richt vervolgens de REDCR op het gecontroleerde voertuig en vraagt de gegevens op via de communicatie op afstand. De REDCR start een 5,8 GHz DSRC-interfacesessie met de DSRC-VU van het gecontroleerde voertuig, en vraagt de gegevens op. De gegevens worden via het draadloze communicatiesysteem naar de REDCR overgebracht als DSRC-attribuut met behulp van het GET-commando van de toepassing, zoals omschreven in punt 5.4. Het attribuut bevat de gecodeerde payloadgegevens en de DSRC-beveiligingsgegevens.

g. De gegevens worden geanalyseerd door de REDCR en doorgegeven aan de controleambtenaar.

h. Aan de hand van deze gegevens kan de controleambtenaar beslissen om het voertuig al dan niet tegen te houden voor nadere controle, of kan hij een collega vragen het voertuig tegen te houden.

5.2.2 *Interpretatie van de via de DSRC-interface ontvangen gegevens*

DSC_26 De via de 5,8 GHz DSRC-interface ontvangen gegevens mogen uitsluitend worden opgevat in de betekenis en binnen de draagwijdte die daaraan worden gegeven in punten 5.4.4 en 5.4.5 hieronder. Deze gegevens moeten worden begrepen in het licht van de hierbij nagestreefde doelstellingen. Overeenkomstig de tachograafverordening worden de gegevens uitsluitend gebruikt om ter zake dienende informatie te verstrekken aan de bevoegde controleambtenaar zodat die kan beslissen of het voertuig moet worden tegengehouden voor nadere controle. Nadien worden deze gegevens gewist zoals voorgeschreven in artikel 9 van de tachograafverordening.

5.3 **Fysieke DSRC-interfaceparameters voor communicatie op afstand**

5.3.1 *Beperkingen met betrekking tot de gebruikslocatie*

DSC_27 Het op een 5,8 GHz DSRC-interface gebaseerde systeem voor ondervraging op afstand van voertuigen mag niet worden gebruikt op minder dan 200 m van een 5,8 GHz DSRC-wegportaal.

5.3.2 *Downlink- en uplinkparameters*

DSC_28 De voor de tachograafcontrole op afstand (RTM) gebruikte apparatuur moet voldoen aan en functioneren overeenkomstig ERC-aanbeveling 70-03 en de in tabellen 14.1 en 14.2 hieronder aangegeven parameters.

DSC_29 De gebruikte RTM-apparatuur voldoet bovendien aan de in EN 12253 en EN 13372 vastgestelde parameters ter waarborging van de compatibiliteit met de operationele parameters van andere gestandaardiseerde 5,8 GHz DSRC-systemen.

Het betreft met name:

Tabel 14.1

Downlinkparameters

Item No.	Parameter	Value(s)	Remark
D1	Downlink Carrier Frequencies	There are four alternatives which may be used by an REDCR: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	Within ERC 70-03. Carrier Frequencies may be selected by the implementer of the roadside system and need not be known in the DSRC-VU (Consistent with EN 12253, EN 13372)
D1a (*)	Tolerance of Carrier Frequencies	within ± 5 ppm	(Consistent with EN 12253)
D2 (*)	RSU (REDCR) Transmitter Spectrum Mask	Within ERC 70-03. REDCR shall be according to Class B,C as defined in EN 12253. No other specific requirement within this Annex	Parameter used for controlling interference between interrogators in proximity (as defined in EN 12253 and EN 13372).
D3	OBU(DSRC-VU) Minimum Frequency Range	5,795 — 5,815 GHz	(Consistent with EN 12253)
D4 (*)	Maximum E.I.R.P.	Within ERC 70-03 (unlicensed) and within National Regulation Maximum + 33 dBm	(Consistent with EN 12253)
D4a	Angular E.I.R.P. mask	According to declared and published specification of interrogator designer	(Consistent with EN 12253)
D5	Polarisation	Left hand circular	(Consistent with EN 12253)
D5a	Cross-Polarisation	XPD: In bore sight: (REDCR) RSU t ≥ 15 dB (DSRC-VU) OBU r ≥ 10 dB At -3 dB area: (REDCR) RSU t ≥ 10 dB (DSRC-VU) OBU r ≥ 6 dB	(Consistent with EN 12253)
D6 (*)	Modulation	Two level amplitude modulation.	(Consistent with EN 12253)
D6a (*)	Modulation Index	0,5 … 0,9	(Consistent with EN 12253)

Item No.	Parameter	Value(s)	Remark
D6b	Eye Pattern	≥ 90 % (time) / ≥ 85 % (amplitude)	
D7 (*)	Data Coding	FM0 "1" bit has transitions only at the beginning and end of the bit interval. "0" bit has an additional transition in the middle of the bit interval compared to the "1" bit.	(Consistent with EN 12253)
D8 (*)	Bit rate	500 kBit/s	(Consistent with EN 12253)
D8a	Tolerance of Bit Clock	better than ± 100 ppm	(Consistent with EN 12253)
D9 (*)	Bit Error Rate (B.E.R.) for communication	$\leq 10^{-6}$ when incident power at OBU (DSRC-VU) is in the range given by [D11a to D11b].	(Consistent with EN 12253)
D10	Wake-up trigger for OBU (DSRC-VU)	OBU (DSRC-VU) shall wake up on receiving any frame with 11 or more octets (including preamble)	No special wake-up pattern is necessary. DSRC-VU may wake up on receiving a frame with less than 11 octets (Consistent with EN 12253)
D10a	Maximum Start Time	≤ 5 ms	(Consistent with EN 12253)
D11	Communication zone	Spatial region within which a B.E.R. according to D9a is achieved	(Consistent with EN 12253)
D11a (*)	Power Limit for communication (upper).	– 24dBm	(Consistent with EN 12253)
D11b (*)	Power Limit for communication (lower).	Incident power: – 43 dBm (boresight) – 41 dBm (within – 45° – + 45° Corresponding to the plane parallel to the road surface when the DSRC-VU later is installed in the vehicle (Azimuth))	(Consistent with EN 12253) Extended requirement for horizontal angles up to ± 45°, due to the use cases defined in this annex.
D12 (*)	Cut-off power level of (DSRC-VU)	– 60 dBm	(Consistent with EN 12253)
D13	Preamble	Preamble is mandatory.	(Consistent with EN 12253)
D13a	Preamble Length and Pattern	16 bits ± 1 bit of FM0 coded "1" bits	(Consistent with EN 12253)

Item No.	Parameter	Value(s)	Remark
D13b	Preamble Wave form	An alternating sequence of low level and high level with pulse duration of 2 µs. The tolerance is given byD8a	(Consistent with EN 12253)
D13c	Trailing Bits	The RSU (REDCR) is permitted to transmit a maximum of 8 bits after the end flag. An OBU (DSRC-VU) is not required to take these additional bits into account.	(Consistent with EN 12253)

(*) – Downlink parameters subject to conformance testing in accordance with relevant parameter test from EN 300 674-1

Tabel 14.2

Uplinkparameters

Item No.	Parameter	Value(s)	Remark
U1 (*)	Sub-carrier Frequencies	A OBU (DSRC-VU) shall support 1,5 MHz and 2,0 MHz An RSU (REDCR) shall support 1,5 MHz or 2,0 MHz or both. U1-0: 1,5 MHz U1-1: 2,0 MHz	Selection of sub-carrier frequency (1,5 MHz or 2,0 MHz) depends on the EN 13372 profile selected.
U1a (*)	Tolerance of Sub- carrier Frequencies	within ± 0,1 %	(Consistent with EN 12253)
U1b	Use of Side Bands	Same data on both sides	(Consistent with EN 12253)
U2 (*)	OBU (DSRC-VU) Transmitter Spectrum Mask	According to EN12253 1) Out band power: see ETSI EN 300674-1 2) In band power: [U4a] dBm in 500 kHz 3) Emission in any other uplink channel: U2(3)-1 = – 35 dBm in 500 kHz	(Consistent with EN 12253)
U4a (*)	Maximum Single Side Band E.I.R.P. (boresight)	Two options: U4a-0: – 14 dBm U4a-1: – 21 dBm	According to declared and published specification of equipment designer
U4b (*)	Maximum Single Side Band E.I.R.P. (35°)	Two options: — Not applicable — – 17dBm	According to declared and published specification of equipment designer
U5	Polarisation	Left hand circular	(Consistent with EN 12253)

Item No.	Parameter	Value(s)	Remark
U5a	Cross Polarisation	XPD: In bore sight: (REDCR) RSU r ≥ 15 dB (DSRC-VU) OBU t ≥ 10 dB At – 3 dB: (REDCR) RSU r ≥ 10 dB (DSRC-VU) OBU t ≥ 6 dB	(Consistent with EN 12253)
U6	Sub-Carrier Modulation	2-PSK Encoded data synchronised with sub-carrier: Transitions of encoded data coincide with transitions of sub- carrier.	(Consistent with EN 12253)
U6b	Duty Cycle	Duty Cycle: 50 % ± α, α ≤ 5 %	(Consistent with EN 12253)
U6c	Modulation on Carrier	Multiplication of modulated sub- carrier with carrier.	(Consistent with EN 12253)
U7 (*)	Data Coding	NRZI (No transition at beginning of "1" bit, transition at beginning of "0" bit, no transition within bit)	(Consistent with EN 12253)
U8 (*)	Bit Rate	250 kbit/s	(Consistent with EN 12253)
U8a	Tolerance of Bit Clock	Within ± 1 000 ppm	(Consistent with EN 12253)
U9	Bit Error Rate (B.E.R.) for communication	$\leq 10^{-6}$	(Consistent with EN 12253)
U11	Communication Zone	The spatial region within which the DSRC-VU is situated such that its transmissions are received by the REDCR with a B.E.R. of less than that given by U9a.	(Consistent with EN 12253)
U12a (*)	Conversion Gain (lower limit)	1 dB for each side band Range of angle: Circularly symmetric between bore sight and ± 35° and	
		within – 45° — + 45°Corresponding to the plane parallel to the road surface when the DSRC-VU later is installed in the vehicle (Azimuth)	Greater that the specified value range for horizontal angles up to ± 45°, due to the use cases defined in this annex.
U12b (*)	Conversion Gain (upper limit)	10 dB for each side band	Less than the specified value range for each side band within a circular cone around boresight of ± 45° opening angle
U13	Preamble	Preamble is mandatory.	(Consistent with EN 12253)

Item No.	Parameter	Value(s)	Remark
U13a	Preamble Length and Pattern	32 to 36 µs modulated with sub- carrier only, then 8 bits of NRZI coded "0" bits.	(Consistent with EN 12253)
U13b	Trailing Bits	The DSRC-VU is permitted to transmit a maximum of 8 bits after the end flag. A RSU (REDCR) is not required to take these additional bits into account.	(Consistent with EN 12253)

(*) – Uplink parameters subject to conformance testing in accordance with relevant parameter test from EN 300 674-1

5.3.3 *Antenneontwerp*

5.3.3.1 REDCR-antenne

DSC_30 Het ontwerp van de REDCR-antenne wordt bepaald door de commerciële vormgeving en met het oog op de werking binnen de in punt 5.3.2 bepaalde grenswaarden, waar nodig aangepast om de leesprestaties van de DSRC-REDCR optimaal af te stemmen op het specifieke gebruiksdoel en de werkingsomstandigheden waarvoor de REDCR is ontworpen.

5.3.3.2 VU-antenne

DSC_31 Het ontwerp van de antenne van de DSRC-VU wordt bepaald door de commerciële vormgeving en met het oog op de werking binnen de in punt 5.3.2 bepaalde grenswaarden, waar nodig aangepast om de leesprestaties van de DSRC-REDCR optimaal af te stemmen op het specifieke gebruiksdoel en de werkingsomstandigheden waarvoor de REDCR is ontworpen.

DSC_32 De VU-antenne wordt bevestigd op of nabij de voorruit van het voertuig, zoals gespecificeerd in punt 5.1 hierboven.

DSC_33 Een DSRC-VU-antenne die, overeenkomstig punt 5.1 hierboven, aan de binnenzijde van een heldere standaardvoorruit is vastgemaakt, kan in de testomgeving van een werkplaats (zie punt 6.3) een succesvolle verbinding tot stand brengen met standaardtestapparatuur en met succes een RTM-transactie uitvoeren op de in dit aanhangsel omschreven wijze, op een afstand van 2 tot en met 10 m, met een slaagpercentage van meer dan 99 %, berekend als gemiddelde over 1 000 ondervragingen met leestoegang.

5.4 **DSRC-protocolvereisten voor RTM**

5.4.1 *Overzicht*

DSC_34 Het transactieprotocol om de gegevens te downloaden via de 5,8 GHz DSRC-interface verloopt in de hieronder toegelichte stappen. De beschrijving van de transactiestroom in dit gedeelte berust op ideale omstandigheden zonder hertransmissie of onderbreking van de communicatie.

Opmerking: het doel van de initialisatiefase (stap 1) is tweeledig: enerzijds de verbindingsopbouw tussen de REDCR en de DSRC-VU's die binnen het bereik van de 5,8 GHz DSRC-interface (op master-slavebasis) zijn gekomen, maar nog niet in verbinding staan met de REDCR en anderzijds de aanmelding van toepassingsprocedures.

— **Stap 1** Initialisatie De REDCR verzendt een frame met een dienstrooster radiobaken (BST) waarin de toepassingsidentificatoren (AID's) van de lijst van ondersteunde diensten zijn opgenomen. Voor de RTM-toepassing is dit doorgaans de dienst waarvan de AID gelijk is aan 2 („Freight&Fleet"). De DSRC-VU onderzoekt de ontvangen BST, verzendt als antwoord (zie verder) de lijst van ondersteunde toepassingen in het domein „Freight&Fleet", of antwoordt niet indien geen toepassingen worden ondersteund. Indien de REDCR geen AID=2 verzendt, geeft de DSRC-VU geen antwoord aan de REDCR.

— **Stap 2** De DSRC-VU verzendt een frame met een verzoek om toewijzing van een tijdvenster.

— **Stap 3** De REDCR verzendt een frame met het toegewezen tijdvenster.

— **Stap 4** De DSRC-VU verzendt binnen het toegewezen tijdvenster een frame met het dienstrooster voertuig (VST). Deze VST bevat een lijst van alle toepassingen die deze DSRC-VU ondersteunt in het domein „Freight&Fleet" (AID=2). De verschillende toepassingen worden geïdentificeerd door unieke elementidentificatoren (EID's), gekoppeld aan een parameterwaarde van de contextmarkering die de ondersteunde norm en toepassing aangeeft.

— **Stap 5** De REDCR analyseert de ontvangen VST. Indien de VST irrelevant is (bijvoorbeeld een VST ontvangen van een DSRC-VU die geen ondersteuning biedt aan de RTM-transactie), verbreekt de REDCR de verbinding (Release-commando). Indien de ontvangen VST geschikt wordt bevonden, begint de REDCR de toepassing te concretiseren.

— **Stap 6** Daartoe verzendt de REDCR een frame met een commando om de RTM-gegevens op te halen, waarbij de geconcretiseerde RTM-toepassing wordt geïdentificeerd op basis van de corresponderende identificator die de DSRC-VU in de VST heeft gespecificeerd. Verder wijst de REDCR een tijdvenster toe.

— **Stap 7** De DSRC-VU verzendt binnen het nieuw toegewezen tijdvenster een frame met de adresidentificator die voor de geconcretiseerde RTM-toepassing in de VST is opgegeven, gevolgd door het attribuut *RtmData* (payloadelement + beveiligingselement).

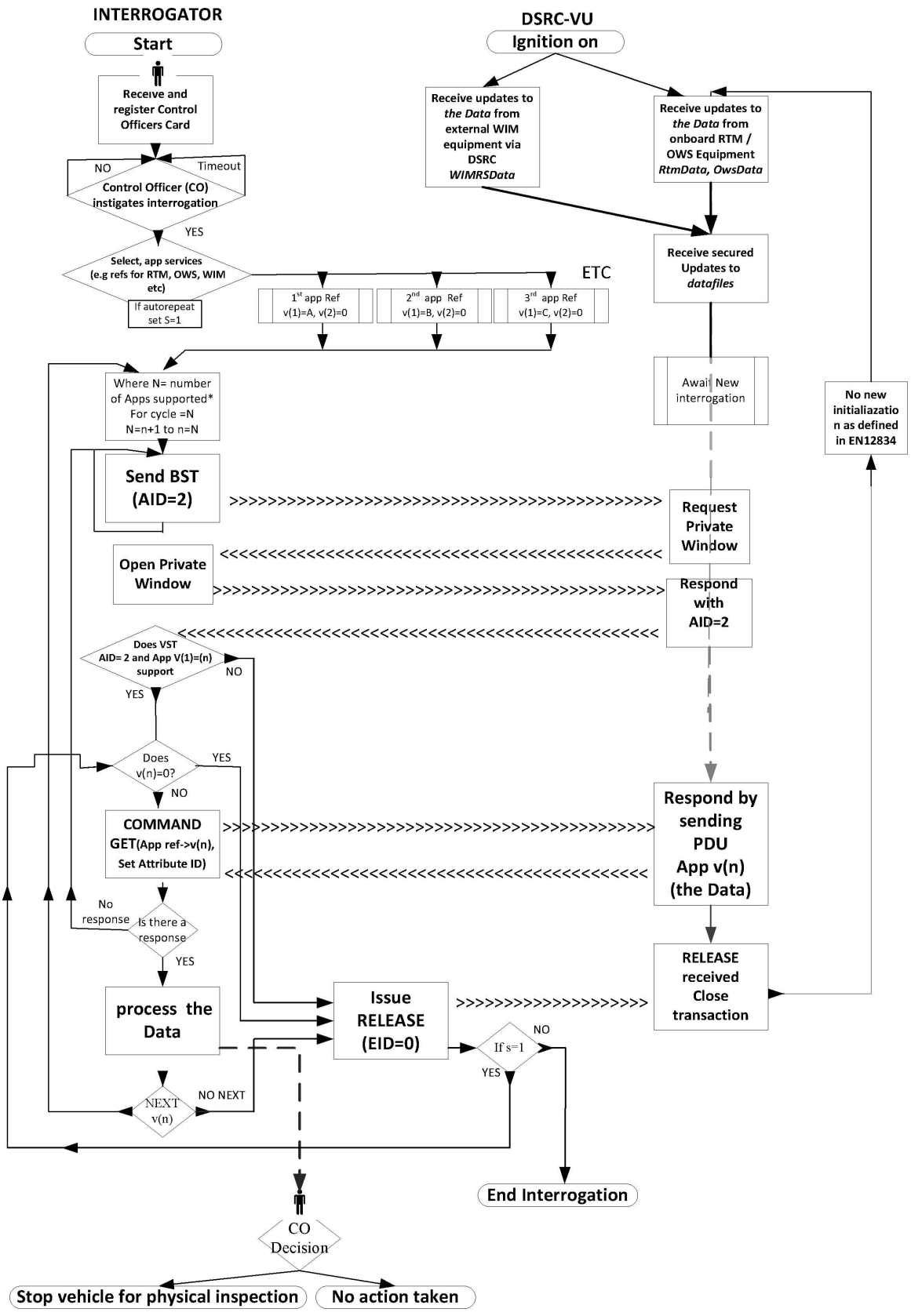
— **Stap 8** Indien meerdere diensten worden aangeroepen, wordt de waarde 'n' gewijzigd in het volgende referentienummer van de dienst, en wordt de procedure opnieuw uitgevoerd.

— **Stap 9** De REDCR bevestigt ontvangst van de gegevens door een frame met een Release-commando naar de DSRC-VU te verzenden om de sessie te beëindigen OF gaat terug naar stap 6 indien de REDCR er niet in geslaagd is de geslaagde ontvangst van de LDPU te valideren.

Het transactieprotocol wordt grafisch verduidelijkt in figuur 14.6.

Figuur 14.6

Stroomschema RTM-proces via 5,8 GHz DSRC-interface



5.4.2 *Commando's*

DSC_35 De volgende commando's zijn de enige functies die tijdens de RTM-transactie worden gebruikt:

— **INITIALISATION.request**: door de REDCR verzonden commando met de definitie van de door de REDCR ondersteunde toepassingen.

— **INITIALISATION.response**: antwoord waarin de DSRC-VU de verbinding bevestigt en waarin een lijst is opgenomen van ondersteunde toepassingen met kenmerken en nadere informatie om deze aan te roepen (EID).

— **GET.request**: door de REDCR naar de DSRC-VU verzonden commando waarin nauwkeurig wordt aangegeven welke toepassing moet worden aangeroepen met behulp van een bepaalde EID in de ontvangen VST, en waarin de DSRC-VU wordt gevraagd de geselecteerde attributen te verzenden met de gegevens. Het Get-commando zorgt ervoor dat de REDCR de gegevens verkrijgt van de DSRC-VU.

— **GET.response**: antwoord van de DSRC-VU waarin de gevraagde gegevens zijn opgenomen.

— **ACTION.request ECHO**: commando waarin de DSRC-VU wordt gevraagd gegevens terug te zenden naar de REDCR. Dankzij het Echo-commando kunnen werkplaatsen of testcentra voor typegoedkeuring de werking van de DSRC-interface testen zonder toegang te moeten krijgen tot beveiligingsreferenties.

— **ACTION.response ECHO**: antwoord van de DSRC VU op het Echo-commando.

— **EVENT_REPORT.request RELEASE**: commando waarin de DSRC-VU wordt opgedragen de transactie te beëindigen. Het Release-commando heeft tot doel de sessie met de DSRC-VU te beëindigen. Na ontvangst van het Release-commando reageert de DSRC-VU niet meer op aanvullende ondervragingen tijdens de huidige verbinding. Overeenkomstig EN 12834 maakt de DSRC-VU niet nogmaals verbinding met hetzelfde ondervragingssysteem tenzij de DSRC-VU zich gedurende 255 seconden buiten het communicatiegebied heeft bevonden, of de baken-ID van het ondervragingssysteem wordt gewijzigd.

5.4.3 *Volgorde van ondervragingscommando's*

DSC_36 Rekening houdend met de volgorde van commando's en antwoorden kan de transactie als volgt worden omschreven:

Sequence	Sender		Receiver	Description	Action
1	REDCR	>	DSRC-VU	Initialisation of the communication link — Request	REDCR broadcasts BST
2	*DSRC-VU*	>	*REDCR*	*Initialisation of the communication link — Response*	*If BST supports AID=2 then DSRC-VU Requests a private window*
3	REDCR	>	DSRC-VU	Grants a private window	Sends Frame containing private window allocation
4	*DSRC-VU*	>	*REDCR*	*Sends VST*	*Sends Frame comprising VST*
5	REDCR	>	DSRC-VU	Sends GET.request for data in Attribute for specific EID	
6	*DSRC-VU*	>	*REDCR*	*Sends GET.response with requested Attribute for specific EID*	*Sends Attribute (RTMData, OWS-Data….) with data for specific EID*

Sequence	Sender		Receiver	Description	Action
7	REDCR	>	DSRC-VU	Sends GET.request for data other Attribute (if appropriate)	
8	*DSRC-VU*	>	*REDCR*	*Sends GET.response with requested Attribute*	*Sends Attribute with data for specific EID*
9	REDCR	>	DSRC-VU	Acknowledges successful receipt of data	Sends RELEASE command which closes transaction
10	*DSRC-VU*			*Closes transaction*	

De transactievolgorde en de inhoud van de uitgewisselde frames worden aan de hand van een voorbeeld verduidelijkt in punten 5.4.7 en 5.4.8.

5.4.4 *Gegevensstructuren*

DSC_37 De semantische structuur van de via de 5,8 GHz DSRC-interface uitgewisselde gegevens stemt overeen met de in dit aanhangsel vervatte beschrijving. In dit punt wordt uiteengezet hoe deze gegevens worden gestructureerd.

DSC_38 De payloadgegevens (RTM-gegevens) bestaan uit de samenvoeging van:

1. EncryptedTachographPayload data, zijnde de codering van de in punt 5.4.5 van ASN.1 gedefinieerde TachographPayload. De coderingsmethode wordt nader toegelicht in aanhangsel 11.

2. DSRCSecurityData, zoals gespecificeerd in aanhangsel 11.

DSC_39 De RTM-gegevens worden aangeroepen met RTM-attribuut=1 en overgebracht in RtmContainer=10.

DSC_40 Rtm-ContextMark identificeert het deel van de ondersteunde norm uit de TARV-normenreeks (voor RTM is dit deel 9).

De ASN.1-module voor de DSRC-interfacegegevens in de RTM-toepassing wordt als volgt gedefinieerd:

```
    TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}
    DEFINITIONS AUTOMATIC TAGS
    ::= BEGIN
    IMPORTS
    -- Imports data attributes and elements from EFC which are used for RTM
    LPN
    FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

    -- Imports function parameters from the EFC Application Interface Definition
    SetMMIRq
    FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

    -- Imports the L7 DSRCData module data from the EFC Application Interface Definition
    Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
    Attributes,
    BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
    EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
    ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
    FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};


    -- Definitions of the RTM functions:
    RTM-InitialiseComm-Request ::= BST
    RTM-InitialiseComm-Response::= VST
    RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT,iid
    ABSENT,  attrIdList})
    RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
    RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
    eventType (0)})

    RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
    (15), accessCredentials ABSENT, iid ABSENT})

    RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
    (0), iid ABSENT})

    -- Definitions of the RTM attributes:
    RtmData ::= SEQUENCE {
          encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting
    TachographPayload as per Appendix 11 --}),
          DSRCSecurityData OCTET STRING
          }
    TachographPayload ::= SEQUENCE {
                tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
                tp15638SpeedingEvent            BOOLEAN,  -- 1= Irregularities in speed (see Annex 1C)
                tp15638DrivingWithoutValidCard  BOOLEAN,     -- 1= Invalid card usage (see Annex 1C)
                tp15638DriverCard               BOOLEAN,-- 0= Indicates a valid driver card  (see Annex 1C)
                tp15638CardInsertion            BOOLEAN, -- 1= Card insertion while driving (see Annex 1C)
                tp15638MotionDataError          BOOLEAN, -- 1= Motion data error (see Annex 1C)
                tp15638VehicleMotionConflict    BOOLEAN, -- 1= Motion conflict (see Annex 1C)
                tp156382ndDriverCard            BOOLEAN, -- 1= Second driver card inserted (see Annex 1C)
                tp15638CurrentActivityDriving   BOOLEAN, -- 1= other activity selected;
                                                          -- 0= driving selected
                tp15638LastSessionClosed        BOOLEAN, -- 1= improperly, 0= properly, closed
                tp15638PowerSupplyInterruption  INTEGER (0..127), -- Supply interrupts in the last 10 days
                tp15638SensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
    -- All subsequent time related types as defined in Annex 1C.
                tp15638TimeAdjustment           INTEGER(0..4294967295), -- Time of the last time adjustment
                tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
                tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
                tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration data
                tp15638DateTachoConnected       INTEGER(0..4294967295), -- Date tachograph connected
                tp15638CurrentSpeed             INTEGER (0..255), -- Last current recorded speed
                tp15638Timestamp                INTEGER(0..4294967295) -- Timestamp of current record[2]
                }
Rtm-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version

  RtmCommProfile          INTEGER {
                                  C1 (1),
                                  C2 (2)
                                  } (0..255) DEFAULT 1
  }
RtmTransferAck ::= INTEGER {
                  Ok (1),
                  NoK (2)
                  } SIZE (1..255)
```

```
StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
        integer                         [0]    INTEGER,
        bitstring                       [1]    BIT STRING,
        octetstring                     [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString                 [3]    UniversalString,
        beaconId                        [4]    BeaconID,
        t-apdu                          [5]    T-APDUs,
        dsrcApplicationEntityId         [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                     [7]    Dsrc-EID,
        attrIdList                      [8]    AttributeIdList,
        attrList                        [9]    AttributeList{RtmContainer},
        rtmData                         [10]   RtmData,
        rtmContextmark                  [11]   Rtm-ContextMark,
        reserved12                      [12]   NULL,
        reserved13                     [13]   NULL,
        reserved14                      [14]   NULL,
        time                            [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.4.5 *Elementen van RtmData, uitgevoerde acties en definities*

DSC_41 De VU berekent de gegevenswaarden waarmee de beveiligde gegevens in de DSRC-VU worden geactualiseerd, overeenkomstig de regels in tabel 14.3.

Tabel 14.3

Elementen van RtmData, uitgevoerde acties en definities

(1) RTM Data Element	(2) Action performed by the VU		(3) ASN.1 definition of data
RTM1 **Vehicle Registration Plate**	The VU shall set the value of the *tp15638VehicleRegistrationPlate* data element RTM1 from the recorded value of the data type *VehicleRegistrationIdentification* as defined in Appendix 1 *VehicleRegistrationIdentification*	Vehicle Registration Plate expressed as a string of characters	`tp15638VehicleRegstrationPlate LPN, --Vehicle Registration Plate imported from ISO 14906 with the limitation specified in EN 15509 which is a SEQUENCE comprising Country Code followed by an alphabet indicator followed by the plate number itself, which is always 14 octets (padded with zero's) so the EN 15509 LPN type length is always 17 octets, of which 14 are the "real" plate number.`

(1) RTM Data Element	(2) Action performed by the VU		(3) ASN.1 definition of data
RTM2 **Speeding Event**	The VU shall generate a Boolean value for data element RTM2 tp15638SpeedingEvent. The tp15638SpeedingEvent value shall be calculated by the VU from the number of Over Speeding Events recorded in the VU in the last 10 days of occurrence, as defined in Annex 1C. If there is at least one tp15638SpeedingEvent in the last 10 days of occurrence, the tp15638SpeedingEvent value shall be set to TRUE. ELSE if there are no events in the last 10 days of occurrence, the tp15638SpeedingEvent shall be set to FALSE.	1 (TRUE) — Indicates irregularities in speed within last 10 days of occurrence	`tp15638speedingEvent BOOLEAN,`
RTM3 **Driving Without Valid Card**	The VU shall generate a boolean value for data element RTM3 tp15638DrivingWithoutValidCard. The VU shall assign a value of True to the tp15638DrivingWithoutValidCard variable if the VU data has recorded at least one event in the last 10 days of occurrence of type "Driving without an appropriate card" event as defined in Annex 1C. ELSE if there are no events in the last 10 days of occurrence, the tp15638DrivingWithoutValidCard variable shall be set to FALSE.	1 (TRUE) = Indicates invalid card usage	`tp15638DrivingWithoutValidCard` `BOOLEAN,`
RTM4 **Valid Driver Card**	The VU shall generate a boolean value for data element RTM4 tp15638DriverCard on the basis of the data stored in the VU and defined in Appendix 1. If no valid driver card is present the VU shall set the variable to TRUE ELSE if a valid driver card is present the VU shall set the variable to FALSE	0 (FALSE) = Indicates a valid driver card	`tp15638DriverCard BOOLEAN,`
RTM5 **Card Insertion while Driving**	The VU shall generate a boolean value for data element RTM5. The VU shall assign a value of TRUE to the tp15638CardInsertion variable if the VU data has recorded in the last 10 days of occurrence at least one event of type "Card insertion while driving." as defined in Annex 1C. ELSE if there are no such events in the last 10 days of occurrence, the tp15638CardInsertion variable shall be set to FALSE.	1 (TRUE) = Indicates card insertion while driving within last 10 days of occurrence	`tp15638CardInsertion BOOLEAN,`
RTM6 **Motion Data Error**	The VU shall generate a Boolean value for data element RTM6. The VU shall assign a value of TRUE to the tp15638MotionDataError variable if the VU data has in the last 10 days of occurrence recorded at least one event of type "Motion data error" as defined in Annex 1C. ELSE if there are no such events in the last 10 days of occurrence, the tp15638MotionDataError variable shall be set to FALSE.	1 (TRUE) = Indicates motion data error within last 10 days of occurrence	`tp15638motionDataError BOOLEAN,`

(1) RTM Data Element	(2) Action performed by the VU		(3) ASN.1 definition of data
RTM7 **Vehicle Motion Conflict**	The VU shall generate a Boolean value for data element RTM7. The VU shall assign a value of TRUE to the tp15638vehicleMotionConflict variable if the VU data has in the last 10 days recorded at least one event of type Vehicle Motion Conflict (value '0A'H). ELSE if there are no events in the last 10 days of occurrence, the tp15638vehicleMotionConflict variable shall be set to FALSE.	1 (TRUE) = Indicates motion conflict within last 10 days of occurrence	`tp15638vehicleMotionConflict` `BOOLEAN,`
RTM8 **2nd Driver Card**	The VU shall generate a Boolean value for data element RTM8 on the basis of Annex 1C ("Driver Activity Data" CREW and CO-DRIVER). If a 2nd valid driver card is present the VU shall set the variable to TRUE ELSE if a 2nd valid driver card is not present the VU shall set the variable to FALSE	1 (TRUE) = Indicates a second driver card inserted	`tp156382ndDriverCard BOOLEAN,`
RTM9 **Current Activity**	The VU shall generate a booleanvalue for data element RTM9. If the current activity is recorded in the VU as any activity other than "DRIVING" as defined in Annex 1C the VU shall set the variable to TRUE ELSE if the current activity is recorded in the VU as "DRIVING" the VU shall set the variable to FALSE	1 (TRUE) = other activity selected; 0 (FALSE) = driving selected	`tp15638currentActivityDriving` `BOOLEAN`
RTM10 **Last Session Closed**	The VU shall generate a boolean value for data element RTM10. If the last card session was not properly closed as defined in Annex 1C the VU shall set the variable to TRUE. ELSE if the last card session was properly closed the VU shall set the variable to FALSE	1 (TRUE) = improperly closed 0 (FALSE) = properly closed	`tp15638lastSessionClosed` `BOOLEAN`
RTM11 **Power Supply Interruption**	The VU shall generate an integer value for data element RTM11. The VU shall assign a value for the tp15638PowerSupplyInterruption variable equal to the longest power supply interruption according to Article 9, Reg (EU) 165/2014 of type "Power supply interruption" as defined in Annex 1C. ELSE if in the last 10 days of occurrence there are have been no Power supply interruption events the value of the integer shall be set to 0.	— Number of power supply interruptions in last 10 days of occurrence	`tp15638powerSupplyInterruption` `INTEGER (0..127),`

(1) RTM Data Element	(2) Action performed by the VU		(3) ASN.1 definition of data
RTM12 **Sensor Fault**	The VU shall generate an integer value for data element RTM12. The VU shall assign to the variable sensorFault a value of: — 1 if an event of type '35'H Sensor fault has been recorded in the last 10 days, — 2 if an event of type GNSS receiver fault (either internal or external with enum values '51'H or '52'H) has been recorded in the last 10 days. — 3 if an event of type '53'H External GNSS communication fault has been recorded in the last 10 days of occurrence. — 4 If both Sensor Fault and GNSS receiver faults have been recorded in the last 10 days of occurrence — 5 If both Sensor Fault and External GNSS communication faults have been recorded in the last 10 days of occurrence — 6 If both GNSS receiver fault and External GNSS communication fault have been recorded in the last 10 days of occurrence — 7 If all three sensor faults, have been recorded in the last 10 days of occurrence ELSE it shall assign a value of 0 if no events have been recorded in the last 10 days of occurrence	— sensor fault one octet as per data dictionary	`tp15638SensorFault INTEGER (0..255),`
RTM13 **Time Adjustment**	The VU shall generate an integer value (timeReal from Appendix 1) for data element RTM13 on the basis of the presence of Time Adjustment data as defined in Annex 1C. The VU shall assign the value of time at which the last time adjustment data event has occurred. ELSE if no "Time Adjustment" event. as defined in Annex 1C is present in the VU data it shall set a value of 0	Time of the last time adjustment	`tp15638TimeAdjustment INTEGER(0..4294967295),`
RTM14 **Security Breach Attempt**	The VU shall generate an integer value (timeReal from Appendix 1) for data element RTM14 on the basis of the presence of a Security breach attempt event as defined in Annex 1C. The VU shall set the value of the time of the latest security breach attempt event recorded by the VU. ELSE if no "security breach attempt" event as defined in Annex 1C is present in the VU data it shall set a value of 0x00FF.	Time of last breach attempt — Default value =0x00FF	`tp15638LatestBreachAttempt INTEGER(0..4294967295),`
RTM15 **Last Calibration**	The VU shall generate an integer value (timeReal from Appendix 1) for data element RTM15 on the basis of the presence of Last Calibration data as defined in Annex 1C. The VU shall set the value of time of the latest two calibrations (RTM15 and RTM16), which are set in VuCalibrationData defined in Appendix 1. The VU shall set the value for RTM15 to the timeReal of the latest calibration record.	Time of last calibration data	`tp15638LastCalibrationData INTEGER(0..4294967295),`

(1) RTM Data Element	(2) Action performed by the VU		(3) ASN.1 definition of data
RTM16 **Previous Calibration**	The VU shall generate an integer value (timeReal from Appendix 1) for data element RTM16 of the calibration record preceding that of the last calibration ELSE if there has been no previous calibration the VU shall set the value of RTM16 to 0.	Time of previous calibration data	`tp15638PrevCalibrationData` `INTEGER(0..4294967295),`
RTM17 **Date Tachograph Connected**	For data element RTM17 the VU shall generate an integer value (timeReal from Appendix 1). The VU shall set the value of the time of the initial installation of the VU. The VU shall extract this data from the VuCalibrationData (Appendix 1) from the vuCalibrationRecords with CalibrationPurpose equal to: '03'H	Date tachograph connected	`tp15638DateTachoConnected` `INTEGER(0..4294967295),`
RTM18 **Current Speed**	The VU shall generate an integer value for data element RTM18. The VU shall set the value for RTM16 to the last current recorded speed at the time of the latest update of the RtmData.	Last current recorded speed	`tp15638CurrentSpeed` `INTEGER (0..255),`
RTM19 **Timestamp**	For data element RTM19 the VU shall generate an integer value (timeReal from Appendix 1). The VU shall set the value for RTM19 to the time of the latest update of the RtmData.	Timestamp of current TachographPayload record	`tp15638Timestamp` `INTEGER(0..4294967295),`

5.4.6 *Mechanisme voor gegevensoverdracht*

DSC_42 Eerder gedefinieerde payloadgegevens worden na de initialisatiefase opgevraagd door de REDCR en vervolgens door de DSRC-VU verzonden binnen het toegewezen tijdvenster. De REDCR gebruikt het Get-commando om de gegevens op te halen.

DSC_43 Voor elke uitwisseling via DSRC-interfaces worden de gegevens gecodeerd op basis van PER (Packed Encoding Rules).

5.4.7 *Gedetailleerde beschrijving van transacties via DSRC-interfaces*

DSC_44 De initialisatie wordt uitgevoerd overeenkomstig de voorschriften DSC_44 tot en met DSC_48 en de tabellen 14.4 tot en met 14.9. Bij aanvang van de initialisatiefase verzendt de REDCR een frame met een dienstrooster radiobaken (BST) overeenkomstig EN 12834 en EN 13372, punten 6.2, 6,3, 6,4 en 7.1, waarvan de instellingen worden gespecificeerd in de onderstaande tabel 14.4.

Tabel 14.4

Initialisatie: instellingen BST-frame

Field	Settings
Link Identifier	Broadcast address
BeaconId	As per EN 12834
Time	As per EN 12834
Profile	No extension, 0 or 1 to be used
MandApplications	No extension, EID not present, Parameter not present, AID= 2 Freight&Fleet
NonMandApplications	Not present
ProfileList	No extension, number of profiles in list = 0
Fragmentation header	No fragmentation
Layer 2 settings	Command PDU, UI command

In de onderstaande tabel 14.5 worden de instellingen van tabel 14.4 verduidelijkt aan de hand van een praktijkvoorbeeld, met aanduiding van de bitcodering.

Tabel 14.5

Initialisatie: voorbeeld inhoud BST-frame

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Broadcast ID	1111 1111	Broadcast address
3	MAC Control Field	1010 0000	Command PDU
4	LLC Control field	0000 0011	UI command
5	Fragmentation header	1xxx x001	No fragmentation

Octet #	Attribute/Field	Bits in octet	Description
6	BST	1000	Initialisation request
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	NonMand applications not present
		xxx	Manufacturer Identifier
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	27 bit ID available for manufacturer
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	32 bit UNIX real time
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,…)	0000 0000	No extension. Example profile 0
17	MandApplications SEQUENCE (SIZE(0..127, …)) OF {	0000 0001	No extension, Number of mandApplications=1
18	SEQUENCE {		
	OPTION indicator	0	EID not present
	OPTION indicator	0	Parameter not present
	AID DSRCApplicationEntityID } }	00 0010	No extension. AID= 2 Freight&Fleet

Octet #	Attribute/Field	Bits in octet	Description
19	ProfileList SEQUENCE (0..127,…) OF Profile }	0000 0000	No extension, number of profiles in list = 0
20	FCS	xxxx xxxx	Frame check sequence
21		xxxx xxxx	
22	Flag	0111 1110	End Flag

DSC_45 Bij ontvangst van een BST verzendt de DSRC-VU een verzoek om toewijzing van een tijdvenster, als bedoeld in EN 12795 en EN 13372, punt 7.1.1, zonder specifieke RTM-instellingen. In tabel 14.6 staat een voorbeeld van de bitcodering.

Tabel 14.6

Initialisatie: frame-inhoud verzoek om toewijzing van tijdvenster

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of specific DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0110 0000	Private window request
7	FCS	xxxx xxxx	Frame check sequence
8		xxxx xxxx	
9	Flag	0111 1110	End Flag

DSC_46 De REDCR beantwoordt dit verzoek door een tijdvenster toe te wijzen, als bedoeld in EN 12795 en EN 13372, punt 7.1.1, zonder specifieke RTM-instellingen.

In tabel 14.7 staat een voorbeeld van de bitcodering.

Tabel 14.7

Initialisatie: frame-inhoud toewijzing van tijdvenster

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0010 s000	Private window allocation
7	FCS	xxxx xxxx	Frame check sequence
8		xxxx xxxx	
9	Flag	0111 1110	End Flag

DSC_47 Bij ontvangst van het toegewezen tijdvenster verzendt de DSRC-VU het dienstrooster voertuig (VST), als bedoeld in EN 12834 en EN 13372, punten 6.2, 6,3, 6.4 en 7.1, volgens de in tabel 14.8 gespecificeerde instellingen en binnen het toegewezen tijdvenster voor verzending.

Tabel 14.8

Initialisatie: instellingen VST-frame

Field	Settings
Private LID	As per EN 12834
VST parameters	Fill=0, then for each supported application: EID present, parameter present, AID=2, EID as generated by the OBU
Parameter	No extension, Contains the RTM Context Mark
ObeConfiguration	The optional ObeStatus field may be present, but shall not be used by the REDCR
Fragmentation header	No fragmentation
Layer 2 settings	Command PDU, UI command

DSC_48 De DSRC-VU ondersteunt de toepassing „Freight and Fleet", geïdentificeerd door toepassingsidentificator (AID) '2'. Mogelijk worden andere toepassingsidentificatoren ondersteund, maar die staan niet in deze VST, aangezien de BST alleen AID=2 vereist. Het veld „Toepassingen" bevat een lijst van ondersteunde toepassingen in de DSRC-VU. Voor elke ondersteunde toepassing wordt een verwijzing naar de toepasselijke norm opgegeven, met name Rtm-ContextMark, bestaande uit een objectidentificator die de bijbehorende norm voorstelt, het deel van de norm (deel 9 voor RTM) en in voorkomend geval de versie daarvan, alsook een EID die door de DSRC-VU wordt gegenereerd en die aan deze toepassing gekoppeld is.

In de onderstaande tabel 14.9 worden de instellingen van tabel 14.8 verduidelijkt aan de hand van een praktijkvoorbeeld, met aanduiding van de bitcodering.

Tabel 14.9

Initialisatie: voorbeeld inhoud VST-frame

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1100 0000	Command PDU
7	LLC Control field	0000 0011	UI command
8	Fragmentation header	1xxx x001	No fragmentation
9	VST SEQUENCE {	1001	Initialisation response
	Fill BIT STRING (SIZE(4))	0000	Unused and set to 0
10	Profile INTEGER (0..127,...) Applications SEQUENCE OF {	0000 0000	No extension. Example profile 0
11		0000 0001	No extension, 1 application
12	SEQUENCE {		
	OPTION indicator	1	EID present
	OPTION indicator	1	Parameter present
	AID DSRCApplicationEntityID	00 0010	No extension. AID= 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Defined within the OBU and identifying the application instance.

Octet #	Attribute/Field	Bits in octet	Description
14	Parameter Container {	0000 0010	No extension, Container Choice = 02, Octet string
15		0000 1000	No extension, Rtm Context Mark length = 8
16	Rtm-ContextMark::= SEQUENCE { StandardIdentifier standardIdentifier	0000 0110	Object Identifier of the supported standard, part, and version. Example: ISO (1) Standard (0) TARV (15638) part9 (9) Version1 (1). First octet is 06H, which is the Object Identifier Second octet is 06H, which is its length. Subsequent 6 octets encode the example Object Identifier Note that only one element of the sequence is present (the optional RtmCommProfile element is omitted)
17		0000 0110	
18		0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0000 1001	
23		0000 0001	
24	ObeConfiguration Sequence { OPTION indicator	0	ObeStatus not present
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	Manufacturer identifier for the DSRC-VU as described in ISO 14816 Register
27		xxxx xxxx	
28	FCS	xxxx xxxx	Frame check sequence
29		xxxx xxxx	
30	Flag	0111 1110	End Flag

DCS_49 De REDCR leest vervolgens de gegevens door een Get-commando te verzenden, zoals gedefinieerd in EN 13372, punten 6.2, 6.3 en 6.4 en in EN 12834, met de in tabel 14.10 gespecificeerde instellingen.

Tabel 14.10

Overzicht: instellingen GET.request-frame

Field	Settings
Invoker Identifier (IID)	Not present
Link Identifier (LID)	Link address of the specific DSRC-VU
Chaining	No

Field	Settings
Element Identifier (EID)	As specified in the VST. No extension
Access Credentials	No
AttributeIdList	No extension, 1 attribute, AttributeID = 1 (RtmData)
Fragmentation	No
Layer2 settings	Command PDU, Polled ACn command

In tabel 14.11 wordt aan de hand van een voorbeeld verduidelijkt hoe de RTM-gegevens worden gelezen.

Tabel 14.11

Overzicht: voorbeeld GET.request-frame

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	Command PDU
7	LLC Control field	n111 0111	Polled ACn commando, n-bit
8	Fragmentation header	1xxx x001	No fragmentation
9	Get.request SEQUENCE {	0110	Get request
	OPTION indicator	0	Access Credentials not present
	OPTION indicator	0	IID not present
	OPTION indicator	1	AttributeIdList present
	Fill BIT STRING(SIZE(1))	0	Set to 0.
10	EID INTEGER(0..127,…)	xxxx xxxx	The EID of the RTM application instance, as specified in the VST. No extension
11	AttributeIdList SEQUENCE OF { AttributeId }}	0000 0001	No extension, number of attributes = 1
12		0000 0001	AttributeId=1, RtmData. No extension

Octet #	Attribute/Field	Bits in octet	Description
13	FCS	xxxx xxxx	Frame check sequence
14		xxxx xxxx	
15	Flag	0111 1110	End Flag

DSC_50 Bij ontvangst van een verzoek om gegevens op te halen (Get-commando) verzendt de DSRC-VU een antwoord met de opgevraagde gegevens, zoals gedefinieerd in EN 13372, punten 6.2, 6.3 en 6.4 en in EN 12834, met de in tabel 14.12 gespecificeerde instellingen.

Tabel 14.12

Overzicht: instellingen GET.response-frame

Field	Settings
Invoker Identifier (IID)	Not present
Link Identifier (LID)	As per EN 12834
Chaining	No
Element Identifier (EID)	As specified in the VST.
Access Credentials	No
Fragmentation	No
Layer2 settings	Response PDU, Response available and command accepted, ACn command

In tabel 14.13 wordt aan de hand van een voorbeeld verduidelijkt hoe de RTM-gegevens worden gelezen.

Tabel 14.13

Overzicht: voorbeeld inhoud antwoordframe

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	

Octet #	Attribute/Field	Bits in octet	Description
6	MAC Control field	1101 0000	Response PDU
7	LLC Control field	n111 0111	Response available, ACn command n bit
8	LLC Status field	0000 0000	Response available and command accepted
9	Fragmentation header	1xxx x001	No fragmentation
10	Get.response SEQUENCE {	0111	Get response
	OPTION indicator	0	IID not present
	OPTION indicator	1	Attribute List present
	OPTION indicator	0	Return status not present
	Fill BIT STRING(SIZE(1))	0	Not used
11	EID INTEGER(0..127,…)	xxxx xxxx	Responding from the RTM application Instance. No extension,
12	AttributeList SEQUENCE OF {	0000 0001	No extension, number of attributes = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	No extension, AttributeId=1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	No extension, Container Choice = 10_{10}.
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	Frame check sequence
n+2		xxxx xxxx	
n+3	Flag	0111 1110	End Flag

DSC_51 De REDCR verbreekt vervolgens de verbinding door een Event_Report, Release-commando te verzenden overeenkomstig EN 13372, punten 6.2, 6.3 en 6.4 en EN 12834, punt 7.3.8, zonder specifieke RTM-instellingen. In tabel 14.14 staat een voorbeeld van de bitcodering voor het Release-commando.

Tabel 14.14

Verbindingsverbreking Frame-inhoud Event_Report Release-commando

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1000 s000	The frame contains a command LPDU
7	LLC Control field	0000 0011	UI command
8	Fragmentation header	1xxx x001	No fragmentation
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Access Credentials not present
	OPTION indicator	0	Event parameter not present
	OPTION indicator	0	IID not present
	Mode BOOLEAN	0	No response expected
10	EID INTEGER (0..127,…)	0000 0000	No extension, EID = 0 (System)
11	EventType INTEGER (0..127,…) }	0000 0000	Event type 0 = Release
12	FCS	xxxx xxxx	Frame check sequence
13		xxxx xxxx	
14	Flag	0111 1110	End Flag

DSC_52 De DSRC-VU dient het Release-commando niet te beantwoorden. De verbinding wordt daarop verbroken.

5.4.8 *Beschrijving van de testtransactie via DSRC-interfaces*

DSC_53 Zoals vastgelegd in aanhangsel 11 „Algemene beveiligingsmechanismen” moeten met behulp van het hierboven toegelichte Get-commando volledige tests, met inbegrip van gegevensbeveiliging, worden uitgevoerd door personen die over de nodige bevoegdheden beschikken om toegang te krijgen tot beveiligingsprocedures.

DSC_54 Zoals voorgeschreven in aanhangsel 11 „Algemene beveiligingsmechanismen" en in aanhangsel 9 „Lijst van minimaal vereiste typegoedkeuringstests" moeten op het ogenblik van inbedrijfstelling en bij periodieke controles tests worden uitgevoerd.

Niettemin kan de basisfunctie voor communicatie op afstand via DSRC-interfaces worden getest met behulp van het Echo-commando. Deze tests kunnen niet alleen worden vereist op het ogenblik van inbedrijfstelling of bij periodieke controles, maar ook indien de bevoegde controleautoriteit dit verlangt of indien de tachograafverordening zulks voorschrijft (zie punt 6 hieronder).

DSC_55 Om deze basistest uit te voeren, verzendt de REDCR het Echo-commando tijdens een verbindingssessie, dat wil zeggen nadat de initialisatiefase met succes is voltooid. De volgorde van interacties is derhalve vergelijkbaar met die van een ondervraging:

— Stap 1 De REDCR verzendt een dienstrooster radiobaken (BST) met de toepassingsidentificatoren (AID's) in de lijst van ondersteunde diensten. Voor RTM-toepassingen is dit doorgaans de dienst waarvan de AID gelijk is aan 2.

De DSRC-VU onderzoekt de ontvangen BST en verzendt een antwoord indien blijkt dat in de BST de toepassing „Freight&Fleet" (AID=2) wordt aangeroepen. Indien de REDCR geen AID=2 verzendt, beëindigt de DSRC-VU de transactie met de REDCR.

— Stap 2 De DSRC-VU verzendt een verzoek om toewijzing van een tijdvenster.

— Stap 3 De REDCR verzendt een toegewezen tijdvenster.

— Stap 4 De DSRC-VU verzendt binnen het toegewezen tijdvenster een frame met het dienstrooster voertuig (VST). Deze VST bevat een lijst van alle toepassingen die deze DSRC-VU ondersteunt in het domein „Freight&Fleet" (AID=2). De verschillende toepassingen worden geïdentificeerd door unieke elementidentificatoren (EID's), gekoppeld aan een parameterwaarde die de ondersteunde toepassing aangeeft.

— Stap 5 De REDCR analyseert de ontvangen VST. Indien de VST als irrelevant wordt beschouwd (bijvoorbeeld een VST ontvangen van een DSRC-VU die geen RTM-VU is), verbreekt de REDCR de verbinding (Release-commando). Wordt de ontvangen VST geschikt bevonden, dan begint de REDCR de toepassing te concretiseren.

— Stap 6 De REDCR verzendt een Echo-commando naar de betrokken DSRC-VU, en wijst een tijdvenster toe.

— Stap 7 De DSRC-VU verzendt binnen het toegewezen tijdvenster een Echo-antwoordframe.

De gegevensuitwisseling in het kader van een Echo-commando wordt verduidelijkt aan de hand van het praktijkvoorbeeld in de volgende tabellen.

DSC_56 De initialisatie wordt uitgevoerd overeenkomstig punt 5.4.7 (DSC_44 tot en met DSC_48) en tabellen 14.4 tot en met 14.9.

DSC_57 De REDCR verzendt een Action, Echo-commando overeenkomstig ISO 14906 met 100 gegevensbytes en zonder specifieke RTM-instellingen. De inhoud van het door de REDCR verzonden frame wordt verduidelijkt in tabel 14.15.

Tabel 14.15

Voorbeeld van het Action, Echo-verzoekframe

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific DSRC-VU
3		xxxx xxxx	

Octet #	Attribute/Field	Bits in octet	Description
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	Command PDU
7	LLC Control field	n111 0111	Polled ACn commando, n-bit
8	Fragmentation header	1xxx x001	No fragmentation
9	ACTION.request SEQUENCE {	0000	Action request (ECHO)
	OPTION indicator	0	Access Credentials not present
	OPTION indicator	1	Action parameter present
	OPTION indicator	0	IID not present
	Mode BOOLEAN	1	Response expected
10	EID INTEGER (0..127,…)	0000 0000	No extension, EID = 0 (System)
11	ActionType INTEGER (0..127,…)	0000 1111	No extension, Action type ECHO request
12	ActionParameter CONTAINER {	0000 0010	No extension, Container Choice = 2
13		0110 0100	No extension. String length = 100 octets
14		xxxx xxxx	Data to be echoed
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Frame check sequence
115		xxxx xxxx	
116	Flag	0111 1110	End Flag

DSC_58 Bij ontvangst van het Echo-verzoek verzendt de DSRC-VU een Echo-antwoord van 100 bytes waarin het ontvangen commando wordt weergegeven overeenkomstig ISO 14906, zonder specifieke RTM-instellingen. In tabel 14.16 wordt de bitcodering verduidelijkt aan de hand van een voorbeeld.

Tabel 14.16

Voorbeeld van het Action, Echo-antwoordframe

Octet #	Attribute/Field	Bits in octet	Description
1	FLAG	0111 1110	Start flag
2	Private LID	xxxx xxxx	Link address of the specific VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	Response PDU
7	LLC Control field	n111 0111	ACn command n bit
8	LLC status field	0000 0000	Response available
9	Fragmentation header	1xxx x001	No fragmentation
10	ACTION.response SEQUENCE {	0001	ACTION response (ECHO)
	OPTION indicator	0	IID not present
	OPTION indicator	1	Response parameter present
	OPTION indicator	0	Return status not present
	Fill BIT STRING (SIZE (1))	0	Not used
11	EID INTEGER (0..127,…)	0000 0000	No extension, EID = 0 (System)
12	ResponseParameter CONTAINER {	0000 0010	No extension, Container Choice = 2
13		0110 0100	No extension. String length = 100 octets
14		xxxx xxxx	Echoed data
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Frame check sequence
115		xxxx xxxx	
116	Flag	0111 1110	End Flag

5.5 **Naleving van Richtlijn (EU) 2015/71**

5.5.1 *Overzicht*

DSC_59 Ter ondersteuning van Richtlijn (EU) 2015/719 met betrekking tot de maximaal toegestane afmetingen en gewichten voor zware vrachtvoertuigen 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 objectidentificator van de TARV-norm verwijst naar deel 20 van de norm ISO 15638 (TARV) met betrekking tot WOB/OWS.

5.5.2 *Commando's*

DSC_60 Voor de OWS-transactie wordt hetzelfde commando gebruikt als voor een RTM-transactie.

5.5.3 *Volgorde van ondervragingscommando's*

DSC_61 De volgorde van ondervragingscommando's voor OWS-gegevens is identiek aan die voor RTM-gegevens.

5.5.4 *Gegevensstructuren*

DSC_62 De payloadgegevens (OWS-gegevens) bestaan uit de samenvoeging van:

1. EncryptedOwsPayload data, zijnde de codering van de in punt 5.5.5 van ASN.1 gedefinieerde OwsPayload. Zoals gespecificeerd in aanhangsel 11, wordt dezelfde coderingsmethode toegepast als voor RtmData.

2. DSRCSecurityData, berekend met dezelfde algoritmen als voor de RtmData, zoals gespecificeerd in aanhangsel 11.

5.5.5 *ASN.1-module voor de OWS-transactie via DSRC-interface*

DSC_63 De ASN.1-module voor de DSRC-interfacegegevens in de RTM-toepassing wordt als volgt gedefinieerd:

```
   TarvOws {iso(1) standard(0) 15638 part20(20)
   version1(1)} DEFINITIONS AUTOMATIC TAGS
   ::= BEGIN
   IMPORTS
   -- Imports data attributes and elements from EFC which are used for OWS
   LPN
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports function parameters from the EFC Application Interface Definition
   SetMMIRq
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Imports the L7 DSRCData module data from the EFC Application Interface Definition
   Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
   Attributes,
   BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
   EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
   ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
   FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};

   -- Definitions of the OWS functions:
   OWS-InitialiseComm-Request ::= BST
   OWS-InitialiseComm-Response::= VST
   OWS-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials
   ABSENT, iid ABSENT, attrIdList})
   OWS-DataRetrieval-Response::= Get-Response {OwsContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
   OWS-TerminateComm::= Event-Report-Request {OwsContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
   eventType (0)})
   OWS-TestComm-Request::= Action-Request {OwsContainer} (WITH COMPONENTS {..., eid (0), actionType
   (15), accessCredentials ABSENT, iid ABSENT})
   OWS-TestComm-Response::= Action-Response {OwsContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
   (0), iid ABSENT})

   -- Definitions of the OWS attributes:
   OwsData :: = SEQUENCE {
        encryptedOwsPayload OCTET STRING (SIZE(51)) (CONSTRAINED BY { -- calculated encrypting
   OwsPayload as per Appendix 11 --}),
        DSRCSecurityData OCTET STRING
        }
   OwsPayload :: = SEQUENCE {
              tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
              recordedWeight INTEGER (0..65535),           -- 0= Total measured weight of the  heavy
   goods vehicle                                                          -- with 10 Kg
   resolution.
              axlesConfiguration OCTET STRING SIZE (3),     -- 0= 20 bits allowed for the number
                                                                  -- of axles for 10 axles.
              axlesRecordedWeight OCTET STRING SIZE (20),   -- 0= Recorded Weight for each axle
                                                                -- with 10 Kg resolution.
              tp15638Timestamp              INTEGER(0..4294967295)      -- Timestamp of current record
        }

Ows-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version
        }

StandardIdentifier ::= OBJECT IDENTIFIER
  OwsContainer ::= CHOICE {
        integer                       [0]    INTEGER,
        bitstring                     [1]    BIT STRING,
        octetstring                   [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString               [3]    UniversalString,
        beaconId                      [4]    BeaconID,
        t-apdu                        [5]    T-APDUs,
        dsrcApplicationEntityId       [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                   [7]    Dsrc-EID,
        attrIdList                    [8]    AttributeIdList,
        attrList                      [9]    AttributeList{RtmContainer},
        reserved10                    [10]   NULL,
        OwsContextmark                [11]   Ows-ContextMark,
        OwsData                       [12]   OwsData,
        reserved13                    [13]   NULL,
        reserved14                    [14]   NULL,
        time                          [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.5.6 *Elementen van OwsData, uitgevoerde acties en definities*

De elementen van OwsData worden gedefinieerd ter ondersteuning van Richtlijn (EU) 2015/719 met betrekking tot de maximaal toegestane afmetingen en gewichten voor zware vrachtvoertuigen („vrachtwagens"). Ze hebben de volgende betekenis:

— recordedWeight is het gemeten totale gewicht van de vrachtwagen, uitgedrukt in een hoeveelheidseenheid van 10 kg als bedoeld in EN ISO 14906. Zo komt een waarde van 2 500 bijvoorbeeld overeen met een totaal gewicht van 25 ton.

— axlesConfiguration is de opbouw van de vrachtwagen wat het aantal assen betreft. De opbouw wordt gedefinieerd met het volgende 20-bits masker (overeenkomstig EN ISO 14906).

Een 2-bits masker stelt de opbouw van een as voor in het volgende formaat:

— De waarde '00B' betekent „niet beschikbaar" omdat het voertuig niet uitgerust is met apparatuur om de asbelasting te registreren.

— De waarde '01B' betekent dat er geen as aanwezig is.

— De waarde '10B' betekent dat een as aanwezig is, dat de asbelasting werd berekend en geregistreerd en beschikbaar wordt gesteld in het veld axlesRecordedWeight.

— De waarde '11B' is gereserveerd voor toekomstig gebruik (RFU).

De laatste vier bits zijn gereserveerd voor toekomstig gebruik (RFU).

Aantal assen										
Aantal assen trekker			Aantal assen oplegger/aanhangwagen							
00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	RFU (4 bits)

— axlesRecordedWeight is de specifieke asbelasting die voor elke as werd geregistreerd, uitgedrukt in een hoeveelheidseenheid van 10 kg. Voor elke as worden twee bytes gebruikt. Zo komt een waarde van 150 bijvoorbeeld overeen met een totale asbelasting van 1 500 kg.

De andere gegevenstypes worden vastgelegd in punt 5.4.5.

5.5.7 *Mechanisme voor gegevensoverdracht*

DSC_64 Voor de overdracht van OWS-gegevens tussen het ondervragingssysteem en de DSRC-module in het voertuig wordt hetzelfde mechanisme gebruikt als voor RTM-gegevens (zie 5.4.6).

DSC_65 De gegevensoverdracht tussen het platform dat de gegevens over de maximale gewichten verzamelt, en de DSRC-module in het voertuig berust op de in punt 5.6 gedefinieerde fysieke verbinding, interfaces en protocollen.

5.6 **Gegevensoverdracht tussen DSRC-VU en VU**

5.6.1 *Fysieke verbinding en interfaces*

DSC_66 De verbinding tussen de VU en de DSRC-VU kan bestaan uit een fysieke kabel of een draadloze BLE-verbinding voor korteafstandscommunicatie op basis van Bluetooth v4.0.

DSC_67 De volgende voorschriften moeten worden nageleefd, ongeacht de gekozen fysieke verbinding en interface:

DSC_68 a) De verbinding tussen de VU en de DSRC-VU moet berusten op een open industrienorm 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

i) een vaste kabel met een lengte van ten minste 2 m die via een goedgekeurde Straight DIN 41612-conforme 11-pens H11-stekker van de DSRC-VU wordt aangesloten op een soortgelijke DIN/ISO-conforme contrastekker van de VU,

ii) een BLE(Bluetooth Low Energy)-verbinding,

iii) een standaardverbinding die voldoet aan ISO 11898 of SAE J1939.

DSC_69 b) De definitie van de interfaces en verbinding tussen de VU en de DSRC-VU moet ondersteuning bieden aan de in punt 5.6.2 gedefinieerde commando's van het toepassingsprotocol.

DSC_70 c) De VU en de DSRC-VU moeten de gegevensoverdracht via de verbinding ondersteunen wat prestaties en stroomvoorziening betreft.

5.6.2 *Toepassingsprotocol*

DSC_71 Het toepassingsprotocol tussen de VU-inrichting voor communicatie op afstand en de DSRC-VU staat in voor de periodieke gegevensoverdracht tussen de VU en de DSRC-VU.

DSC_72 De belangrijkste commando's zijn:

1. Verzoek om initialisatie van de communicatieverbinding
2. Antwoord op het verzoek om initialisatie van de communicatieverbinding
3. Gegevens verzenden met de identificator van de RTM-toepassing en de door RtmData gedefinieerde payloadgegevens
4. Ontvangstbevestiging van de gegevens
5. Verzoek om verbreking van de communicatieverbinding
6. Antwoord op het verzoek om verbreking van de communicatieverbinding

DSC_73 In ASN1.0 kunnen de vorige commando's als volgt worden gedefinieerd:

```
Remote Communication DT Protocol DEFINITIONS ::= BEGIN

     RCDT-Communication Link Initialization - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

     RCDT-Communication Link Initialization - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

          RCDT- Send Data ::=
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER, RCDTData
          SignedTachographPayload
     }

          RCDT Data Acknowledgment ::
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER,
          answer         BOOLEAN
     }

          RCDT-Communication Link Termination - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

          RCDT-Communication Link Termination - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

End
```

DSC_74 Beschrijving van de commando's en parameters:

— `RCDT-Communication Link Initialization – Request` wordt gebruikt om de communicatieverbinding te initialiseren. Dit commando wordt door de VU verzonden naar de DSRC-VU. De verbindingsidentificator (LID) wordt ingesteld door de VU en doorgegeven aan de DSRC-VU om een specifieke communicatieverbinding op te sporen.

(Opmerking: dit is bedoeld ter ondersteuning van toekomstige verbindingen en andere toepassingen/modules, zoals weging aan boord van het voertuig).

— `RCDT-Communication Link Initialization – Response` wordt door de DSRC-VU gebruikt als antwoord op het verzoek om de communicatieverbinding te initialiseren. Dit commando wordt door de DSRC-VU verzonden naar de VU. Het commando geeft als resultaat van de initialisatie '1' (Geslaagd) of '0' (Mislukt).

DSC_75 De communicatieverbinding wordt uitsluitend geïnitialiseerd na installatie, kalibrering en inschakeling van de motor/VU.

— `RCDT-Send Data` wordt door de VU gebruikt om de getekende RCDTData (dat wil zeggen de gegevens van de communicatie op afstand) naar de DSRC-VU te verzenden. De gegevens worden iedere 60 seconden verzonden. De parameter DataTransactionId identificeert de specifieke datatransmissie. De verbindingsidentificator (LID) wordt ook gebruikt om te waarborgen dat de verbinding juist tot stand is gebracht.

— `RCDT-Data Acknowledgment` wordt door de DSRC-VU verzonden om feedback te geven aan de VU over de gegevensontvangst via het commando `RCDT–Send Data` dat wordt geïdentificeerd door de parameter DataTransactionId. Het antwoord heeft de waarde '1' (Geslaagd) of '0' (Mislukt). Indien een VU meer dan drie antwoorden met de waarde '0' ontvangt of indien de VU geen RCDT-Data Acknowledgment ontvangt voor een eerder verzonden RCDT–Send Data met een specifieke DataTransactionId, genereert en registreert de VU een voorval.

— `RCDT-Communication Link Termination request` wordt door de VU verzonden naar de DSRC-VU om de verbinding voor een specifieke verbindingsidentificator (LID) te verbreken.

DSC_76 Bij het herstarten van de DSRC-VU of een VU moeten alle bestaande communicatieverbindingen worden verbroken om te vermijden dat er „hangende" verbindingen bestaan als gevolg van de plotselinge uitschakeling van een VU.

— `RCDT-Communication Link Termination – Response` wordt door de DSRC-VU verzonden naar de VU ter bevestiging van het door de VU verzonden verzoek om de verbinding voor de specifieke verbindingsidentificator (LID) te verbreken.

5.7 **Behandeling van fouten**

5.7.1 *Registratie en doorgifte van de gegevens in de DSRC-VU*

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 '62'H *Fout in de inrichting voor communicatie op afstand*, alsook met de tijdaanduiding.

DSC_78 Om interne communicatiestoringen van de VU te registreren, houdt de VU een bestand bij met een unieke naam die eenvoudig identificeerbaar is voor de controleurs.

DSC_79 Indien de VUPM er niet in slaagt VU-gegevens van de beveiligingsmodule te verkrijgen (om die aan de DSRC-VU door te geven), wordt deze storing geregistreerd op basis van een voorval van het type EventFaultType met de enum-waarde *'62'H Fout in de inrichting voor communicatie op afstand*, samen met de tijdaanduiding. De communicatiestoring wordt vastgesteld indien het bericht `RCDT Data Acknowledgment` meer dan drie keer na elkaar niet wordt ontvangen voor het bijbehorende bericht `RCDT Send Data` (dat wil zeggen met dezelfde DataTransactionId in de berichten `Send Data en Acknowledgment`).

5.7.2 *Fouten in de draadloze communicatie*

DSC_80 Communicatiefouten worden behandeld overeenkomstig de desbetreffende DSRC-normen, met name EN 300 674-1, EN 12253, EN 12795, EN 12834 en de toepasselijke parameters van EN 13372.

5.7.2.1 *Fouten in codering en handtekening*

DSC_81 Fouten in codering en handtekening worden behandeld zoals toegelicht in aanhangsel 11 „Algemene beveiligingsmechanismen", en worden niet opgenomen in foutmeldingen die verband houden met de gegevensoverdracht via DSRC-interfaces.

5.7.2.2 *Registratie van fouten*

Als dynamisch instrument voor draadloze communicatie functioneert de DSRC-interface in een onzekere omgeving die wordt gekenmerkt door uiteenlopende weersomstandigheden en (storings)invloeden van buitenaf. Dit is met name het geval bij gebruik van de draagbare REDCR in combinatie met rijdende voertuigen. Bijgevolg moet onderscheid worden gemaakt tussen de 'mislukking' van een leesbewerking en een 'foutconditie'. Bij transacties via een draadloze interface komt het vaak voor dat leesbewerkingen mislukken. In dit geval wordt doorgaans een nieuwe poging ondernomen door de BST opnieuw te verzenden en de transacties nogmaals uit te voeren. In de meeste gevallen wordt de communicatieverbinding dan met succes tot stand gebracht en worden de gegevens met succes overgedragen, tenzij het gecontroleerde voertuig zich inmiddels buiten bereik bevindt. Om een leesbewerking met succes uit te voeren, worden doorgaans meerdere (nieuwe) pogingen ondernomen.

Een leesbewerking kan mislukken doordat de antennes niet juist zijn gekoppeld (storing bij het 'richten') of doordat een van de antennes is afgeschermd. Een antenne kan opzettelijk worden afgeschermd, maar ook ongewild als gevolg van de fysieke aanwezigheid van een ander voertuig, radiostoringen, in het bijzonder van in de 5,8 GHz-frequentieband werkende WiFi-apparatuur of andere publiek toegankelijke draadloze communicatienetwerken. Verder kan een leesbewerking mislukken als gevolg van radarstoringen of ongunstige weersomstandigheden (bijvoorbeeld onweer) of doordat het gecontroleerde voertuig zich buiten het bereik van de DSRC-communicatieapparatuur bevindt. Afzonderlijke gevallen waarin leesbewerkingen mislukken kunnen per definitie niet worden geregistreerd om de eenvoudige reden dat er geen communicatie heeft plaatsgehad.

Indien de controleambtenaar een specifiek voertuig wil controleren door de DSRC-VU ervan te ondervragen, maar er niet in slaagt gegevens over te brengen, kan dat ook het gevolg zijn van opzettelijke manipulatie. Daarom heeft de controleambtenaar een hulpmiddel nodig om dit voorval in een logboek te registreren en collega's in het vervolgtraject te waarschuwen dat er mogelijk sprake is van een inbreuk. Zo kunnen deze collega's het voertuig tegenhouden en aan een nadere controle onderwerpen. Aangezien de communicatie mislukt is, kunnen daarover echter geen gegevens in de DSRC-VU worden geregistreerd. Bijgevolg moet deze rapportage deel uitmaken van het functionele ontwerp van de REDCR.

Technisch gezien is het 'mislukken' van een leesbewerking niet hetzelfde als het optreden van een 'fout'. In het kader van de tachograaftoepassing betekent een 'fout' dat een onjuiste waarde werd verkregen.

De gegevens zijn al beveiligd wanneer ze aan de DSRC-VU worden doorgegeven. Bijgevolg moet de verstrekker van de gegevens ze verifiëren (zie punt 5.4).

Gegevens die vervolgens via de ether worden overgebracht, ondergaan cyclische redundantiecontroles (CRC) op het niveau van de communicatieverbinding. Een geslaagde CRC betekent dat de gegevens juist zijn. Indien de CRC mislukt, moeten de gegevens opnieuw worden verzonden. De kans dat gegevens waarvoor de CRC mislukt toch met succes worden overgebracht, is statistisch gezien zo klein dat ze te verwaarlozen is.

Indien de CRC mislukt en er geen tijd is om de juiste gegevens opnieuw te verzenden en te ontvangen, is het resultaat geen fout, maar de concretisering van een mislukte leesbewerking.

Het enige betekenisvolle gegeven dat over deze 'mislukking' kan worden geregistreerd, is het aantal keren dat transacties met succes werden geïnitialiseerd, zij het zonder succesvolle gegevensoverdracht naar de REDCR.

DSC_82 De REDCR registreert bijgevolg — met tijdaanduiding — hoeveel keren de initialisatiefase van een ondervraging via de DSRC-interface met succes werd voltooid, maar de transactie niettemin werd beëindigd voordat de REDCR de gegevens met succes heeft kunnen ophalen. Deze gegevens worden aan de controleambtenaar beschikbaar gesteld en opgeslagen in het geheugen van de REDCR. De daartoe gebruikte middelen hangen af van het productontwerp of van de specificaties van de bevoegde controleautoriteiten.

Het enige betekenisvolle gegeven dat over de 'fout' kan worden geregistreerd, is het aantal keren dat de REDCR er niet in geslaagd is de ontvangen gegevens te decoderen. Dit heeft echter alleen te maken met de doelmatigheid van de REDCR-software. Zelfs na decodering kunnen gegevens semantisch gezien betekenisloos zijn.

DSC_83 De REDCR registreert bijgevolg — met tijdaanduiding — het aantal mislukte pogingen om de via de DSRC-interface ontvangen gegevens te decoderen.

6 TESTS BIJ INBEDRIJFSTELLING EN PERIODIEKE CONTROLE VAN DE FUNCTIE VOOR COMMUNICATIE OP AFSTAND

6.1 **Algemeen**

DSC_84 In het kader van de functie voor communicatie op afstand worden twee tests uitgevoerd:

1) Een Echo-test om de draadloze tweerichtingsverbinding tussen de DSRC-REDCR en de DSRC-VU te bevestigen.

2) Een beveiligingstest tussen bron en bestemming om te waarborgen dat een werkplaatskaart toegang kan krijgen tot de gecodeerde en getekende gegevens van de VU die via de draadloze communicatieverbinding worden verzonden.

6.2 **Echo-commando**

De specifieke testvoorschriften in dit punt zijn bedoeld om na te gaan of de tweerichtingsverbinding tussen DSRC-REDCR en DSRC-VU volledig operationeel is.

Dankzij het Echo-commando kunnen werkplaatsen of testcentra voor typegoedkeuring de werking van de DSRC-interface testen zonder toegang te moeten krijgen tot beveiligingsreferenties. De bediener van het testapparaat hoeft bijgevolg alleen een verbinding via de DSRC-interface te initialiseren (door een BST met AID=2 te verzenden) en daarna het Echo-commando te verzenden. Indien de DSRC-interface operationeel is, ontvangt hij daarna het antwoord op het Echo-commando. Zie punt 5.4.8 voor meer informatie. Indien dit antwoord correct wordt ontvangen, mag ervan worden uitgegaan dat de DSRC-interface (tweerichtingsverbinding tussen DSRC-REDCR en DSRC-VU) correct functioneert.

6.3 **Tests om de beveiligde gegevensinhoud te bevestigen**

DSC_85 Met deze test wordt de beveiligde gegevensstroom tussen bron en bestemming bevestigd. Voor deze test moet de DSRC-testlezer worden gebruikt. De DSRC-testlezer voert dezelfde functies uit en wordt geïmplementeerd overeenkomstig dezelfde specificaties als de door controleambtenaren gebruikte lezer. Het enige verschil is dat de gebruiker van de DSRC-testlezer wordt geauthenticeerd op basis van een werkplaatskaart, en niet op basis van een controlekaart. De test kan worden uitgevoerd op het ogenblik dat de slimme tachograaf voor het eerst wordt geactiveerd of na afloop van de kalibreringsprocedure. Zodra de tachograaf is geactiveerd, genereert de voertuigunit de beveiligde gegevens voor vroegtijdige detectie, en geeft die door aan de DSRC-VU.

DSC_86 De werkplaatsmedewerker plaatst de DSRC-testlezer op een afstand tussen 2 en 10 m vóór het voertuig.

DSC_87 Vervolgens brengt de werkplaatsmedewerker een werkplaatskaart in de DSRC-testlezer om de voertuigunit te ondervragen en gegevens over vroegtijdige detectie te verkrijgen. Indien de ondervraging met succes verloopt, leest de werkplaatsmedewerker de ontvangen gegevens om de integriteit ervan te controleren en zeker te stellen dat ze juist werden gedecodeerd.

Aanhangsel 15

MIGRATIE: DE COËXISTENTIE VAN VERSCHILLENDE GENERATIES APPARATUUR BEHEREN

INHOUDSOPGAVE

1. DEFINITIES 497

2. ALGEMENE BEPALINGEN 497

2.1. Overzicht van de overgang 497

2.2. Interoperabiliteit tussen VU's en kaarten 498

2.3. Interoperabiliteit tussen VU's en bewegingssensoren 498

2.4. Interoperabiliteit tussen voertuigunits, tachograafkaarten en apparatuur voor het downloaden van gegevens 498

2.4.1 Kaarten rechtstreeks downloaden met intelligente toepassingsgerichte apparatuur (IDE) 498

2.4.2 Het downloaden van een kaart via een voertuigunit 499

2.4.3 Het downloaden van een voertuigunit 499

2.5. Interoperabiliteit tussen VU's en kalibratieapparatuur 499

3. BELANGRIJKSTE STAPPEN IN DE PERIODE VÓÓR DE DATUM VAN INVOERING 499

4. BEPALINGEN VOOR DE PERIODE NA DE DATUM VAN INVOERING 499

1. DEFINITIES

Met het oog op de toepassing van dit aanhangsel wordt verstaan onder:

slim tachograafsysteem: zoals gedefinieerd in deze bijlage (hoofdstuk 1: definitie bbb);

tachograafsysteem van de eerste generatie: zoals gedefinieerd in deze verordening (artikel 2: definitie 1);

tachograafsysteem van de tweede generatie: zoals gedefinieerd in deze verordening (artikel 2: definitie 7);

datum van invoering: zoals gedefinieerd in deze bijlage (hoofdstuk 1: definitie ccc);

Intelligente toepassingsgerichte apparatuur: apparatuur die wordt gebruikt voor het downloaden van gegevens, zoals gedefinieerd in aanhangsel 7 van deze bijlage.

2. ALGEMENE BEPALINGEN

2.1. **Overzicht van de overgang**

In de preambule van deze bijlage wordt een overzicht gegeven van de overgang tussen de tachograafsystemen van de eerste en de tweede generatie.

In aanvulling op de bepalingen van deze preambule:

— zijn bewegingssensoren van de eerste generatie niet interoperabel met voertuigunits van de tweede generatie.

— begint de installatie van bewegingssensoren van de tweede generatie in voertuigen op hetzelfde ogenblik als de installatie van voertuigunits van de tweede generatie.

— apparatuur voor het downloaden van gegevens en kalibreren moet evolueren om het gebruik van beide generaties controleapparaten en tachograafkaarten te ondersteunen.

2.2. **Interoperabiliteit tussen VU's en kaarten**

Er wordt van uitgegaan dat tachograafkaarten van de eerste generatie interoperabel zijn met voertuigunits van de eerste generatie (overeenkomstig bijlage IB bij deze verordening), en dat tachograafkaarten van de tweede generatie interoperabel zijn met voertuigunits van de tweede generatie (overeenkomstig bijlage 1C bij deze verordening). Voorts zijn ook de onderstaande voorschriften van toepassing.

MIG_001 Behoudens het bepaalde in voorschrift MIG_004 en MIG_005, mogen tachograafkaarten van de eerste generatie verder worden gebruikt in voertuigunits van de tweede generatie tot het einde van hun geldigheidsduur. De houders kunnen evenwel vragen ze te vervangen door tachograafkaarten van de tweede generatie zodra deze beschikbaar zijn.

MIG_002 Het moet mogelijk zijn elke geldige bestuurders-, controle- en bedrijfskaart van de eerste generatie te gebruiken in voertuigunits van de tweede generatie.

MIG_003 Werkplaatsen kunnen dit definitief onmogelijk maken, zodat tachograafkaarten van de eerste generatie niet meer worden aanvaard. Dit mag alleen gebeuren nadat de Europese Commissie is gestart met een procedure die tot doel heeft werkplaatsen te verzoeken dit te doen, bijvoorbeeld tijdens elke periodieke inspectie van de tachograaf.

MIG_004 Voertuigunits van de tweede generatie mogen alleen werkplaatskaarten van de tweede generatie kunnen gebruiken.

MIG_005 Om de werkingsmodus te bepalen, houden voertuigunits van de tweede generatie alleen rekening met het type geldige kaarten dat wordt ingebracht, ongeacht de generatie.

MIG_006 Elke geldige tachograafkaart van de tweede generatie kan in voertuigunits van de eerste generatie worden gebruikt op exact dezelfde wijze als hetzelfde type tachograafkaarten van de eerste generatie.

2.3. **Interoperabiliteit tussen VU's en bewegingssensoren**

Er wordt van uitgegaan dat bewegingssensoren van de eerste generatie interoperabel zijn met voertuigunits van de eerste generatie, en dat bewegingssensoren van de tweede generatie interoperabel zijn met voertuigunits van de tweede generatie. Voorts zijn ook de onderstaande voorschriften van toepassing.

MIG_007 Voertuigunits van de tweede generatie kunnen niet worden gekoppeld aan en gebruikt met bewegingssensoren van de eerste generatie.

MIG_008 Bewegingssensoren van de tweede generatie kunnen worden gekoppeld aan en gebruikt met uitsluitend voertuigunits van de tweede generatie of met beide generaties voertuigunits.

2.4. **Interoperabiliteit tussen voertuigunits, tachograafkaarten en apparatuur voor het downloaden van gegevens**

MIG_009 Apparatuur voor het downloaden van gegevens kan worden gebruikt met slechts één generatie van voertuigunits en tachograafkaarten of met beide.

2.4.1 *Kaarten rechtstreeks downloaden met intelligente toepassingsgerichte apparatuur (IDE)*

MIG_010 De gegevens worden gedownload door IDE van tachograafkaarten van één generatie die in hun kaartlezers worden ingebracht, met gebruikmaking van de beveiligingsmechanismen en het downloadprotocol van deze generatie, en alle gedownloade gegevens hebben het formaat dat voor deze generatie is gedefinieerd.

MIG_011 Om de controle van bestuurders door autoriteiten van buiten de EU mogelijk te maken, is het ook mogelijk om gegevens van bestuurders- (en werkplaats-)kaarten van de tweede generatie te downloaden op exact dezelfde wijze als van bestuurders- (en werkplaats-)kaarten van de eerste generatie. Een dergelijke download omvat:

— de `IC` en `ICC` van niet-ondertekende EF's,

— het `Card_Certificate` en `CA_Certificate` van niet-ondertekende EF's (1ste generatie),

— de andere gegevensbestanden van de EF's (in TACHO DF) 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 TACHO_G2 DF).

2.4.2 *Het downloaden van een kaart via een voertuigunit*

MIG_012 De gegevens worden gedownload van een kaart van de tweede generatie die is ingebracht in een voertuigunit van de eerste generatie, met gebruikmaking van het downloadprotocol van de eerste generatie. De kaart reageert op exact dezelfde wijze als een kaart van de eerste generatie op de commando's van de voertuigunit en de gedownloade gegevens hebben hetzelfde formaat als gegevens die zijn gedownload van een kaart van de eerste generatie.

MIG_013 De gegevens worden gedownload van een kaart van de eerste generatie die is ingebracht in een voertuigunit van de tweede generatie met gebruikmaking van het in aanhangsel 7 van deze bijlage gedefinieerde downloadprotocol. De voertuigunit zendt commando's naar de kaart op precies dezelfde wijze als een voertuigunit van de eerste generatie, en de gedownloade gegevens beantwoorden aan het formaat dat is gedefinieerd voor kaarten van de eerste generatie.

2.4.3 *Het downloaden van een voertuigunit*

MIG_014 Voor het downloaden van gegevens van een voertuigunit van de tweede generatie wordt gebruik gemaakt 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 en werkplaatsen van buiten de EU de mogelijkheid te geven om gegevens van voertuigunits te downloaden, kan het ook mogelijk zijn om gegevens van voertuigunits van de tweede generatie te downloaden met de beveiligingsmechanismen en het downloadprotocol van de eerste generatie. De gedownloade gegevens hebben 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.

2.5. **Interoperabiliteit tussen VU's en kalibratieapparatuur**

MIG_016 Kalibratieapparatuur is in staat kalibraties te verrichten van tachografen van elke generatie, met gebruikmaking van het kalibreringsprotocol van deze generatie. Kalibratieapparatuur kan worden gebruikt met één generatie tachografen of met beide.

3. BELANGRIJKSTE STAPPEN IN DE PERIODE VÓÓR DE DATUM VAN INVOERING

MIG_017 Testsleutels en -certificaten worden uiterlijk **30 maanden** voor de datum van invoering ter beschikking gesteld van de fabrikanten.

MIG_018 De interoperabiliteitstesten zijn uiterlijk **15 maanden** voor de datum van invoering klaar om van start te gaan, op verzoek van fabrikanten.

MIG_019 Officiële sleutels en certificaten worden uiterlijk **12 maanden** voor de datum van invoering ter beschikking gesteld van de fabrikanten.

MIG_020 De lidstaten kunnen uiterlijk **3 maanden** voor de datum van invoering werkplaatskaarten van de tweede generatie afgeven.

MIG_021 De lidstaten kunnen uiterlijk **1 maand** voor de datum van invoering alle types tachograafkaarten van de tweede generatie afgeven.

4. BEPALINGEN VOOR DE PERIODE NA DE DATUM VAN INVOERING

MIG_022 Na de invoering geven de lidstaten alleen nog tachograafkaarten van de tweede generatie af.

MIG_023 Fabrikanten van voertuigunits / bewegingssensoren mogen voertuigunits / bewegingssensoren van de eerste generatie blijven produceren zolang deze worden gebruikt op het terrein, zodat defecte onderdelen kunnen worden vervangen.

MIG_024 Fabrikanten van voertuigunits / bewegingssensoren kunnen het behoud van de typegoedkeuring van voertuigunits / bewegingssensoren van de eerste generatie waarvoor reeds typegoedkeuring is verkregen, vragen en krijgen.

Aanhangsel 16

ADAPTER VOOR VOERTUIGEN VAN DE CATEGORIEËN M1 EN N1

INHOUD

1. AFKORTINGEN EN REFERENTIEDOCUMENTEN 501

1.1. Afkortingen 501

1.2. Referentienormen 501

2. ALGEMENE KENMERKEN EN FUNCTIES VAN DE ADAPTER 502

2.1. Algemene beschrijving van de adapter 502

2.2. Functies 502

2.3. Beveiliging 502

3. EISEN VOOR HET CONTROLEAPPARAAT WANNEER EEN ADAPTER IS GEÏNSTALLEERD 502

4. FABRICAGE EN FUNCTIONELE VEREISTEN VAN DE ADAPTER 503

4.1. Totstandbrenging van interfaces en aanpassing van inkomende snelheidsimpulsen 503

4.2. Invoering van de inkomende impulsen in de ingebouwde bewegingssensor 503

4.3. Ingebouwde bewegingssensor 503

4.4. Veiligheidsvoorschriften 503

4.5. Prestatiekenmerken 504

4.6. Materialen 504

4.7. Merktekens 504

5. INSTALLATIE VAN HET CONTROLEAPPARAAT WANNEER EEN ADAPTER WORDT GEBRUIKT 504

5.1. Installatie 504

5.2. Verzegeling 505

6. CONTROLES, INSPECTIES EN HERSTELLINGEN 505

6.1. Periodieke controles 505

7. TYPEGOEDKEURING VAN HET CONTROLEAPPARAAT WANNEER EEN ADAPTER WORDT GEBRUIKT 505

7.1. Algemeen 505

7.2. Functioneel certificaat 506

1. AFKORTINGEN EN REFERENTIEDOCUMENTEN

1.1. **Afkortingen**

TBD Nog vast te stellen

VU Voertuigunit

1.2. **Referentienormen**

ISO16844-3 Road vehicles — Tachograph systems — Part 3: Motion sensor interface

2. ALGEMENE KENMERKEN EN FUNCTIES VAN DE ADAPTER

2.1. **Algemene beschrijving van de adapter**

ADA_001 De adapter levert beveiligde bewegingsgegevens die permanent representatief zijn voor de snelheid en afgelegde afstand van het voertuig aan de aangesloten VU.

De adapter is alleen bestemd voor voertuigen die overeenkomstig deze verordening met een controleapparaat moeten worden uitgerust.

De adapter wordt alleen geïnstalleerd en gebruikt in de onder (yy) "adapter" van bijlage IC gedefinieerde voertuigtypen, wanneer het mechanisch niet mogelijk is een ander bestaand type bewegingssensor te installeren dat verenigbaar is met de bepalingen van deze bijlage en met de aanhangsels 1 tot en met 16 daarbij.

De adapter mag geen mechanische interface met een bewegend deel van het voertuig omvatten, maar moet aangesloten zijn op de snelheids-/afstandsimpulsen die worden gegenereerd door geïntegreerde sensoren of alternatieve interfaces.

ADA_002 Een bewegingssensor waarvoor typegoedkeuring is verleend (volgens de voorschriften van deze bijlage IC, punt 8, Typegoedkeuring van controleapparaten en tachograafkaarten) wordt gemonteerd in de adapterbehuizing, die eveneens een impulsomvormer omvat welke de inkomende impulsen invoert in de ingebouwde bewegingssensor. De ingebouwde bewegingssensor zelf wordt aangesloten op de voertuigunit, zodat de interface tussen de voertuigunit en de adapter voldoet aan de eisen van ISO16844-3.

2.2. **Functies**

ADA_003 De adapter heeft de volgende functies:

— fungeert als interface en past de inkomende snelheidsimpulsen aan,

— invoering van de inkomende impulsen in de ingebouwde bewegingssensor,

— alle functies van de ingebouwde bewegingssensor die beveiligde bewegingsgegevens aan de voertuigunit leveren.

2.3. **Beveiliging**

ADA_004 Er hoeft geen veiligheidscertificering van de adapter te worden uitgevoerd overeenkomstig de in aanhangsel 10 bij deze bijlage vastgestelde algemene beveiligingsdoelstelling voor de bewegingssensor. In plaats daarvan zijn de in punt 4.4 van dit aanhangsel gespecificeerde veiligheidseisen van toepassing.

3. EISEN VOOR HET CONTROLEAPPARAAT WANNEER EEN ADAPTER IS GEÏNSTALLEERD

Uit de in de volgende hoofdstukken vermelde eisen blijkt hoe de voorschriften van deze bijlage moeten worden verstaan wanneer een adapter wordt gebruikt. Tussen haakjes is het nummer van het voorschrift van bijlage IC vermeld.

ADA_005 Het controleapparaat van een voertuig dat met een adapter is uitgerust, moet voldoen aan alle voorschriften van deze bijlage, tenzij anders gespecificeerd in dit aanhangsel.

ADA_006 Wanneer een adapter is geïnstalleerd, omvat het controleapparaat kabels, de adapter (met inbegrip van een bewegingssensor) en een voertuigunit [01].

ADA_007 De functie voor het detecteren van voorvallen en/of fouten van het controleapparaat wordt als volgt gewijzigd:

— wanneer de stroomvoorziening van de ingebouwde bewegingssensor [79] gedurende meer dan 200 milliseconden wordt onderbroken, veroorzaakt de voertuigunit, wanneer deze zich niet in de kalibreringsmodus bevindt, het voorval "onderbreking in de stroomvoorziening";

— wanneer de normale gegevensstroom tussen de ingebouwde bewegingssensor en de voertuigunit wordt onderbroken en/of wanneer zich een fout voordoet in de integriteit van de gegevens of in de authenticatie van de gegevens tijdens de gegevensuitwisseling tussen de ingebouwde bewegingssensor en de voertuigunit [83], veroorzaakt de voertuigunit het voorval "fout in de bewegingsgegevens";

— wanneer zich een ander voorval voordoet dat de beveiliging van de ingebouwde bewegingssensor aantast, wanneer deze zich niet in kalibreringsmodus bevindt, veroorzaakt de voertuigunit het voorval "poging tot inbreuk op de beveiliging" [85];

— wanneer zich een fout in de ingebouwde bewegingssensor voordoet, wanneer deze zich niet in kalibreringsmodus bevindt, veroorzaakt de voertuigunit het voorval "fout in het controleapparaat" [88].

ADA_008 De fouten van de adapter die door het controleapparaat kunnen worden vastgesteld, zijn die welke verband houden met de ingebouwde bewegingssensor [88].

ADA_009 De kalibreringsmodus van de voertuigunit moet het mogelijk maken de ingebouwde bewegingssensor automatisch te verbinden met koppelen de voertuigunit [202, 204].

4. FABRICAGE EN FUNCTIONELE VEREISTEN VAN DE ADAPTER

4.1. **Totstandbrenging van interfaces en aanpassing van inkomende snelheidsimpulsen**

ADA_011 De inputinterface van de adapter aanvaardt frequentie-impulsen die representatief zijn voor de snelheid van het voertuig en de afgelegde afstand. De elektrische kenmerken van de inkomende impulsen zijn: *nader vast te stellen door de fabrikant*. Aanpassingen die alleen kunnen worden uitgevoerd door de fabrikant van de adapter en de goedgekeurde werkplaats die de adapter heeft geïnstalleerd, maken de correcte interface tussen de adapterinput en het voertuig mogelijk, voor zover van toepassing.

ADA_012 De inputinterface van de adapter moet, voor zover van toepassing, in staat zijn de frequentie-impulsen van de inkomende snelheidsimpulsen te vermenigvuldigen met of te delen door een vaste factor, teneinde het signaal te herleiden tot het in deze bijlage gedefinieerde bereik van de k-factor (4 000 tot 25 000 impulsen/km). Deze vaste factor mag alleen worden geprogrammeerd door de fabrikant van de adapter en door de goedgekeurde werkplaats die de adapter heeft geïnstalleerd.

4.2. **Invoering van de inkomende impulsen in de ingebouwde bewegingssensor**

ADA_013 De inkomende impulsen, eventueel aangepast zoals hierboven uiteengezet, worden zodanig in de ingebouwde bewegingssensor ingevoerd dat elke inkomende impuls door de bewegingssensor wordt gedetecteerd.

4.3. **Ingebouwde bewegingssensor**

ADA_014 De ingebouwde bewegingssensor wordt gestimuleerd door de ingevoerde impulsen, waardoor hij bewegingsgegevens kan voortbrengen die accuraat de beweging van het voertuig weergeven, alsof er een mechanische interface bestond tussen de sensor en een bewegend deel van het voertuig.

ADA_015 De identificatiegegevens van de ingebouwde bewegingssensor worden door de voertuigunit gebruikt om de adapter te identificeren [95].

ADA_016 De in de ingebouwde bewegingssensor opgeslagen installatiegegevens worden geacht de installatiegegevens van de adapter te vertegenwoordigen [122].

4.4. **Veiligheidsvoorschriften**

ADA_017 De behuizing van de adapter wordt zodanig ontworpen dat ze niet kan worden geopend. Ze wordt verzegeld, zodat pogingen om ermee te knoeien gemakkelijk kunnen worden vastgesteld (bijv. door een visuele inspectie, zie ADA_035). De verzegeling moet voldoen aan dezelfde eisen als zegels van bewegingsopnemers [398 tot en met 406]

ADA_018 Het mag niet mogelijk zijn de ingebouwde bewegingssensor los te maken van de adapter zonder het zegel/de zegels van de adapterbehuizing of het zegel tussen de sensor en de adapterbehuizing te verbreken (zie ADA_034).

ADA_019 De adapter moet ervoor zorgen dat bewegingsgegevens uitsluitend kunnen worden verwerkt en afgeleid van de adapterinput.

4.5. **Prestatiekenmerken**

ADA_020 De adapter moet volledig operationeel zijn binnen het door de fabrikant vastgestelde temperatuurbereik.

ADA_021 De adapter moet volledig operationeel zijn binnen het vochtigheidsbereik van 10 % tot 90 % [214].

ADA_022 De adapter moet tegen overspanning, polariteitomkering en kortsluiting worden beveiligd [216].

ADA_023 De adapter moet:

— reageren op een magnetisch veld dat de detectie van beweging van het voertuig stoort. In dat geval, wordt door de voertuigunit een fout in de sensor [88] geregistreerd en opgeslagen, ofwel

— een aftastelement bevatten dat beschermd is tegen, of ongevoelig is voor, een magnetisch veld [217].

ADA_024 De adapter moet voldoen aan het internationale reglement VN ECE R 10 met betrekking tot elektromagnetische compatibiliteit en moet tegen elektrostatische ontladingen en stootspanning worden beveiligd [218]

4.6. **Materialen**

ADA_025 De adapter moet voldoen aan beschermingsklasse (*nader vast te stellen door de fabrikant, afhankelijk van de installatiepositie*) [220, 221].

ADA_026 De kleur van de adapterbehuizing moet geel zijn.

4.7. **Merktekens**

ADA_027 Op de adapter moet een opschriftenplaatje worden bevestigd waarop de volgende gegevens zijn vermeld:

— naam en adres van de fabrikant van de adapter,

— onderdeelnummer van de fabrikant en bouwjaar van de adapter,

— goedkeuringsmerkteken van het type adapter of van het type controleapparaat met adapter,

— de datum waarop de adapter is geïnstalleerd,

— het voertuigidentificatienummer van het voertuig waarin de adapter is geïnstalleerd.

ADA_028 Op het opschriftenplaatje moeten ook de volgende bijzonderheden worden vermeld (indien niet direct leesbaar aan de buitenzijde van de ingebouwde bewegingssensor):

— naam van de fabrikant van de ingebouwde bewegingssensor,

— onderdeelnummer van de fabrikant en bouwjaar van de ingebouwde bewegingssensor,

— goedkeuringsmerkteken van de ingebouwde bewegingssensor.

5. INSTALLATIE VAN HET CONTROLEAPPARAAT WANNEER EEN ADAPTER WORDT GEBRUIKT

5.1. **Installatie**

ADA_029 Adapters voor installatie in voertuigen mogen alleen worden geïnstalleerd door voertuigfabrikanten of door erkende werkplaatsen die gemachtigd zijn om digitale en slimme tachografen te installeren, te activeren en te kalibreren.

ADA_030 Een erkende werkplaats die een adapter installeert, stelt de inputinterface in en selecteert de verdeelverhouding van het inputsignaal (indien van toepassing).

ADA_031 Een erkende werkplaats die een adapter installeert, verzegelt de adapterbehuizing.

ADA_032 De adapter wordt zo dicht mogelijk geïnstalleerd bij het deel van het voertuig dat de inkomende impulsen levert.

ADA_033 De kabels voor de stroomvoorziening van de adapter zijn rood (positief) en zwart (aarding).

5.2. **Verzegeling**

ADA_034 De volgende verzegelingseisen zijn van toepassing:

— de behuizing van de adapter wordt verzegeld (zie ADA_017),

— de behuizing van de ingebouwde sensor wordt verzegeld aan de adapterbehuizing, tenzij het onmogelijk is de sensor uit de adapterbehuizing te verwijderen zonder het zegel/de zegels van de adapterbehuizing te verbreken (zie ADA_018),

— de adapterbehuizing wordt verzegeld aan het voertuig,

— de verbinding tussen de adapter en de apparatuur die de inkomende impulsen verstuurt, wordt aan beide uiteinden verzegeld (voor zover redelijkerwijze mogelijk).

6. CONTROLES, INSPECTIES EN HERSTELLINGEN

6.1. **Periodieke controles**

ADA_035 Wanneer een adapter wordt gebruikt, moet bij elke periodieke inspectie (overeenkomstig voorschrift [409] tot en met [413] van bijlage 1C) van het controleapparaat worden gecontroleerd:

— of de passende typegoedkeuringsmerktekens op de adapter zijn aangebracht,

— of de zegels op de adapter en de verbindingen intact zijn,

— of de adapter geïnstalleerd is zoals aangegeven op het installatieplaatje,

— of de adapter geïnstalleerd is zoals gespecificeerd door de aanpasser en/of fabrikant van het voertuig,

— of het monteren van een adapter is toegestaan voor het geïnspecteerde voertuig.

ADA_036 Bij deze controles moet een kalibrering plaatsvinden en moeten alle zegels, ongeacht de staat waarin ze zich bevinden, worden vervangen.

7. TYPEGOEDKEURING VAN HET CONTROLEAPPARAAT WANNEER EEN ADAPTER WORDT GEBRUIKT

7.1. **Algemeen**

ADA_037 Het volledige controleapparaat, met de adapter, wordt ter typegoedkeuring ingediend [425].

ADA_038 Een adapter kan met het oog op de typegoedkeuring van de adapter zelf of met het oog op de typegoedkeuring als onderdeel van een controleapparaat worden ingediend.

ADA_039 Een dergelijke typegoedkeuring moet functionele tests van de adapter omvatten. Positieve testresultaten worden op een relevant certificaat vermeld [426].

7.2. **Functioneel certificaat**

ADA_040 Alleen als de adapter met succes de onderstaande tests heeft doorstaan, wordt een functioneel certificaat voor de adapter of voor het controleapparaat dat de adapter omvat, afgegeven aan de fabrikant van de adapter.

Nr.	Test	Beschrijving	Gerelateerde voorschriften
1.	**Administratieve controle**		
1.1	Documentatie	Correctheid van de documentatie van de adapter	
2.	**Visuele inspectie**		
2.1.	Overeenstemming van de adapter met de documentatie		
2.2.	Identificatie van/opschriften op de adapter		ADA_027, ADA_028
2.3	Materialen van de adapter		[219] tot en met [223] ADA_026
2.4.	Verzegeling		ADA_017, ADA_018, ADA_034
3.	**Functionele tests**		
3.1	Invoering van de snelheidsimpulsen in de ingebouwde bewegingssensor		ADA_013
3.2	Totstandbrenging van interfaces en aanpassing van inkomende snelheidsimpulsen		ADA_011, ADA_012
3.3	Juistheid van bewegingsmeting		[30] tot en met [35], [217]
4.	**Milieutests**		
4.1	Testresultaten van de fabrikant	Resultaten van de milieutests van de fabrikant.	ADA_020, ADA_021, ADA_022, ADA_024
5.	**EMC**		
5.1	Stralingsemissies en gevoeligheid	Controleer de overeenstemming met Richtlijn 2006/28/EG	ADA_024
5.2	Testresultaten van de fabrikant	Resultaten van de milieutests van de fabrikant.	ADA_024