I

(Besluiten waarvan de publicatie voorwaarde is voor de toepassing)

VERORDENING (EG) Nr. 1360/2002 VAN DE COMMISSIE

van 13 juni 2002

betreffende de zevende aanpassing aan de vooruitgang van de techniek van Verordening (EEG) nr. 3821/85 van de Raad betreffende het controleapparaat in het wegvervoer

(Voor de EER relevante tekst)

DE COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap,

Gelet op Verordening (EEG) nr. 3821/85 van de Raad van 20 december 1985 betreffende het controleapparaat in het wegvervoer ([1]), laatstelijk gewijzigd bij Verordening (EG) nr. 2135/98 ([2]), en met name op de artikelen 17 en 18,

Overwegende hetgeen volgt:

(1) De technische specificaties van bijlage I B bij Verordening (EEG) nr. 3821/85 moeten worden aangepast aan de technische vooruitgang, in het bijzonder met het oog op de algemene veiligheid van het systeem en de interoperabiliteit tussen het controleapparaat en de bestuurderskaarten.

(2) De aanpassing van de apparatuur vereist tevens een aanpassing van bijlage II bij Verordening (EEG) nr. 3821/85, waarin de goedkeuringsmerken en -certificaten zijn omschreven.

(3) Het bij artikel 18 van Verordening (EEG) nr. 3821/85 ingestelde comité heeft geen advies uitgebracht over de in het voorstel vervatte maatregelen en de Commissie heeft dan ook aan de Raad een voorstel in verband met deze maatregelen voorgelegd.

(4) Bij het aflopen van de termijn vastgesteld in artikel 18, lid 5, onder b), van Verordening (EEG) nr. 3821/85, had de Raad geen besluit genomen en het is derhalve aan de Commissie deze maatregelen vast te stellen,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

De bijlage bij Verordening (EG) nr. 2135/98 wordt vervangen door de bijlage bij deze verordening.

Artikel 2

Bijlage II bij Verordening (EEG) nr. 3821/85 wordt als volgt gewijzigd:

1. Hoofdstuk I, punt 1, eerste alinea, wordt als volgt gewijzigd:
   — Het onderscheidingsteken voor Griekenland „GR” wordt vervangen door „23”;
   — Het onderscheidingsteken voor Ierland „IRL” wordt vervangen door „24”;
   — Het onderscheidingsnummer „12” wordt toegevoegd voor Oostenrijk;
   — Het onderscheidingsnummer „17” wordt toegevoegd voor Finland;
   — Het onderscheidingsnummer „5” wordt toegevoegd voor Zweden.
2. Hoofdstuk I, punt 1, tweede alinea, wordt als volgt gewijzigd:
   — De woorden „of van een tachograafkaart” worden tussengevoegd na het woord „registratieblad”.
3. Hoofdstuk I, punt 2, wordt als volgt gewijzigd:
   — De woorden „en op elke tachograafkaart” worden tussengevoegd na het woord „registratieblad”.
4. In hoofdstuk II worden de volgende woorden aan de titel toegevoegd „VOOR PRODUCTEN DIE VOLDOEN AAN BIJLAGE I”.

([1]) PB L 370 van 31.12.1985, blz. 8.
([2]) PB L 274 van 9.10.1998, blz. 1.

5. Het volgende hoofdstuk III wordt toegevoegd:

„III. GOEDKEURINGSCERTIFICAAT VOOR PRODUCTEN DIE VOLDOEN AAN BIJLAGE I B

De staat die de goedkeuring heeft afgegeven, verleent de aanvrager een goedkeuringscertificaat volgens onderstaand model. Voor de mededeling aan de overige lidstaten van afgegeven goedkeuringen of eventuele intrekkingen gebruikt elke lidstaat kopieën van dit document.

GOEDKEURINGSCERTIFICAAT VOOR PRODUCTEN DIE VOLDOEN AAN BIJLAGE I B

Naam van de bevoegde instantie .....

Mededeling betreffende (*):

☐ goedkeuring van

☐ intrekking van de goedkeuring van

☐ model van het controleapparaat

☐ component van het controleapparaat (**) .....

☐ bestuurderskaart

☐ werkplaatskaart

☐ bedrijfskaart

☐ controlekaart

Nummer goedkeuring .....

1. Fabrieks- of handelsmerk .....
2. Benaming van het model .....
3. Naam van de fabrikant .....
4. Adres van de fabrikant .....
5. Ter goedkeuring aangeboden op .....
6. Beproevingslaboratorium(s) .....
7. Datum en nummer van de test(s) .....
8. Datum van goedkeuring .....
9. Datum van intrekking van de goedkeuring .....
10. Model van de component(en) van het controleapparaat in combinatie waarmee de component kan worden gebruikt .....
11. Plaats .....
12. Datum .....
13. Bijgevoegde beschrijvende documenten .....

---

14. Opmerkingen (en ruimte voor eventuele zegels)

.....
(handtekening)

(*) Aankruisen wat van toepassing is.
(**) Vermeld de component waarop de kennisgeving betrekking heeft.”.

Artikel 3

Deze verordening treedt in werking op de twintigste dag volgende op die van haar bekendmaking in het *Publicatieblad van de Europese Gemeenschappen*.

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

Gedaan te Brussel, 13 juni 2002.

Voor de Commissie
Loyola DE PALACIO
Vice-voorzitster

BIJLAGE

„BIJLAGE I B

CONSTRUCTIE-, BEPROEVINGS-, INSTALLATIE- EN CONTROLEVOORSCHRIFTEN

Teneinde de interoperabiliteit van de software van de in deze bijlage omschreven apparatuur te behouden, zijn bepaalde afkortingen, termen en uitdrukkingen op het gebied van informatica in de tekst opgenomen in de taal van het origineel, namelijk het Engels. Bij bepaalde uitdrukkingen is voor de duidelijkheid tussen haakjes een letterlijke vertaling toegevoegd.

INHOUD

I. DEFINITIES 8

II. ALGEMENE KENMERKEN EN FUNCTIES VAN HET CONTROLEAPPARAAT 12

1. Algemene kenmerken 12

2. Functies 12

3. Werkingsmodi 13

4. Beveiliging 14

III. FUNCTIONELE EN CONTRUCTIE-EISEN AAN HET CONTROLEAPPARAAT 14

1. Bewaking van het inbrengen en uitnemen van controlekaarten 14

2. Meting van snelheid en afgelegde afstand 14

2.1. Meting van de afgelegde afstand 15

2.2. Meting van de snelheid 15

3. Tijdmeting 15

4. Controleren van de activiteiten van de bestuurder 16

5. Controleren van de status van de bestuurders 16

6. Handmatige invoer door de bestuurders 16

6.1. Invoer van begin- en eindpunt van de dagelijkse werkperiode 16

6.2. Handmatige invoer van de activiteiten van de bestuurder 16

6.3. Invoer van specifieke omstandigheden 18

7. Beheer van bedrijfsvergrendelingen 18

8. Bewaking van controleactiviteiten 18

9. Detecteren van voorvallen en/of fouten 18

9.1. „Inbrengen van een ongeldige kaart” 18

9.2. „kaartconflict” 19

9.3. „Tijdsoverlapping” 19

9.4. „Rijden zonder een geschikte kaart” 19

9.5. „Inbrengen van de kaart tijdens het rijden” 19

9.6. „Laatste kaartsessie niet correct afgesloten” 19

9.7. „Snelheidsoverschrijding” 19

9.8. „Onderbreking van de stroomvoorziening” 20

9.9. „Fout in de bewegingsgegevens” 20

9.10. „Poging tot inbreuk op de beveiliging” 20

9.11. „Kaart”-fout 20

9.12. „Controleapparaat”-fout 20

10. Ingebouwde beproeving en zelfbeproeving 20

11. Lezen van het geheugen 21

12. Registratie en opslag in het geheugen 21

12.1. Identificatiegegevens van het apparaat 21

12.1.1. Identificatiegegevens van de voertuigunit 21

12.1.2. Identificatiegegevens van de bewegingsopnemer 22

12.2. Beveiligingselementen 22

12.3. Gegevens over het inbrengen en uitnemen van de bestuurderskaart 22

12.4. Gegevens over de activiteiten van de bestuurder 23

12.5. Plaatsen waar dagelijkse werkperioden beginnen en/of eindigen 23

12.6. Gegevens over de kilometerstand 23

12.7. Gedetailleerde snelheidsgegevens 23

12.8. Gegevens over voorvallen 23

12.9. Gegevens over fouten 25

12.10. Kalibreringsgegevens 26

12.11. Tijdafstellingsgegevens 26

12.12. Gegevens over controleactiviteiten 26

12.13. Gegevens over bedrijfsvergrendelingen 27

12.14. Gegevens over overbrengingsactiviteiten 27

12.15. Gegevens over specifieke omstandigheden 27

13. Aflezen van de tachograafkaart 27

14. Registratie en opslag op een tachograafkaart 27

15. Visuele weergave 28

15.1 Standaardleesvenster 28

15.2. Waarschuwingsleesvenster 29

15.3. Toegang tot het menu 29

15.4. Andere leesvensters 29

16. Afdrukken 29

17. Waarschuwingssignalen 30

18. Overbrengen van gegevens naar externe media 31

19. Uitvoeren van gegevens naar additionele externe inrichtingen 31

20. Kalibrering 32

21. Tijdafstelling 32

22. Prestatiekenmerken . . . 32
23. Materialen . . . 32
24. Aanduidingen . . . 33
IV. FUNCTIONELE EN CONSTRUCIE-EISEN VOOR TACHOGRAAFKAARTEN . . . 33
1. Zichtbare gegevens . . . 33
2. Beveiliging . . . 36
3. Normen . . . 36
4. Milieu- en elektrotechnische specificaties . . . 36
5. Gegevensopslag . . . 36
5.1. Identificatie van de kaart en veiligheidsgegevens . . . 37
5.1.1. Toepassingsidentificatie . . . 37
5.1.2. Chipidentificatie . . . 37
5.1.3. IC-kaartidentificatie . . . 37
5.1.4. Beveiligingselementen . . . 37
5.2. Bestuurderskaart . . . 37
5.2.1. Kaartidentificatie . . . 37
5.2.2. Identificatie van de kaarthouder . . . 38
5.2.3. Informatie over het rijbewijs . . . 38
5.2.4. Gegevens over het gebruik van voertuigen . . . 38
5.2.5. Gegevens over de activiteiten van de bestuurder . . . 38
5.2.6. Plaatsen waar dagelijkse werkperioden beginnen en/of eindigen . . . 39
5.2.7. Gegevens over voorvallen . . . 39
5.2.8. Gegevens over fouten . . . 40
5.2.9. Gegevens over controleactiviteiten . . . 40
5.2.10. Gegevens over kaartsessies . . . 40
5.2.11. Gegevens over specifieke omstandigheden . . . 40
5.3. Werkplaatskaart . . . 41
5.3.1. Beveiligingselementen . . . 41
5.3.2. Kaartidentificatie . . . 41
5.3.3. Identificatie van de kaarthouder . . . 41
5.3.4. Gegevens over het geburik van voertuigen . . . 41
5.3.5. Gegevens over de activiteiten van de bestuurder . . . 41
5.3.6. Gegevens over begin en einde van dagelijkse werkperioden . . . 41
5.3.7. Gegevens over voorvallen en fouten . . . 41
5.3.8. Gegevens over controleactiviteiten . . . 41
5.3.9. Gegevens over kalibrering en tijdafstelling . . . 42
5.3.10. Gegevens over specifieke omstandigheden . . . 42
5.4. Controlekaart . . . 42

5.4.1. Kaartidentificatie . . . 42
5.4.2. Identificatie van de kaarthouder . . . 42
5.4.3. Gegevens over controleactiviteiten . . . 42
5.5. Bedrijfskaart . . . 43
5.5.1. Kaartidentificatie . . . 43
5.5.2. Identificatie van de kaarthouder . . . 43
5.5.3. Gegevens over bedrijfsactiviteiten . . . 43
V. INSTALLATIE VAN HET CONTROLEAPPARAAT . . . 43
1. Installatie . . . 43
2. Installatieplaatje . . . 44
3. Verzegeling . . . 44
VI. CONTROLES, INSPECTIES EN REPARATIES . . . 45
1. Erkenning van installateurs of werkplaatsen . . . 45
2. Controle van nieuwe of herstelde inrichtingen . . . 45
3. Controle van de installatie . . . 45
4. Periodieke controles . . . 45
5. Vaststelling van afwijkingen . . . 46
6. Reparaties . . . 46
VII. KAARTAFGIFTE . . . 46
VIII. GOEDKEURING VAN HET CONTROLEAPPARAAT EN DE TACHOGRAAFKAARTEN . . . 46
1. Algemeen . . . 46
2. Veiligheidscertificaat . . . 47
3. Functiecertificaat . . . 47
4. Interoperabiliteitscertificaat . . . 47
5. Typegoedkeuringscertificaat . . . 48
6. Bijzondere procedure: eerste interoperabiliteitscertificaten . . . 48
Appendix 1: Verklarende woordenlijst van de gegevens
Appendix 2: Specificatie van tachograafkaarten
Appendix 3: Pictogrammen
Appendix 4: Afdrukken
Appendix 5: Leesvenster
Appendix 6: Externe interfaces
Appendix 7: Protocollen voor gegevensoverdracht
Appendix 8: Kalibratieprotocol
Appendix 9: TYPEGOEDKEURING — LIJST VAN MINIMAAL VEREISTE BEPROEVINGEN
Appendix 10: ALGEMENE BEVEILIGINGSDOELSTELLINGEN
Appendix 11: ALGEMENE BEVEILIGINGSMECHANISMEN

I. DEFINITIES

In deze bijlage wordt verstaan onder:

a) **„activering"**:

fase waarin het controleapparaat volledig operationeel wordt en alle functies, inclusief veiligheidsfuncties, uitvoert;

Het activeren van een controleapparaat vereist het gebruik van een werkplaatskaart en het invoeren van de pincode.

b) **„authenticatie"**:

een functie bestemd voor het vaststellen en verifiëren van een opgegeven identiteit;

c) **„authenticiteit"**:

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

d) **„ingebouwd beproevingssysteem (BIT)"**:

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

e) **„kalenderdag"**:

een dag van 00.00 uur tot en met 24.00 uur. Alle kalenderdagen hebben betrekking op de UTC-tijd (gecoördineerde wereldtijd);

f) **„kalibrering"**:

het bijwerken of bevestigen van voertuigparameters die in het geheugen opgeslagen zijn. Voertuigparameters zijn onder andere voertuigidentificatie (VIN-nummer, kentekennummer en de lidstaat van registratie) en voertuigkenmerken (w, k, l, bandenmaat, snelheidsbegrenzer (indien van toepassing), actuele UTC-tijd, actuele kilometerstand);

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 (indien van toepassing), een vervangingsindex en een vernieuwingsindex;

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 afgegeven zijn aan een bedrijf of aan een instantie die meerdere tachograafkaarten mag bezitten. Het bedrijf of de 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 van het onderdeel van het voertuig (secundaire as van de versnellingsbak of wiel van voertuig) dat is verbonden met het controleapparaat wanneer het voertuig de afstand van één kilometer aflegt, gemeten onder normale beproevingsomstandigheden (zie hoofdstuk VI.5). De kenmerkende coëfficiënt wordt in impulsen per kilometer (w = … imp/km) uitgedrukt;

l) **„bedrijfskaart"**:

een door de autoriteiten van een lidstaat aan de eigenaar of houder van met het controleapparaat uitgeruste voertuigen afgegeven tachograafkaart;

De bedrijfskaart identificeert het bedrijf en met de bedrijfskaart kunnen de in het controleapparaat van dit bedrijf opgeslagen gegevens zichtbaar gemaakt, overgebracht en afgedrukt worden.

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) **„rijtijdperiode" wordt in het controleapparaat berekend als** [1]:

de op dat moment verzamelde rijtijden van elke bestuurder afzonderlijk sinds de laatste BESCHIKBAARHEID of RUSTPAUZE of ONBEKENDE [2] periode van 45 minuten of meer (deze periode kan in een aantal periodes van 15 minuten of meer worden opgedeeld). 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 geheugenregistraties over 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 de bevoegde autoriteiten afgegeven tachograafkaart;

De controlekaart identificeert de controle-instantie en mogelijk de met de controle belaste ambtenaar en verschaft toegang tot de in het geheugen of op de bestuurderskaart opgeslagen gegevens om deze te lezen, af te drukken en/of over te brengen.

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

de cumulatieve onderbreking van de rijtijd wordt berekend als de op dat moment verzamelde BESCHIKBAARHEID of RUSTPAUZE of ONBEKENDE [2] perioden van 15 minuten of meer van elke bestuurder afzonderlijk, sinds zijn laatste BESCHIKBAARHEID of RUSTPAUZE of ONBEKENDE [2] periode van 45 minuten of meer (deze periode kan in een aantal periodes van 15 minuten of meer worden opgedeeld).

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 geheugenregistraties met betrekking tot de lopende periode waarin geen kaart ingebracht was, en met betrekking tot de relevante lezer;

q) **„geheugen"**:

een elektronisch geheugenmedium dat in het controleapparaat ingebouwd is;

r) **„digitale handtekening"**:

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

s) **„overbrengen"**:

het kopiëren, samen met een digitale handtekening, van (een gedeelte van) de gegevens die in het geheugen van het voertuig of in het geheugen van de tachograafkaart opgeslagen zijn;

Bij het overbrengen mogen opgeslagen gegevens niet gewijzigd of gewist worden.

---

[1] Door deze berekeningswijze van de rijtijdperiode en de cumulatieve rusttijd kan het controleapparaat de rijtijdwaarschuwing berekenen. Hiermee wordt niet vooruitgelopen op de wettelijke interpretatie van deze tijden.

[2] ONBEKENDE periodes komen overeen met periodes waarin de bestuurderskaart niet in het controleapparaat ingebracht was en de activiteiten van de bestuurder niet handmatig werden ingevoerd.

t) **„bestuurderskaart”**:

een door de autoriteiten van een lidstaat aan elke bestuurder afzonderlijk afgegeven tachograafkaart;

De bestuurderskaart identificeert de bestuurder en registreert de activiteiten van de bestuurder.

u) **„effectieve omtrek van de wielbanden”**:

gemiddelde afstand, afgelegd door elk van de wielen die het voertuig aandrijven, (aandrijfwielen) bij een volledige omwenteling. Het meten van deze afstanden moet geschieden onder normale beproevingsomstandigheden (hoofdstuk VI.5) en wordt als volgt uitgedrukt: „l = … mm”. Voertuigfabrikanten kunnen het meten van deze afstanden vervangen door een theoretische calculatie waarbij wordt uitgegaan van de verdeling van het gewicht op de assen, ongeladen voertuig in normale rijklare toestand ([1]). De methoden voor deze theoretische calculatie moeten door de bevoegde autoriteit van de lidstaat worden goedgekeurd;

v) **„voorval”**:

een door het controleapparaat ontdekt abnormaal functioneren dat mogelijk het gevolg is van een fraudepoging;

w) **„fout”**:

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

x) **„installatie”**:

het plaatsen van het controleapparaat in een voertuig;

y) **„bewegingsopnemer”**:

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

z) **„ongeldige kaart”**:

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

aa) **„niet verplicht”**:

wanneer het gebruik van het controleapparaat volgens de bepalingen van Verordening (EEG) nr. 3820/85 van de Raad niet vereist is.

bb) **„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 de maximumsnelheid waarop de snelheidsbegrenzer is afgesteld overschrijdt, zoals vastgelegd in 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 ([2]).

cc) **„periodieke controle”**:

een reeks verrichtingen die worden uitgevoerd om te controleren of het controleapparaat goed werkt en de instellingen overeenkomen met de voertuigparameters;

dd) **„printer”**:

deel van het controleapparaat dat opgeslagen gegevens afdrukt;

ee) **„controleapparaat”**:

het volledige in wegvoertuigen in te bouwen apparaat om gegevens betreffende het rijden van deze voertuigen en bepaalde werktijden van hun bestuurder aan te geven en automatisch of semi-automatisch te registreren en op te slaan;

([1]) Richtlijn 97/27/EG van het Europees Parlement en de Raad van 22 juli 1997 betreffende de massa's en afmetingen van bepaalde categorieën motorvoertuigen en aanhangwagens daarvan en tot wijziging van Richtlijn 70/156/EEG (PB L 233 van 25.8.1997, blz. 1).

([2]) PB L 57 van 2.3.1992, blz. 27.

ff) **„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 zijn;

gg) **„reparatie"**:

reparatie van een bewegingsopnemer of van een voertuigunit die moet worden losgekoppeld van de stroomvoorziening of van andere componenten van het controleapparaat, of die moet worden geopend;

hh) **„vervanging"**:

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 twee geldige kaarten in omloop zijn;

ii) **„veiligheidscertificatie"**:

proces ter certificering, door een certificeringsinstantie van de ITSEC ([1]), dat het onderzochte controleapparaat (of een component daarvan) of de tachograafkaart voldoet aan de veiligheidseisen zoals vastgelegd in appendix 10 Algemene veiligheidsdoelstellingen;

jj) **„zelfbeproeving"**:

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

kk) **„tachograafkaart"**:

smartcard voor gebruik in het controleapparaat. Het controleapparaat kan door middel van een tachograafkaart de identiteit (of identiteitsgroep) van de kaarthouder vaststellen en gegevens verzenden en opslaan. Een tachograafkaart is er in de volgende uitvoeringen:

— bestuurderskaart,

— controlekaart,

— werkplaatskaart,

— bedrijfskaart;

ll) **„typegoedkeuring"**:

een proces ter certificering, door een lidstaat, dat het onderzochte controleapparaat (of een component daarvan) of de tachograafkaart voldoet aan de eisen van deze verordening;

mm) **„bandenmaat"**:

de omschrijving van de afmetingen van de banden (externe aandrijfwielen) overeenkomstig Richtlijn 92/23/EEG ([2]);

nn) **„identificatienummer van het voertuig"**:

nummers die het voertuig identificeren: het kentekennummer van het voertuig met een indicatie van de lidstaat van registratie en het Voertuigidentificatienummer (VIN-nummer) ([3]);

oo) **„voertuigunit (VU)"**:

het controleapparaat met uitzondering van de bewegingsopnemer en de kabels waarmee de bewegingsopnemer aangesloten is. De voertuigunit mag uit een enkele unit bestaan of uit verscheidene units verspreid over het voertuig, mits de voertuigunit voldoet aan de veiligheidseisen van deze verordening;

([1]) Aanbeveling 95/144/EG van de Raad van 7 april 1995 inzake gemeenschappelijke veiligheidsbeoordelingscriteria voor informatietechnologie (PB L 93 van 26.4.1995, blz. 27).
([2]) PB L 129 van 14.5.1992, blz. 95.
([3]) Richtlijn 76/114/EEG van 18.12.1975 (PB L 24 van 30.1.1976, blz. 1).

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

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

qq) **„werkplaatskaart"**:

een door de autoriteiten van een lidstaat aan een fabrikant van controleapparatuur, een installateur, een voertuigfabrikant of werkplaats afgegeven en door die lidstaat goedgekeurde tachograafkaart.

De werkplaatskaart identificeert de kaarthouder en met de werkplaatskaart kan het controleapparaat beproefd en gekalibreerd worden en/of kunnen gegevens worden overgebracht.

II. ALGEMENE KENMERKEN EN FUNCTIES VAN HET CONTROLEAPPARAAT

000 Ieder met het controleapparaat uitgerust voertuig dat voldoet aan de bepalingen van deze bijlage, moet voorzien zijn van een aanwijsinrichting voor de snelheid en een kilometerteller. Deze functies kunnen in het controleapparaat worden opgenomen.

1. **Algemene kenmerken**

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

001 Het controleapparaat bestaat uit kabels, een bewegingsopnemer en een voertuigunit.

002 De voertuigunit bestaat uit een verwerkingseenheid, een geheugen, een tijdklok, twee smartcard-interfaces (bestuurder en bijrijder), een printer, een leesvenster, een visueel waarschuwingssignaal, een kalibrerings-/overbrengingsverbinding en voorzieningen voor de invoer van gebruikersgegevens.

Het controleapparaat kan door middel van additionele verbindingen aan andere inrichtingen worden gekoppeld.

003 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 de Verordening.

Gebruikers van controleapparaten identificeren zich door middel van een tachograafkaart.

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

Het controleapparaat registreert en slaat gegevens op in het geheugen en op de tachograafkaart.

Dit gebeurt in overeenstemming met 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 ([1]).

2. **Functies**

005 Het controleapparaat moet onderstaande functies kunnen uitvoeren:

— bewaken van inbrengen en uitnemen van de kaart,

— opnemen van snelheid en afstand,

— opnemen van de tijd,

— bewaken van de activiteiten van de bestuurder,

— bewaken van de status van de bestuurders,

— handmatige invoer door de bestuurders:

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

  — handmatige invoer van de activiteiten van de bestuurder,

  — invoer van specifieke omstandigheden,

([1]) PB L 281 van 23.11.1995, blz. 31.

— beheer van de bedrijfsvergrendelingen,

— bewaken van controleactiviteiten,

— detecteren van voorvallen en/of fouten,

— ingebouwde beproeving en zelfbeproeving,

— lezen van het geheugen,

— registreren en opslaan in het geheugen,

— lezen van de tachograafkaart,

— registreren en opslaan op de tachograafkaart,

— tonen,

— afdrukken,

— waarschuwen,

— gegevens overbrengen naar externe media,

— gegevens uitvoeren naar additionele externe inrichtingen,

— kalibrering,

— tijdafstelling.

3. **Werkingsmodi**

006 Het controleapparaat heeft vier werkingsmodi:

— operationele modus,

— controlemodus,

— kalibreringsmodus,

— bedrijfsmodus.

007 Het controleapparaat wisselt naar de volgende werkingsmodus overeenkomstig de geldige tachograafkaart die in de kaartinterface ingebracht is:

Werkingsmodus		Lezer bestuurder				
		Geen kaart	Bestuurderskaart	Controlekaart	Werkplaatskaart	Bedrijfskaart
Lezer van de bijrijder	Geen kaart	Operationeel	Operationeel	Controle	Kalibrering	Bedrijf
	Bestuurderskaart	Operationeel	Operationeel	Controle	Kalibrering	Bedrijf
	Controlekaart	Controle	Controle	Controle (*)	Operationeel	Operationeel
	Werkplaatskaart	Kalibrering	Kalibrering	Operationeel	Kalibrering (*)	Operationeel
	Bedrijfskaart	Bedrijf	Bedrijf	Operationeel	Operationeel	Bedrijf (*)

008 (*) In deze situaties gebruikt het controleapparaat uitsluitend de tachograafkaart die in de lezer van de bestuurder ingebracht is.

009 Het controleapparaat negeert ingebrachte ongeldige kaarten. Het blijft echter mogelijk om gegevens op ongeldige kaarten zichtbaar te maken, af te drukken of over te brengen.

010 Alle functies vermeld onder II.2 werken in iedere werkingsmodus met de onderstaande uitzonderingen:

— de kalibreringsfunctie is alleen toegankelijk in de kalibreringsmodus,

— de tijdafstellingsfunctie is beperkt buiten de kalibreringmodus,

— handmatige invoer door de bestuurder kan alleen plaatsvinden in de operationele modus of de kalibreringsmodus,

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

— het bewaken van controleactiviteiten werkt alleen in de controlemodus,

— de overbrengingsfunctie is niet toegankelijk in de operationele modus (behoudens het bepaalde in voorschrift 150).

011 Het controleapparaat kan gegevens uitvoeren naar leesvenster, 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 gedeeltelijk niet getoond (alle oneven tekens — gelezen van links naar rechts — worden niet getoond)

— in de bedrijfsmodus: gegevens over de bestuurder (voorschriften 081, 084 en 087) kunnen alleen worden uitgevoerd tijdens perioden 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: gegevens over de bestuurder kunnen alleen worden uitgevoerd voor de huidige en de 8 voorafgaande kalenderdagen.

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, en dat de integriteit en authenticiteit van uitgewisselde gegevens tussen de bewegingsopnemer en de voertuigunit en de integriteit en authenticiteit van uitgewisselde gegevens tussen het controleapparaat en de tachograafkaart worden beveiligd en de integriteit en authenticiteit van overgebrachte gegevens geverifieerd worden.

012 Om de systeemveiligheid te realiseren, moet het controleapparaat voldoen aan de beveiligingseisen zoals gespecificeerd in de algemene beveiligingsdoelstellingen voor de bewegingsopnemer en voertuigunit (appendix 10).

III. FUNCTIONELE EN CONSTRUCTIE-EISEN AAN HET CONTROLEAPPARAAT

1. **Bewaking van het inbrengen en uitnemen van controlekaarten**

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

014 Bij het inbrengen van de kaart moet het controleapparaat bepalen of de ingebrachte kaart een geldige tachograafkaart is; indien dit het geval is, wordt het kaarttype geïdentificeerd.

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

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

2. **Meting van snelheid en afgelegde afstand**

017 Deze functie meet continu de kilometerstand die overeenkomt met de totale door het voertuig afgelegde afstand en kan deze weergeven.

018 Deze functie meet continu en geeft de snelheid van het voertuig.

019 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 bewegingsopnemer waarneemt; als dit niet het geval is, wordt aangenomen dat het voertuig stilstaat.

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 eisen betreffende de maximumtoleranties die vastgelegd zijn in deze bijlage (hoofdstuk III.2.1 en III.2.2).

2.1. ***Meting van de afgelegde afstand***

020 De afgelegde afstand kan worden gemeten:

— hetzij bij vooruitrijden en achteruitrijden,

— hetzij uitsluitend bij vooruitrijden.

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

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

— ± 1 % vóór installatie,

— ± 2 % bij installatie en periodieke controle,

— ± 4 % tijdens gebruik.

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

2.2. ***Meting van de snelheid***

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

025 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).

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

025a 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.

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

3. **Tijdmeting**

027 De tijdmetingsfunctie moet voortdurend operationeel zijn en de UTC-datum en UTC-tijd digitaal leveren.

028 De UTC-datum en UTC-tijd worden gebruikt voor datering in het controleapparaat (registraties, afdrukken, gegevensuitwisseling, leesvenster, …).

029 Om de plaatselijke tijd zichtbaar te maken, is het mogelijk om de in het leesvenster getoonde tijd in stappen van een half uur te wijzigen.

030 Afwijkingen mogen niet meer dan ± 2 seconden per dag bedragen onder typegoedkeuringsvoorwaarden.

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

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

4. **Controleren van de activiteiten van de bestuurder**

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

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

035 De bestuurder en/of de bijrijder hebben de mogelijkheid om WERKEN, BESCHIKBAARHEID of RUSTPAUZE handmatig te selecteren.

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

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

038 De eerste verandering van activiteit die zich binnen 120 seconden na de automatische verandering naar WERK ten gevolge van het stoppen van het voertuig voordoet, wordt beschouwd als hebbende plaatsgevonden op het moment van het stoppen van het voertuig (de verandering naar WERK kan om die reden geannuleerd worden).

039 Deze functie moet veranderingen van activiteiten naar de registratiefuncties uitvoeren met een resolutie van een minuut.

040 Wanneer RIJDEN heeft plaatsgevonden binnen een kalenderminuut, dan wordt de hele minuut beschouwd als RIJDEN.

041 Wanneer RIJDEN heeft plaatsgevonden binnen de onmiddellijk voorafgaande en de onmiddellijk volgende kalenderminuut, dan wordt de hele minuut beschouwd als RIJDEN.

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

043 Deze functie moet ook voortdurend de rijtijdperiode en de cumulatieve rusttijd van de bestuurder controleren.

5. **Controleren van de status van de bestuurders**

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

045 De status MET EEN PLOEG wordt geselecteerd wanneer twee geldige bestuurderskaarten in het apparaat worden ingebracht, de status ALLEEN wordt in alle andere gevallen geselecteerd.

6. **Handmatige invoer door de bestuurders**

6.1. ***Invoer van begin- en eindpunt van de dagelijkse werkperiode***

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

047 Plaatsen worden gedefinieerd als het land en — voorzover relevant — de regio.

048 Op het moment van uitnemen van een bestuurderskaart (of werkplaatskaart) moet het controleapparaat de bestuurder (bijrijder) vragen een „plaats waar de dagelijkse werkperiode eindigt" in te voeren.

049 Dit verzoek kan in het controleapparaat genegeerd worden.

050 Het is mogelijk om plaatsen waar de dagelijkse werkperiode begint en/of eindigt, zonder kaart in te voeren, of om ze in te voeren op andere tijdstippen dan tijdens het inbrengen of uitnemen van de kaart.

6.2. ***Handmatige invoer van de activiteiten van de bestuurder***

050a Bij het inbrengen van de bestuurderskaart (of werkplaatskaart) — en alleen op dat moment — moet het controleapparaat:

— de kaarthouder de datum en tijd van zijn laatste kaartuitneming doorgeven en,

— de kaarthouder vragen zich te identificeren wanneer de huidige kaartinvoer een voortzetting van de lopende dagelijkse werkperiode inhoudt.

De kaarthouder kan de vraag onbeantwoord laten of positief dan wel negatief antwoorden:

— als de kaarthouder de vraag negeert, vraagt het controleapparaat de kaarthouder naar een „plaats waar de dagelijkse werkperiode begint". Deze vraag kan in het controleapparaat genegeerd worden. Wanneer een plaats wordt ingevoerd, wordt deze geregistreerd in het geheugen en op de tachograafkaart en gerelateerd aan de tijd van kaartinvoer.

— in het geval van een positief of negatief antwoord vraagt het controleapparaat aan de kaarthouder om activiteiten handmatig in te voeren, met begin- en einddatum en begin- en eindtijd, waarbij uitsluitend WERKEN, BESCHIKBAARHEID of RUSTPAUZE mogen worden ingevoerd, en zulks uitsluitend voor de periode van de laatste kaartuitneming tot de actuele invoer. Deze activiteiten mogen elkaar niet overlappen. De onderstaande procedures moeten hierbij in acht worden genomen:

  — Wanneer de kaarthouder positief op de vraag antwoordt, moet het controleapparaat de kaarthouder vragen de activiteiten handmatig in te voeren, in chronologische volgorde, voor de periode na de laatste kaartuitneming tot de actuele invoer. Het proces eindigt wanneer de eindtijd van een handmatig ingevoerde activiteit gelijk is aan de tijd van kaartinvoer.

  — Als de kaarthouder negatief op de vraag antwoordt, moet het controleapparaat:

    — De kaarthouder vragen handmatig de activiteiten in chronologische volgorde in te voeren vanaf het tijdstip van kaartuitneming tot het tijdstip van het einde van de betreffende dagelijkse werkperiode (of wanneer de dagelijkse werkperiode doorgaat, het vermelden van de activiteiten met betrekking tot het betrokken voertuig op een registratieblad). Het controleapparaat moet daarom, voordat de kaarthouder iedere activiteit handmatig kan invoeren, de kaarthouder vragen of de eindtijd van de laatst geregistreerde activiteit het einde van een voorafgaande werkperiode weergeeft (zie onderstaande opmerking).

      Opmerking: als de kaarthouder verzuimt de eindtijd van de voorafgaande werkperiode op te geven, en handmatig een activiteit invoert waarvan de eindtijd gelijk is aan de tijd van kaartinvoer, dan moet het controleapparaat:

      — aannemen dat de dagelijkse werkperiode is geëindigd bij het begin van de eerste RUSTPAUZE (of ONBEKENDE periode) na kaartuitneming of op het tijdstip van kaartuitneming wanneer geen rustpauze werd ingevoerd (en wanneer geen periode ONBEKEND is);

      — aannemen dat de begintijd (zie hieronder) gelijk is aan de tijd van kaartinvoer;

      — de onderstaande stappen volgen.

    — Vervolgens, indien de eindtijd van de betreffende werkperiode afwijkt van de tijd van kaartuitneming, of wanneer op dat moment geen plaats van einde van de dagelijkse werkperiode ingevoerd is, de kaarthouder vragen „de plaats waar de dagelijkse werkperiode is geëindigd, te bevestigen of in te voeren" (deze vraag kan in het controleapparaat genegeerd worden). Wanneer een plaats wordt ingevoerd, wordt deze alleen geregistreerd op de tachograafkaart en alleen wanneer deze afwijkt van de plaats die ingevoerd is bij kaartuitneming (indien een plaats werd ingevoerd), en wanneer deze betrekking heeft op de eindtijd van de werkperiode.

    — Vervolgens de kaarthouder vragen „de begintijd in te voeren" van de lopende dagelijkse werkperiode (of van de activiteiten met betrekking tot het onderhavige voertuig wanneer de kaarthouder eerder een registratieblad tijdens deze periode gebruikte) en de kaarthouder verzoeken om een „plaats waar de dagelijkse werkperiode begint" (deze vraag kan in het controleapparaat genegeerd worden). Wanneer een plaats wordt ingevoerd, wordt deze geregistreerd op de tachograafkaart en gerelateerd aan deze begintijd. Wanneer deze begintijd gelijk is aan de tijd van kaartinvoer, dan wordt de plaats ook in het geheugen geregistreerd.

    — Vervolgens, wanneer deze begintijd afwijkt van de tijd van kaartinvoer, de kaarthouder vragen om handmatig activiteiten in chronologische volgorde in te voeren vanaf deze begintijd tot de tijd van kaartinvoer. Het proces eindigt wanneer de eindtijd van een handmatig ingevoerde activiteit gelijk is aan de tijd van kaartinvoer.

  — De kaarthouder kan vervolgens een handmatig ingevoerde activiteit in het controleapparaat wijzigen tot de validatie door middel van selectie van een specifieke opdracht. Daarna is een wijziging niet meer mogelijk.

  — Antwoorden op de eerste vraag waarop geen invoer van activiteiten volgt, worden door het controleapparaat geïnterpreteerd als zijnde genegeerd door de kaarthouder.

Tijdens dit hele proces zal het controleapparaat niet langer dan de onderstaande time-outs wachten op invoer:

— wanneer gedurende 1 minuut geen interactie met de manuele interface van het controleapparaat plaatsvindt (met een visueel en mogelijk hoorbaar waarschuwingssignaal na 30 seconden) of,

— wanneer de kaart wordt uitgenomen of een andere bestuurderskaart (of werkplaatskaart) ingebracht wordt of,

— zodra het voertuig begint te rijden,

in dit geval moet het controleapparaat de reeds ingevoerde gegevens valideren.

6.3. ***Invoer van specifieke omstandigheden***

050b De bestuurder kan de twee onderstaande specifieke omstandigheden in real-time in het controleapparaat invoeren:

— „NIET VERPLICHT (begin, einde)"

— „VERVOER PER VEERBOOT/TREIN"

Een „VERVOER PER VEERBOOT/TREIN" mag niet voorkomen 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.

7. **Beheer van bedrijfsvergrendelingen**

051 Deze functie beheert de vergrendelingen die een bedrijf aanbrengt, zodat het bedrijf alleen toegang heeft tot de gegevens in de bedrijfsmodus.

052 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).

053 Vergrendelingen kunnen alleen in real-time „ingeschakeld" of „uitgeschakeld" worden.

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

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

055a 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".

8. **Bewaking van controleactiviteiten**

056 Deze functie moet controle uitoefenen op het TONEN en AFDRUKKEN, op de activiteit van de VU en KAARTOVERBRENGINGEN die in de controlemodus uitgevoerd worden.

057 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 leesvenster gezonden is, of wanneer gegevens over „voorvallen en fouten" uit het VU-geheugen worden overgebracht.

9. **Detecteren van voorvallen en/of fouten**

058 Deze functie detecteert de onderstaande voorvallen en/of fouten:

9.1. ***„Inbrengen van een ongeldige kaart"***

059 Dit voorval treedt op bij het inbrengen van een ongeldige kaart en/of wanneer de geldigheid van een ingebrachte kaart verloopt.

9.2. ***„Kaartconflict"***

060 Dit voorval treedt op wanneer een van de combinaties van geldige kaarten die in de onderstaande tabel met een X gemerkt zijn, voorkomt:

Lezer van de bestuurder		Kaartconflict				
		Geen kaart	Bestuurderskaart	Controlekaart	Werkplaatskaart	Bedrijfskaart
Lezer van de bijrijder	Geen kaart					
	Bestuurderskaart				X	
	Controlekaart			X	X	X
	Werkplaatskaart		X	X	X	X
	Bedrijfskaart			X	X	X

9.3. ***„Tijdsoverlapping"***

061 Dit voorval treedt op wanneer de datum/tijd van de laatste uitneming van een bestuurderskaart, zoals van de kaart wordt gelezen, later is dan de actuele datum/tijd van het controleapparaat waarin de kaart ingebracht is.

9.4. ***„Rijden zonder een geschikte kaart"***

062 Dit voorval treedt op wanneer een van de combinaties van tachograafkaarten die in de onderstaande tabel met een X gemerkt zijn, voorkomt wanneer de activiteit van de bestuurder verandert in RIJDEN, of wanneer de werkingsmodus tijdens het RIJDEN verandert:

Rijden zonder een geschikte kaart		Lezer van de bestuurder				
		Geen (of ongeldige) kaart	Bestuurderskaart	Controlekaart	Werkplaatskaart	Bedrijfskaart
Lezer van de 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

9.5. ***„Inbrengen van de kaart tijdens het rijden"***

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

9.6. ***„Laatste kaartsessie niet correct afgesloten"***

064 Dit voorval treedt op wanneer het controleapparaat bij kaartinvoer ontdekt dat, niettegenstaande de bepalingen van hoofdstuk III, punt 1, de voorafgaande kaartsessie niet correct afgesloten is (de kaart is uitgenomen voordat alle relevante gegevens op de kaart opgeslagen zijn). Dit voorval mag alleen optreden bij de bestuurderskaart en de werkplaatskaart. In dit geval moet de voertuigunit trachten zoveel mogelijk gegevens op de kaart te interpreteren en te recupereren.

9.7. ***„Snelheidsoverschrijding"***

065 Dit voorval treedt op bij elke snelheidsoverschrijding.

9.8. ***„Onderbreking van de stroomvoorziening"***

066 Dit voorval treedt op bij een onderbreking van ten minste 200 milliseconden in de stroomvoorziening van de bewegingsopnemer en/of de voertuigunit, echter niet in de kalibreringsmodus. De drempel van de onderbreking wordt door de fabrikant bepaald. De spanningsval ten gevolge van het starten van de motor van het voertuig mag dit voorval niet veroorzaken.

9.9. ***„Fout in de bewegingsgegevens"***

067 Dit voorval treedt op in het geval van een onderbreking in de normale gegevensstroom tussen de bewegingsopnemer en de voertuigunit en/of in het geval van een fout in de integriteit van de gegevens of in de authenticatie van de gegevens tijdens de gegevensuitwisseling tussen de bewegingsopnemer en de voertuigunit.

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

068 Dit voorval treedt op bij elk ander voorval dat de beveiliging van de bewegingsopnemer en/of de voertuigunit aantast zoals gespecificeerd in de algemene beveiligingsdoelstellingen van deze componenten, echter niet in de kalibreringsmodus.

9.11. ***„Kaart"-fout***

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

9.12. ***„Controleapparaat"-fout***

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

— VU interne fout

— Printerfout

— Fout in het leesvenster

— Overbrengingsfout

— Fout in de opnemer.

10. **Ingebouwde beproeving en zelfbeproeving**

071 Het controleapparaat moet zelf fouten detecteren door middel van zelfbeproevingen en ingebouwde beproevingen overeenkomstig onderstaande tabel:

Onderdelen ter beproeving	Zelfbeproeving	Ingebouwde beproeving
Software		Integriteit
Geheugen	Toegang	Toegang, gegevensintegriteit
Kaartinterfaces	Toegang	Toegang
Toetsenbord		Handmatige controle
Printer	(afhankelijk van de fabrikant)	Afdruk
Leesvenster		Visuele controle
Overbrenging (alleen uitgevoerd tijdens het overbrengen)	Correcte werking	
Opnemer	Correcte werking	Correcte werking

11. **Lezen van het geheugen**

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

12. **Registratie en opslag in het geheugen**

In 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 kaartuitneming en 256 wijzigingen in de activiteiten. „365 dagen" omvat derhalve ten minste 2 190 bestuurders (bijrijders), 2 190 cycli van kaartinvoer en kaartuitneming en 93 440 wijzigingen in de activiteiten;

— worden tijden geregistreerd met een resolutie van een minuut, tenzij anders aangegeven;

— kilometerstanden worden geregistreerd met een resolutie van een kilometer;

— snelheden worden geregistreerd met een resolutie van 1 km/h.

073 De in het geheugen opgeslagen gegevens mogen niet worden beïnvloed door een externe stroomonderbreking van minder dan 12 maanden onder typegoedkeuringsvoorwaarden.

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

12.1. ***Identificatiegegevens van het apparaat***

12.1.1. *Identificatiegegevens van de voertuigunit*

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

— naam van de fabrikant,

— adres van de fabrikant,

— onderdeelnummer,

— serienummer,

— nummer van de softwareversie,

— datum van installatie van de softwareversie,

— bouwjaar,

— goedkeuringsnummer.

076 Identificatiegegevens van de voertuigunit worden door de fabrikant van de voertuigunit definitief geregistreerd en opgeslagen, met uitzondering van softwaregerelateerde gegevens en het goedkeuringsnummer die in geval van een softwareupgrade gewijzigd kunnen worden.

12.1.2. *Identificatiegegevens van de bewegingsopnemer*

077 De bewegingsopnemer moet in zijn geheugen de volgende identificatiegegevens opslaan:

— naam van de fabrikant,

— onderdeelnummer,

— serienummer,

— goedkeuringsmerk,

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

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

078 Identificatiegegevens van de bewegingsopnemer worden door de fabrikant van de bewegingsopnemer definitief in de bewegingsopnemer geregistreerd en opgeslagen.

079 De voertuigunit moet in zijn geheugen de volgende gekoppelde identificatiegegevens van de bewegingsopnemer registreren en opslaan:

— serienummer,

— goedkeuringsnummer,

— datum van eerste koppeling.

12.2. ***Beveiligingselementen***

080 Het controleapparaat moet de volgende beveiligingselementen kunnen opslaan:

— Europese openbare sleutel,

— lidstaatcertificaat,

— apparatuurcertificaat,

— individuele sleutel van het apparaat.

De beveiligingselementen van het controleapparaat worden door de fabrikant van de voertuigunit in het apparaat ingebracht.

12.3. ***Gegevens over het inbrengen en uitnemen van de bestuurderskaart***

081 Telkens wanneer een bestuurders- of werkplaatskaart in het apparaat ingebracht of uitgenomen wordt, moet het controleapparaat in zijn geheugen het volgende registreren en opslaan:

— de naam en voornaam van de kaarthouder zoals opgeslagen op de kaart;

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

— datum en tijd van inbrengen;

— de kilometerstand bij kaartinvoer;

— de lezer waarin de kaart wordt ingebracht;

— datum en tijd van uitnemen;

— de kilometerstand bij kaartuitneming;

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

  — kentekennummer en registerende lidstaat;

  — datum en tijd van kaartuitneming;

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

082 Het geheugen moet deze gegevens ten minste 365 dagen vasthouden.

083 Wanneer de geheugencapaciteit volledig is gebruikt, komen de meest recente gegevens in de plaats van de oudste gegevens.

12.4. ***Gegevens over de activiteiten van de bestuurder***

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

— de status van de bestuurders (ALLEEN/MET EEN PLOEG);

— de lezer (BESTUURDER, BIJRIJDER);

— de status van de kaart in de betreffende lezer (INGEBRACHT, NIET INGEBRACHT) (Zie opmerking);

— de activiteiten (RIJDEN, BESCHIKBAARHEID, WERKEN, RUSTPAUZE);

— de datum en tijd van de wijziging.

Opmerking: 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 bijv. wel een bedrijfskaart ingebracht of er is geen kaart ingebracht).

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

085 Het geheugen moet de gegevens over de activiteiten van de bestuurder ten minste 365 dagen vasthouden.

086 Wanneer de geheugencapaciteit volledig is gebruikt, komen de meest recente gegevens in de plaats van de oudste gegevens.

12.5. ***Plaatsen waar dagelijkse werkperioden beginnen en/of eindigen***

087 Telkens wanneer een bestuurder (bijrijder) een plaats invoert waar een dagelijkse werkperiode begint en/of eindigt, moet het controleapparaat in zijn geheugen registreren en opslaan:

— indien van toepassing, het bestuurderskaartnummer en de lidstaat van afgifte;

— de datum en tijd van de invoer (of de datum/tijd gerelateerd aan de invoer wanneer deze door middel van de handmatige invoerprocedure wordt ingevoerd);

— de soort invoer (begin of einde, omstandigheid van invoer);

— het ingevoerde land en de ingevoerde regio;

— de kilometerstand.

088 Het geheugen moet de begin- en/of eindgegevens van dagelijkse werkperioden ten minste 365 dagen vasthouden (in de veronderstelling dat een bestuurder twee registraties per dag invoert).

089 Wanneer de geheugencapaciteit volledig is gebruikt, komen de meest recente gegevens in de plaats van de oudste gegevens.

12.6. ***Gegevens over de kilometerstand***

090 Het controleapparaat moet elke kalenderdag om 0.00 uur de kilometerstand van het voertuig en de corresponderende datum in zijn geheugen registreren.

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

092 Wanneer de geheugencapaciteit volledig is gebruikt, komen de meest recente gegevens in de plaats van de oudste gegevens.

12.7. ***Gedetailleerde snelheidsgegevens***

093 Het controleapparaat moet voor elke seconde van ten minste de laatste 24 uur waarin het voertuig gebruikt is, de snelheid van het voertuig en de corresponderende datum en tijd registeren en in het geheugen opslaan.

12.8. ***Gegevens over voorvallen***

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

094 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
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, nummer en lidstaat van afgifte van de twee kaarten die het conflict veroorzaken
Rijden zonder een geschikte kaart	— het langste voorval op elk van de laatste 10 dagen waarop een dergelijk voorval plaatshad — 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, nummer en lidstaat van afgifte van een bij het begin en/of einde van het voorval ingebrachte kaart — aantal vergelijkbare voorvallen op die dag
Inbrengen van de kaart tijdens het rijden	— het laatste voorval op elk van de laatste 10 dagen waarop een dergelijk voorval plaatshad	— datum en tijd van het voorval — kaartsoort, nummer en lidstaat van afgifte — aantal vergelijkbare voorvallen op die dag
Laatste kaartsessie niet correct afgesloten	— de 10 meest recente voorvallen	— datum en tijd van kaartinvoer — kaartsoort, nummer en lidstaat van afgifte — laatste sessiegegevens zoals af te lezen van de kaart: — datum en tijd van kaartinvoer — kentekennummer en lidstaat van registratie
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 opgetreden is na de laatste kalibrering	— datum en tijd van het begin van het voorval — datum en tijd van het einde van het voorval — maximumsnelheid gemeten tijdens het voorval — rekenkundige maximumsnelheid gemeten tijdens het voorval — kaartsoort, nummer en lidstaat van afgifte van de bestuurder (indien van toepassing) — aantal vergelijkbare voorvallen op die dag

Voorval	Opslagvoorschriften	Te registreren gegevens per voorval
Onderbreking in de stroomvoorziening ([2])	— het langste voorval op elk van de laatste 10 dagen waarop een dergelijk voorval plaatshad — 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, nummer en lidstaat van afgifte van de kaart die bij 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 plaatshad — 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, nummer en lidstaat van afgifte van de kaart die bij 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, nummer en lidstaat van afgifte van de kaart die bij begin en/of einde van het voorval ingebracht is — soort voorval

095 ([1]) Het controleapparaat moet ook in zijn geheugen registreren en opslaan:
— de datum en tijd van de laatste CONTROLE VAN DE SNELHEIDSOVERSCHRIJDING;
— de datum en tijd van de eerste snelheidsoverschrijding na deze CONTROLE VAN DE SNELHEIDSOVERSCHRIJDING;
— het aantal snelheidsoverschrijdingen sinds de laatste CONTROLE VAN DE SNELHEIDSOVERSCHRIJDING.

([2]) Deze gegevens kunnen alleen na herstel van de stroomvoorziening worden geregistreerd; tijden kunnen op de minuut nauwkeurig bekend zijn.

12.9. ***Gegevens over fouten***

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

096 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 tijd van het begin van de fout — datum en tijd van het einde van de fout — kaartsoort, nummer en lidstaat van afgifte
Fouten controleapparaat	— 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, nummer en lidstaat van afgifte van de kaart die bij begin en/of einde van de fout ingebracht is

12.10. ***Kalibreringsgegevens***

097 Het controleapparaat moet gegevens registreren en in het geheugen opslaan 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-nummer);

— de 5 meest recente kalibreringen (wanneer een aantal kalibreringen op dezelfde kalenderdag plaatsvinden, wordt alleen de laatste kalibrering van de dag opgeslagen).

098 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;

— VIN-nummer van het voertuig;

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

099 De bewegingsopnemer moet de volgende installatiegegevens van de bewegingsopnemer 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).

12.11. ***Tijdafstellingsgegevens***

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

— de meest recente tijdafstelling,

— de 5 belangrijkste tijdafstellingen sinds de laatste kalibrering,

uitgevoerd in de kalibreringsmodus buiten het kader van een normale kalibrering (def. f).

101 De volgende gegevens moeten voor elke tijdafstelling worden geregistreerd:

— datum en tijd, oude waarde;

— datum en tijd, nieuwe waarde;

— naam en adres van de werkplaats;

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

12.12. ***Gegevens over controleactiviteiten***

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

— datum en tijd van de controle;

— controlekaartnummer en de lidstaat die de kaart afgeeft;

— aard van de controle (tonen en/of afdrukken en/of VU overbrengen en/of kaart overbrengen).

103 In het geval van overbrengen worden de data van de oudste en van de meest recent overgebrachte dagen ook geregistreerd.

12.13. ***Gegevens over bedrijfsvergrendelingen***

104 Het controleapparaat moet de volgende gegevens met betrekking tot de 20 meest recente bedrijfsvergrendelingen registreren en in zijn geheugen opslaan:

— datum en tijd van vergrendeling;

— datum en tijd van ontgrendeling;

— bedrijfskaartnummer en de lidstaat die de kaart afgeeft;

— naam en adres van het bedrijf.

12.14. ***Gegevens over overbrengingsactiviteiten***

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

— datum en tijd van overbrenging;

— bedrijfskaart- of werkplaatskaartnummer en de lidstaat die de kaart afgeeft;

— naam van het bedrijf of de werkplaats.

12.15. ***Gegevens over specifieke omstandigheden***

105a Het controleapparaat moet de volgende gegevens met betrekking tot specifieke omstandigheden in zijn geheugen registreren:

— datum en tijd van de invoer;

— aard van de specifieke omstandigheid.

105b Het geheugen moet gegevens over specifieke omstandigheden ten minste 365 dagen vasthouden (in de veronderstelling dat gemiddeld 1 omstandigheid per dag wordt geopend en gesloten). Wanneer de opslagcapaciteit volledig is gebruikt, komen de meest recente gegevens in de plaats van de oudste gegevens.

13. **Aflezen van de tachograafkaart**

106 Het controleapparaat moet van de tachograafkaart de noodzakelijke gegevens aflezen:

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

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

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

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

— om een bestuurderskaart naar externe media over te brengen.

107 In het geval van een leesfout moet het controleapparaat dezelfde leesopdracht maximaal drie keer opnieuw uitvoeren. Wanneer dit niet lukt moet de kaart defect en ongeldig worden verklaard.

14. **Registratie en opslag op een tachograafkaart**

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

109 Het controleapparaat moet de gegevens die op een geldige bestuurderskaart, werkplaatskaart en/of controlekaart opgeslagen zijn, 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. De gegevens die op deze kaarten moeten worden opgeslagen, worden gespecificeerd in hoofdstuk IV.

109a Het controleapparaat moet de gegevens over de activiteiten van de bestuurder en de plaats (zoals gespecificeerd in hoofdstuk IV, punten 5.2.5 en 5.2.6) bijwerken, die opgeslagen zijn op een geldige bestuurderskaart of werkplaatskaart, waarbij de gegevens over activiteiten en plaats handmatig door de kaarthouder worden ingevoerd.

110 Het bijwerken van gegevens op de tachograafkaart moet zodanig geschieden dat, indien noodzakelijk en rekening houdend met de opslagcapaciteit van de kaart, nieuwe gegevens in de plaats komen van de oudste gegevens.

111 In het geval van een schrijffout moet het controleapparaat dezelfde schrijfopdracht maximaal drie keer opnieuw uitvoeren. Wanneer dit niet lukt moet de kaart defect en ongeldig worden verklaard.

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

15. **Visuele weergave**

113 Het leesvenster moet ten minste 20 tekens bevatten.

114 De tekens moeten minimaal 5 mm hoog en 3,5 mm breed zijn.

114a Het leesvenster ondersteunt de in ISO 8859, deel 1 en 7, gedefinieerde tekensets Latin1 en Greek, als gespecificeerd in appendix 1, hoofdstuk 4 „Tekensets". Het leesvenster kan vereenvoudigde tekens gebruiken (bijv. letters met een accent kunnen zonder accent worden getoond, of onderkastletters kunnen als bovenkastletters worden getoond).

115 Het leesvenster moet voorzien zijn van een voldoende sterke, niet verblindende verlichting.

116 Aanwijzingen moeten aan de buitenzijde van het controleapparaat zichtbaar zijn.

117 Het controleapparaat moet:

— standaardgegevens;

— gegevens met betrekking tot waarschuwingssignalen;

— gegevens met betrekking tot de toegang tot het menu;

— andere door de gebruiker opgevraagde gegevens

zichtbaar maken.

Aanvullende informatie kan door het controleapparaat worden getoond, mits deze duidelijk te onderscheiden is van de hierboven vermelde vereiste informatie.

118 Het leesvenster van het controleapparaat moet de pictogrammen of pictogramcombinaties zoals vermeld in appendix 3 gebruiken. Extra pictogrammen of pictogramcombinaties kunnen ook door het leesvenster worden getoond wanneer deze duidelijk te onderscheiden zijn van de voornoemde pictogrammen of pictogramcombinaties.

119 Het leesvenster moet altijd ingeschakeld zijn wanneer het voertuig rijdt.

120 Het controleapparaat kan een handmatige of automatische voorziening hebben om het leesvenster uit te schakelen wanneer het voertuig stilstaat.

De vorm van het leesvenster wordt gespecificeerd in appendix 5.

15.1. ***Standaardleesvenster***

121 Wanneer geen andere informatie getoond hoeft te worden, moet het controleapparaat standaard de volgende informatie weergeven:

— 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 rijtijdperiode 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;

— informatie met betrekking tot de bijrijder:

  — de lopende duur van zijn activiteit (sinds deze geselecteerd werd).

122 De gegevens met betrekking tot elke bestuurder moeten duidelijk en ondubbelzinnig worden getoond. 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.

123 Als de breedte van het leesvenster onvoldoende is om de werkingsmodus standaard te tonen, moet het controleapparaat kort de nieuwe werkingsmodus tonen wanneer deze wijzigt.

124 Het controleapparaat moet bij kaartinvoer kort de naam van de kaarthouder tonen.

124a Wanneer een „NIET VERPLICHT" omstandigheid wordt geopend, dan moet het standaardleesvenster door middel van het relevante pictogram tonen dat de omstandigheid geopend is (Het is aanvaardbaar dat de lopende activiteit van de bestuurder niet tegelijkertijd wordt getoond).

15.2. ***Waarschuwingsleesvenster***

125 Het controleapparaat moet waarschuwingssignalen voornamelijk door middel van de pictogrammen van appendix 3 tonen, die waar nodig worden aangevuld met additionele numerieke informatie. Een letterlijke beschrijving van de waarschuwing kan in de voorkeurstaal van de bestuurder worden toegevoegd.

15.3. ***Toegang tot het menu***

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

15.4. ***Andere leesvensters***

127 Het is mogelijk om op verzoek selectief zichtbaar te maken:

— de UTC-datum en UTC-tijd;

— de werkingsmodus (indien deze niet standaard wordt getoond);

— de rijtijdperiode en cumulatieve rusttijd van de bestuurder;

— de rijtijdperiode en cumulatieve rusttijd van de bijrijder;

— de rijtijdperiode van de bestuurder van de afgelopen en de lopende week;

— de rijtijdperiode van de bijrijder van de afgelopen en de lopende week;

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

128 De inhoud van de afdrukken moet sequentieel, regel voor regel, worden getoond. Indien de breedte van het leesvenster minder dan 24 tekens is, moet de gebruiker de volledige informatie door middel van een geschikt middel (een aantal regels, scrollen, …) krijgen. Afgedrukte regels van handgeschreven informatie kunnen op het leesvenster worden weggelaten.

16. **Afdrukken**

129 Het controleapparaat moet informatie uit zijn geheugen en/of van de tachograafkaart overeenkomstig de zes onderstaande documenten afdrukken:

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

— dagelijkse afdruk van de voertuigunit (VU) van de activiteiten van de bestuurder;

— afdruk van de kaart van voorvallen en fouten;

— afdruk van de voertuigunit van voorvallen en fouten;

— afdruk van technische gegevens;

— afdruk van snelheidsoverschrijding.

De gedetailleerde vorm en inhoud van deze afdrukken worden gespecificeerd in appendix 4.

Additionele gegevens kunnen aan het einde van de afdruk worden opgenomen.

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

130 De „dagelijkse afdruk van de kaart van de activiteiten van de bestuurder" en de „afdruk van de kaart van voorvallen en fouten" 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.

131 Om de „dagelijkse afdruk van de kaart van de activiteiten van de bestuurder" of de „afdruk van de kaart van voorvallen en fouten" 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 lezer van de bestuurder te selecteren indien twee kaarten in het controleapparaat ingebracht zijn.

132 De printer moet 24 tekens per regel afdrukken.

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

133a De printer ondersteunt de in ISO 8859, deel 1 en 7, gedefinieerde tekensets Latin1 en Greek, zoals gespecificeerd in appendix 1, hoofdstuk 4 „Tekensets".

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

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

136 Op het door het controleapparaat gebruikte papier moet het relevante goedkeuringsmerk staan. Daarnaast moet op het papier vermeld staan voor welk(e) type(n) controleapparatuur dit papier geschikt is. De afdrukken moeten onder normale opslagomstandigheden voor wat betreft lichtsterkte, vochtigheid en temperatuur, gedurende ten minste een jaar duidelijk leesbaar en identificeerbaar blijven.

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

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

17. **Waarschuwingssignalen**

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

140 Een waarschuwing met betrekking tot een onderbreking in de stroomvoorziening kan worden uitgesteld totdat de stroomvoorziening is hersteld.

141 Het controleapparaat moet de bestuurder bij een naderende overschrijding van de maximale rijtijdperiode van vier en een half uur 15 minuten van tevoren waarschuwen.

142 De vorm van de waarschuwingssignalen is visueel en daarnaast kunnen akoestische waarschuwingssignalen worden gegeven.

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

144 De visuele waarschuwingssignalen kunnen in het controleapparaat ingebouwd zijn en/of zich buiten het controleapparaat bevinden.

145 In het laatste geval heeft het een „T"-symbool en is de kleur ervan geel of oranje.

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

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

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

18. **Overbrengen van gegevens naar externe media**

149 Het controleapparaat moet op verzoek vanuit zijn geheugen of vanaf een bestuurderskaart via de kalibrerings-/overbrengingsverbinding gegevens naar externe opslagmedia kunnen overbrengen. Het controleapparaat werkt de opgeslagen gegevens op de betrokken kaart bij voordat met overbrenging van gegevens wordt begonnen.

150 Verder is er een optie waardoor het controleapparaat in elke werkingsmodus gegevens via een andere verbinding naar een door dit kanaal geauthentiseerd bedrijf kan overbrengen. In dit geval zijn de gegevenstoegangsrechten in de bedrijfsmodus van toepassing op deze overbrenging.

151 Opgeslagen gegevens worden door overbrenging niet gewijzigd of verwijderd.

De elektrotechnische interface van de kalibrerings-/overbrengingsverbinding wordt gespecificeerd in appendix 6.

Overbrengingsprotocollen worden gespecificeerd in appendix 7.

19. **Uitvoeren van gegevens naar additionele externe inrichtingen**

152 Wanneer het controleapparaat geen aanwijsinrichtingen voor de tachometer en/of de kilometerteller heeft, moet het controleapparaat uitvoersignalen leveren die de snelheid van het voertuig (tachometer) en/of de totale door het voertuig afgelegde afstand (kilometerstand) tonen.

153 De voertuigunit moet tevens de volgende gegevens uitvoeren met behulp van een geschikte functiegebonden seriële verbinding die niet afhankelijk is van een facultatieve CAN-busverbinding (ISO 11898 Road vehicles — Interchange of digital information — Controller Area Network (CAN) for high speed communication), waardoor de verwerking van deze gegevens door andere elektronische units in het voertuig mogelijk wordt:

— lopende UTC-datum en UTC-tijd;

— snelheid van het voertuig;

— totale door het voertuig afgelegde afstand (kilometerteller);

— lopende door de bestuurder en bijrijder geselecteerde activiteiten;

— informatie of een tachograafkaart in de lezer van de bestuurder en in de lezer van de bijrijder ingebracht is en (indien van toepassing) informatie over de identificatie van de betreffende kaarten (kaartnummer en lidstaat van afgifte).

Naast deze gegevens kunnen ook andere gegevens worden uitgevoerd.

Wanneer de ontsteking van het voertuig ingeschakeld is, worden deze gegevens permanent getoond. Wanneer de ontsteking van het voertuig uitgeschakeld is, genereert iedere wijziging in de activiteiten van de bestuurder of van de bijrijder en/of het inbrengen of uitnemen van een tachograafkaart een overeenkomstige uitvoer van gegevens. In het geval dat uitvoer van de gegevens niet heeft plaatsgevonden terwijl de ontsteking van het voertuig uitgeschakeld is, komen deze gegevens ter beschikking zodra de ontsteking van het voertuig weer ingeschakeld is.

20. **Kalibrering**

154 De kalibreringsfunctie moet:

— de bewegingsopnemer automatisch met de VU verbinden;

— de constante van het controleapparaat (k) digitaal aan de kenmerkende coëfficiënt van het voertuig (w) aanpassen (voertuigen met twee of meer brugoverbrengingen worden uitgerust met een schakeltoestel waarmee deze verschillende overbrengingen automatisch op een lijn worden gebracht met de overbrenging waarvoor het apparaat aan het voertuig aangepast is);

— (onbeperkt) de lopende tijd afstellen;

— de lopende kilometerstand bijstellen;

— in het geheugen opgeslagen identificatiegegevens van de bewegingsopnemer bijwerken;

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

155 Het verbinden van de bewegingsopnemer met de VU moet ten minste bestaan uit:

— het bijwerken van installatiegegevens van de bewegingsopnemer die door de bewegingsopnemer worden vastgehouden (indien nodig);

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

156 De kalibreringsfunctie kan via de kalibrerings-/overbrengingsverbinding essentiële gegevens invoeren in overeenstemming met het kalibreringsprotocol gedefinieerd in appendix 8. Met de kalibreringsfunctie kunnen ook via andere verbindingen essentiële gegevens worden ingevoerd.

21. **Tijdafstelling**

157 Met de tijdafstellingsfunctie kan de lopende tijd met maximaal 1 minuut voor een periode van minimaal 7 dagen worden bijgesteld.

158 In de kalibreringsmodus kan de lopende tijd met de tijdafstellingsfunctie zonder beperkingen worden bijgesteld.

22. **Prestatiekenmerken**

159 De voertuigunit moet binnen het temperatuurbereik van − 20 °C tot + 70 °C naar behoren functioneren en de bewegingsopnemer binnen het temperatuurbereik van − 40 °C tot + 135 °C. De inhoud van het geheugen moet bij temperaturen tot − 40 °C bewaard blijven.

160 Het controleapparaat moet binnen het vochtigheidsbereik van 10 % tot 90 % naar behoren functioneren.

161 Het controleapparaat moet tegen overspanning, polariteitomkering en kortsluiting worden beveiligd.

162 Het controleapparaat moet voldoen aan Richtlijn 95/54/EG van de Commissie ([1]) tot aanpassing aan de technische vooruitgang van Richtlijn 72/245/EEG van de Raad met betrekking tot elektromagnetische compatibiliteit en moet tegen elektrostatische ontladingen en stootspanning worden beveiligd.

23. **Materialen**

163 Alle samenstellende delen van het controleapparaat moeten uitgevoerd zijn in materiaal van voldoende stabiliteit en mechanische sterkte en met onveranderlijke elektrische en magnetische eigenschappen.

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

165 De voertuigunit moet voldoen aan beschermingsklasse IP 40 en de bewegingsopnemer moet voldoen aan beschermingsklasse IP 64, volgens IEC 529.

([1]) PB L 266 van 8.11.1995, blz. 1.

166 Het controleapparaat moet wat het ergonomisch ontwerp betreft, voldoen aan de toepasselijke technische specificaties.

167 Het controleapparaat moet tegen onopzettelijke beschadiging worden beschermd.

24. **Aanduidingen**

168 Indien het controleapparaat de kilometerstand en snelheid van het voertuig toont, moeten onderstaande aanduidingen in het leesvenster 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 tonen, in welk geval voor de snelheidsaanduiding het symbool „mph" gebruikt wordt.

169 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;

— serienummer van het apparaat;

— goedkeuringsmerk van het type controleapparaat.

170 Wanneer er onvoldoende fysieke ruimte is voor alle bovengenoemde gegevens, moeten op het identificatieplaatje ten minste voorkomen: de naam of het logo van de fabrikant en het onderdeelnummer van het controleapparaat.

IV. FUNCTIONELE EN CONSTRUCTIE-EISEN VOOR TACHOGRAAFKAARTEN

1. **Zichtbare gegevens**

De voorkant bevat:

171 naar gelang de soort kaart de vermelding „Bestuurderskaart" of „Controlekaart" of „Werkplaatskaart" of „Bedrijfskaart", in hoofdletters, gedrukt in de taal/talen van de lidstaat die de kaart afgeeft.

172 dezelfde vermelding in de overige talen van de Gemeenschap, op zodanige wijze gedrukt dat deze de achtergrond van de kaart vormen:

ES	TARJETA DEL CONDUCTOR	TARJETA DE CONTROL	TARJETA DEL CENTRO DE ENSAYO	TARJETA DE LA EMPRESA
DK	FØRERKORT	KONTROLKORT	VÆRKSTEDSKORT	VIRKSOMHEDSKORT
DE	FAHRERKARTE	KONTROLLKARTE	WERKSTATTKARTE	UNTERNEHMENSKARTE
EL	ΚΑΡΤΑ ΟΔΗΟΥ	ΚΑΡΤΑ ΕΛΕΓΧΟΥ	ΚΑΡΤΑ ΚΕΝΤΡΟΥ ΔΟΚΙΜΩΝ	ΚΑΡΤΑ ΕΠΙΧΕΙΡΗΣΗΣ
EN	DRIVER CARD	CONTROL CARD	WORKSHOP CARD	COMPANY CARD
FR	CARTE DE CONDUCTEUR	CARTE DE CONTROLEUR	CARTE D'ATELIER	CARTE D'ENTREPRISE
GA	CÁRTA TIOMÁNAÍ	CÁRTA STIÚRTHA	CÁRTA CEARDLAINNE	CÁRTA COMHLACHTA
IT	CARTA DEL CONDUCENTE	CARTA DI CONTROLLO	CARTA DELL'OFFICINA	CARTA DELL'AZIENDA
NL	BESTUURDERSKAART	CONTROLEKAART	WERKPLAATSKAART	BEDRIJFSKAART
PT	CARTÃO DE CONDUTOR	CARTÃO DE CONTROLO	CARTÃO DO CENTRO DE ENSAIO	CARTÃO DE EMPRESA
FIN	KULJETTAJA KORTTILLA	VALVONTA KORTILLA	TESTAUSASEMA KORTILLA	YRITYSKORTILLA
SV	FÖRARKORT	KONTROLLKORT	VERKSTADSKORT	FÖRETAGSKORT

173 de vermelding van de naam van de lidstaat die de kaart afgeeft (facultatief);

174 het onderscheidingsteken van de lidstaat die de kaart afgeeft, negatief afgedrukt in een door twaalf gele sterren omringde blauwe rechthoek. De onderscheidingstekens zijn:

B België

DK Denemarken

D Duitsland

GR Griekenland

E Spanje

F Frankrijk

IRL Ierland

I Italië

L Luxemburg

NL Nederland

A Oostenrijk

P Portugal

FIN Finland

S Zweden

UK Verenigd Koninkrijk

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

	Bestuurderskaart	Controlekaart	Bedrijfs- of Werkplaatskaart
1.	Naam van de bestuurder	Naam van de controle-instantie	Naam van het bedrijf of de werkplaats
2.	Voorna(a)men van de bestuurder	Achternaam van de controleur (indien van toepassing)	Achternaam van de kaarthouder (indien van toepassing)
3.	Geboortedatum van de bestuurder	Voornaam van de controleur (indien van toepassing)	Voornaam van de kaarthouder (indien van toepassing)
4.(a)	De datum van afgifte van de kaart		
(b)	Eventuele datum waarop de kaart ongeldig wordt		
(c)	Naam van de autoriteit die de kaart afgeeft (mag op kant 2 worden gedrukt)		
(d)	Ander nummer dan dat in rubriek 5, dat nuttig is voor de administratie van de kaart (facultatief)		
5.(a)	Rijbewijsnummer (op het moment van afgifte van de bestuurderskaart)		
5.(b)	Kaartnummer		
6.	Foto van de bestuurder	Foto van de controleur (facultatief)	—
7.	Handtekening van de bestuurder	Handtekening van de houder (facultatief)	
8.	Woon- of verblijfplaats of postadres van de houder (facultatief)	Postadres van de controle-instantie	Postadres van het bedrijf of de werkplaats

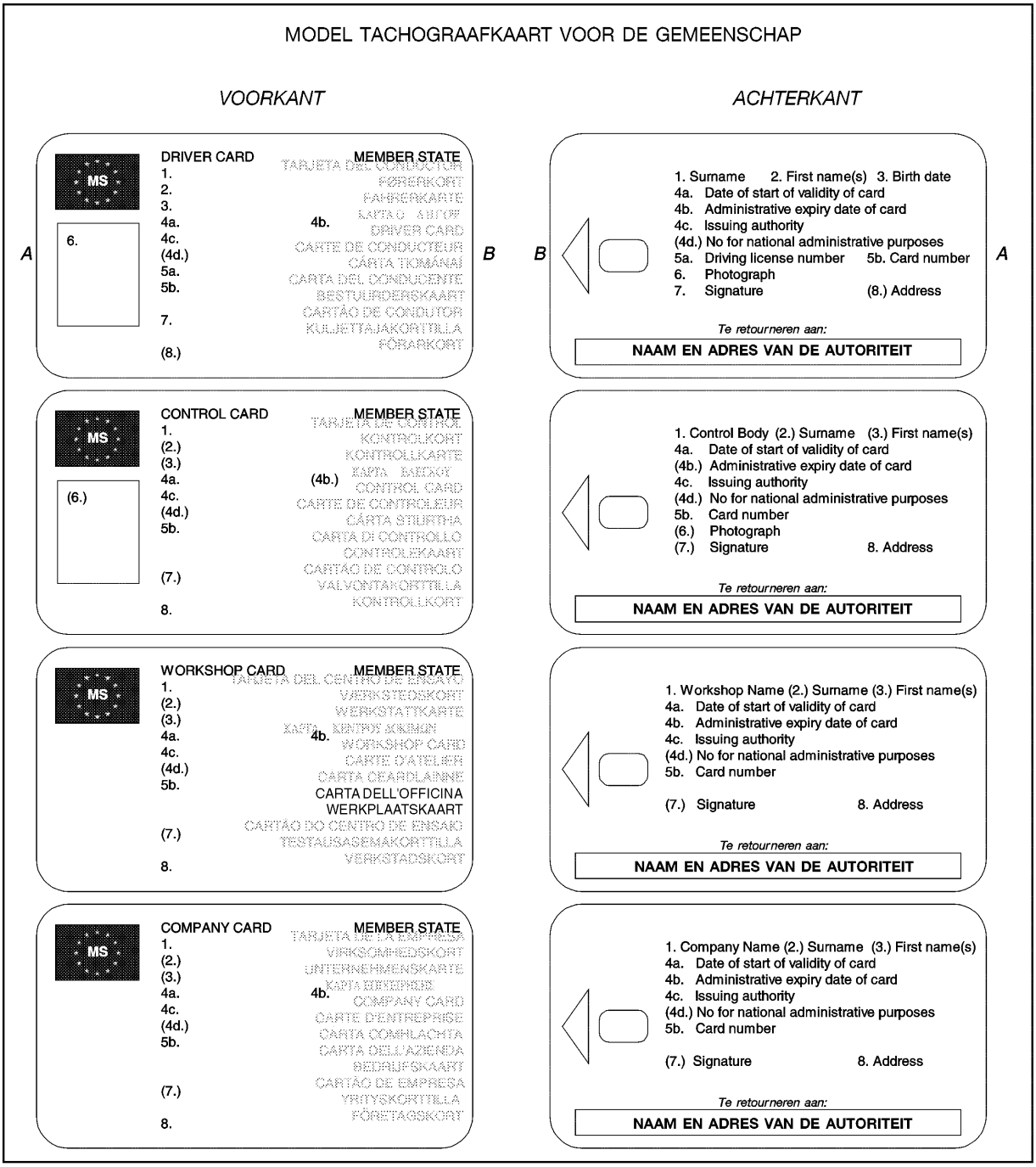
176 data moeten in de vorm van „dd/mm/jjjj" of „dd.mm.jjjj" (dag, maand, jaar) worden geschreven.

De achterkant bevat:

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

178 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.

MODEL TACHOGRAAFKAART VOOR DE GEMEENSCHAP



179 Tachograafkaarten moeten worden gedrukt met de volgende achtergrondkleuren:

— bestuurderskaart: wit,

— controlekaart: blauw,

— werkplaatskaart: rood,

— bedrijfskaart: geel.

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

— een beveiligde achtergrond met fijne guillochepatronen en regenboogdruk,

— bij de foto moeten de beveiligde achtergrond en de foto elkaar overlappen,

— ten minste één tweekleurige microzeefdrukregel.

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

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 gehaald wordt, het uitvoeren van bepaalde schrijfopdrachten op de kaarten uitsluitend mogelijk te maken voor het controleapparaat, het uitsluiten van mogelijke vervalsing van op de kaarten opgeslagen gegevens, alsmede het voorkomen van manipulaties en het detecteren van pogingen daartoe.

182 Teneinde het systeem te beveiligen, moeten tachograafkaarten voldoen aan de eisen zoals vastgelegd in de algemene beveiligingsdoelstellingen voor tachograafkaarten (appendix 10).

183 Tachograafkaarten moeten door andere inrichtingen zoals personal computers gelezen kunnen worden.

3. **Normen**

184 De tachograafkaarten moeten aan de volgende normen voldoen:

— ISO/IEC 7810 Identification cards — Physical characteristics

— ISO/IEC 7816 Identification cards — Integrated circuits with contacts:

  — Deel 1: Physical characteristics,

  — Deel 2: Dimensions and location of the contacts,

  — Deel 3: Electronic signals and transmission protocols,

  — Deel 4: Inter-industry commands for interchange,

  — Deel 8: Security related inter-industry commands,

— ISO/IEC 10373 Identification cards — Test methods.

4. **Milieu- en elektrotechnische specificaties**

185 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.

186 De tachograafkaart moet binnen het vochtigheidsbereik van 10 % tot 90 % naar behoren kunnen functioneren.

187 De tachograafkaart moet vijf jaar lang naar behoren kunnen functioneren indien de vastgestelde milieu- en elektrotechnische grenswaarden niet overschreden worden.

188 Tijdens de werking moet de tachograafkaart voldoen aan Richtlijn 95/54/EG van de Commissie van 31 oktober 1995 ([1]) inzake elektromagnetische compatibiliteit en moet de kaart beveiligd zijn tegen elektrostatische ontladingen.

5. **Gegevensopslag**

Voor de toepassing van dit punt

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

— worden kilometerstanden met een resolutie van 1 kilometer geregistreerd;

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

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

([1]) PB L 266 van 8.11.1995, blz. 1.

189 Dit punt specificeert de minimale opslagcapaciteit voor de verschillende gegevensbestanden. De tachograafkaart moet de effectieve opslagcapaciteit van deze gegevensbestanden aan het controleapparaat mededelen.

Eventuele additionele gegevens die op de tachograafkaart kunnen worden opgeslagen en betrekking hebben op andere toepassingen die de kaart eventueel kan ondersteunen, moeten opgeslagen worden overeenkomstig Richtlijn 95/46/EG [1].

5.1. ***Identificatie van de kaart en veiligheidsgegevens***

5.1.1. *Toepassingsidentificatie*

190 De tachograafkaart moet de volgende toepassingsidentificatiegegevens kunnen opslaan:

— toepassingsidentificatie van de tachograaf,

— type tachograafkaartidentificatie.

5.1.2. *Chipidentificatie*

191 De tachograafkaart moet de volgende identificatiegegevens van het Integrated Circuit (IC) opslaan:

— IC-serienummer,

— IC-productiereferenties.

5.1.3. *IC-kaartidentificatie*

192 De tachograafkaart moet de volgende smartcard-identificatiegegevens opslaan:

— serienummer van de kaart (inclusief productiereferenties),

— typegoedkeuringsnummer van de kaart,

— persoonlijke identificatie van de kaart (ID),

— embedder ID,

— IC-identificatiesymbool.

5.1.4. *Beveiligingselementen*

193 De tachograafkaart moet de volgende beveiligingselementen kunnen opslaan:

— Europese openbare sleutel,

— lidstaatcertificaat,

— kaartcertificaat,

— persoonlijke sleutel van de kaart.

5.2. ***Bestuurderskaart***

5.2.1. *Kaartidentificatie*

194 De bestuurderskaart moet de volgende kaartidentificatiegegevens kunnen opslaan:

— kaartnummer,

— lidstaat van afgifte, autoriteit van afgifte, datum van afgifte,

— datum van afgifte van de kaart en datum waarop de kaart ongeldig wordt.

[1] PB L 281 van 23.11.1995, blz. 1.

5.2.2. *Identificatie van de kaarthouder*

195 De bestuurderskaart moet de volgende identificatiegegevens van de kaarthouder kunnen opslaan:

— de naam van de houder,

— de voorna(a)m(en) van de houder,

— geboortedatum,

— voorkeurstaal.

5.2.3. *Informatie over het rijbewijs*

196 De bestuurderskaart moet de volgende rijbewijsgegevens kunnen opslaan:

— lidstaat van afgifte, autoriteit van afgifte,

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

5.2.4. *Gegevens over het gebruik van voertuigen*

197 De 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 cyclus van inbrengen en uitnemen van de betrokken kaart in het voertuig) de volgende gegevens kunnen opslaan:

— datum en tijd 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 tijd 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.

198 De bestuurderskaart moet ten minste 84 registraties kunnen opslaan.

5.2.5. *Gegevens over de activiteiten van de bestuurder*

199 De bestuurderskaart moet voor elke kalenderdag waarop de kaart wordt gebruikt of waarvoor de bestuurder handmatig 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 bestuurders verandert en/of wanneer hij zijn kaart heeft ingebracht of uitgenomen:

  — de status van de bestuurders (ALLEEN/MET EEN PLOEG);

  — de lezer (BESTUURDER, BIJRIJDER);

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

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

  — het tijdstip van de wijziging.

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

201 De gegevens genoemd in de voorschriften 197 en 199 moeten zodanig worden opgeslagen, dat de activiteiten in de volgorde van optreden kunnen worden opgezocht, zelfs in het geval van tijdsoverlapping.

5.2.6. *Plaatsen waar dagelijkse werkperioden beginnen en/of eindigen*

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

— de datum en tijd van de invoer (of de datum/tijd van de invoer indien deze handmatig geschiedt);

— de soort invoer (begin of einde, omstandigheid van invoer);

— het ingevoerde land en de ingevoerde regio;

— de kilometerstand van het voertuig.

203 Het geheugen van de bestuurderskaart moet ten minste 42 registraties kunnen opslaan.

5.2.7. *Gegevens over voorvallen*

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

204 De 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 van de stroomvoorziening;

— fout in de bewegingsgegevens;

— pogingen de beveiliging op te heffen of te omzeilen.

205 De bestuurderskaart moet de volgende gegevens over deze voorvallen kunnen opslaan:

— code van het voorval;

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

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

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

Opmerking: In het geval van „Tijdsoverlapping”:

— moeten datum en tijd van het begin van het voorval overeenkomen met de datum en tijd van kaartuitneming uit het vorige voertuig;

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

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

Opmerking: In het geval van „Laatste kaartsessie niet correct afgesloten”:

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

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

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

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

5.2.8. *Gegevens over fouten*

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

207 De 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.

208 De bestuurderskaart moet de volgende gegevens over deze fouten kunnen opslaan:

— foutcode;

— datum en tijd van het begin van de fout (of van de kaartinvoer indien de fout op dat moment voortduurde);

— datum en tijd van het einde van de fout (of van de kaartuitneming indien de fout op dat moment voortduurde);

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

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

5.2.9. *Gegevens over controleactiviteiten*

210 De bestuurderskaart moet de volgende gegevens met betrekking tot controleactiviteiten opslaan:

— datum en tijd van de controle;

— controlekaartnummer en lidstaat die de kaart heeft afgegeven;

— soort controle (tonen en/of printen en/of VU-overbrenging en/of kaartoverbrenging (zie opmerking));

— overgebrachte periode, in het geval van overbrenging;

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

Opmerking: De beveiligingseisen impliceren dat kaartoverbrenging uitsluitend geregistreerd wordt wanneer de overbrenging plaatsvindt via een controleapparaat.

211 De bestuurderskaart moet één van deze registraties kunnen vasthouden.

5.2.10. *Gegevens over kaartsessies*

212 De bestuurderskaart moet gegevens opslaan met betrekking tot het voertuig waarin de lopende sessie geopend is:

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

— kentekennummer en lidstaat van registratie.

5.2.11. *Gegevens over specifieke omstandigheden*

212a De bestuurderskaart moet de volgende gegevens met betrekking tot specifieke omstandigheden kunnen opslaan, die ingevoerd werden terwijl de kaart in een lezer ingebracht was:

— datum en tijd van de invoer;

— aard van de specifieke omstandigheid.

212b De bestuurderskaart moet 56 van dergelijke registraties kunnen vasthouden.

5.3. ***Werkplaatskaart***

5.3.1. *Beveiligingselementen*

213 De werkplaatskaart moet een Personal Identification Number (pincode) kunnen opslaan.

214 De werkplaatskaart moet de cryptografische sleutels voor het verbinden van de bewegingsopnemers aan de voertuigunits kunnen opslaan.

5.3.2. *Kaartidentificatie*

215 De werkplaatskaart moet de volgende kaartidentificatiegegevens kunnen opslaan:

— kaartnummer;

— lidstaat van afgifte, autoriteit van afgifte, datum van afgifte;

— datum van afgifte van de kaart en datum waarop de kaart ongeldig wordt.

5.3.3. *Identificatie van de kaarthouder*

216 De 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.

5.3.4. *Gegevens over het gebruik van voertuigen*

217 De werkplaatskaart moet de gegevens over het gebruik van voertuigen op dezelfde manier kunnen opslaan als een bestuurderskaart.

218 De werkplaatskaart moet ten minste 4 van dergelijke registraties kunnen opslaan.

5.3.5. *Gegevens over de activiteiten van de bestuurder*

219 De werkplaatskaart moet de gegevens over de activiteiten van de bestuurder op dezelfde manier kunnen opslaan als een bestuurderskaart.

220 De werkplaatskaart moet de gegevens over de activiteiten van de bestuurder ten minste gedurende 1 dag met gemiddelde activiteiten van de bestuurder vasthouden.

5.3.6. *Gegevens over begin en einde van dagelijkse werkperioden*

221 De werkplaatskaart moet de gegevens over begin en einde van dagelijkse werkperioden op dezelfde manier kunnen opslaan als een bestuurderskaart.

222 De werkplaatskaart moet ten minste 3 registraties kunnen vasthouden.

5.3.7. *Gegevens over voorvallen en fouten*

223 De werkplaatskaart moet de gegevens over voorvallen en fouten op dezelfde manier kunnen opslaan als een bestuurderskaart.

224 De 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.

5.3.8. *Gegevens over controleactiviteiten*

225 De werkplaatskaart moet de gegevens over controleactiviteiten op dezelfde manier kunnen opslaan als een bestuurderskaart.

5.3.9. *Gegevens over kalibrering en tijdafstelling*

226 De werkplaatskaart moet registraties van kalibreringen en/of tijdafstellingen kunnen vasthouden die uitgevoerd worden terwijl de kaart in een controleapparaat ingebracht is.

227 Elke kalibreringsregistratie moet de volgende gegevens bevatten:

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

— VIN-nummer van het voertuig;

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

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

228 De werkplaatskaart moet ten minste 88 registraties kunnen opslaan.

229 De werkplaatskaart moet een teller bevatten die het totale aantal kalibreringen aangeeft dat met de kaart uitgevoerd is.

230 De werkplaatskaart moet een teller bevatten die het aantal kalibreringen sinds de laatste overbrenging aangeeft.

5.3.10. *Gegevens over specifieke omstandigheden*

230a De werkplaatskaart moet gegevens over specifieke omstandigheden op dezelfde manier kunnen opslaan als een bestuurderskaart. De werkplaatskaart moet 2 registraties kunnen opslaan.

5.4. ***Controlekaart***

5.4.1. *Kaartidentificatie*

231 De controlekaart moet de volgende kaartidentificatiegegevens opslaan:

— kaartnummer;

— lidstaat van afgifte, autoriteit van afgifte, datum van afgifte;

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

5.4.2. *Identificatie van de kaarthouder*

232 De 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.

5.4.3. *Gegevens over controleactiviteiten*

233 De controlekaart moet de volgende gegevens met betrekking tot controleactiviteiten kunnen opslaan:

— datum en tijd van de controle;

— soort controle (tonen en/of printen en/of VU-overbrenging en/of kaartoverbrenging);

— overgebrachte periode (indien van toepassing);

— kentekennummer en lidstaat waarin het gecontroleerde voertuig geregistreerd staat;

— kaartnummer en lidstaat die de gecontroleerde bestuurderskaart afgegeven heeft.

234 De controlekaart moet ten minste 230 registraties kunnen vasthouden.

5.5. ***Bedrijfskaart***

5.5.1. *Kaartidentificatie*

235 De bedrijfskaart moet de volgende kaartidentificatiegegevens kunnen opslaan:

— kaartnummer;

— lidstaat van afgifte, autoriteit van afgifte, datum van afgifte;

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

5.5.2. *Identificatie van de kaarthouder*

236 De bedrijfskaart moet de volgende identificatiegegevens van de kaarthouder kunnen opslaan:

— naam van het bedrijf;

— adres van het bedrijf.

5.5.3. *Gegevens over bedrijfsactiviteiten*

237 De bedrijfskaart moet de volgende gegevens over bedrijfsactiviteiten kunnen opslaan:

— datum en tijd van de activiteit;

— soort activiteit (vergrendeling en/of ontgrendeling van VU en/of VU-overbrenging en/of kaartoverbrenging);

— overgebrachte periode (indien van toepassing);

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

— kaartnummer en lidstaat die de kaart afgegeven heeft (in het geval van kaartoverbrenging).

238 De bedrijfskaart moet ten minste 230 van dergelijke registraties kunnen vasthouden.

V. INSTALLATIE VAN HET CONTROLEAPPARAAT

1. **Installatie**

239 Nieuwe controleapparaten moeten in niet-geactiveerde toestand geleverd worden aan installateurs of voertuigfabrikanten. Alle kalibreringsparameters, zoals vermeld in hoofdstuk III.20, moeten daarbij ingesteld zijn op de juiste en geldige standaardwaarden. Indien geen specifieke waarde geschikt is, moeten letters op „?" en cijfers op „0" worden gezet.

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

241 Vóór de activering mag het controleapparaat geen gegevens zoals genoemd in punt III.12.3 tot en met III.12.9 en punt III.12.12 tot en met III.12.14 registreren of opslaan.

242 Tijdens de installatie moeten de voertuigfabrikanten alle bekende parameters instellen.

243 Voertuigfabrikanten of installateurs moeten het geïnstalleerde controleapparaat activeren voordat het voertuig het bedrijf verlaat waar de installatie plaatsvond.

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

245 Eventuele specifieke verbindingen tussen de bewegingsopnemer en de voertuigunit moeten voor of tijdens de activering automatisch plaatsvinden.

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

247 De registratie- en opslagfuncties van het controleapparaat moeten na de activering volledig operationeel zijn.

248 Na de installatie moet een kalibrering volgen. Bij de eerste kalibrering wordt het kentekennummer ingevoerd; deze kalibrering vindt binnen 2 weken na de installatie of na de toewijzing van het kentekennummer plaats.

248a Het controleapparaat moet zodanig in het voertuig worden geïnstalleerd dat de bestuurder gemakkelijk vanaf zijn zitplaats toegang heeft tot de noodzakelijke functies.

2. **Installatieplaatje**

249 Na controle van het controleapparaat bij de installatie wordt op, in of naast het controleapparaat een installatieplaatje aangebracht, dat duidelijk zichtbaar en gemakkelijk toegankelijk is. Na iedere controle door een erkende installateur of werkplaats dient het oude plaatje door een nieuw te worden vervangen.

250 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;

— datum waarop de kenmerkende coëfficiënt van het voertuig vastgesteld en de effectieve omtrek van de wielbanden gemeten is;

— VIN-nummer van het voertuig.

3. **Verzegeling**

251 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;

— het installatieplaatje, tenzij het zodanig aangebracht is dat het niet kan worden verwijderd zonder de daarop aangebrachte aanduidingen te vernietigen.

252 De bovengenoemde verzegelingen mogen worden verwijderd:

— in noodgevallen;

— voor het plaatsen, afstellen of repareren van een snelheidsbegrenzer of alle andere tot de verkeersveiligheid bijdragende inrichtingen, op voorwaarde dat het controleapparaat op betrouwbare en juiste wijze blijft functioneren en door een erkende installateur of werkplaats (als bedoeld in hoofdstuk VI) onmiddellijk na het plaatsen van de snelheidsbegrenzer dan wel alle andere tot de verkeersveiligheid bijdragende inrichtingen opnieuw verzegeld wordt, of in alle andere gevallen binnen zeven dagen.

253 Iedere verbreking van deze zegels moet schriftelijk worden gemotiveerd; deze motivering dient ter beschikking van de bevoegde autoriteit te worden gehouden.

VI. CONTROLES, INSPECTIES EN REPARATIES

Voorschriften betreffende de omstandigheden waarin verzegelingen verwijderd mogen worden, zoals vermeld in artikel 12, lid 5 van Verordening (EEG) nr. 3821/85, laatstelijk gewijzigd bij Verordening (EG) nr. 2135/98, worden beschreven in hoofdstuk V.3 van deze bijlage.

1. **Erkenning van installateurs of werkplaatsen**

De lidstaten erkennen, certificeren en controleren regelmatig de instanties die de

— installaties,

— controles,

— inspecties en

— reparaties moeten verrichten.

In het kader van artikel 12, lid 1, van deze verordening worden werkplaatskaarten 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 beschreven in appendix 10.

2. **Controle van nieuwe of herstelde inrichtingen**

254 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 hoofdstuk III.2.1 en III.2.2 vastgelegde grenswaarden moeten worden gehanteerd, door middel van de verzegeling overeenkomstig hoofdstuk V.3 en kalibrering.

3. **Controle van de installatie**

255 Na plaatsing in een voertuig moeten de gehele installatie en het controleapparaat voldoen aan de bepalingen betreffende de maximumtoleranties zoals vastgelegd in hoofdstuk III.2.1 en III.2.2.

4. **Periodieke controles**

256 Periodieke controles van de in de voertuigen geïnstalleerde inrichtingen moeten 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 plaatsvinden.

257 Het volgende moet worden gecontroleerd:

— de goede werking van het controleapparaat, met name de gegevensopslag op de tachograafkaart;

— de naleving van het bepaalde in hoofdstuk III.2.1 en III.2.2 inzake de maximumtoleranties bij installatie;

— de aanwezigheid van het goedkeuringsmerk op het controleapparaat;

— de aanwezigheid van het installatieplaatje;

— de ongeschonden staat van de zegels van het apparaat en van de andere installatieonderdelen;

— de bandenmaat en de effectieve omtrek van de banden.

258 Bij deze controles moet een kalibrering plaatsvinden.

5. **Vaststelling van afwijkingen**

259 De vaststelling van de afwijkingen bij installatie en gebruik geschiedt onder de volgende omstandigheden, die beschouwd moeten worden als normale beproevingsvoorwaarden:

— 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;

— voortbeweging van het 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. **Reparaties**

260 Werkplaatsen kunnen gegevens van het controleapparaat overbrengen en deze gegevens teruggeven aan de betreffende transportonderneming.

261 Erkende werkplaatsen moeten een certificaat van onmogelijkheid van gegevensoverdracht aan de transportondernemingen afgeven, wanneer vooraf geregistreerde gegevens ten gevolge van de slechte werking van het controleapparaat zelfs na reparatie door de betrokken werkplaats niet kunnen worden overgebracht. De werkplaatsen bewaren een kopie van elk afgegeven certificaat gedurende ten minste een jaar.

VII. KAARTAFGIFTE

De door de lidstaten vastgestelde werkwijze bij kaartafgifte moet aan het volgende voldoen:

262 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.

263 Van de kaartnummers van alle niet-persoonlijke tachograafkaarten, die aan een enkele controle-instantie, een enkele werkplaats of een enkele transportonderneming zijn afgegeven, moeten de eerste 13 cijfers hetzelfde zijn; verder moeten ze allemaal een andere opeenvolgende index hebben.

264 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).

265 Een tachograafkaart die ter vervanging van een bestaande tachograafkaart wordt afgegeven, moet dezelfde vervaldatum hebben als de vervangen kaart.

266 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).

267 Het ruilen van een bestaande tachograafkaart ten einde administratieve gegevens te wijzigen moet in dezelfde lidstaat geschieden volgens de voorschriften voor vernieuwing, of de voorschriften van eerste afgifte wanneer de ruiling plaatsvindt in een andere lidstaat.

268 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.

VIII. GOEDKEURING VAN HET CONTROLEAPPARAAT EN DE TACHOGRAAFKAARTEN

1. **Algemeen**

In dit hoofdstuk betekent het woord „controleapparaat” „controleapparaat of zijn samenstellende delen”. Er is geen goedkeuring vereist voor de verbindingskabel(s) tussen de bewegingsopnemer en de VU. Het in het controleapparaat gebruikte papier wordt als een samenstellend deel van het controleapparaat beschouwd.

269 Het controleapparaat moet met alle geïntegreerde inrichtingen ter goedkeuring worden aangeboden.

270 De goedkeuring van het controleapparaat en van de tachograafkaarten omvat beproevingen van de beveiliging, functiebeproevingen en interoperabiliteitsbeproevingen. Positieve beproevingsresultaten worden op een relevant certificaat vermeld.

271 De goedkeuringsautoriteiten van de lidstaten verlenen geen goedkeuringscertificaat overeenkomstig artikel 5 van deze verordening, zolang zij niet in het bezit zijn van:

— een beveiligingscertificaat,

— een functiecertificaat

— en een interoperabiliteitscertificaat

voor het controleapparaat of de tachograafkaart waarvoor goedkeuring wordt aangevraagd.

272 De autoriteit die de goedkeuring voor het apparaat verleende, moet vooraf over elke wijziging in de software of hardware van het apparaat of in de aard van de voor de fabricage gebruikte materialen worden geïnformeerd. Deze autoriteit moet de verlenging van de goedkeuring aan de fabrikant bevestigen of kan een aanpassing of een bevestiging van de relevante functie-, beveiligings- en/of interoperabiliteitscertificaten eisen.

273 Procedures voor aanpassing van de in-situ software van het controleapparaat moeten worden goedgekeurd door de autoriteit die de typegoedkeuring voor het controleapparaat verleende. Een aanpassing van de software mag de in het controleapparaat opgeslagen gegevens over de activiteiten van de bestuurder wijzigen noch verwijderen. Software mag alleen onder de verantwoordelijkheid van de fabrikant van het apparaat aangepast worden.

2. **Veiligheidscertificaat**

274 Het veiligheidscertificaat wordt afgegeven in overeenstemming met de bepalingen van appendix 10 van deze bijlage.

3. **Functiecertificaat**

275 Eenieder die een typegoedkeuring aanvraagt, moet de goedkeuringsautoriteit van de lidstaat de door die autoriteit noodzakelijk geachte benodigdheden en documentatie verschaffen.

276 Een functiecertificaat wordt alleen aan de fabrikant afgegeven nadat in elk geval alle functiebeproevingen als gespecificeerd in appendix 9, succesvol afgesloten zijn.

277 De goedkeuringsautoriteit 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 beproevingen en behaalde resultaten vermelden.

4. **Interoperabiliteitscertificaat**

278 Interoperabiliteitsbeproevingen worden door een laboratorium in opdracht en onder verantwoordelijkheid van de Europese Commissie uitgevoerd.

279 Het laboratorium moet de verzoeken van fabrikanten om interoperabiliteitsbeproevingen in chronologische volgorde van binnenkomst registreren.

280 Verzoeken worden officieel geregistreerd wanneer het laboratorium in het bezit is van:

— alle benodigdheden en documenten die nodig zijn voor deze interoperabiliteitsbeproevingen;

— het corresponderende beveiligingscertificaat;

— het corresponderende functiecertificaat.

De fabrikant moet over de registratiedatum van het verzoek worden geïnformeerd.

281 Het laboratorium onderwerpt een controleapparaat of een tachograafkaart niet aan interoperabiliteitsbeproevingen wanneer voor dat apparaat of die kaart geen beveiligingscertificaat en functiecertificaat afgegeven is.

282 Een fabrikant die een interoperabiliteitsbeproeving aanvraagt, moet alle benodigdheden en documenten die nodig zijn voor het uitvoeren van de beproeving, aan het voor deze beproeving verantwoordelijke laboratorium verstrekken.

283 Alle typen controleapparatuur en alle tachograafkaarten

— waarvan de goedkeuring nog steeds geldig is of,

— waarvan de goedkeuring aangevraagd is en die een geldig interoperabiliteitscertificaat hebben,

moeten overeenkomstig de bepalingen van punt 5 van appendix 9 van deze bijlage onderworpen worden aan interoperabiliteitsbeproevingen.

284 Het laboratorium geeft het interoperabiliteitscertificaat alleen aan de fabrikant af nadat alle vereiste interoperabiliteitsbeproevingen succesvol afgerond zijn.

285 Indien de interoperabiliteitsbeproevingen bij een of meer controleapparaten of tachograafkaarten, als vereist volgens voorschrift 283, niet succesvol afgerond zijn, wordt het interoperabiliteitscertificaat pas afgegeven nadat de betreffende fabrikant de noodzakelijke wijzigingen heeft aangebracht en de apparatuur respectievelijk kaarten de daaropvolgende interoperabiliteitsbeproevingen met succes hebben doorstaan. Het laboratorium moet de oorzaak van het probleem met hulp van de betreffende fabrikanten vaststellen en moet de fabrikant die het verzoek ingediend heeft, helpen bij het vinden van een technische oplossing. Als de fabrikant zijn product heeft gewijzigd, dient hij bij de bevoegde instantie na te vragen of het veiligheidscertificaat en het functiecertificaat nog steeds geldig zijn.

286 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.

287 Elk onderdeel dat de oorzaak kan zijn van een interoperabiliteitsfout, mag niet worden gebruikt om voordelen of een dominante positie te verkrijgen.

5. **Typegoedkeuringscertificaat**

288 De goedkeuringsautoriteit van de lidstaat geeft het goedkeuringscertificaat af zodra de autoriteit in het bezit is van de drie vereiste certificaten.

289 Op het moment van afgifte aan de fabrikant moet de goedkeuringsautoriteit een kopie van het goedkeuringscertificaat aan het voor de interoperabiliteitsbeproevingen verantwoordelijke laboratorium verstrekken.

290 Het voor de interoperabiliteitsbeproevingen bevoegde laboratorium moet een publiek toegankelijke website beheren waarop de lijst van typen controleapparaten of tachograafkaarten wordt bijgewerkt:

— waarvoor een verzoek om interoperabiliteitsbeproevingen geregistreerd is;

— die een interoperabiliteitscertificaat (ook tijdelijk) hebben ontvangen;

— die een typegoedkeuringscertificaat hebben ontvangen.

6. **Bijzondere procedure: eerste interoperabiliteitscertificaten**

291 Tot vier maanden nadat het eerste controleapparaat met de tachograafkaarten (bestuurders-, werkplaats-, controle- en bedrijfskaart) als interoperabel gecertificeerd is, wordt een afgegeven interoperabiliteitscertificaat (inclusief het allereerste) met betrekking tot tijdens deze periode geregistreerde verzoeken, als tijdelijk beschouwd.

292 Wanneer aan het einde van deze periode alle betreffende producten onderling interoperabel zijn, worden alle corresponderende interoperabiliteitscertificaten definitief.

293 Wanneer tijdens deze periode interoperabiliteitsfouten worden ontdekt, moet het voor de interoperabiliteitsbeproevingen verantwoordelijke laboratorium de oorzaak van de problemen met hulp van alle betrokken fabrikanten vaststellen en moeten de fabrikanten de noodzakelijke wijzigingen aanbrengen.

294 Indien zich aan het einde van deze periode nog steeds interoperabiliteitsproblemen voordoen, moet het voor de interoperabiliteitsbeproevingen 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 interoperabiliteitsbeproevingen verantwoordelijke laboratorium beslist welke apparaten en kaarten een definitief interoperabiliteitscertificaat krijgen. De Commissie motiveert haar beslissing.

295 Elk verzoek om interoperabiliteitsbeproevingen dat door het laboratorium geregistreerd wordt tussen het einde van de periode van vier maanden nadat het eerste tijdelijke interoperabiliteitscertificaat afgegeven is, en de datum waarop de Commissie haar beslissing zoals genoemd onder 294, moet worden opgeschort totdat de aanvankelijke interoperabiliteitsproblemen opgelost zijn. Deze verzoeken worden vervolgens in chronologische volgorde van registratie behandeld.

Appendix 1

VERKLARENDE WOORDENLIJST VAN DE GEGEVENS

INHOUD

1.	Inleiding	54
1.1.	Methoden ter definitie van gegevenssoorten	54
1.2.	Referenties	54
2.	Definities van gegevenssoorten	55
2.1.	ActivityChangeInfo (Informatie over wijziging van de activiteiten)	55
2.2.	Adres	56
2.3.	BCDString (Binair-decimale codenotatie)	56
2.4.	CalibrationPurpose (Kalibreringsdoel)	56
2.5.	CardActivityDailyRecord (Dagelijkse registratie van de activiteiten op de kaart)	57
2.6.	CardActivityLengthRange (Lengtebereik van de activiteiten op de kaart)	57
2.7.	CardApprovalNumber (Goedkeuringsnummer van de kaart)	57
2.8.	CardCertificate (Kaartcertificaat)	57
2.9.	CardChipIdentification (Identificatie van de kaartchip)	57
2.10.	CardConsecutiveIndex (Opeenvolgende index van de kaart)	58
2.11.	CardControlActivityDataRecord (Gegevensregistratie van controleactiviteiten op de kaart)	58
2.12.	CardCurrentUse (Huidig gebruik kaart)	58
2.13.	CardDriverActivity (Bestuurdersactiviteiten op de kaart)	58
2.14.	CardDrivingLicenceInformation (Rijbewijsinformatie op kaart)	59
2.15.	CardEventData (Voorvalgegevens op kaart)	59
2.16.	CardEventRecrord (Voorvalregistratie op kaart)	59
2.17.	CardFaultData (Foutgegevens op kaart)	60
2.18.	CardFaultRecord (Registratie van kaartfouten)	60
2.19.	CardIccIdentification (IC-Identificatie kaart)	60
2.20.	CardIdentification (Kaartidentificatie)	61
2.21.	CardNumber (Kaartnummer)	61
2.22.	CardPlaceDailyWorkPeriod (Plaatsen van dagelijkse werkperiodes)	61
2.23.	CardPrivateKey (Particuliere sleutel van de kaart)	62
2.24.	CardPublicKey (Openbare sleutel van de kaart)	62
2.25.	CardRenewalIndex (Vernieuwingsindex van de kaart)	62
2.26.	CardReplacementIndex (Vervangingsindex van de kaart)	62
2.27.	CardSlotNumber (Nummer van de kaartlezer)	62
2.28.	CardSlotsStatus (Status van de kaartlezers)	62
2.29.	CardStructureVersion (Versie van de kaartstructuur)	63

2.30. CardVehicleRecord (Registratie van het gebruik van het voertuig) . . . 63
2.31. CardVehiclesUsed (Gebruikte voertuigen op de kaart) . . . 63
2.32. Certificate (Certificaat) . . . 64
2.33. CertificateContent (Inhoud van het certificaat) . . . 64
2.34. CertificateHolderAuthorisation (Autorisatie van de certificaathouder) . . . 64
2.35. CertificateRequestID (ID van verzoek om certificaat) . . . 65
2.36. CertificationAuthorityKID (Sleutel-ID van de certificeringsautoriteit) . . . 65
2.37. CompanyActivityData (Gegevens over bedrijfsactiviteiten) . . . 65
2.38. CompanyActivityType (Sort bedrijfsactiviteit) . . . 66
2.39. CompanyCardApplicationIdentification (Toepassingsidentificatie van de bedrijfskaart) . . . 66
2.40. CompanyCardHolderIdentification (Identificatie van de bedrijfskaarthouder) . . . 66
2.41. ControlCardApplicationIdentification (Toepassingsidentificatie van de controlekaart) . . . 67
2.42. ControlCardControlActivityData (Gegevens over controleactiviteiten van de controlekaart) . . . 67
2.43. ControlCardHolderIdentification (Identificatie van de controlekaarthouder) . . . 67
2.44. ControlType (Soort controle) . . . 68
2.45. CurrentDateTime (Huidige datum en tijd) . . . 68
2.46. DailyPresenceCounter (Dagelijkse-aanwezigheidsteller) . . . 68
2.47. Datef (Datumeenheid) . . . 69
2.48. Distance (Afstand) . . . 69
2.49. DriverCardApplicationIdentification (Toepassingsidentificatie van de bestuurderskaart) . . . 69
2.50. DriverCardHolderIdentification (Identificatie van de bestuurderskaarthouder) . . . 69
2.51. EntryTypeDailyWorkPeriod (Soort invoer van de dagelijkse werkperiode) . . . 70
2.52. EquipmentType (Soort inrichting) . . . 70
2.53. EuropeanPublicKey (Europese openbare sleutel) . . . 70
2.54. EventFaultType (Soorten voorvallen en fouten) . . . 70
2.55. EventFaultRecordPurpose (Doel van de voorvallen-foutenregistratie) . . . 71
2.56. ExtendedSerialNumber (Verlengd serienummer) . . . 72
2.57. FullCardNumber (Volledig kaartnummer) . . . 72
2.58. HighResOdometer (Zeer nauwkeurige kilometerteller) . . . 72
2.59. HighResTripDistance (Zeer nauwkeurige reisafstand) . . . 72
2.60. HolderName (Naam van de houder) . . . 72
2.61. K-ConstantOfRecordingEquipment (K-Constante van het controleapparaat) . . . 73
2.62. KeyIdentifier (Sleutelidentificatiesymbool) . . . 73
2.63. L-TyreCircumference (L-omtrek van de wielbanden) . . . 73
2.64. Language (Taal) . . . 73
2.65. LastCardDownload . . . 73
2.66. ManualInputFlag (Label voor handmatige invoer) . . . 73
2.67. ManufacturerCode (Code van de fabrikant) . . . 74

2.68. MemberStateCertificate (Lidstaatcertificaat) . . . 74
2.69. MemberStatePublicKey (Openbare sleutel van een lidstaat) . . . 75
2.70. Name (Naam) . . . 75
2.71. NationAlpha (Alfanumerieke code van een land) . . . 75
2.72. NationNumeric (Numerieke code van een land) . . . 76
2.73. NoOfCalibrationRecords (Aantal kalibreringsregistraties) . . . 77
2.74. NoOfCalibrationSinceDonwload (Aantal kalibreringen sinds de laatste overbrenging) . . . 77
2.75. NoOfCardPlaceRecords (Aantal plaatsregistraties) . . . 77
2.76. NoOfCardVehicleRecords (Aantal voertuigregistraties) . . . 77
2.77. NoOfCompanyActivityRecords (Aantal registraties van bedrijfsactiviteiten) . . . 77
2.78. NoOfControlActivityRecords (Aantal registraties van controleactiviteiten) . . . 78
2.79. NoOfEventsPerType (Aantal voorvallen per soort) . . . 78
2.80. NoOfFaultsPerType (Aantal fouten per soort) . . . 78
2.81. OdometerValueMidnight (Kilometerstand om 0.00 uur) . . . 78
2.82. OdometerShort (Verkorte kilometerstand) . . . 78
2.83. OverspeedNumber (Aantal snelheidoverschrijdingen) . . . 78
2.84. PlaceRecord (Plaatsregistratie) . . . 78
2.85. PreviousVehicleInfo (Informatie over het vorige voertuig) . . . 79
2.86. PublicKey (Openbare sleutel) . . . 79
2.87. RegionAlpha (Alfanumerieke code van een regio) . . . 79
2.88. RegionNumeric (Numerieke code van een regio) . . . 79
2.89. RSAKeyModulus (Modulus van de RSA sleutel) . . . 80
2.90. RSAKeyPrivateExponent (Particuliere exponent van de RSA sleutel) . . . 80
2.91. RSAKeyPublicExponent (Openbare exponent van de RSA-sleutel) . . . 80
2.92. SensorApprovalNumber (Goedkeuringsnummer van de opnemer) . . . 80
2.93. SensorIdentification (Identificatie van de opnemer) . . . 80
2.94. SensorInstallation (Installatie van de opnemer) . . . 81
2.95. SensorInstallationSecData (Beveiligingsgegevens over de installatie van de opnemer) . . . 81
2.96. SensorOSIdentifiee (Identificatiesymbool van het OS van de opnemer) . . . 81
2.97. SensorPaired (Verbonden opnemer) . . . 81
2.98. SensorPairingDate (Datum van verbinding van de opnemer) . . . 82
2.99. SensorSerialNumber (Serienummer van de opnemer) . . . 82
2.100. SensorSCIdentifier (Identificatiesymbool van de beveiligingscomponent van de opnemer) . . . 82
2.101. Signature (Handtekening) . . . 82
2.102. SimilarEventsNumber (Aantal vergelijkbare voorvallen) . . . 82
2.103. SpecificConditionType (Soort specifieke omstandigheid) . . . 82
2.104. SpecificConditionRecord (Registratie van een specifieke omstandigheid) . . . 82
2.105. Speed (Snelheid) . . . 83

2.106. SpeedAuthorised (Toegestane snelheid) . . . 83
2.107. SpeedAverage (Gemiddelde snelheid) . . . 83
2.108. SpeedMax (Maximumsnelheid) . . . 83
2.109. TDesSessionKey (TDes-sessiesleutel) . . . 83
2.110. TimeReal (Tijdklok) . . . 83
2.111. TyreSize (Bandenmaat) . . . 83
2.112. VehicleIdentificationNumber (Voertuigidentificatienummer) . . . 84
2.113. VehicleRegistrationIdentification (Identificatie van de voertuigregistratie) . . . 84
2.114. VehicleRegistrationNumber (Kentekennummer) . . . 84
2.115. VuActivityDailyData (Gegevens over de dagelijkse activiteiten van de VU) . . . 84
2.116. VuApprovalNumber (Goedkeuringsnummer van de VU) . . . 84
2.117. VuCalibrationData (Kalibreringsgegevens van de VU) . . . 84
2.118. VuCalibrationRecord (Kalibreringsregistratie van de VU) . . . 85
2.119. VuCardIWData (Gegevens over het inbrengen en uitnemen van een kaart) . . . 85
2.120. VuCardIWRecord (Registratie van het inbrengen en uitnemen van een kaart) . . . 86
2.121. VuCertificate (VU-certificaat) . . . 86
2.122. VuCompanyLocksData (Gegevens over bedrijfsvergrendelingen van de VU) . . . 86
2.123. VuCompanyLocksRecord (Registratie van bedrijfsvergrendelingen van de VU) . . . 87
2.124. VuControlActivityData (Gegevens over controleactiviteiten van de VU) . . . 87
2.125. VuControlActivityRecord (Registratie van controleactiviteiten van de VU) . . . 87
2.126. VuDataBlockCounter (Teller van gegevensblokken van de VU) . . . 87
2.127. VuDetailedSpeedBlock (Gedetailleerd snelheidsblok van de VU) . . . 87
2.128. VuDetailedSpeedData (Gedetailleerde snelheidsgegevens van de VU) . . . 88
2.129. VuDownloadablePeriod (Over te brengen periode van de VU) . . . 88
2.130. VuDownloadActivityData (Gegevens over overbrengingsactiviteiten van de VU) . . . 88
2.131. VuEventData (Gegevens over voorvallen van de VU) . . . 88
2.132. VuEventRecord (Voorvallenregistratie van de VU) . . . 89
2.133. VuFaultData (Gegevens over fouten van de VU) . . . 89
2.134. VuFaultRecord (Foutenregistratie van de VU) . . . 89
2.135. VuIdentification (Identificatie van de VU) . . . 90
2.136. VuManufacturerAddress (Adres van de fabrikant van de VU) . . . 90
2.137. VuManufacturerName (Naam van de fabrikant van de VU) . . . 90
2.138. VuManufacturingDate (Bouwjaar van de VU) . . . 90
2.139. VuOverSpeedingControlData (Controlegegevens over snelheidsoverschrijding van de VU) . . . 91
2.140. VuOverSpeedingEventData (Gegevens over voorvallen van snelheidsoverschrijding van de VU) . . . 91
2.141. VuOverSpeedingEventRecord (Voorvallenregistraties van snelheidsoverschrijding van de VU) . . . 91
2.142. VuPartNumber (Onderdeelnummer van de VU) . . . 91
2.143. VuPlaceDailyWorkPeriodData (Gegevens over plaatsen van dagelijkse werkperiodes van de VU) . . . 92

2.144. VuPlaceDailyWorkPeriodRecord (Registraties van plaatsen van dagelijkse werkperiodes van de VU) . 92
2.145. VuPrivateKey (Particuliere sleutel van de VU) 92
2.146. VuPublicKey (Openbare sleutel van de VU) 92
2.147. VuSerialNumber (Serienummer van de VU) 92
2.148. VuSoftInstallationDate (Datum van installatie van de software in de VU) 92
2.149. VuSoftwareIdentification (Identificatie van de software van de VU) 92
2.150. VuSoftwareVersion (Softwareversie van de VU) 93
2.151. VuSpecificConditionData (Gegevens over specifieke omstandigheden van de VU) 93
2.152. VuTimeAdjustmentData (Tijdafstellingsgegevens van de VU) 93
2.153. VuTimeAdjustmentRecord (Tijdafstellingsregistraties van de VU) 93
2.154. W-VehicleCharacteristicConstant (Kenmerkende coëfficiënt van het voertuig) 93
2.155. WorkshopCardApplicationIdentification (Toepassingsidentificatie van de werkplaatskaart) 94
2.156. WorkshopCardCalibrationData (Kalibreringsgegevens van de werklaatskaart) 94
2.157. WorkshopCardCalibrationRecord (Kalibreringsregistratie van de werkplaatskaaart) 94
2.158. WorkshopCardHolderIdentification (Identificatie van de werkplaatskaarthouder) 95
2.159. WorkshopCardPIN (PIN-code van de werkplaatskaart) 95
3. Definities van waardenbereik en afmetingenbereik 96
3.1. Definities voor de bestuurderskaart 96
3.2. Definities voor de werkplaatskaart 96
3.3. Definities voor de controlekaart 96
3.4. Definities voor de bedrijfskaart 96
4. Tekensets 96
5. Codering 96

1. INLEIDING

Deze appendix specificeert gegevensvormen, gegevenselementen en gegevensstructuren voor gebruik in het controleapparaat en de tachograafkaarten.

1.1. **Methoden ter definitie van gegevenssoorten**

Deze appendix gebruikt Abstract Syntax Notation One (ASN.1) om gegevenssoorten te definiëren. Hierdoor is het zonder een toepassings- en omgevingsafhankelijke specifieke overdrachtssyntaxis (coderingsregels) mogelijk enkelvoudige en gestructureerde gegevens te definiëren.

ASN.1-conventies voor soortbenaming worden gebruikt in overeenstemming met ISO/IEC 8824-1. Dit betekent dat:

— waar mogelijk de betekenis van de gegevenssoort door middel van de geselecteerde benamingen wordt aangeduid;

— daar 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;

— over het algemeen hebben de benamingen van de gegevenssoorten betrekking op de benaming van de gegevenssoorten waaruit ze samengesteld zijn, de inrichting waarin de gegevens opgeslagen zijn en de aan de gegevens gerelateerde functie.

Indien een ASN.1-soort als onderdeel van een andere norm reeds gedefinieerd is en indien hij relevant is voor gebruik in het controleapparaat, dan wordt deze ASN.1-soort in deze appendix gedefinieerd.

Om verscheidene soorten coderingsregels mogelijk te maken, is een aantal ASN.1-soorten in deze appendix beperkt door identificatiesymbolen voor het waardenbereik. Deze identificatiesymbolen worden in paragraaf 3 gedefinieerd.

1.2. **Referenties**

De onderstaande referenties worden in deze appendix gebruikt:

ISO 639	Code for the representation of names of languages. First Edition: 1988.
EN 726-3	Identification cards systems — Telecommunications integrated circuit(s) cards and terminals — Part 3: Application independent card requirements. December 1994.
ISO 3779	Road vehicles — Vehicle identification number (VIN) — Content and structure. Edition 3: 1983.
ISO/IEC 7816-5	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 5: Numbering system and registration procedure for application identifiers. First edition: 1994 + Amendment 1: 1996.
ISO/IEC 8824-1	Information technology — Abstract Syntax Notation 1 (ASN.1): Specification of basic notation. Edition 2: 1998.
ISO/IEC 8825-2	Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). Edition 2: 1998.
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. First edition: 1987.
ISO 16844-3	Road vehicles — Tachograph systems — Motion Sensor Interface. WD 3-20/05/99.

2. DEFINITIES VAN GEGEVENSSOORTEN

Voor elk van de onderstaande gegevenssoorten bestaat de standaardwaarde voor een „onbekende" of een „niet-toepasbare" inhoud in het opvullen van het gegevenselement met 'FF' bytes.

2.1. **ActivityChangeInfo (Informatie over wijziging van de activiteiten)**

Met deze gegevenssoort kunnen een lezerstatus op 00:00 en/of een bestuurderstatus op 00:00 en/of wijzigingen van activiteiten en/of wijzigingen in de rijstatus van bestuurders en/of wijzigingen in de status van de kaart voor een bestuurder of een bijrijder gecodeerd worden binnen een woord van twee bytes. Deze gegevenssoort is gerelateerd aan de voorschriften 084, 109a, 199 en 219.

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

Waardetoekenning — octet-uitgericht: 'scpaatttttttttttt'B (16 bits)

Voor geheugenregistraties (of lezerstatus):

's'B Lezer:

'0'B: BESTUURDER,

'1'B: BIJRIJDER,

'c'B Status van de bestuurders:

'0'B: ALLEEN,

'1'B: MET EEN PLOEG,

'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: ONDERBREKING/RUST,

'01'B: BESCHIKBAARHEID,

'10'B: WERK,

'11'B: RIJDEN,

'ttttttttttt'B Tijd van de wijziging: aantal minuten vanaf 00.00 uur op de betreffende dag.

Voor bestuurderskaartregistraties (of werkplaatskaartregistraties) (en bestuurderstatus):

's'B Lezer (niet relevant wanneer 'p' = 1, behoudens onderstaande opmerking):

'0'B: BESTUURDER,

'1'B: BIJRIJDER,

'c'B Status van de bestuurders (geval 'p' = 0) of Volgende status van de activiteiten (geval 'p' = 1):

'0'B: ALLEEN, '0'B: MET EEN PLOEG,

'1'B: ONBEKEND '1'B: BEKEND (= handmatig 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 wanneer 'p' = 1 en 'c' = 0 behoudens onderstaande opmerking):

'00'B: ONDERBREKING/RUST,

'01'B: BESCHIKBAARHEID,

'10'B: WERK,

'11'B: RIJDEN,

'ttttttttttt'B Tijd van de wijziging: aantal minuten vanaf 00.00 uur op de betreffende dag.

Opmerking in geval van „kaartuitneming":

Wanneer de kaart wordt uitgenomen:

— 's' is relevant en geeft de lezer aan waarvan de kaart wordt 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 handmatige 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. **Adres**

Een adres.

```
Address ::= SEQUENCE {
   codePage                                    INTEGER (0..255),
   address                                     OCTET STRING (SIZE(35))
}
```

codePage specificeert het onderdeel van ISO/IEC 8859 dat wordt gebruikt om het adres te coderen,

address is een overeenkomstig ISO/IEC 8859-codePage gecodeerd adres.

2.3. **BCDString (binair-decimale codenotatie)**

De BCDString wordt toegepast voor de BCD-weergave (Binary Code Decimal). Deze gegevenssoort 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.

De toegestane cijfers zijn: 0, 1, … 9.

2.4. **CalibrationPurpose (Kalibreringsdoel)**

Code die verklaart waarom een verzameling kalibreringsparameters geregistreerd werd. Deze gegevenssoort is gerelateerd aan de voorschriften 097 en 098.

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

Waardetoekenning:

'00'H gereserveerde waarde,

'01'H activering: registratie van kalibreringsparameters die op het moment van activering van de VU, bekend zijn,

'02'H eerste installatie: eerste kalibrering van de VU na activering,

'03'H installatie: eerste kalibrering van de VU in het huidige voertuig,

'04'H periodieke controle.

2.5. **CardActivityDailyRecord (Dagelijkse registratie van de activiteiten op de kaart)**

Op een kaart opgeslagen informatie met betrekking tot de activiteiten van de bestuurder op een bepaalde dag. Deze gegevenssoort is gerelateerd aan de voorschriften 199 en 219.

```
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 registraties bevat (zie CardActivityLengthRange paragraaf 3). Wanneer deze registratie de oudste dagelijkse registratie is, moet de waarde van activityPreviousRecordLength op 0 worden gezet.

activityRecordLength is de totale lengte in bytes van deze registratie. De maximale waarde wordt toegekend door de lengte van de OCTET STRING die deze registraties bevat.

activityRecordDate is de datum van de registratie.

activityDailyPresenceCounter is de dagelijkse aanwezigheidsteller voor de kaart op deze dag.

activityDayDistance is de totale op deze dag afgelegde afstand.

activityChangeInfo is de verzameling ActivityChangeInfo-gegevens voor de bestuurder op deze dag. Het kan maximaal 1 440 waarden bevatten (één wijziging van de activiteiten per minuut). Deze verzameling bevat altijd de activityChangeInfo waarmee de bestuurderstatus op 00:00 wordt gecodeerd.

2.6. **CardActivityLengthRange (Lengtebereik van de activiteiten op de kaart)**

Aantal beschikbare bytes op een bestuurders- of werkplaatskaart voor het opslaan van registraties van de activiteiten van de bestuurder.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Waardetoekenning: zie paragraaf 3.

2.7. **CardApprovalNumber (Goedkeuringsnummer van de kaart)**

Goedkeuringsnummer van de kaart.

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

Waardetoekenning: niet gespecificeerd.

2.8. **CardCertificate (Kaartcertificaat)**

Certificaat van de openbare sleutel van een kaart.

```
CardCertificate ::= Certificate
```

2.9. **CardChipIdentification (Identificatie van de kaartchip)**

Op een kaart opgeslagen informatie met betrekking tot de identificatie van het integrated circuit (IC) van de kaart (voorschrift 191).

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                          OCTET STRING (SIZE(4)),
   icManufacturingReferences               OCTET STRING (SIZE(4))
}
```

icSerialNumber is het serienummer van het IC zoals gedefinieerd in EN 726-3.

icManufacturingReferences is het identificatiesymbool van de fabrikant van het IC en fabricage-elementen zoals gedefinieerd in EN 726-3.

2.10. **CardConsecutiveIndex (Opeenvolgende index van de kaart)**

Een opeenvolgende index van de kaart (definitie h)).

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

Waardetoekenning: (zie hoofdstuk VII van deze bijlage)

Volgorde voor verhoging: '0, …, 9, A, … , Z, a, … , z'

2.11. **CardControlActivityDataRecord (Gegevensregistratie van controleactiviteiten op de kaart)**

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de laatste controle van de bestuurder (voorschriften 210 en 225).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                          controlType,
   controlTime                          TimeReal,
   controlCardNumber                    FullCardNumber,
   controlVehicleRegistration           VehicleRegistrationIdentification,
   controlDownloadPeriodBegin           TimeReal,
   controlDownloadPeriodEnd             TimeReal,
}
```

controlType is het type controle.

controlTime is de datum en tijd 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 overgebrachte periode in geval van overbrenging.

2.12. **CardCurrentUse (Huidig gebruik kaart)**

Informatie over het werkelijke gebruik van de kaart (voorschrift 212).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                      TimeReal,
   sessionOpenVehicle                   VehicleRegistrationIdentification
}
```

sessionOpenTime is de tijd waarop de kaart voor het huidige gebruik ingebracht wordt. Dit element wordt bij kaartuitneming op nul gezet.

sessionOpenVehicle is de identificatie van het thans gebruikte voertuig, die ingesteld wordt bij kaartinbrenging. Dit element wordt bij kaartuitneming op nul gezet.

2.13. **CardDriverActivity (Bestuurdersactiviteiten op de kaart)**

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de activiteiten van de bestuurder (voorschriften 199 en 219).

```
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 beschikbare ruimte voor het opslaan van gegevens over de activiteiten van de bestuurder (gegevensstructuur: CardActivityDailyRecord) voor elke kalenderdag waarop de kaart gebruikt is.

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 het voorgaande record toegevoegd. Wanneer 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 (uitbreiding van de lopende activityDailyRecord, of invoeren van een nieuwe activityDailyRecord), die oudere gegevens over activiteiten vervangen, moet het activityPointerOldestDayRecord bijgewerkt worden om de nieuwe locatie van de oudste volledige dagregistratie weer te geven; de activityPreviousRecordLength van deze (nieuwe) oudste volledige dagregistratie moet op 0 worden teruggezet.

2.14. **CardDrivingLicenceInformation (Rijbewijsinformatie op kaart)**

Op een bestuurderskaart opgeslagen informatie met betrekking tot de rijbewijsgegevens van de kaarthouder (voorschrift 196).

```
CardDrivingLicenceInformation ::= SEQUENCE {

   drivingLicenceIssuingAuthority          Name,

   drivingLicenceIssuingNation             NationNumeric,

   drivingLicenceNumber                    IA5String(SIZE(16))

}
```

drivingLicenceIssuingAuthority is de autoriteit die verantwoordelijk is voor afgifte van het rijbewijs.

drivingLicenceIssuingNation is de nationaliteit van de autoriteit die het rijbewijs heeft afgegeven.

drivingLicenceNumber is het nummer van het rijbewijs.

2.15. **CardEventData (Voorvalgegevens op kaart)**

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de aan de kaarthouder te wijten voorvallen (voorschriften 204 en 223).

```
CardEventData ::= SEQUENCE SIZE(6) OF {

   cardEventRecords                        SET SIZE(NoOfEventsPerType) OF
                                           CardEventRecord

}
```

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

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

2.16. **CardEventRecord (Voorvalregistratie op kaart)**

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot een aan de kaarthouder te wijten voorval (voorschriften 205 en 223).

```
CardEventRecord ::= SEQUENCE {

   eventType                               EventFaultType,

   eventBeginTime                          TimeReal,

   eventEndTime                            TimeReal,

   eventVehicleRegistration                VehicleRegistrationIdentification

}
```

eventType is het type voorval.

eventBeginTime is de datum en tijd van het begin van het voorval.

eventEndTime is de datum en tijd van het einde van het voorval.

eventVehicleRegistration is het kentekennummer van de registrerende lidstaat van het voertuig waarin het voorval plaatsvond.

2.17. **CardFaultData (Foutgegevens op kaart)**

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de aan de kaarthouder te wijten fouten (voorschriften 207 en 223).

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

CardFaultData is een sequentie van een registratieverzameling van controleapparaatfouten gevolgd door een registratieverzameling van kaartfouten.

cardFaultRecords is een reeks foutenregistraties van een bepaalde foutencategorie (controleapparaat of kaart).

2.18. **CardFaultRecord (Registratie van kaartfouten)**

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot een aan de kaarthouder te wijten fout (voorschriften 208 en 223).

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

faultType is het type fout.

faultBeginTime is de datum en tijd van het begin van de fout.

faultEndTime is de datum en tijd van het einde van de fout.

faultVehicleRegistration is het kentekennummer en de registrerende lidstaat van het voertuig waarin de fout plaatsvond.

2.19. **CardIccIdentification (IC-identificatie kaart)**

Op een kaart opgeslagen informatie met betrekking tot de identificatie van het integrated circuit (IC) van de kaart (voorschrift 192).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                           OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardApprovalNumber                  CardApprovalNumber
   cardPersonaliserID                  OCTET STRING (SIZE(1)),
   embedderIcAssemblerId               OCTET STRING (SIZE(5)),
   icIdentifier                        OCTET STRING (SIZE(2))
}
```

clockStop is de klokonderbrekingsmodus zoals gedefinieerd in EN 726-3.

cardExtendedSerialNumber is het serienummer en de fabricagereferentie van de IC-kaart zoals gedefinieerd in EN 726-3 en nader gespecificeerd door de gegevenssoort ExtendedSerialNumber.

cardApprovalNumber is het goedkeuringsnummer van de kaart.

cardPersonaliserID is de persoonlijke identificatie (ID) van de kaart zoals gedefinieerd in EN 726-3.

embedderIcAssemblerId is het identificatiesymbool van de embedder/IC-assembleur zoals gedefinieerd in EN 726-3.

icIdentifier is het identificatiesymbool van de IC op de kaart en van de fabrikant van het IC zoals gedefinieerd in EN 726-3.

2.20. **CardIdentification (Kaartidentificatie)**

Op een kaart opgeslagen informatie met betrekking tot de identificatie van de kaart (voorschriften 194, 215, 231, 235).

```
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 kaartnummer 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.

2.21. **CardNumber (Kaartnummer)**

Een 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.

2.22. **CardPlaceDailyWorkPeriod (Plaatsen van dagelijkse werkperioden)**

Op een bestuurders- en werkplaatskaart opgeslagen informatie met betrekking tot de plaatsen waar dagelijkse werkperioden beginnen en/of eindigen (voorschriften 202 en 221).

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

placePointerNewestRecord is de index van de laatst bijgewerkte plaatsregistratie.

Waardetoekenning: Cijfer dat correspondeert met de teller van de plaatsregistratie, beginnend met '0' voor de eerste plaatsregistratie in de structuur.

placeRecords is de reeks registraties die de informatie met betrekking tot ingevoerde plaatsen bevat.

2.23. **CardPrivateKey (Particuliere sleutel van de kaart)**

De particuliere sleutel van een kaart.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.24. **CardPublicKey (Openbare sleutel van de kaart)**

De openbare sleutel van een kaart.

```
CardPublicKey ::= PublicKey
```

2.25. **CardRenewalIndex (Vernieuwingsindex van de kaart)**

Een 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'

2.26. **CardReplacementIndex(Vervangingsindex van de kaart)**

Een 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'

2.27. **CardSlotNumber (Nummer van de kaartlezer)**

Code ter onderscheiding van de twee lezers van een voertuigunit.

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

Waardetoekenning: niet nader gespecificeerd.

2.28. **CardSlotsStatus (Status van de kaartlezers)**

Code die de soort kaarten aangeeft die in de twee lezers van de voertuigunit ingebracht zijn.

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

Waardetoekenning — octet-uitgericht: 'ccccdddd'B:

'cccc'B Identificatie van de soort kaart die ingebracht is in de lezer van de bijrijder,

'dddd'B Identificatie van de soort kaart die ingebracht is in de lezer van de bestuurder,

met de onderstaande 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.

2.29. **CardStructureVersion (Versie van de kaartstructuur)**

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,

'bb'H Index voor wijzigingen betreffende het gebruik van de voor de structuur gedefinieerde gegevenselementen, gegeven door de high byte.

2.30. **CardVehicleRecord (Registratie van het gebruik van het voertuig)**

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de gebruiksperiode van een voertuig gedurende een kalenderdag (voorschriften 197 en 217).

```
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 tijd van het begin van de gebruiksperiode van het voertuig.

vehicleLastUse is de datum en tijd 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.

2.31. **CardVehiclesUsed (Gebruikte voertuigen op de kaart)**

Op een bestuurders- of werkplaatskaart opgeslagen informatie met betrekking tot de door de kaarthouder gebruikte voertuigen (voorschriften 197 en 217).

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

vehiclePointerNewestRecord is de index van de laatst bijgewerkte voertuigregistratie.

Waardetoekenning: Cijfer dat correspondeert met de teller van de voertuigregistratie, beginnend met '0' voor de eerste voertuigregistratie in de structuur.

cardVehicleRecords is de reeks registraties die informatie over gebruikte voertuigen bevat.

2.32. **Certificate (Certificaat)**

Het certificaat van een openbare sleutel afgegeven door een certificeringsautoriteit.

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

Waardetoekenning: digitale handtekening met gedeeltelijk herstel van een CertificateContent overeenkomstig appendix 11 Algemene beveiligingsinrichtingen: handtekening (128 bytes) || restant openbare sleutel (58 bytes) || referentie certificeringsautoriteit (8 bytes).

2.33. **CertificateContent (Inhoud van het certificaat)**

De (duidelijke) inhoud van het certificaat van een openbare sleutel overeenkomstig appendix 11 Algemene veiligheidsinrichtingen.

```
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 deze 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 dit certificaat gecertificeerd wordt.

2.34. **CertificateHolderAuthorisation (Autorisatie van de certificaathouder)**

Identificatie van de rechten van een certificaathouder.

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

tachographApplicationID is het toepassingsidentificatiesymbool voor de tachograaftoepassing.

Waardetoekenning: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Deze AID is een particulier niet-geregistreerd toepassingsidentificatiesymbool overeenkomstig ISO/IEC 7816-5.

equipmentType is de identificatie van het type inrichting waarvoor het certificaat bedoeld is.

Waardetoekenning: overeenkomstig gegevenssoort EquipmentType. 0 indien het een certificaat van een lidstaat betreft.

2.35. **CertificateRequestID (ID van verzoek om certificaat)**

Unieke identificatie van een certificaatverzoek. Het kan ook als een identificatiesymbool van de openbare sleutel van een voertuigunit worden gebruikt indien het serienummer van de voertuigunit 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 de maand (twee cijfers) en het 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.

2.36. **CertificationAuthorityKID (Sleutel-ID van de certificeringsautoriteit)**

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'.

2.37. **CompanyActivityData (Gegevens over bedrijfsactiviteiten)**

Op een bedrijfskaart opgeslagen informatie met betrekking tot activiteiten die met de kaart worden uitgevoerd (voorschrift 237).

```
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 registratie van bedrijfsactiviteiten, beginnend met '0' voor de eerste registratie van bedrijfsactiviteiten in de structuur.

companyActivityRecords is de verzameling van alle registraties van bedrijfsactiviteiten.

companyActivityRecord is de sequentie van informatie met betrekking tot één bedrijfsactiviteit.

companyActivityType is de soort bedrijfsactiviteit.

companyActivityTime is de datum en tijd van de bedrijfsactiviteit.

cardNumberInformation is het kaartnummer en de lidstaat van afgifte van de overgebrachte kaart, indien van toepassing.

vehicleRegistrationInformation is het kentekennummer en de registrerende lidstaat van het overgebrachte, vergrendelde of ontgrendelde voertuig.

downloadPeriodBegin en **downloadPeriodEnd** is de vanaf de VU overgebrachte periode, indien van toepassing.

2.38. **CompanyActivityType (Soort bedrijfsactiviteit)**

Code die een door een bedrijf met gebruikmaking van zijn bedrijfskaart uitgevoerde activiteit aangeeft.

```
CompanyActivityType ::= INTEGER {
    card downloading                    (1),
    VU downloading                      (2),
    VU lock-in                          (3),
    VU lock-out                         (4)
}
```

2.39. **CompanyCardApplicationIdentification (Toepassingsidentificatie van de bedrijfskaart)**

Op een bedrijfskaart opgeslagen informatie met betrekking tot de toepassingsidentificatie van de kaart (voorschrift 190).

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

typeOfTachographCardId specificeert de geïmplementeerde kaartsoort.

cardStructureVersion specificeert de versie van de structuur die op de kaart geïmplementeerd is.

noOfCompanyActivityRecords specificeert de versie van de structuur die op de kaart geïmplementeerd is.

2.40. **CompanyCardHolderIdentification (Identificatie van de bedrijfskaarthouder)**

Op een bedrijfskaart opgeslagen informatie met betrekking tot de identificatie van de kaarthouder (voorschrift 236).

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

companyName is de naam van het bedrijf.

companyAddress is het adres van het bedrijf.

cardHolderPreferredLanguage is de voorkeurtaal van de kaarthouder.

2.41. **ControlCardApplicationIdentification (Toepassingsidentificatie van de controlekaart)**

Op een controlekaart opgeslagen informatie met betrekking tot de toepassingsidentificatie van de kaart (voorschrift 190).

```
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 registraties van controleactiviteiten die op de kaart kunnen worden opgeslagen.

2.42. **ControlCardControlActivityData (Gegevens over controleactiviteiten van de controlekaart)**

Op een controlekaart opgeslagen informatie met betrekking tot met de kaart uitgevoerde controleactiviteiten (voorschrift 233).

```
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 registratie van controleactiviteiten.

Waardetoekenning: Cijfer corresponderend met de teller van de registratie van controleactiviteiten, beginnend met '0' voor de eerste registratie van de controleactiviteiten die in de structuur voorkomt.

controlActivityRecords is de verzameling van alle registraties van controleactiviteiten.

controlActivityRecord is de sequentie van informatie met betrekking tot een controle.

controlType is de soort controle.

controlTime is de datum en tijd 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 uiteindelijk overgebrachte periode.

2.43. **ControlCardHolderIdentification (Identificatie van de controlekaarthouder)**

Op een controlekaart opgeslagen informatie met betrekking tot de identificatie van de kaarthouder (voorschrift 232).

```
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.

2.44. **ControlType (Soort controle)**

Code die de tijdens een controle uitgevoerde activiteiten aangeeft. Deze gegevenssoort is gerelateerd aan de voorschriften 102, 210 en 225.

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

Waardetoekenning — octet-uitgericht: `'cvpdxxxx'B` (8 bits)

`'c'B` kaartoverbrenging:

`'0'B`: kaart niet overgebracht tijdens deze controleactiviteit,

`'1'B`: kaart overgebracht tijdens deze controleactiviteit

`'v'B` VU-overbrenging:

`'0'B`: VU niet overgebracht tijdens deze controleactiviteit,

`'1'B`: VU overgebracht tijdens deze controleactiviteit

`'p'B` afdrukken:

`'0'B`: geen afdrukken gemaakt tijdens deze controleactiviteit,

`'1'B`: afdrukken gemaakt tijdens deze controleactiviteit

`'d'B` leesvenster:

`'0'B`: geen leesvenster gebruikt tijdens deze controleactiviteit,

`'1'B`: leesvenster gebruikt tijdens deze controleactiviteit

`'xxxx'B` Niet gebruikt.

2.45. **CurrentDateTime (Huidige datum en tijd)**

De huidige datum en tijd van het controleapparaat.

```
CurrentDateTime ::= TimeReal
```

Waardetoekenning: niet nader gespecificeerd.

2.46. **DailyPresenceCounter (Dagelijkse-aanwezigheidsteller)**

Op een bestuurders- of werkplaatskaart opgeslagen teller die voor elke kalenderdag waarop de kaart in een VU ingebracht is, met één wordt opgehoogd. Deze gegevenssoort is gerelateerd aan de voorschriften 199 en 219.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Waardetoekenning: opeenvolgend cijfer met een maximale waarde = 9 999, waarna het opnieuw met 0 begint. Bij de eerste afgifte van de kaart wordt het cijfer op 0 gezet.

2.47. **Datef (Datumeenheid)**

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.

2.48. **Distance (Afstand)**

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 0 tot 9999 km.

2.49. **DriverCardApplicationIdentification (Toepassingsidentificatie van de bestuurderskaart)**

Op een bestuurderskaart opgeslagen informatie met betrekking tot de toepassingsidentificatie van de kaart (voorschrift 190).

```
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 structuur die op de kaart geïmplementeerd is.

noOfEventsPerType is het aantal voorvallen per soort voorval dat de kaart kan opslaan.

noOfFaultsPerType is het aantal fouten per soort fout dat de kaart kan opslaan.

activityStructureLength geeft het aantal beschikbare bytes voor het opslaan van registraties van activiteiten aan.

noOfCardVehicleRecords is het aantal voertuigregistraties dat de kaart kan bevatten.

noOfCardPlaceRecords is het aantal plaatsen dat de kaart kan registreren.

2.50. **DriverCardHolderIdentification (Identificatie van de bestuurderskaarthouder)**

Op een bestuurderskaart opgeslagen informatie met betrekking tot de identificatie van de kaarthouder (voorschrift 195).

```
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.

2.51. **EntryTypeDailyWorkPeriod (Soort invoer van de dagelijkse werkperiode)**

Code die een onderscheid maakt tussen begin en einde van invoer van een plaats van de dagelijkse werkperiode en voorwaarde van de invoer.

```
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.

2.52. **EquipmentType (Soort inrichting)**

Code die de verschillende soorten inrichtingen voor de tachograaftoepassing onderscheidt.

```
EquipmentType ::= INTEGER(0..255)
- - 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.

2.53. **EuropeanPublicKey (Europese openbare sleutel)**

De Europese openbare sleutel.

```
EuropeanPublicKey ::= PublicKey
```

2.54. **EventFaultType (Soorten voorvallen en fouten)**

Code die een voorval of een fout aanduidt.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Waardetoekenning:

'0x'H	Algemene voorvallen,
'00'H	Geen nadere details,
'01'H	Inbrengen van een ongeldige kaart,
'02'H	Kaartconflict,
'03'H	Tijdsoverlapping,
'04'H	Rijden zonder een 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 .. '0F'H	RFU,
'1x'H	Poging tot inbreuk op de beveiliging van de voertuigunit,
'10'H	Geen nadere details,
'11'H	Authentificatiefout van de bewegingsopnemer,
'12'H	Authentificatiefout van de tachograafkaart,
'13'H	Niet-geautoriseerde wijziging van de bewegingsopnemer,
'14'H	Integriteitsfout in de gegevensinvoer op de kaart,
'15'H	Integriteitsfout in de opgeslagen gebruikersgegevens,
'16'H	Overdrachtsfout in de interne gegevens
'16'H	Overdrachtsfout in de interne gegevens,
'17'H	Niet-geautoriseerde opening van de kast,
'18'H	Hardwaresabotage,
'19'H .. '1F'H	RFU,
'2x'H	Poging tot inbreuk op de beveiliging van de opnemer,
'20'H	Geen nadere details,
'21'H	Authentificatiefout,
'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 .. '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	Fout in het leesvenster,
'34'H	Fout in de overbrenging,
'35'H	Fout in de opnemer,
'36'H .. '3F'H	RFU,
'4x'H	Kaartfouten,
'40'H	Geen nadere details,
'41'H .. '4F'H	RFU,
'50'H .. '7F'H	RFU,
'80'H .. 'FF'H	Specifiek voor de fabrikant.

2.55. **EventFaultRecordPurpose (Doel van de voorvallen-foutenregistratie)**

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 van optreding
'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 van optreding
'04'H	het ernstigste voorval gedurende een van de laatste 10 dagen van optreding
'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 .. '7F'H	RFU
'80'H .. 'FF'H	Specifiek voor de fabrikant

2.56. **ExtendedSerialNumber (Verlengd serienummer)**

Unieke identificatie van een inrichting. Het kan ook als een identificatiesymbool van de openbare sleutel van de inrichting worden gebruikt.

```
ExtendedSerialNumber ::= SEQUENCE {
   serialNumber                          INTEGER(0..2^32-1)
   monthYear                             BCDString(SIZE(2))
   type OCTET                            STRING(SIZE(1))
   manufacturerCode                      ManufacturerCode
}
```

serialNumber is een serienummer voor de inrichting, uniek voor de fabrikant, de soort inrichting en de onderstaande maand.

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 de soort inrichting.

Waardetoekenning: specifiek voor de fabrikant, met 'FFh' gereserveerde waarde.

manufacturerCode is de numerieke code van de fabrikant van de inrichting.

2.57. **FullCardNumber (Volledig kaartnummer)**

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.

2.58. **HighResOdometer (Zeer nauwkeurige kilometerteller)**

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 0 tot 21 055 406 km.

2.59. **HighResTripDistance (Zeer nauwkeurige reisafstand)**

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 0 tot 21 055 406 km.

2.60. **HolderName (Naam van de houder)**

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 holderSurname dezelfde informatie als companyName of workshopName of controlBodyName.

holderFirstNames omvat de voornaam (voornamen) en initialen van de houder.

2.61. **K-ConstantOfRecordingEquipment (K-constante van het controleapparaat)**

Constante van het controleapparaat (definitie m).

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Waardetoekenning: pulsen per kilometer in het operationele bereik 0 tot 64 255 pulsen/km.

2.62. **KeyIdentifier (Sleutelidentificatiesymbool)**

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.

2.63. **L-TyreCircumference (L-omtrek van de wielbanden)**

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 0 tot 8 031 mm.

2.64. **Language (Taal)**

Code die een taal identificeert.

```
Language ::= IA5String(SIZE(2))
```

Waardetoekenning: een code van twee onderkastletters overeenkomstig ISO 639.

2.65. **LastCardDownload**

Op een bestuurderskaart opgeslagen datum en tijd van het downloaden van de laatste kaart (voor andere doeleinden dan controle). Deze datum kan worden aangepast door een VU of een kaartlezer.

```
LastCardDownload ::= TimeReal
```

Waardetoekenning: niet nader gespecificeerd.

2.66. **ManualInputFlag (Label voor handmatige invoer)**

Code die aangeeft of een kaarthouder handmatig activiteiten van de bestuurder bij kaartinbrenging heeft ingevoerd (voorschrift 081).

```
ManualInputFlag ::= INTEGER {
   noEntry                          (0)
   manualEntries                    (1)
}
```

Waardetoekenning: niet nader gespecificeerd.

2.67. **ManufacturerCode (Code van de fabrikant)**

Code die een fabrikant identificeert.

```
ManufacturerCode ::= INTEGER(0..255)
```

Waardetoekenning:

'00'H	Geen informatie beschikbaar
'01'H	Gereserveerde waarde
'02'H .. '0F'H	Gereserveerd voor toekomstig gebruik
'10'H	ACTIA
'11'H .. '17'H	Gereserveerd voor fabrikanten van wie de naam met een 'A' begint
'18'H .. '1F'H	Gereserveerd voor fabrikanten van wie de naam met een 'B' begint
'20'H .. '27'H	Gereserveerd voor fabrikanten van wie de naam met een 'C' begint
'28'H .. '2F'H	Gereserveerd voor fabrikanten van wie de naam met een 'D' begint
'30'H .. '37'H	Gereserveerd voor fabrikanten van wie de naam met een 'E' begint
'38'H .. '3F'H	Gereserveerd voor fabrikanten van wie de naam met een 'F' begint
'40'H	Giesecke & Devrient GmbH
'41'H	GEM plus
'42'H .. '47'H	Gereserveerd voor fabrikanten van wie de naam met een 'G'
'48'H .. '4F'H	Gereserveerd voor fabrikanten van wie de naam met een 'H' begint
'50'H .. '57'H	Gereserveerd voor fabrikanten van wie de naam met een 'I' begint
'58'H .. '5F'H	Gereserveerd voor fabrikanten van wie de naam met een 'J' begint
'60'H .. '67'H	Gereserveerd voor fabrikanten van wie de naam met een 'K' begint
'68'H .. '6F'H	Gereserveerd voor fabrikanten van wie de naam met een 'L' begint
'70'H .. '77'H	Gereserveerd voor fabrikanten van wie de naam met een 'M' begint
'78'H .. '7F'H	Gereserveerd voor fabrikanten van wie de naam met een 'N' begint
'80'H	OSCARD
'81'H .. '87'H	Gereserveerd voor fabrikanten van wie de naam met een 'O' begint
'88'H .. '8F'H	Gereserveerd voor fabrikanten van wie de naam met een 'P' begint
'90'H .. '97'H	Gereserveerd voor fabrikanten van wie de naam met een 'Q' begint
'98'H .. '9F'H	Gereserveerd voor fabrikanten van wie de naam met een 'R' begint
'A0'H	SETEC
'A1'H	SIEMENS VDO
'A2'H	STONERIDGE
'A3'H .. 'A7'H	Gereserveerd voor fabrikanten van wie de naam met een 'S' begint
'AA'H	TACHOCONTROL
'AB'H .. 'AF'H	Gereserveerd voor fabrikanten van wie de naam met een 'T' begint
'B0'H .. 'B7'H	Gereserveerd voor fabrikanten van wie de naam met een 'U' begint
'B8'H .. 'BF'H	Gereserveerd voor fabrikanten van wie de naam met een 'V' begint
'C0'H .. 'C7'H	Gereserveerd voor fabrikanten van wie de naam met een 'W' begint
'C8'H .. 'CF'H	Gereserveerd voor fabrikanten van wie de naam met een 'X' begint
'D0'H .. 'D7'H	Gereserveerd voor fabrikanten van wie de naam met een 'Y' begint
'D8'H .. 'DF'H	Gereserveerd voor fabrikanten van wie de naam met een 'Z' begint

2.68. **MemberStateCertificate (lidstaatcertificaat)**

Het door de Europese certificeringsautoriteit afgegeven certificaat van de openbare sleutel van een lidstaat.

```
MemberStateCertificate ::= Certificate
```

2.69. **MemberStatePublicKey (Openbare sleutel van een lidstaat)**

De openbare sleutel van een lidstaat.

```
MemberStatePublicKey ::= PublicKey
```

2.70. **Name (Naam)**

Een naam.

```
Name ::= SEQUENCE {
   codePage                                    INTEGER (0..255),
   name                                        OCTET STRING (SIZE(35))
}
```

codePage specificeert het deel van ISO/IEC 8859 dat wordt gebruikt om de naam te coderen,

name is een overeenkomstig ISO/IEC 8859-codePage gecodeerde naam.

2.71. **NationAlpha (Alfanumerieke code van een land)**

Alfabetische verwijzing naar een land in overeenstemming met de gebruikelijke codering van landen op bumperstickers van auto's en/of zoals gebruikt in internationaal geharmoniseerde autoverzekeringspapieren (groene kaart).

```
NationAlpha ::= IA5String(SIZE(3))
```

Waardetoekenning:

' '	Geen informatie beschikbaar,
'A'	Oostenrijk,
'AL'	Albanië,
'AND'	Andorra,
'ARM'	Armenië,
'AZ'	Azerbeidzjan,
'B'	België,
'BG'	Bulgarije,
'BIH'	Bosnië en Herzegovina,
'BY'	Wit-Rusland,
'CH'	Zwitserland,
'CY'	Cyprus,
'CZ'	Republiek Tsjechië,
'D'	Duitsland,
'DK'	Denemarken,
'E'	Spanje,
'EST'	Estland,
'F'	Frankrijk,
'FIN'	Finland,
'FL'	Liechtenstein,
'FR'	Faeröer Eilanden,
'UK'	Verenigd Koninkrijk, Alderney, Guernsey, Jersey, Isle of Man, Gibraltar,
'GE'	Georgië,
'GR'	Griekenland,
'H'	Hongarije,
'HR'	Kroatië,
'I'	Italië,
'IRL'	Ierland,
'IS'	IJsland,
'KZ'	Kazachstan,
'L'	Luxemburg,
'LT'	Litouwen,
'LV'	Letland,
'M'	Malta,
'MC'	Monaco,

'MD'	Republiek Moldavië,
'MK'	Macedonië,
'N'	Noorwegen,
'NL'	Nederland,
'P'	Portugal,
'PL'	Polen,
'RO'	Roemenië,
'RSM'	San Marino,
'RUS'	Russische Federatie,
'S'	Zweden,
'SK'	Slowakije,
'SLO'	Slovenië,
'TM'	Turkmenistan,
'TR'	Turkije,
'UA'	Oekraïne,
'V'	Vaticaanstad,
'YU'	Joegoslavië,
'UNK'	Onbekend,
'EC'	Europese Gemeenschap,
'EUR'	Rest van Europa,
'WLD'	Rest van de wereld.

2.72. **NationNumeric (Numerieke code van een land)**

Numerieke verwijzing naar een land.

`NationNumeric ::= INTEGER(0..255)`

Waardetoekenning:

- - Geen informatie beschikbaar	(00)H,
- - Oostenrijk	(01)H,
- - Albanië	(02)H,
- - Andorra	(03)H,
- - Armenië	(04)H,
- - Azerbeidzjan	(05)H,
- - België	(06)H,
- - Bulgarije	(07)H,
- - Bosnië en Herzegovina	(08)H,
- - Wit-Rusland	(09)H,
- - Zwitserland	(0A)H,
- - Cyprus	(0B)H,
- - Republiek Tsjechië	(0C)H,
- - Duitsland	(0D)H,
- - Denemarken	(0E)H,
- - Spanje	(0F)H,
- - Estland	(10)H,
- - Frankrijk	(11)H,
- - Finland	(12)H,
- - Liechtenstein	(13)H,
- - Faeröer Eilanden	(14)H,
- - Verenigd Koninkrijk	(15)H,
- - Georgië	(16)H,
- - Griekenland	(17)H,
- - Hongarije	(18)H,
- - Kroatië	(19)H,
- - Italië	(1A)H,
- - Ierland	(1B)H,
- - IJsland	(1C)H,

- - Kazachstan (1D)H,
- - Luxemburg (1E)H,
- - Litouwen (1F)H,
- - Letland (20)H,
- - Malta (21)H,
- - Monaco (22)H,
- - Republiek Moldavië (23)H,
- - Macedonië (24)H,
- - Noorwegen (25)H,
- - Nederland (26)H,
- - Portugal (27)H,
- - Polen (28)H,
- - Roemenië (29)H,
- - San Marino (2A)H,
- - Russische Federatie (2B)H,
- - Zweden (2C)H,
- - Slowakije (2D)H,
- - Slovenië (2E)H,
- - Turkmenistan (2F)H,
- - Turkije (30)H,
- - Oekraïne (31)H,
- - Vaticaanstad (32)H,
- - Joegoslavië (33)H,
- - RFU (34..FC)H,
- - Europese Gemeenschap (FD)H,
- - Rest van Europa (FE)H,
- - Rest van de wereld (FF)H

2.73. **NoOfCalibrationRecords (Aantal kalibreringsregistraties)**

Aantal kalibreringsregistraties dat een werkplaatskaart kan opslaan.

NoOfCalibrationRecords ::= INTEGER(0..255)

Waardetoekenning: zie paragraaf 3.

2.74. **NoOfCalibrationsSinceDownload (Aantal kalibreringen sinds de laatste overbrenging)**

Teller die het aantal met een werkplaatskaart uitgevoerde kalibreringen sinds de laatste overbrenging aangeeft (voorschrift 230).

NoOfCalibrationsSinceDownload ::= INTEGER(0..2^{16}-1),

Waardetoekenning: niet nader gespecificeerd.

2.75. **NoOfCardPlaceRecords (Aantal plaatsregistraties)**

Aantal plaatsregistraties dat een bestuurders- of werkplaatskaart kan opslaan.

NoOfCardPlaceRecords ::= INTEGER(0..255)

Waardetoekenning: zie paragraaf 3.

2.76. **NoOfCardVehicleRecords (Aantal voertuigregistraties)**

Aantal registraties van gebruikte voertuigen dat een bestuurders- of werkplaatskaart kan opslaan.

NoOfCardVehicleRecords ::= INTEGER(0..2^{16}-1)

Waardetoekenning: zie paragraaf 3.

2.77. **NoOfCompanyActivityRecords (Aantal registraties van bedrijfsactiviteiten)**

Aantal registraties van bedrijfsactiviteiten dat een bedrijfskaart kan opslaan.

NoOfCompanyActivityRecords ::= INTEGER(0..2^{16}-1)

Waardetoekenning: zie paragraaf 3.

2.78. **NoOfControlActivityRecords (Aantal registraties van controleactiviteiten)**

Aantal registraties van controleactiviteiten dat een controlekaart kan opslaan.

```
NoOfControlActivityRecords ::= INTEGER(0..2^16-1)
```

Waardetoekenning: zie paragraaf 3.

2.79. **NoOfEventsPerType (Aantal voorvallen per soort)**

Aantal voorvallen per soort voorval dat een kaart kan opslaan.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Waardetoekenning: zie paragraaf 3.

2.80. **NoOfFaultsPerType (Aantal fouten per soort)**

Aantal fouten per soort fout dat een kaart kan opslaan.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Waardetoekenning: zie paragraaf 3.

2.81. **OdometerValueMidnight (Kilometerstand om 0.00 uur)**

De kilometerstand van het voertuig om 0.00 uur op een bepaalde dag (voorschrift 090).

```
OdometerValueMidnight ::= OdometerShort
```

Waardetoekenning: niet nader gespecificeerd.

2.82. **OdometerShort (Verkorte kilometerstand)**

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 0 tot 9 999 999 km.

2.83. **OverspeedNumber (Aantal snelheidoverschrijdingen)**

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.

2.84. **PlaceRecord (Plaatsregistratie)**

Informatie met betrekking tot een plaats waar een dagelijkse werkperiode begint of eindigt (voorschriften 087, 202, 221).

```
PlaceRecord ::= SEQUENCE {
   entryTime                              TimeReal,
   entryTypeDailyWorkPeriod               EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry                 NationNumeric,
   dailyWorkPeriodRegion                  RegionNumeric,
   vehicleOdometerValue                   OdometerShort
}
```

entryTime is een datum en tijd 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.

2.85. **PreviousVehicleInfo (Informatie over het vorige voertuig)**

Informatie met betrekking tot het vorige door een bestuurder gebruikte voertuig wanneer hij zijn kaart in een voertuig-unit inbrengt (voorschrift 081).

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification        VehicleRegistrationIdentification,
   cardWithdrawalTime                       TimeReal
}
```

vehicleRegistrationIdentification is het kentekennummer en de registrerende lidstaat van het voertuig.

cardWithdrawalTime is de datum en tijd van kaartuitneming.

2.86. **PublicKey (Openbare sleutel)**

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.

2.87. **RegionAlpha (Alfanumerieke code van een regio)**

Alfabetische verwijzing naar een regio in een gespecificeerd land.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Waardetoekenning:

' '	Geen informatie beschikbaar,

Spanje:

'AN'	Andalucía,
'AR'	Aragón,
'AST'	Asturias,
'C'	Cantabrica,
'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

2.88. **RegionNumeric (Numerieke code van een regio)**

Numerieke verwijzing naar een regio in een gespecificeerd land.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Waardetoekenning:

'OO'H	Geen informatie beschikbaar,
Spain:	
'O1'H	Andalucía,
'O2'H	Aragón,
'O3'H	Asturias,
'O4'H	Cantabrica,
'O5'H	Cataluña,
'O6'H	Castilla-León,
'O7'H	Castilla-La-Mancha,
'O8'H	Valencia,
'O9'H	Extremadura,
'OA'H	Galicia,
'OB'H	Baleares,
'OC'H	Canarias,
'OD'H	La Rioja,
'OE'H	Madrid,
'OF'H	Murcia,
'1O'H	Navarra,
'11'H	País Vasco

2.89. **RSAKeyModulus (Modulus van de RSA sleutel)**

De modulus van een RSA-sleutelpaar.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Waardetoekenning: niet gespecificeerd.

2.90. **RSAKeyPrivateExponent (Particuliere exponent van de RSA sleutel)**

De particuliere exponent van een RSA-sleutelpaar.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Waardetoekenning: niet gespecificeerd.

2.91. **RSAKeyPublicExponent (Openbare exponent van de RSA-sleutel)**

De openbare exponent van een RSA sleutelpaar.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Waardetoekenning: niet gespecificeerd.

2.92. **SensorApprovalNumber (Goedkeuringsnummer van de opnemer)**

Goedkeuringsnummer van de opnemer.

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

Waardetoekenning: niet gespecificeerd.

2.93. **SensorIdentification (Identificatie van de opnemer)**

In een bewegingsopnemer opgeslagen informatie met betrekking tot de identificatie van de bewegingsopnemer (voorschrift 077).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorSCIdentifier                    SensorSCIdentifier,
   sensorOSIdentifier                    SensorOSIdentifier
}
```

sensorSerialNumber is het verlengde serienummer van de bewegingsopnemer (inclusief onderdeelnummer en code van de fabrikant).

sensorApprovalNumber is het goedkeuringsnummer van de bewegingsopnemer.

sensorSCIdentifier is het identificatiesymbool van de beveiligingscomponent van de bewegingsopnemer.

sensorOSIdentifier is het identificatiesymbool van het besturingssysteem van de bewegingsopnemer.

2.94. **SensorInstallation (Installatie van de opnemer)**

In de bewegingsopnemer opgeslagen informatie met betrekking tot de installatie van de bewegingsopnemer (voorschrift 099).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst                  SensorPairingDate,
   firstVuApprovalNumber                   VuApprovalNumber,
   firstVuSerialNumber                     VuSerialNumber,
   sensorPairingDateCurrent                SensorPairingDate,
   currentVuApprovalNumber                 VuApprovalNumber,
   currentVUSerialNumber                   VuSerialNumber
}
```

sensorPairingDateFirst is de datum van de eerste verbinding van de bewegingsopnemer met de voertuigunit.

firstVuApprovalNumber is het goedkeuringsnummer van de eerste voertuigunit die met de bewegingsopnemer verbonden wordt.

firstVuSerialNumber is het serienummer van de eerste met de bewegingsopnemer verbonden voertuigunit.

sensorPairingDateCurrent is de datum van de huidige verbinding van de bewegingsopnemer met de voertuigunit.

currentVuApprovalNumber is het goedkeuringsnummer van de op dat moment met de bewegingsopnemer verbonden voertuigunit.

currentVUSerialNumber is het serienummer van de op dat moment met de bewegingsopnemer verbonden voertuigunit.

2.95. **SensorInstallationSecData (Beveiligingsgegevens over de installatie van de opnemer)**

Op een werkplaatskaart opgeslagen informatie met betrekking tot de benodigde beveiligingsgegevens bij verbinding van een bewegingsopnemer met een voertuigunit (voorschrift 214).

```
SensorInstallationSecData ::= TDesSessionKey
```

Waardetoekenning: overeenkomstig ISO 16844-3.

2.96. **SensorOSIdentifier (Identificatiesymbool van het OS van de opnemer)**

Identificatiesymbool van het besturingssysteem van de bewegingsopnemer.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Waardetoekenning: specifiek voor de fabrikant.

2.97. **SensorPaired (Verbonden opnemer)**

In een voertuigunit opgeslagen informatie met betrekking tot de identificatie van de met de voertuigunit verbonden bewegingsopnemer (voorschrift 079).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                      SensorSerialNumber,
   sensorApprovalNumber                    SensorApprovalNumber,
   sensorPairingDateFirst                  SensorPairingDate
}
```

sensorSerialNumber is het serienummer van de op dat moment met de voertuigunit verbonden bewegingsopnemer.

sensorApprovalNumber is het goedkeuringsnummer van de op dat moment met de voertuigunit verbonden bewegingsopnemer.

sensorPairingDateFirst is de datum van de eerste verbinding met een voertuigunit van de op dat moment met de voertuigunit verbonden bewegingsopnemer.

2.98. **SensorPairingDate (Datum van verbinding van de opnemer)**

Datum van een verbinding van de bewegingsopnemer met een voertuigunit.

```
SensorPairingDate ::= TimeReal
```

Waardetoekenning: niet gespecificeerd.

2.99. **SensorSerialNumber (Serienummer van de opnemer)**

Serienummer van de bewegingsopnemer.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.100. **SensorSCIdentifier (Identificatiesymbool van de beveiligingscomponent van de opnemer)**

Identificatiesymbool van de beveiligingscomponent van de bewegingsopnemer.

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

Waardetoekenning: specifiek voor de fabrikant van de component.

2.101. **Signature (Handtekening)**

Een digitale handtekening.

```
Signature ::= OCTET STRING (SIZE(128))
```

Waardetoekenning: overeenkomstig appendix 11 (Algemene beveiligingsinrichtingen).

2.102. **SimilarEventsNumber (Aantal vergelijkbare voorvallen)**

Het aantal vergelijkbare voorvallen op een bepaalde dag (voorschrift 094).

```
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.

2.103. **SpecificConditionType (Soort specifieke omstandigheid)**

Code die een specifieke omstandigheid identificeert (voorschriften 050b, 105a, 212a en 230a).

```
SpecificConditionType ::= INTEGER(0..255)
```

Waardetoekenning:

'O0'H	RFU
'O1'H	Buiten bereik — Begin
'O2'H	Buiten bereik — Einde
'O3'H	Vervoer per veerboot/trein
'O4'H .. 'FF'H	RFU

2.104. **SpecificConditionRecord (Registratie van een specifieke omstandigheid)**

Op een bestuurderskaart, een werkplaatskaart of in een voertuigunit opgeslagen informatie met betrekking tot een specifieke omstandigheid (voorschriften 105a, 212a en 230a).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                                TimeReal,
   specificConditionType                    SpecificConditionType
}
```

entryTime is de datum en tijd van de invoer.

specificConditionType is de code die de specifieke omstandigheid identificeert.

2.105. **Speed (Snelheid)**

Snelheid van het voertuig (km/h).

```
Speed ::= INTEGER(0..255)
```

Waardetoekenning: kilometer per uur in het operationele bereik van 0 tot 220 km/h.

2.106. **SpeedAuthorised (Toegestane snelheid)**

Toegestane maximumsnelheid van het voertuig (definitie bb).

```
SpeedAuthorised ::= Speed
```

2.107. **SpeedAverage (Gemiddelde snelheid)**

Gemiddelde snelheid tijdens een vooraf gedefinieerde periode (km/h).

```
SpeedAverage ::= Speed
```

2.108. **SpeedMax (Maximumsnelheid)**

Maximumsnelheid gemeten tijdens een vooraf gedefinieerde periode.

```
SpeedMax ::= Speed
```

2.109. **TDesSessionKey (TDes-sessiesleutel)**

Een triple DES-sessiesleutel.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                                 OCTET STRING (SIZE(8))
   tDesKeyB                                 OCTET STRING (SIZE(8))
}
```

Waardetoekenning: niet nader gespecificeerd.

2.110. **TimeReal (Tijdklok)**

Code voor een gecombineerd veld voor datum en tijd, waarin datum en tijd 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.

2.111. **TyreSize (Bandenmaat)**

Aanduiding van de afmetingen van de banden.

```
TyreSize ::= IA5String(SIZE(15))
```

Waardetoekenning: overeenkomstig Richtlijn 92/23/EEG 31.3.1992, PB L 129, blz. 95.

2.112. **VehicleIdentificationNumber (Voertuigidentificatienummer)**

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.

2.113. **VehicleRegistrationIdentification (Identificatie van de voertuigregistratie)**

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).

2.114. **VehicleRegistrationNumber (Kentekennummer)**

Kentekennummer van het voertuig (VRN). Het kentekennummer wordt door de autoriteit afgegeven die de vergunning verleent.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                                 INTEGER (0..255),
   vehicleRegNumber                         OCTET STRING (SIZE(13))
}
```

codePage specificeert het deel van ISO/IEC 8859 dat gebruikt wordt om het vehicleRegNumber te coderen.

vehicleRegNumber is een overeenkomstig ISO/IEC 8859-codePage gecodeerd kentekennummer.

Waardetoekenning: specifiek voor een land.

2.115. **VuActivityDailyData (Gegevens over de dagelijkse activiteiten van de VU)**

In een VU opgeslagen informatie met betrekking tot wijzigingen in de activiteiten en/of wijzigingen in de rijstatus en/of wijzigingen in de status van de kaart voor een bepaalde kalenderdag (voorschrift 084) 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 activityChangeInfos-reeks.

activityChangeInfos is de reeks in de VU opgeslagen ActivityChangeInfo-woorden voor de dag.

2.116. **VuApprovalNumber (Goedkeuringsnummer van de VU)**

Goedkeuringsnummer van de voertuigunit.

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

Waardetoekenning: niet gespecificeerd.

2.117. **VuCalibrationData (Kalibreringsgegevens van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot de kalibreringen van het controleapparaat (voorschrift 098).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords                 INTEGER(0..255),
   vuCalibrationRecords SET                 SIZE(noOfVuCalibrationRecords) OF
                                            VuCalibrationRecord
}
```

noOfVuCalibrationRecords is het aantal registraties in de vuCalibrationRecords reeks.

vuCalibrationRecords is de reeks kalibreringsregistraties.

2.118. **VuCalibrationRecord (Kalibreringsregistratie van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot een kalibrering van het controleapparaat (voorschrift 098).

```
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-nummer.

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 uitgevoerd moet worden.

2.119. **VuCardIWData (Gegevens over het inbrengen en uitnemen van een kaart)**

In een voertuigunit opgeslagen informatie met betrekking tot cycli van inbrengen in- en uitnemen uit een voertuigunit van bestuurderskaarten of werkplaatskaarten (voorschrift 081).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                         INTEGER(0..216-1),
   vuCardIWRecords                       SET SIZE(noOfIWRecords) OF
                                         VuCardIWRecord
}
```

noOfIWRecords is het aantal registraties in de reeks vuCardIWRecords.

vuCardIWRecords is een reeks registraties met betrekking tot cycli van inbrengen en uitnemen van een kaart.

2.120. **VuCardIWRecord (Registratie van het inbrengen en uitnemen van een kaart)**

In een voertuigunit opgeslagen informatie met betrekking tot cycli van inbrengen in- en uitnemen uit een voertuigunit van een bestuurderskaart of een werkplaatskaart (voorschrift 081).

```
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 tijd van inbrenging.

vehicleOdometerValueAtInsertion is de kilometerstand van het voertuig bij kaartinbrenging.

cardSlotNumber is de lezer waarin de kaart ingebracht is.

cardWithdrawalTime is de datum en tijd 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 label dat identificeert of de kaarthouder bij de kaartinbrenging handmatig activiteiten van de bestuurder heeft ingevoerd.

2.121. **VuCertificate (VU-certificaat)**

Certificaat van de openbare sleutel van een voertuigunit.

```
VuCertificate ::= Certificate
```

2.122. **VuCompanyLocksData (Gegevens over bedrijfsvergrendelingen van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot bedrijfsvergrendelingen (voorschrift 104).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                               INTEGER(0..20),
   vuCompanyLocksRecords                   SET SIZE(noOfLocks) OF
                                           VuCompanyLocksRecord
}
```

noOfLocks is het aantal in vuCompanyLocksRecords opgenomen vergrendelingen.

vuCompanyLocksRecords is de reeks registraties van bedrijfsvergrendelingen.

2.123. **VuCompanyLocksRecord (Registratie van bedrijfsvergrendelingen van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot een bedrijfsvergrendeling (voorschrift 104).

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumber                   FullCardNumber
}
```

lockInTime, lockOutTime zijn de datum en tijd 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.

2.124. **VuControlActivityData (Gegevens over controleactiviteiten van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot controles die met deze VU worden uitgevoerd (voorschrift 102).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

noOfControls is het aantal in vuControlActivityRecords opgenomen controles.

vuControlActivityRecords is de reeks registraties van controleactiviteiten.

2.125. **VuControlActivityRecord (Registratie van controleactiviteiten van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot een controle die met deze VU wordt uitgevoerd (voorschrift 102).

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                         ControlType,
   controlTime                         TimeReal,
   controlCardNumber                   FullCardNumber,
   downloadPeriodBeginTime             TimeReal,
   downloadPeriodEndTime               TimeReal
}
```

controlType is de soort controle.

controlTime is de datum en tijd van de controle.

ControlCardNumber identificeert de bij de controle gebruikte controlekaart.

downloadPeriodBeginTime is de begintijd van de overgebrachte periode, in geval van overbrenging.

downloadPeriodEndTime is de eindtijd van de overgebrachte periode, in geval van overbrenging.

2.126. **VuDataBlockCounter (Teller van gegevensblokken van de VU)**

Op een kaart opgeslagen teller die de cycli van kaartinbrenging in en kaartuitname uit voertuigunits opeenvolgend identificeert.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Waardetoekenning: opeenvolgend cijfer met een maximale waarde van 9 999, waarna het opnieuw met 0 begint.

2.127. **VuDetailedSpeedBlock (Gedetailleerd snelheidsblok van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot de gedetailleerde snelheid van het voertuig gedurende een minuut waarin het voertuig rijdt (voorschrift 093).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate                    TimeReal,
   speedsPerSecond                        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate is de datum en tijd 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).

2.128. **VuDetailedSpeedData (Gedetailleerde snelheidsgegevens van de VU)**

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.

2.129. **VuDownloadablePeriod (Over te brengen periode van de VU)**

De eerste en laatste datum waarvan een voertuigunit gegevens met betrekking tot activiteiten van de bestuurder vasthoudt (voorschriften 081, 084 of 087).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                    TimeReal
   maxDownloadableTime                    TimeReal
}
```

minDownloadableTime is de datum en tijd 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 tijd van de laatste in de VU opgeslagen kaartuitneming, van de wijziging van activiteiten of van invoer van de plaats.

2.130. **VuDownloadActivityData (Gegevens over overbrengingsactiviteiten van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot de laatste overbrenging (voorschrift 105).

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                        TimeReal,
   fullCardNumber                         FullCardNumber,
   companyOrWorkshopName                  Name
}
```

downloadingTime is de datum en tijd van overbrenging.

fullCardNumber identificeert de kaart die wordt gebruikt om de overbrenging te autoriseren.

companyOrWorkshopName is de naam van het bedrijf of de werkplaats.

2.131. **VuEventData (Gegevens over voorvallen van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot voorvallen (voorschrift 094 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 voorvallenregistraties.

2.132. **VuEventRecord (Voorvallenregistratie van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot een voorval (voorschrift 094 met uitzondering van snelheidsoverschrijding).

```
VuEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   cardNumberDriverSlotBegin          FullCardNumber,
   cardNumberCodriverSlotBegin        FullCardNumber,
   cardNumberDriverSlotEnd            FullCardNumber,
   cardNumberCodriverSlotEnd          FullCardNumber,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType is de soort voorval.

eventRecordPurpose is het doel waarvoor dit voorval geregistreerd werd.

eventBeginTime is de datum en tijd van het begin van het voorval.

eventEndTime is de datum en tijd 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.

2.133. **VuFaultData (Gegevens over fouten van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot fouten (voorschrift 096).

```
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 foutenregistraties.

2.134. **VuFaultRecord (Foutenregistratie van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot een fout (voorschrift 096).

```
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 tijd van het begin van de fout.

faultEndTime is de datum en tijd 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.

2.135. **VuIdentification (Identificatie van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot de identificatie van de voertuigunit (voorschrift 075).

```
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 voertuigunit.

vuSoftwareIdentification identificeert de software die in de voertuigunit geïmplementeerd is.

vuManufacturingDate is het bouwjaar van de voertuigunit.

vuApprovalNumber is het typegoedkeuringsnummer van de voertuigunit.

2.136. **VuManufacturerAddress(Adres van de fabrikant van de VU)**

Adres van de fabrikant van de voertuigunit.

```
VuManufacturerAddress ::= Address
```

Waardetoekenning: niet gespecificeerd.

2.137. **VuManufacturerName (Naam van de fabrikant van de VU)**

Naam van de fabrikant van de voertuigunit.

```
VuManufacturerName ::= Name
```

Waardetoekenning: niet gespecificeerd.

2.138. **VuManufacturingDate (Bouwjaar van de VU)**

Bouwjaar van de voertuigunit.

```
VuManufacturingDate ::= TimeReal
```

Waardetoekenning: niet gespecificeerd.

2.139. **VuOverSpeedingControlData (Controlegegevens over snelheidsoverschrijding van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot snelheidsoverschrijdingen sinds de laatste controle van de snelheidsoverschrijding (voorschrift 095).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime                TimeReal,
   firstOverspeedSince                     TimeReal,
   numberOfOverspeedSince                  OverspeedNumber
}
```

lastOverspeedControlTime is de datum en tijd van de laatste controle van de snelheidsoverschrijding.

firstOverspeedSince is de datum en tijd van de eerste snelheidsoverschrijding na deze controle van de snelheidsoverschrijding.

numberOfOverspeedSince is het aantal snelheidsoverschrijdingen na de laatste controle van de snelheidsoverschrijding.

2.140. **VuOverSpeedingEventData (Gegevens over voorvallen van snelheidsoverschrijding van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot voorvallen van snelheidsoverschrijding (voorschrift 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 voorvallenregistraties van snelheidsoverschrijding.

2.141. **VuOverSpeedingEventRecord (Voorvallenregistraties van snelheidsoverschrijding van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot voorvallen van snelheidsoverschrijding (voorschrift 094).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                               EventFaultType,
   eventRecordPurpose                      EventFaultRecordPurpose,
   eventBeginTime                          TimeReal,
   eventEndTime                            TimeReal,
   maxSpeedValue                           SpeedMax,
   averageSpeedValue                       SpeedAverage,
   cardNumberDriverSlotBegin               FullCardNumber,
   similarEventsNumber                     SimilarEventsNumber
}
```

eventType is de soort voorval.

eventRecordPurpose is het doel waarvoor dit voorval geregistreerd werd.

eventBeginTime is de datum en tijd van het begin van het voorval.

eventEndTime is de datum en tijd 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.

2.142. **VuPartNumber (Onderdeelnummer van de VU)**

Onderdeelnummer van de voertuigunit.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Waardetoekenning: specifiek voor de fabrikant van de VU.

2.143. **VuPlaceDailyWorkPeriodData (Gegevens over plaatsen van dagelijkse werkperioden van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot plaatsen waar bestuurders een dagelijkse werkperiode beginnen of eindigen (voorschrift 087).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                        INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords           SET SIZE(noOfPlaceRecords) OF
                                           VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords is het aantal in de vuPlaceDailyWorkPeriodRecords-reeks opgenomen registraties.

vuPlaceDailyWorkPeriodRecords is een reeks registraties met betrekking tot de plaats.

2.144. **VuPlaceDailyWorkPeriodRecord (Registraties van plaatsen van dagelijkse werkperioden van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot een plaats waar een bestuurder een dagelijkse werkperiode begint of eindigt (voorschrift 087).

```
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.

2.145. **VuPrivateKey (Particuliere sleutel van de VU)**

De particuliere sleutel van een voertuigunit.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.146. **VuPublicKey (Openbare sleutel van de VU)**

De openbare sleutel van een voertuigunit.

```
VuPublicKey ::= PublicKey
```

2.147. **VuSerialNumber (Serienummer van de VU)**

Serienummer van de voertuigunit (voorschrift 075).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.148. **VuSoftInstallationDate (Datum van installatie van de software in de VU)**

Datum van installatie van de softwareversie in de voertuigunit.

```
VuSoftInstallationDate ::= TimeReal
```

Waardetoekenning: niet gespecificeerd.

2.149. **VuSoftwareIdentification (Identificatie van de software van de VU)**

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 voertuigunit.

vuSoftInstallationDate is de datum van installatie van de softwareversie.

2.150. **VuSoftwareVersion (Softwareversie van de VU)**

Nummer van de softwareversie van de voertuigunit.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Waardetoekenning: niet gespecificeerd.

2.151. **VuSpecificConditionData (Gegevens over specifieke omstandigheden van de VU)**

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 registraties.

specificConditionRecords is een reeks registraties met betrekking tot specifieke omstandigheden.

2.152. **VuTimeAdjustmentData (Tijdafstellingsgegevens van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot de buiten het kader van een geregelde kalibrering uitgevoerde tijdafstellingen (voorschrift 101).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                      INTEGER(0..6),
   vuTimeAdjustmentRecords                   SET SIZE(noOfVuTimeAdjRecords) OF
                                             VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords is het aantal registraties in de vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords is een reeks tijdafstellingsregistraties.

2.153. **VuTimeAdjustmentRecord (Tijdafstellingsregistraties van de VU)**

In een voertuigunit opgeslagen informatie met betrekking tot een buiten het kader van een geregelde kalibrering uitgevoerde tijdafstelling (voorschrift 101).

```
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.

2.154. **W-VehicleCharacteristicConstant (Kenmerkende coëfficiënt van het voertuig)**

Kenmerkende coëfficiënt van het voertuig (definitie k).

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Waardetoekenning: impulsen per kilometer in het operationele bereik 0 tot 64255 pulsen/km.

2.155. **WorkshopCardApplicationIdentification (Toepassingsidentificatie van de werkplaatskaart)**

Op een werkplaatskaart opgeslagen informatie met betrekking tot de toepassingsidentificatie van de kaart (voorschrift 190).

```
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 registraties van activiteiten.

noOfCardVehicleRecords is het aantal voertuigregistraties dat de kaart kan bevatten.

noOfCardPlaceRecords is het aantal plaatsen dat de kaart kan registreren.

noOfCalibrationRecords is het aantal kalibreringsregistraties dat de kaart kan opslaan.

2.156. **WorkshopCardCalibrationData (Kalibreringsgegevens van de werkplaatskaart)**

Op een werkplaatskaart opgeslagen informatie met betrekking tot de met de kaart uitgevoerde activiteiten van de werkplaats (voorschriften 227 en 229).

```
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 kalibreringsregistratie.

Waardetoekenning: getal dat correspondeert met de teller van de kalibreringsregistratie, beginnend met '0' voor de eerste kalibreringsregistratie in de structuur.

calibrationRecords is de reeks registraties die informatie over kalibrering en/of tijdafstelling bevat.

2.157. **WorkshopCardCalibrationRecord (Kalibreringsregistratie van de werkplaatskaart)**

Op een werkplaatskaart opgeslagen informatie met betrekking tot een met de kaart uitgevoerde kalibrering (voorschrift 227).

```
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-nummer.

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 die op het voertuig liggen.

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.

2.158. **WorkshopCardHolderIdentification (Identificatie van de werkplaatskaarthouder)**

Op een werkplaatskaart opgeslagen informatie met betrekking tot de identificatie van de kaarthouder (voorschrift 216).

```
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.

2.159. **WorkshopCardPIN (PIN-code van de werkplaatskaart)**

Personal identification number (PIN-code) van de werkplaatskaart (voorschrift 213).

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

Waardetoekenning: de bij de kaarthouder bekende PIN-code, rechts met 'F' bytes tot maximaal 8 bytes opgevuld.

3. DEFINITIES VAN WAARDENBEREIK EN AFMETINGENBEREIK

Definitie van variabele waarden die gebruikt zijn bij de definities in paragraaf 2.

`TimeRealRange ::= 2^32-1`

3.1. **Definities voor de bestuurderskaart:**

Naam van de variabele waarde	Min	Max
`CardActivityLengthRange`	5 544 bytes (28 dagen 93 activiteiten-wijzigingen per dag)	13 776 bytes (28 dagen 240 activiteiten-wijzigingen per dag)
`NoOfCardPlaceRecords`	84	112
`NoOfCardVehicleRecords`	84	200
`NoOfEventsPerType`	6	12
`NoOfFaultsPerType`	12	24

3.2. **Definities voor de werkplaatskaart:**

Naam van de variabele waarde	Min	Max
`CardActivityLengthRange`	198 bytes (1 dag 93 activiteiten-wijzigingen)	492 bytes (1 dag 240 activiteiten-wijzigingen)
`NoOfCardPlaceRecords`	6	8
`NoOfCardVehicleRecords`	4	8
`NoOfEventsPerType`	3	3
`NoOfFaultsPerType`	6	6
`NoOfCalibrationRecords`	88	255

3.3. **Definities voor de controlekaart:**

Naam van de variabele waarde	Min	Max
`NoOfControlActivityRecords`	230	520

3.4. **Definities voor de bedrijfskaart:**

Naam van de variabele waarde	Min	Max
`NoOfCompanyActivityRecords`	230	520

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, VehicleRegistratonNumber) gebruiken bovendien de tekens die worden gedefinieerd door de codes 192 tot en met 255 van ISO/IEC 8859-1 (Latijn1 tekenset) of ISO/IEC 8859-7 (Griekse tekenset).

5. CODERING

In het geval van codering met ASN.1-coderegels moeten alle gedefinieerde gegevenssoorten gecodeerd worden overeenkomstig ISO/IEC 8825-2, uitgerichte variant.

Appendix 2

SPECIFICATIE VAN TACHOGRAAFKAARTEN

INHOUD

1.	Inleiding	99
1.1.	Afkortingen	99
1.2.	Referenties	100
2.	Elektronische en fysieke kenmerken	100
2.1.	Toevoerspanning en stroomverbruik	100
2.2.	Programmeerspanning V_{pp}	101
2.3.	Klokgenerering en klokfrequentie	101
2.4.	I/O-contact	101
2.5.	Statussen van de kaart	101
3.	Hardware en communicatie	101
3.1.	Inleiding	101
3.2.	Transmissieprotocol	101
3.2.1.	Protocollen	101
3.2.2.	ATR	102
3.2.3.	PTS	103
3.3.	Toegangscondities (AC)	103
3.4.	Gegevenscodering	104
3.5.	Overzicht van commando's en foutcodes	104
3.6.	Beschrijving van commando's	105
3.6.1.	Select File (Selecteer bestand)	105
3.6.1.1.	Selectie op naam (AID)	105
3.6.1.2.	Selectie van een hoofdbestand met behulp van het bestandsidentificatiesymbool daarvan	106
3.6.2.	Read Binary (Lees binair getal)	106
3.6.2.1.	Commando zonder beveiligde berichtenuitwisseling	107
3.6.2.2.	Commando met beveiligde berichtenuitwisseling	107
3.6.3.	Update Binary (Bijwerken van binair getal)	109
3.6.3.1.	Commando zonder beveiligde berichtenuitwisseling	109
3.6.3.2.	Commando met beveiligde berichtenuitwisseling	110
3.6.4.	Get Challenge (Vraag naar identiteit)	111
3.6.5.	Verify (Verifieer)	111
3.6.6.	Get Response (Haal antwoord op)	112
3.6.7.	PSO: Verify Certificate (PSO: verifieer certificaat)	112
3.6.8.	Internal Authenticate (Interne authenticatie)	113

3.6.9. External Authenticate (Externe authenticatie) 114
3.6.10. Manage Security Environment (Beheer beveiligingsomgeving) 115
3.6.11. PSO: Hash (PSO: Hash) 116
3.6.12. Perform Hash of File (Voer hash van bestand uit) 116
3.6.13. PSO: Compute Digital Signature (PSO: bereken digitale handtekning) 117
3.6.14. PSO: Verify Digital Signature (PSO: verifieer digitale handtekening) 118
4. Structuur van de tachograafkaarten 118
4.1. Structuur van de bestuurderskaart 119
4.2. Structuur van de werkplaatskaart 121
4.3. Structuur van de controlekaart 123
4.4. Structuur van de bedrijfskaart 125

1. INLEIDING

1.1. **Afkortingen**

In deze appendix worden de volgende afkortingen gebruikt.

AC	Toegangscondities
AID	Toepassingsidentificatiesymbool
ALW	Altijd
APDU	Toepassingsprotocol gegevensunit (structuur van een commando)
ATR	Antwoord op terugstellen
AUT	Geauthentiseerd
C6, C7	Contacten nrs. 6 en 7 van de kaart zoals omschreven in ISO/IEC 7816-2
cc	klokcycli
CHV	Verificatie-informatie van de kaarthouder
CLA	Bytecategorie van een APDU-commando
DF	Toepassingsgericht bestand. Een DF kan andere bestanden (EF of DF) bevatten
EF	Hoofdbestand
ENC	Gecodeerd: toegang is alleen mogelijk door het coderen van gegevens
etu	elementaire tijdunit
IC	Integrated circuit
ICC	IC-kaart
ID	Identificatiesymbool
IFD	Interface-inrichting
IFS	Grootte van informatieveld
IFSC	Grootte van informatieveld voor de kaart
IFSD	Inrichting voor grootte van het informatieveld (voor het werkstation)
INS	Instructiebyte van een APDU-commando
Lc	Lengte van de invoergegevens voor een APDU-commando
Le	Lengte van de verwachte gegevens (uitvoergegevens voor een commando)
MF	Stambestand (wortel DF)
P1-P2	Parameterbytes
NAD	Node adres gebruikt in het T=1 protocol
NEV	Nooit
PIN	Personal Identification Number (PIN-code)
PRO SM	Beschermd door beveiligde berichtenuitwisseling
PTS	Protocol voor transmissieselectie
RFU	Gereserveerd voor toekomstig gebruik

RST	Terugstellen (van de kaart)
SM	Beveiligde berichtenuitwisseling
SW1-SW2	Statusbytes
TS	Initieel ATR-teken
VPP	Programmeerspanning
XXh	Waarde XX in hexadecimale notatie
||	Verbindingssymbool 03||04=0304

1.2. **Referenties**

De onderstaande referenties worden in deze appendix gebruikt:

EN 726-3	Identification cards systems — Telecommunications integrated circuit(s) cards and terminals — Part 3: Application independent card requirements. December 1994.
ISO/CEI 7816-2	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts. First edition: 1999.
ISO/CEI 7816-3	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocol. Edition 2: 1997.
ISO/CEI 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/CEI 7816-6	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements. First Edition: 1996 + Cor 1: 1998.
ISO/CEI 7816-8	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands. First Edition: 1999.
ISO/CEI 9797	Information technology — Security techniques — Data integrity mechanism using a cryptographic check function employing a block cipher algorithm. Edition 2: 1994.

2. ELEKTRONISCHE EN FYSIEKE KENMERKEN

TCS_200 Alle elektronische signalen moeten in overeenstemming zijn met ISO/IEC 7816-3 tenzij anders gespecificeerd.

TCS_201 De plaats en de afmetingen van de contacten van de kaart moeten voldoen aan ISO/IEC 7816-2.

2.1. **Toevoerspanning en stroomverbruik**

TCS_202 De kaart moet overeenkomstig de specificaties binnen de verbruikslimieten gespecificeerd in ISO/IEC 7816-3 werken.

TCS_203 De kaart moet met V_{cc} = 3 V (+/− 0,3 V) of met V_{cc} = 5 V (+/− 0,5 V) werken.

Spanningsselectie moet overeenkomstig ISO/IEC 7816-3 worden uitgevoerd.

2.2. **Programmeerspanning V_{pp}**

TCS_204 De kaart mag geen programmeerspanning op pin C6 gebruiken. Aangenomen wordt dat C6 niet aangesloten is in een IFD. Contact C6 kan worden verbonden met V_{cc} in de kaart maar mag niet met de aarde verbonden worden. Deze spanning mag in geen geval worden omgezet.

2.3. **Klokgenerering en klokfrequentie**

TCS_205 De kaart moet binnen een frequentiebereik van 1 tot 5 MHz werken. Binnen een kaartsessie mag 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_206 Onder de in kaartbestand EF_{ICC} opgenomen voorwaarden kan de externe klok stilgezet worden. De eerst byte van het EF_{ICC}-bestandsdeel codeert de voorwaarden voor de klokonderbrekingsmodus (zie EN 726-3 voor verdere details):

Laag	Hoog		
Bit 3	Bit 2	Bit 1	
0	0	1	Klokonderbreking toegestaan, geen voorkeurniveau
0	1	1	Klokonderbreking toegestaan, bij voorkeur hoog niveau
1	0	1	Klokonderbreking toegestaan, bij voorkeur laag niveau
0	0	0	Klokonderbreking niet toegestaan
0	1	0	Klokonderbreking alleen toegestaan op hoog niveau
1	0	0	Klokonderbreking alleen toegestaan op laag niveau

De bits 4 tot en met 8 worden niet gebruikt.

2.4. **I/O-contact**

TCS_207 Het I/O-contact C7 wordt gebruikt om gegevens van de IFD te ontvangen en om gegevens naar de IFD over te brengen. Alleen tijdens de werking moet ofwel de kaart ofwel de IFD in overbrengingsmodus zijn. Wanneer beide units in overbrengingsmodus zijn, mag er geen schade aan de kaart ontstaan. Wanneer de kaart niet overbrengt, moet hij in de ontvangstmodus zijn.

2.5. **Statussen van de kaart**

TCS_208 De kaart werkt in twee statussen wanneer de toevoerspanning aangesloten is:

— operationele status bij het uitvoeren van commando's of bij verbinding met de digitale unit,

— niet werkzame status op alle andere tijdstippen; in deze status moet de kaart alle gegevens vasthouden.

3. HARDWARE EN COMMUNICATIE

3.1. **Inleiding**

Deze paragraaf beschrijft de minimale voor tachograafkaarten en VU's vereiste functionaliteit om een correcte werking en interoperabiliteit te waarborgen.

Tachograafkaarten voldoen zoveel mogelijk aan de beschikbare, toepasselijke ISO/IEC normen (vooral ISO/IEC 7816). Commando's en protocollen worden echter volledig beschreven om beperkt gebruik of aanwezige verschillen te specificeren. De gespecificeerde commando's voldoen volledig aan de genoemde normen behalve waar aangegeven.

3.2. **Overbrengingsprotocol**

TCS_300 Het overbrengingsprotocol moet voldoen aan ISO/IEC 7816-3. De VU moet in het bijzonder door de kaart gezonden verlengingen van de wachttijd herkennen.

3.2.1. ***Protocollen***

TCS_301 De kaart moet zowel protocol T=0 als protocol T=1 leveren.

TCS_302 T=0 is het standaardprotocol, een PTS-commando is daarom noodzakelijk om het protocol in T=1 te wijzigen.

TCS_303 Inrichtingen moeten directe conventie in beide protocollen ondersteunen: de directe conventie is daarom verplicht voor de kaart.

TCS_304 De byte voor de afmeting van het informatieveld voor de kaart moet aanwezig zijn in de ATR in teken TA3. Deze waarde moet ten minste 'F0h' (= 240 bytes) zijn.

De onderstaande beperkingen zijn op de protocollen van toepassing:

TCS_305 T=0

— De interface-inrichting moet een antwoord op I/O ondersteunen na de oplopende rand van het signaal bij RST vanaf 400 cc.

— De interface-inrichting moet met 12 etu gescheiden tekens kunnen lezen.

— De interface-inrichting moet een foutief teken en de herhaling daarvan indien gescheiden met 13 etu kunnen lezen. Wanneer een foutief teken wordt opgespoord, kan de foutsignalering op I/O tussen 1 etu en 2 etu voorkomen. De inrichting moet een vertraging van 1 etu ondersteunen.

— De interface-inrichting moet een ATR van 33 bytes (TS+32) aanvaarden.

— Wanneer TC1 in de ATR aanwezig is, moet de extra bewakingstijd aanwezig zijn voor door de interface-inrichting gezonden tekens, hoewel door de kaart gezonden tekens nog steeds met 12 etu gescheiden kunnen worden. Dit geldt ook voor het door de kaart gezonden ACK-teken na een door de interface-inrichting uitgezonden P3-teken.

— De interface-inrichting moet rekening houden met een door de kaart gezonden NUL-teken.

— De interface-inrichting moet de complementaire modus voor ACK aanvaarden.

— Het GET RESPONSE-commando kan niet in kettingmodus worden gebruikt om een gegeven op te halen dat langer zou kunnen zijn dan 255 bytes.

TCS_306 T=1

— NAD-byte: niet gebruikt (NAD moet op '00' worden gezet).

— S-blok ABORT: niet gebruikt.

— S-blok VPP-statusfout: niet gebruikt.

— De totale kettinglengte voor een gegevensveld is niet langer dan 255 bytes (te waarborgen door de IFD).

— De inrichting voor de afmeting van het informatieveld (IFSD) moet onmiddellijk na de ATR door de IFD worden aangegeven: de IFD moet het S-Blok IFS-verzoek na de ATR overbrengen en de kaart moet het S-Blok IFS terugzenden. De aanbevolen waarde voor IFSD is 254 bytes.

— De kaart zal niet om een IFS-bijstelling vragen.

3.2.2. ***ATR***

TCS_307 De inrichting controleert ATR-bytes overeenkomstig ISO/IEC 7816-3. ATR historische tekens 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')	Afmeting van het informatieveld voor de kaart (IFSC)
TH1 tot en met TH5	'XXh'	Historische tekens
TCK	'XXh'	Controleer teken (exclusief OR)

TCS_308 Na het antwoord op terugstellen (ATR) wordt het stambestand (MF) impliciet geselecteerd en wordt de geldige directory.

3.2.3. ***PTS***

TCS_309 Het standaardprotocol is T=0. Om het T=1 protocol in te stellen moet de inrichting een PTS (ook PPS genoemd) naar de kaart sturen.

TCS_310 Aangezien de protocollen T=0 en T=1 verplicht zijn voor de kaart, is het basis-PTS voor protocolwisseling verplicht voor de kaart.

Het PTS kan, zoals aangegeven in ISO/IEC 7816-3, 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_311 Indien geen andere baudsnelheid dan de standaardsnelheid wordt ondersteund (of indien de geselecteerde baudsnelheid niet wordt ondersteund), moet de kaart correct op het PTS reageren, overeenkomstig ISO/IEC 7816-3, door het weglaten van de PPS1-byte.

Voorbeelden van het basis-PTS voor protocolselectie zijn de volgende:

Teken	Waarde	Opmerkingen
PPSS	'FFh'	Initieel teken
PPS0	'00h' of '01h'	PPS1 tot PPS3 zijn niet aanwezig; '00h' om T0 te selecteren, '01h' om T1 te selecteren
PK	'XXh'	Controleer teken: 'XXh' = 'FFh' als PPS0 = '00h' 'XXh' = 'FEh' als PPS0 = '01h'

3.3. **Toegangscondities (AC)**

Toegangscondities (AC) voor de commando's UPDATE_BINARY en READ_BINARY worden voor elk hoofdbestand gedefinieerd.

TCS_312 Aan de AC voor het geldige bestand moet worden voldaan voordat via deze commando's toegang kan worden verkregen tot het bestand.

De definities van de beschikbare toegangscondities luiden als volgt:

— ALW: de actie is altijd mogelijk en kan zonder enige beperking worden uitgevoerd.

— NEV: de actie is nooit mogelijk.

— AUT: de rechten met betrekking tot een succesvolle externe authentificatie moeten geopend zijn (uitgevoerd door het EXTERNAL_AUTHENTICATE-commando).

— PRO SM: het commando moet met een cryptografische controlesom worden overgebracht met gebruikmaking van beveiligde berichtenuitwisseling (zie appendix 11).

— AUT en PRO SM (samengevoegd).

Bij de verwerkingscommando's (UPDATE_BINARY en READ_BINARY) kunnen de volgende toegangscondities in de kaart worden ingesteld:

	UPDATE BINARY	READ BINARY
ALW	Ja	Ja
NEV	Ja	Ja
AUT	Ja	Ja
PRO SM	Ja	Nee
AUT en PRO SM	Ja	Nee

De toegangsconditie PRO SM is niet beschikbaar bij het READ_BINARY-commando. Dit betekent dat de aanwezigheid van een cryptografische controlesom voor een READ-commando nooit verplicht is. Bij gebruikmaking van de 'OC'-waarde voor de categorie is het echter mogelijk om het READ_BINARY-commando met beveiligde berichtenuitwisseling te gebruiken, zoals omschreven in paragraaf 3.6.2.

3.4. **Gegevenscodering**

Wanneer de vertrouwelijkheid van de gegevens die van een bestand worden ingelezen, beschermd moet worden, wordt het bestand gemerkt met „Encrypted" (gecodeerd). De codering geschiedt met beveiligde berichtenuitwisseling (zie appendix 11).

3.5. **Overzicht van commando's en foutcodes**

Commando's en bestandsorganisatie zijn afgeleid van en voldoen aan ISO/IEC 7816-4.

TCS_313 Deze paragraaf beschrijft de volgende APDU-commandoantwoordparen:

Commando	INS
SELECT FILE	A4
READ BINARY	B0
UPDATE BINARY	D6
GET CHALLENGE	84
VERIFY	20
GET RESPONSE	C0
PERFORM SECURITY OPERATION: VERIFY CERTIFICATE COMPUTE DIGITAL SIGNATURE VERIFY DIGITAL SIGNATURE HASH	2A
INTERNAL AUTHENTICATE	88
EXTERNAL AUTHENTICATE	82
MANAGE SECURITY ENVIRONMENT: SETTING A KEY	22
PERFORM HASH OF FILE	2A

TCS_314 De statuswoorden SW1 en SW2 worden in een antwoordbericht teruggezonden en geven het verwerkingsstadium van het commando aan.

SW1	SW2	Betekenis
90	00	Normale verwerking
61	XX	Normale verwerking. XX = aantal beschikbare antwoordbytes
62	81	Waarschuwende verwerking. Deel van teruggezonden gegevens kan verminkt zijn
63	CX	Foutieve CHV (PIN). 'X' levert de 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 foutief cryptogram (tijdens externe authentificatie) of ongeldige handtekening (tijdens handtekeningverificatie)
67	00	Foutieve lengte (foutieve Lc of Le)
69	00	Verboden commando (geen antwoord beschikbaar in T=0)
69	82	Niet voldaan aan beveiligingsstatus
69	83	Authentificatiemethode geblokkeerd
69	85	Niet voldaan aan gebruiksvoorwaarden
69	86	Commando niet toegestaan (geen geldig EF)
69	87	Verwachte gegevensobjecten voor beveiligde berichtenuitwisseling ontbreken
69	88	Onjuiste gegevensobjecten voor beveiligde berichtenuitwisseling
6A	82	Bestand niet gevonden
6A	86	Foutieve parameters P1-P2
6A	88	Referentiegegevens niet gevonden
6B	00	Onjuiste parameters (aangegeven buiten het EF)

SW1	SW2	Betekenis
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

3.6. **Beschrijving van commando's**

De verplichte commando's voor de tachograafkaarten worden in dit hoofdstuk beschreven.

Additionele relevante details in verband met de betreffende cryptografische operaties worden in appendix 11 (Algemene beveiligingsinrichtingen) verstrekt.

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 betreffende lengte, waarde en omschrijving leeg.

TCS_315 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 zendt het commando als beschreven met P3=Lc + gegevens en zendt vervolgens een GET RESPONSE-commando (zie paragraaf 3.6.6) met P3=Le.

TCS_316 Indien beide lengtebytes vereist zijn en Le=0 (beveiligde berichtenuitwisseling):

— moet de kaart bij protocol T=1 op Le=0 antwoorden door het zenden van alle beschikbare uitvoergegevens;

— moet bij protocol T=0 de IFD het eerste commando met P3=Lc + gegevens zenden, de kaart (op deze impliciete Le=0) antwoorden met de statusbytes '61La', waarbij La het aantal beschikbare antwoordbytes is. De IFD moet vervolgens een GET RESPONSE-commando met P3=La genereren om de gegevens te kunnen lezen.

3.6.1. ***Select file (Selecteer bestand)***

Dit commando voldoet aan ISO/IEC 7816-4, maar heeft in vergelijking met het in de norm gedefinieerde commando een beperkt gebruik.

Het SELECT FILE commando wordt gebruikt:

— om een DF-toepassing te selecteren (selectie op naam moet worden gebruikt);

— om een hoofdbestand te selecteren dat correspondeert met het opgegeven bestands-ID.

3.6.1.1. *Selectie op naam (AID)*

Met dit commando kan een DF-toepassing op de kaart geselecteerd worden.

TCS_317 Dit commando kan overal in de bestandsstructuur worden uitgevoerd (na het ATR of wanneer dan ook).

TCS_318 De selectie van een toepassing stelt de actuele beveiligingsomgeving terug. Na uitvoering van de toepassingsselectie wordt geen actuele openbare sleutel meer geselecteerd en de vorige sessiesleutel is niet langer beschikbaar voor beveiligde berichtenuitwisseling. De AUT-toegangsconditie is ook verloren gegaan.

TCS_319 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 gezonden bytes (lengte van het AID): '06h' voor de tachograaftoepassing
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' voor de tachograaftoepassing

Een antwoord op het SELECT FILE-commando is niet nodig (Le afwezig in T=1, of geen antwoord gevraagd in T=0).

TCS_320 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 het AID corresponderende toepassing niet wordt gevonden, is de teruggezonden verwerkingsstatus '6A82'.

— In T=1, indien byte Le aanwezig is, is de teruggezonden status '6700'.

— In T=0, indien na het SELECT FILE-commando een antwoord wordt gevraagd, is de teruggezonden status '6900'.

— Indien de geselecteerde toepassing verminkt is (binnen de bestandsattributen is een integriteitsfout ontdekt), is de teruggezonden verwerkingsstatus '6400' of '6581'.

3.6.1.2. *Selectie van een hoofdbestand met behulp van het bestandsidentificatiesymbool daarvan*

TCS_321 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Selectie van een EF in de geldige DF
P2	1	'0Ch'	Geen antwoord verwacht
Lc	1	'02h'	Aantal naar de kaart gezonden bytes
#6-#7	2	'XXXXh'	Bestandsidentificatiesymbool

Een antwoord op het SELECT FILE-commando is niet nodig (Le afwezig in T=1, of geen antwoord gevraagd in T=0).

TCS_322 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 het bestandsidentificatiesymbool corresponderende bestand niet wordt gevonden, is de teruggezonden verwerkingsstatus '6A82'.

— In T=1, indien byte Le aanwezig is, is de teruggezonden status '6700'.

— In T=0, indien na het SELECT FILE-commando een antwoord wordt gevraagd, is de teruggezonden status '6900'.

— Indien het geselecteerde bestand verminkt is (binnen de bestandsattributen is een integriteitsfout ontdekt), is de teruggezonden verwerkingsstatus '6400' of '6581'.

3.6.2. ***Read Binary (Lees binair getal)***

Dit commando voldoet aan ISO/IEC 7816-4, maar heeft in vergelijking met het in de norm gedefinieerde commando een beperkt gebruikt.

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.

TCS_323 Het commando kan alleen worden uitgevoerd indien de beveiligingsstatus voldoet aan de voor het EF gedefinieerde beveiligingskenmerken voor de READ-functie.

3.6.2.1. *Commando zonder beveiligde berichtenuitwisseling*

Met dit commando kan de IFD gegevens van het thans geselecteerde EF zonder beveiligde berichtenuitwisseling lezen.

TCS_324 Het lezen van gegevens van een met „encrypted" gemerkt bestand is met dit commando niet mogelijk.

TCS_325 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	Geen beveiligde berichtenuitwisseling gevraagd
INS	1	'B0h'	
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

Aantekening: bit 8 van P1 moet op 0 worden gezet.

TCS_326 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 , is de teruggezonden verwerkingsstatus '6986'.

— Indien niet wordt voldaan aan de toegangscontrole van het geselecteerde bestand, wordt het commando onderbroken met '6982'.

— Indien de Offset niet compatibel is met de grootte van het EF (Offset > EF grootte), is de teruggezonden verwerkingsstatus '6B00'.

— Indien de grootte van het te lezen bestand niet compatibel is met de grootte van het EF (Offset + Le > EF grootte), is de teruggezonden verwerkingsstatus '6700' of '6Cxx', waarbij 'xx' de exacte lengte aangeeft.

— Indien binnen de bestandsattributen een integriteitsfout wordt ontdekt, moet de kaart het bestand als verminkt en verloren beschouwen; de teruggezonden verwerkingsstatus is '6400' of '6581'.

— Indien binnen de opgeslagen gegevens een integriteitsfout wordt ontdekt, moet de kaart de gevraagde gegevens terugzenden; de teruggezonden verwerkingsstatus is '6281'.

3.6.2.2. *Commando met beveiligde berichtenuitwisseling*

Met dit commando kan de IDF gegevens van het thans geselecteerde 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 het EF met „encrypted" gemerkt is.

TCS_327 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'0Ch'	Beveiligde berichtenuitwisseling gevraagd
INS	1	'B0h'	INS
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	'09h'	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 (origineel Le): aantal te lezen bytes

Byte	Lengte	Waarde	Omschrijving
#9	1	'8Eh'	T_{CC}: label voor cryptografische controlesom
#10	1	'04h'	L_{CC}: lengte van volgende cryptografische controlesom
#11-#14	4	'XX..XXh'	Cryptografische controlesom (4 meest significante bytes)
Le	1	'00h'	Zoals gespecificeerd in ISO/IEC 7816-4

TCS_328 Antwoordbericht indien EF niet met „encrypted" gemerkt is en indien invoerformaat van beveiligde berichtenuitwisseling correct is:

Byte	Lengte	Waarde	Omschrijving
#1	1	'81h'	T_{PV}: label voor gegevens met ongecodeerde waarde
#2	L	'NNh' of '81 NNh'	L_{PV}: lengte van teruggezonden gegevens (= origineel Le) L is 2 bytes indien L_{PV}>127 bytes
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Ongecodeerde gegevenswaarde
#(2+L+NN)	1	'8Eh'	T_{CC}: label voor cryptografische controlesom
#(3+L+NN)	1	'04h'	L_{CC}: lengte van volgende cryptografische controlesom
#(4+L+NN)-#(7+L+NN)	4	'XX..XXh'	Cryptografische controlesom (4 meest significante bytes)
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

TCS_329 Antwoordbericht indien EF met „encrypted" is gemerkt en indien invoerformaat van 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 origineel Le van het commando ten gevolge van padding) L is 2 bytes indien $L_{PI\ CG}$ > 127 bytes
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Gecodeerde gegevens: paddingaanwijzer en cryptogram
#(2+L+MM)	1	'8Eh'	T_{CC}: label voor cryptografische controlesom
#(3+L+MM)	1	'04h'	L_{CC}: lengte van volgende cryptografische controlesom
#(4+L+MM)-#(7+L+MM)	4	'XX..XXh'	Cryptografische controlesom (4 meest significante bytes)
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

De teruggezonden gecodeerde gegevens bevatten een eerste byte die de gebruikte paddingmodus aangeeft. Voor de tachograaftoepassing heeft de paddingaanwijzer altijd de waarde '01h', waarmee wordt aangegeven dat de gebruikte paddingmodus de modus is die in ISO/IEC 7816-4 wordt gespecificeerd (een byte met waarde '80h' gevolgd door een aantal nulbytes: ISO/IEC 9797 methode 2).

De „gewone" verwerkingsstatussen, omschreven voor het READ BINARY-commando zonder beveiligde berichtenuitwisseling (zie paragraaf 3.6.2.1), kunnen met gebruikmaking van de boven omschreven antwoordberichtstructuren worden teruggezonden.

Bovendien kan zich een aantal fouten voordoen dat met name verband houdt met beveiligde berichtenuitwisseling. In dat geval wordt de verwerkingsstatus gewoon teruggezonden zonder beveiligde berichtenuitwisselingsstructuur:

TCS_330 Antwoordbericht indien invoerformaat van beveiligde berichtenuitwisseling niet correct is:

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Indien geen lopende sessiesleutel beschikbaar is, wordt verwerkingsstatus '6A88' teruggezonden. Dit gebeurt wanneer de sessiesleutel nog niet gegenereerd is of wanneer de geldigheid van de sessiesleutel verlopen is (in dit geval moet de IFD opnieuw een wederzijds authentificatieproces uitvoeren om een nieuwe sessiesleutel in te stellen).

— Indien een aantal verwachte gegevensobjecten (zoals hierboven gespecificeerd) in het formaat van de beveiligde berichtenuitwisseling ontbreekt, wordt 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 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 verwerkingsstatus '6688' teruggezonden.

3.6.3. ***Update Binary (Bijwerken van binair getal)***

Dit commando voldoet aan ISO/IEC 7816-4, maar heeft in vergelijking met het in de norm gedefinieerde commando een beperkt gebruik.

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.

TCS_331 Het commando kan alleen worden uitgevoerd indien de beveiligingsstatus voldoet aan de voor het EF gedefinieerde beveiligingskenmerken voor de UPDATE-functie (Indien de toegangscontrole van de UPDATE-functie PRO SM bevat, moet een beveiligde berichtenuitwisseling aan het commando worden toegevoegd).

3.6.3.1. *Commando zonder beveiligde berichtenuitwisseling*

Met dit commando kan de IFD gegevens naar het thans geselecteerde EF schrijven, zonder dat de kaart de integriteit van de ontvangen gegevens verifieert. Deze gewone modus is alleen toegestaan indien het betreffende bestand niet met „encrypted" gemerkt is.

TCS_332 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	Geen beveiligde berichtenuitwisseling gevraagd
INS	1	'D6h'	
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

Aantekening: bit 8 van P1 moet op 0 worden gezet.

TCS_333 Antwoordbericht

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '9000' terug.

— Indien geen EF geselecteerd is, is de teruggezonden verwerkingsstatus '6986'.

— Indien niet wordt voldaan aan de toegangscontrole van het geselecteerde bestand, wordt het commando onderbroken met '6982'.

— Indien de offset niet compatibel is met de grootte van het EF (offset > EF grootte), is de teruggezonden verwerkingsstatus '6B00'.

— Indien de grootte van de te schrijven gegevens niet compatibel is met de grootte van het EF (offset + Le > EF grootte), is de teruggezonden verwerkingsstatus '6700'.

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

— Indien het schrijven niet succesvol is, is de teruggezonden verwerkingsstatus '6581'.

3.6.3.2. *Commando met beveiligde berichtenuitwisseling*

Met dit commando kan de IFD gegevens naar het thans geselecteerde EF schrijven, waarbij de kaart de integriteit van de ontvangen gegevens verifieert. Wanneer vertrouwelijkheid niet vereist is, worden de gegevens niet gecodeerd.

TCS_334 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'OCh'	Beveiligde berichtenuitwisseling gevraagd
INS	1	'D6h'	INS
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
#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	'04h'	L_{CC}: lengte van volgende cryptografische controlesom
#(9+L+NN)-#(12+L+NN)	4	'XX..XXh'	Cryptografische controlesom (4 meest significante bytes)
Le	1	'00h'	Zoals gespecificeerd in ISO/IEC 7816-4

TCS_335 Antwoordbericht bij correct invoerformaat van beveiligde berichtenuitwisseling

Byte	Lengte	Waarde	Omschrijving
#1	1	'99h'	T_{SW}: label voor statuswoorden (door CC te beveiligen)
#2	1	'02h'	L_{SW}: lengte van teruggezonden statuswoorden
#3-#4	2	'XXXXh'	Statuswoorden (SW1, SW2)
#5	1	'8Eh'	T_{CC}: label voor cryptografische controlesom
#6	1	'04h'	L_{CC}: lengte van volgende cryptografische controlesom
#7-#10	4	'XX..XXh'	Cryptografische controlesom (4 meest significante bytes)
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

De „gewone" verwerkingsstatussen, omschreven voor het UPDATE BINARY-commando zonder beveiligde berichtenuitwisseling (zie paragraaf 3.6.3.1), kunnen met gebruikmaking van de boven omschreven antwoordberichtstructuur worden teruggezonden.

Bovendien kan zich een aantal fouten voordoen dat met name verband houdt met beveiligde berichtenuitwisseling. In dat geval wordt de verwerkingsstatus gewoon teruggezonden zonder beveiligde berichtenuitwisselingsstructuur.

TCS_336 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 verwerkingsstatus '6A88' teruggezonden.

— Indien een aantal verwachte gegevensobjecten (zoals hierboven gespecificeerd) in het formaat van de beveiligde berichtenuitwisseling ontbreekt, wordt 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 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 verwerkingsstatus '6688' teruggezonden.

3.6.4. ***Get Challenge (Vraag naar identiteit)***

Dit commando voldoet aan ISO/IEC 7816-4, maar heeft in vergelijking met het in de norm gedefinieerde commando een beperkt gebruik.

Het GET CHALLENGE-commando vraagt de kaart een identiteit af te geven voor gebruik in een beveiligingsprocedure waarbij een cryptogram of een aantal gecodeerde gegevens naar de kaart wordt gezonden.

TCS_337 De door de kaart afgegeven identiteit geldt alleen voor het volgende naar de kaart gezonden commando dat een identiteit gebruikt.

TCS_338 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (Lengte van de verwachte identiteit)

TCS_339 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 afwijkt van '08h', is de verwerkingsstatus '6700'.

— Indien de parameters P1-P2 niet correct zijn, is de verwerkingsstatus '6A86'.

3.6.5. ***Verify (Verifieer)***

Dit commando voldoet aan ISO/IEC 7816-4, maar heeft in vergelijking met het in de norm gedefinieerde commando een beperkt gebruik.

Het VERIFY-commando start de vergelijking in de kaart van de door het commando gezonden CHV-gegevens (PIN) met de op de kaart opgeslagen referentie CHV.

Opmerking: De door de gebruiker ingevoerde PIN-code moet rechts door de IFD met 'FFh'-bytes tot een lengte van 8 bytes worden opgevuld.

TCS_340 Indien het commando succesvol is, worden de rechten overeenkomstig de CHV-presentatie geopend en wordt de teller voor de resterende CHV-pogingen opnieuw geïnitialiseerd.

TCS_341 Een niet-succesvolle vergelijking wordt op de kaart geregistreerd om het aantal latere pogingen om de referentie-CHV te gebruiken, te beperken.

TCS_342 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	CLA
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_343 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 gevonden wordt, is de teruggezonden verwerkingsstatus '6A88'.

— Indien de CHV geblokkeerd is (de teller voor resterende CHV-pogingen is nul), is de teruggezonden verwerkingsstatus '6983'. Eenmaal in die status kan de CHV niet meer succesvol gepresenteerd worden.

— Indien de vergelijking niet succesvol is, wordt de teller voor resterende pogingen verlaagd en de status '63CX' teruggezonden (X > 0 en X zijn gelijk aan de teller voor de resterende CHV-pogingen. Als X = 'F', is de teller voor de CHV-pogingen groter dan 'F').

— Indien de referentie-CHV verminkt is, is de teruggezonden verwerkingsstatus '6400' of '6581'.

3.6.6. ***Get Response (Haal antwoord op)***

Dit commando voldoet aan ISO/IEC 7816-4.

Dit commando (alleen nodig en beschikbaar bij het T=0 protocol) wordt gebruikt om uitgewerkte gegevens van de kaart naar de interface-inrichting over te brengen (geval waarin een commando zowel Lc als Le bevatte).

Het GET_RESPONSE-commando moet onmiddellijk na het commando dat de gegevens uitwerkt, worden gegeven, anders gaan de gegevens verloren. Na de uitvoering van het GET_RESPONSE-commando (behalve wanneer de fout '61xx' of '6Cxx' optreedt, zie hieronder) zijn de reeds uitgewerkte gegevens niet langer ter beschikking.

TCS_344 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Aantal verwachte bytes

TCS_345 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 geen gegevens door de kaart uitgewerkt zijn, is de teruggezonden verwerkingsstatus '6900' of '6F00'.

— Indien Le het aantal beschikbare bytes overschrijdt of indien Le nul is, is de teruggezonden verwerkingsstatus '6Cxx', waarbij 'xx' het exacte aantal beschikbare bytes aangeeft. In dat geval zijn de uitgewerkte gegevens nog beschikbaar voor een volgend GET_RESPONSE-commando.

— Indien Le niet nul is en kleiner is dan het aantal beschikbare bytes, worden de vereiste gegevens gewoon door de kaart gezonden en is de teruggezonden verwerkingsstatus '61xx', waarbij 'xx' een aantal extra bytes aangeeft die nog beschikbaar zijn voor een volgend GET_RESPONSE-commando.

— Indien het commando niet ondersteund wordt (protocol T=1), zendt de kaart '6D00' terug.

3.6.7. ***PSO: Verify Certificate (PSO: verifieer certificaat)***

Dit commando voldoet aan ISO/IEC 7816-8, maar heeft in vergelijking met het in de norm gedefinieerde commando een beperkt gebruik.

Het VERIFY CERTIFICATE-commando wordt door de kaart gebruikt om een openbare sleutel van buitenaf te verkrijgen en de geldigheid ervan te controleren.

TCS_346 Wanneer een VERIFY CERTIFICATE-commando succesvol is, wordt de openbare sleutel voor toekomstig gebruik in de beveiligingsomgeving opgeslagen. Deze sleutel moet expliciet voor het gebruik in commando's met betrekking tot de beveiliging (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE of VERIFY CERTIFICATE) ingesteld worden door het MSE-commando (zie paragraaf 3.6.10), met gebruikmaking van zijn sleutelidentificatiesymbool.

TCS_347 In ieder geval gebruikt het VERIFY CERTIFICATE-commando de door het MSE-commando vooraf geselecteerde openbare sleutel om het certificaat te openen. Deze openbare sleutel moet die van een lidstaat of van Europa zijn.

TCS_348 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	CLA
INS	1	'2Ah'	Voer beveiligingsoperatie uit
P1	1	'00h'	P1
P2	1	'AEh'	P2: niet met BER-TLV gecodeerde gegevens (verbinding van gegevenselementen)
Lc	1	'CEh'	Lc: Lengte van het certificaat, 194 bytes
#6-#199	194	'XX..XXh'	Certificaat: verbinding van gegevenselementen (zoals omschreven in appendix 11)

TCS_349 Antwoordbericht

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statusbytes (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '9000' terug.

— Indien de certificaatverificatie mislukt, is de teruggezonden verwerkingsstatus '6688'. Het proces van verificatie en unwrapping van het certificaat wordt in appendix 11 beschreven.

— Indien geen openbare sleutel in de beveiligingsomgeving aanwezig is, wordt '6A88' teruggezonden.

— Indien de geselecteerde openbare sleutel (gebruikt om het certificaat open te maken) verminkt is, is de teruggezonden verwerkingsstatus '6400' of '6581'.

— Indien de geselecteerde openbare sleutel (gebruikt om het certificaat open te maken) een andere CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) heeft dan '00' (d.w.z. niet die van een lidstaat of van Europa is), is de teruggezonden verwerkingsstatus '6985'.

3.6.8. ***Internal Authenticate (Interne authenticatie)***

Dit commando voldoet aan ISO/IEC 7816-4.

Met het INTERNAL AUTHENTICATE-commando kan de IFD de kaart authentiseren.

Het authenticatieproces wordt in appendix 11 beschreven. Het bevat de onderstaande instructies:

TCS_350 Het INTERNAL AUTHENTICATE-commando gebruikt de particuliere sleutel van de kaart (impliciet geselecteerd) om authenticatiegegevens inclusief K1 (eerste element voor overeenkomst van de sessiesleutel) en RND1 te ondertekenen en gebruikt de thans geselecteerde openbare sleutel (met het laatste MSE-commando) om de handtekening te coderen en het authenticatieteken te ontwikkelen (meer details in appendix 11).

TCS_351 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 gezonden gegevens
#6-#13	8	'XX..XXh'	Identiteit gebruikt om de kaart te authentiseren
#14-#21	8	'XX..XXh'	VU.CHR (zie appendix 11)
Le	1	'80h'	Lengte van de gegevens die van de kaart verwacht worden

TCS_352 Antwoordbericht

Byte	Lengte	Waarde	Omschrijving
#1-#128	128	'XX..XXh'	Kaartauthenticatieteken (zie appendix 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, is de teruggezonden verwerkingsstatus '6A88'.

— Indien geen particuliere sleutel in de beveiligingsomgeving aanwezig is, is de teruggezonden verwerkingsstatus '6A88'.

— Indien VU.CHR niet overeenstemt met het identificatiesymbool van de huidige openbare sleutel, is de teruggezonden verwerkingsstatus '6A88'.

— Indien de geselecteerde particuliere sleutel verminkt is, is de teruggezonden verwerkingsstatus '6400' of '6581'.

TCS_353 Indien het INTERNAL AUTHENTICATE-commando succesvol is, wordt de actuele sessiesleutel, indien aanwezig, gewist en is niet langer ter beschikking. Om een nieuwe sessiesleutel ter beschikking te krijgen, moet het EXTERNAL AUTHENTICATE-commando succesvol uitgevoerd worden.

3.6.9. ***External Authenticate (Externe authenticatie)***

Dit commando voldoet aan ISO/IEC 7816-4.

Met het EXTERNAL AUTHENTICATE commando kan de kaart de IFD authentiseren.

Het authenticatieproces wordt in appendix 11 beschreven. Het bevat de onderstaande instructies:

TCS_354 Een GET CHALLENGE-commando moet onmiddellijk aan het EXTERNAL AUTHENTICATE-commando voorafgaan. De kaart geeft een identiteit af naar buiten (RND3).

TCS_355 De verificatie van het cryptogram gebruikt RND3 (door de kaart afgegeven identiteit), de particuliere sleutel van de kaart (impliciet geselecteerd) en de vooraf door het MSE-commando geselecteerde openbare sleutel.

TCS_356 De kaart verifieert het cryptogram en indien het correct is, wordt de AUT-toegangsconditie geopend.

TCS_357 Het invoercryptogram draagt het tweede element voor overeenkomst van sessiesleutel K2.

TCS_358 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (de te gebruiken openbare sleutel is impliciet bekend en werd vooraf door het MSE-commando ingesteld)
Lc	1	'80h'	Lc (lengte van de naar de kaart gezonden gegevens)
#6-#133	128	'XX..XXh'	Cryptogram (zie appendix 11)

TCS_359 Antwoordbericht

Byte	Lengte	Waarde	Omschrijving
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 '6A88' teruggezonden.

— Indien de CHA van de thans ingestelde openbare sleutel niet de verbinding is van de AID van de tachograaftoepassing en van een soort VU-inrichting, is de teruggezonden verwerkingsstatus '6F00' (zie appendix 11).

— Indien geen particuliere sleutel in de beveiligingsomgeving aanwezig is, is de teruggezonden verwerkingsstatus '6A88'.

— Indien de verificatie van het cryptogram mislukt, is de teruggezonden verwerkingsstatus '6688'.

— Indien het commando niet onmiddellijk wordt voorafgegaan door een GET CHALLENGE-commando, is de teruggezonden verwerkingsstatus '6985'.

— Indien de geselecteerde particuliere sleutel verminkt is, is de teruggezonden verwerkingsstatus '6400' of '6581'.

TCS_360 Indien het EXTERNAL AUTHENTICATE-commando succesvol is en indien het eerste deel van de sessiesleutel van een recent uitgevoerde succesvolle INTERNAL AUTHENTICATE beschikbaar is, wordt de sessiesleutel voor toekomstige commando's met beveiligde berichtenuitwisseling ingesteld.

TCS_361 Indien het eerste deel van de sessiesleutel niet beschikbaar is van een voorafgaand INTERNAL AUTHENTICATE-commando, wordt het tweede deel van de door de IFD gezonden sessiesleutel niet op de kaart opgeslagen. Dit mechanisme waarborgt dat het wederzijds authenticatieproces overeenkomstig de in appendix 11 gespecificeerde voorschriften uitgevoerd wordt.

3.6.10. ***Manage Security Environment (Beheer beveiligingsomgeving)***

Dit commando wordt gebruikt om een openbare sleutel voor authentificatiedoeleinden in te stellen.

Dit commando voldoet aan ISO/IEC 7816-8. Het gebruik van dit commando is met betrekking tot de betreffende norm beperkt.

TCS_362 De in het MSE-gegevensveld genoemde sleutel is geldig voor elk bestand van het DF van de tachograaf.

TCS_363 De in het MSE-gegevensveld genoemde sleutel blijft de huidige openbare sleutel tot het volgende correcte MSE-commando.

TCS_364 Indien de genoemde sleutel niet (reeds) in de kaart aanwezig is, blijft de beveiligingsomgeving ongewijzigd.

TCS_365 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: genoemde sleutel, geldig voor alle cryptografische operaties
P2	1	'B6h'	P2: genoemde gegevens betreffende digitale handtekening
Lc	1	'0Ah'	Lc: lengte van het volgende gegevensveld
#6	1	'83h'	Label voor verwijzing naar een openbare sleutel in asymmetrische gevallen
#7	1	'08h'	Lengte van de sleutelreferentie (sleutelidentificatiesymbool)
#8-#15	08h	'XX..XXh'	Sleutelidentificatiesymbool zoals gespecificeerd in appendix 11

TCS_366 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, is de teruggezonden verwerkingsstatus '6A88'.

— Indien een aantal verwachte gegevensobjecten in het beveiligde berichtenuitwisselingsformaat ontbreken, wordt verwerkingsstatus '6987' teruggezonden. Dit kan gebeuren wanneer het label '83h' ontbreekt.

— Indien een aantal gegevensobjecten niet correct is, is de teruggezonden verwerkingsstatus '6988'. Dit kan gebeuren wanneer de lengte van het sleutelidentificatiesymbool niet gelijk is aan '08h'.

— Indien de geselecteerde sleutel verminkt is, is de teruggezonden verwerkingsstatus '6400' of '6581'.

3.6.11. ***PSO: Hash (PSO: Hash)***

Dit commando wordt gebruikt om het resultaat van een hashberekening van een aantal gegevens naar de kaart te zenden. Dit commando wordt gebruikt voor de verificatie van digitale handtekeningen. De hashwaarde wordt in EEPROM opgeslagen voor het volgende commando „verifieer digitale handtekening".

Dit commando voldoet aan ISO/IEC 7816-8. Het gebruik van dit commando is met betrekking tot de betreffende norm beperkt.

TCS_367 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	CLA
INS	1	'2Ah'	Voer beveiligingsoperatie uit
P1	1	'90h'	Zend hashcode terug
P2	1	'A0h'	Label: gegevensveld bevat voor hashing relevante DO's
Lc	1	'16h'	Lengte Lc van het volgende gegevensveld
#6	1	'90h'	Label voor de hashcode
#7	1	'14h'	Lengte van de hashcode
#8-#27	20	'XX..XXh'	Hashcode

TCS_368 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 verwerkingsstatus '6987' teruggezonden. Dit kan gebeuren wanneer een van de labels '90h' ontbreekt.

— Indien een aantal gegevensobjecten niet correct is, is de teruggezonden verwerkingsstatus '6988'. Deze fout treedt op wanneer het vereiste label aanwezig is maar een lengte heeft die afwijkt van '14h'.

3.6.12. ***Perform Hash of File (Voer hash van bestand uit)***

Dit commando voldoet niet aan ISO/IEC 7816-8. De CLA-byte van dit commando geeft dus een particulier gebruik van de PERFORM SECURITY OPERATION/HASH aan.

TCS_369 Het PERFORM HASH OF FILE-commando wordt gebruikt om het gegevensgebied van het thans geselecteerde transparante EF te hashen.

TCS_370 Het resultaat van de hashoperatie wordt op 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. Dit resultaat blijft beschikbaar voor het COMPUTE DIGITAL SIGNATURE-commando tot het volgende succesvolle PERFORM HASH OF FILE-commando.

TCS_371 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'80h'	CLA
INS	1	'2Ah'	Voer beveiligingsoperatie uit
P1	1	'90h'	Label: hash
P2	1	'00h'	P2: hash de gegevens van het thans geselecteerde transparante bestand

TCS_372 Antwoordbericht

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '9000' terug.

— Indien geen toepassing geselecteerd is, wordt verwerkingsstatus '6985' teruggezonden.

— Indien het geselecteerde EF verminkt is (integriteitsfouten in bestandsattributen of opgeslagen gegevens), is de teruggezonden verwerkingsstatus '6400' of '6581'.

— Indien het geselecteerde bestand geen transparant bestand is, is de teruggezonden verwerkingsstatus '6986'.

3.6.13. ***PSO: Compute Digital Signature (PSO: bereken digitale handtekening)***

Dit commando wordt gebruikt om de digitale handtekening van een vooraf berekende hashcode te berekenen (zie PERFORM HASH OF FILE, paragraaf 3.6.12).

Dit commando voldoet aan ISO/IEC 7816-8. Het gebruik van dit commando is met betrekking tot de betreffende norm beperkt.

TCS_373 De particuliere sleutel van de kaart wordt gebruikt om de digitale handtekening te berekenen en is impliciet bij de kaart bekend.

TCS_374 De kaart voert een digitale handtekening uit met een paddingmethode overeenkomstig PKCS1 (zie appendix 11 voor details).

TCS_375 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	CLA
INS	1	'2Ah'	Voer beveiligingsoperatie uit
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 (hash van bestand)
Le	1	'80h'	Lengte van de verwachte handtekening

TCS_376 Antwoordbericht

Byte	Lengte	Waarde	Omschrijving
#1-#128	128	'XX..XXh'	Handtekening van de vooraf berekende hash
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '9000' terug.

— Indien de impliciet geselecteerde particuliere sleutel verminkt is, is de teruggezonden verwerkingsstatus '6400' of '6581'.

3.6.14. ***PSO: Verify Digital Signature (PSO: verifieer digitale handtekening)***

Dit commando wordt gebruikt om de digitale handtekening te verifiëren die geleverd is als een invoer overeenkomstig PKCS1 van een bericht waarvan de hash 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 met betrekking tot de betreffende norm beperkt.

TCS_377 Het VERIFY DIGITAL SIGNATURE-commando gebruikt altijd de door het voorafgaande MANAGE SECURITY ENVIRONMENT-commando geselecteerde openbare sleutel en de voorafgaande, door een PSO: HASH-commando ingevoerde hashcode.

TCS_378 Commandobericht

Byte	Lengte	Waarde	Omschrijving
CLA	1	'00h'	CLA
INS	1	'2Ah'	Voer beveiligingsoperatie uit
P1	1	'00h'	
P2	1	'A8h'	Label: gegevensveld bevat voor verificatie relevante DO's
Lc	1	'83h'	Lengte Lc van het volgende gegevensveld
#28	1	'9Eh'	Label voor digitale handtekening
#29-#30	2	'8180h'	Lengte van digitale handtekening (128 bytes, gecodeerd overeenkomstig ISO/IEC 7816-6)
#31-#158	128	'XX..XXh'	Inhoud van de digitale handtekening

TCS_379 Antwoordbericht

Byte	Lengte	Waarde	Omschrijving
SW	2	'XXXXh'	Statuswoorden (SW1, SW2)

— Indien het commando succesvol is, zendt de kaart '9000' terug.

— Indien de verificatie van de handtekening mislukt, is de teruggezonden verwerkingsstatus '6688'. Het verificatieproces wordt beschreven in appendix 11.

— Indien geen openbare sleutel geselecteerd wordt, is de teruggezonden verwerkingsstatus '6A88'.

— Indien een aantal verwachte gegevensobjecten (zoals hierboven gespecificeerd) ontbreekt, wordt verwerkingsstatus '6987' teruggezonden. Dit kan gebeuren wanneer een van de vereiste labels ontbreekt.

— Indien geen hashcode beschikbaar is om het commando te verwerken (ten gevolge van een voorafgaand PSO: HASH-commando), is de teruggezonden verwerkingsstatus '6985'.

— Indien een aantal gegevensobjecten niet correct is, is de teruggezonden verwerkingsstatus '6988'. Dit kan gebeuren wanneer een van vereiste lengtes van de gegevensobjecten niet correct is.

— Indien de geselecteerde openbare sleutel verminkt is, is de teruggezonden verwerkingsstatus '6400' of '6581'.

4. STRUCTUUR VAN DE TACHOGRAAFKAARTEN

Deze paragraaf specificeert de bestandsstructuren van de tachograafkaarten voor het opslaan van toegankelijke gegevens.

De interne structuren die specifiek zijn voor de fabrikant van de kaart, zoals bijv. koptitels van bestanden, worden niet gespecificeerd, evenmin als de opslag en verwerking van gegevenselementen voor intern gebruik zoals `EuropeanPublicKey`, `CardPrivateKey`, `TDesSessionKey` of `WorkshopCardPin`.

De bruikbare opslagcapaciteit van tachograafkaarten moet minimaal 11 Kb zijn. Een grotere capaciteit kan worden gebruikt. In dit geval blijft de structuur van de kaart hetzelfde, maar wordt het aantal registraties van enkele elementen van de structuur verhoogd. Deze paragraaf specificeert de laagste en hoogste waarden van deze registratieaantallen.

4.1. **Structuur van de bestuurderskaart**

TCS_400 Na personalisatie moet de bestuurderskaart de onderstaande permanente bestandsstructuur en bestandstoegangscondities hebben:

Bestand	ID van bestand	Toegangscondities		
		Lezen	Bijwerken	Gecodeerd
MF	3F00			
├─EF ICC	0002	ALW	NEV	Nee
├─EF IC	0005	ALW	NEV	Nee
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	Nee
├─EF Card_Certificate	C100	ALW	NEV	Nee
├─EF CA_Certificate	C108	ALW	NEV	Nee
├─EF Identification	0520	ALW	NEV	Nee
├─EF Card_Download	050E	ALW	ALW	Nee
├─EF Driving_Licence_Info	0521	ALW	NEV	Nee
├─EF Events_Data	0502	ALW	PRO SM / AUT	Nee
├─EF Faults_Data	0503	ALW	PRO SM / AUT	Nee
├─EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	Nee
├─EF Vehicles_Used	0505	ALW	PRO SM / AUT	Nee
├─EF Places	0506	ALW	PRO SM / AUT	Nee
├─EF Current_Usage	0507	ALW	PRO SM / AUT	Nee
├─EF Control_Activity_Data	0508	ALW	PRO SM / AUT	Nee
└─EF Specific_Conditions	0522	ALW	PRO SM / AUT	Nee

TCS_401 Alle EF-structuren moeten transparant zijn.

TCS_402 Lezen met beveiligde berichtenuitwisseling moet voor alle bestanden in het DF Tachograaf mogelijk zijn.

TCS_403 De bestuurderskaart moet de onderstaande gegevensstructuur hebben:

Bestand/gegevenselement	Aantal registraties	Grootte (bytes) Min	Max	Standaardwaarden
MF		*11411*	*24959*	
╠═EF ICC		*25*	*25*	
╚═CardIccIdentification		*25*	*25*	
├─clockStop		1	1	{00}
├─cardExtendedSerialNumber		8	8	{00..00}
├─cardApprovalNumber		8	8	{20..20}
├─cardPersonaliserID		1	1	{00}
├─embedderIcAssemblerId		5	5	{00..00}
└─icIdentifier		2	2	{00 00}
╠═EF IC		*8*	*8*	
╚═CardChipIdentification		*8*	*8*	
├─icSerialNumber		4	4	{00..00}
└─icManufacturingReferences		4	4	{00..00}
╚═DF Tachograph		*11378*	*24926*	
╠═EF Application_Identification		*10*	*10*	
╚═DriverCardApplicationIdentification		*10*	*10*	
├─typeOfTachographCardId		1	1	{00}
├─cardStructureVersion		2	2	{00 00}
├─noOfEventsPerType		1	1	{00}
├─noOfFaultsPerType		1	1	{00}
├─activityStructureLength		2	2	{00 00}
├─noOfCardVehicleRecords		2	2	{00 00}
└─noOfCardPlaceRecords		1	1	{00}
╠═EF Card_Certificate		*194*	*194*	
╚═CardCertificate		194	194	{00..00}
╠═EF CA_Certificate		*194*	*194*	
╚═MemberStateCertificate		194	194	{00..00}
╠═EF Identification		*143*	*143*	
├─CardIdentification		*65*	*65*	
├─cardIssuingMemberState		1	1	{00}
├─cardNumber		16	16	{20..20}
├─cardIssuingAuthorityName		36	36	{20..20}
├─cardIssueDate		4	4	{00..00}
├─cardValidityBegin		4	4	{00..00}
└─cardExpiryDate		4	4	{00..00}
└─DriverCardHolderIdentification		*78*	*78*	
├─cardHolderName		*72*	*72*	
├─holderSurname		36	36	{00, 20..20}
└─holderFirstNames		36	36	{00, 20..20}
├─cardHolderBirthDate		4	4	{00..00}
└─cardHolderPreferredLanguage		2	2	{20 20}

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_404 De onderstaande waarden, die worden gebruikt om de grootte in de bovenstaande tabel aan te geven, zijn de laagste en hoogste waarden van het aantal registraties dat de gegevensstructuur van de bestuurderskaart moet gebruiken:

		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	5544 bytes (28 dagen * 93 wijzigingen van activiteiten)	13776 bytes (28 dagen * 240 wijzigingen van activiteiten)

4.2. **Structuur van de werkplaatskaart**

TCS_405 Na personalisatie moet de werkplaatskaart de onderstaande permanente bestandsstructuur en bestandstoegangscondities hebben:

Bestand	ID van bestand	Toegangscondities		
		Lezen	Bijwerken	Gecodeerd
MF	3F00			
├─EF ICC	0002	ALW	NEV	Nee
├─EF IC	0005	ALW	NEV	Nee
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	Nee
├─EF Card_Certificate	C100	ALW	NEV	Nee
├─EF CA_Certificate	C108	ALW	NEV	Nee
├─EF Identification	0520	ALW	NEV	Nee
├─EF Card_Download	0509	ALW	ALW	Nee
├─EF Calibration	050A	ALW	PRO SM / AUT	Nee
├─EF Sensor_Installation_Data	050B	ALW	NEV	Ja
├─EF Events_Data	0502	ALW	PRO SM / AUT	Nee
├─EF Faults_Data	0503	ALW	PRO SM / AUT	Nee
├─EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	Nee
├─EF Vehicles_Used	0505	ALW	PRO SM / AUT	Nee
├─EF Places	0506	ALW	PRO SM / AUT	Nee
├─EF Current_Usage	0507	ALW	PRO SM / AUT	Nee
├─EF Control_Activity_Data	0508	ALW	PRO SM / AUT	Nee
└─EF Specific_Conditions	0522	ALW	PRO SM / AUT	Nee

TCS_406 Alle EF-structuren moeten transparant zijn.

TCS_407 Lezen met beveiligde berichtenuitwisseling moet voor alle bestanden in het DF Tachograaf mogelijk zijn.

TCS_408 De werkplaatskaart moet de onderstaande gegevensstructuur hebben:

Bestand/gegevenselement	Aantal registraties	Grootte (Bytes) Min	Grootte (Bytes) Max	Standaardwaarden
MF		*11088*	*29061*	
╠═EF ICC		*25*	*25*	
╚═CardIccIdentification		*25*	*25*	
├─clockStop		1	1	{00}
├─cardExtendedSerialNumber		8	8	{00..00}
├─cardApprovalNumber		8	8	{20..20}
├─cardPersonaliserID		1	1	{00}
├─embedderIcAssemblerId		5	5	{00..00}
└─icIdentifier		2	2	{00 00}
╠═EF IC		*8*	*8*	
╚═CardChipIdentification		*8*	*8*	
├─icSerialNumber		4	4	{00..00}
└─icManufacturingReferences		4	4	{00..00}
╚═DF Tachograph		*11055*	*29028*	
╠═EF Application_Identification		*11*	*11*	
╚═WorkshopCardApplicationIdentification		*11*	*11*	
├─typeOfTachographCardId		1	1	{00}
├─cardStructureVersion		2	2	{00 00}
├─noOfEventsPerType		1	1	{00}
├─noOfFaultsPerType		1	1	{00}
├─activityStructureLength		2	2	{00 00}
├─noOfCardVehicleRecords		2	2	{00 00}
├─noOfCardPlaceRecords		1	1	{00}
└─noOfCalibrationRecords		1	1	{00}

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_409 De onderstaande waarden, die worden gebruikt om de grootte in de bovenstaande tabel aan te geven, zijn de laagste en hoogste waarden van het aantal registraties dat de gegevensstructuur van de werkplaatskaart moet gebruiken:

		Min	Max
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_6	CardActivityLengthRange	88	255
n_5	NoOfCalibrationRecords	198 bytes (1 dag * 93 wijzigingen van activiteiten)	492 bytes (1 dag * 240 wijzigingen van activiteiten)

4.3. **Structuur van de controlekaart**

TCS_410 Na personalisatie moet de controlekaart de onderstaande permanente bestandsstructuur en bestandstoegangscondities hebben:

		Toegangscondities		
Bestand	ID van bestand	Lezen	Bijwerken	Gecodeerd
MF	3F00			
├─EF ICC	0002	ALW	NEV	Nee
├─EF IC	0005	ALW	NEV	Nee
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	Nee
├─EF Card_Certificate	C100	ALW	NEV	Nee
├─EF CA_Certificate	C108	ALW	NEV	Nee
├─EF Identification	0520	AUT	NEV	Nee
└─EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	Nee

TCS_411 Alle EF-structuren moeten transparant zijn.

TCS_412 Lezen met beveiligde berichtenuitwisseling moet voor bestanden in het DF Tachograaf mogelijk zijn.

TCS_413 De controlekaart moet de onderstaande gegevensstructuur hebben:

Bestand/gegevenselement	Aantal registraties	Grootte (Bytes) Min	Grootte (Bytes) Max	Standaardwaarden
MF		*11219*	*24559*	
├EF ICC		*25*	*25*	
│└CardIccIdentification		*25*	*25*	
│ ├clockStop		1	1	{00}
│ ├cardExtendedSerialNumber		8	8	{00..00}
│ ├cardApprovalNumber		8	8	{20..20}
│ ├cardPersonaliserID		1	1	{00}
│ ├embedderIcAssemblerId		5	5	{00..00}
│ └icIdentifier		2	2	{00 00}
├EF IC		*8*	*8*	
│└CardChipIdentification		*8*	*8*	
│ ├icSerialNumber		4	4	{00..00}
│ └icManufacturingReferences		4	4	{00..00}
└DF Tachograph		*11186*	*24526*	
├EF Application_Identification		*5*	*5*	
│└ControlCardApplicationIdentification		*5*	*5*	
│ ├typeOfTachographCardId		1	1	{00}
│ ├cardStructureVersion		2	2	{00 00}
│ └noOfControlActivityRecords		2	2	{00 00}
├EF Card_Certificate		*194*	*194*	
│└CardCertificate		194	194	{00..00}
├EF CA_Certificate		*194*	*194*	
│└MemberStateCertificate		194	194	{00..00}
├EF Identification		*211*	*211*	
│├CardIdentification		*65*	*65*	
││ ├cardIssuingMemberState		1	1	{00}
││ ├cardNumber		16	16	{20..20}
││ ├cardIssuingAuthorityName		36	36	{00, 20..20}
││ ├cardIssueDate		4	4	{00..00}
││ ├cardValidityBegin		4	4	{00..00}
││ └cardExpiryDate		4	4	{00..00}
│└ControlCardHolderIdentification		*146*	*146*	
│ ├controlBodyName		36	36	{00, 20..20}
│ ├controlBodyAddress		36	36	{00, 20..20}
│ ├cardHolderName				
│ │├holderSurname		36	36	{00, 20..20}
│ │└holderFirstNames		36	36	{00, 20..20}
│ └cardHolderPreferredLanguage		2	2	{20 20}
└EF Controller_Activity_Data		*10582*	*23922*	
└ControlCardControlActivityData		*10582*	*23922*	
├controlPointerNewestRecord		2	2	{00 00}
└controlActivityRecords		*10580*	*23920*	
└controlActivityRecord	n_7	*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlledCardNumber				
│├cardType		1	1	{00}
│├cardIssuingMemberState		1	1	{00}
│└cardNumber		16	16	{20..20}
├controlledVehicleRegistration				
│├vehicleRegistrationNation		1	1	{00}
│└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}

TCS_414 De onderstaande waarden, die worden gebruikt om de grootte in de bovenstaande tabel aan te geven, zijn de laagste en hoogste waarden van het aantal registraties dat de gegevensstructuur van de controlekaart moet gebruiken:

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.4. **Structuur van de bedrijfskaart**

TCS_415 Na personalisatie moet de bedrijfskaart de onderstaande permanent bestandsstructuur en bestandstoegangscondities hebben:

Bestand	ID van bestand	Toegangscondities		
		Lezen	Bijwerken	Gecodeerd
MF	3F00			
├─EF ICC	0002	ALW	NEV	Nee
├─EF IC	0005	ALW	NEV	Nee
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	Nee
├─EF Card_Certificate	C100	ALW	NEV	Nee
├─EF CA_Certificate	C108	ALW	NEV	Nee
├─EF Identification	0520	AUT	NEV	Nee
└─EF Company_Activity_Data	050D	ALW	PRO SM / AUT	Nee

TCS_416 Alle EF-structuren moeten transparant zijn.

TCS_417 Lezen met beveiligde berichtenuitwisseling moet voor alle bestanden in het DF Tachograaf mogelijk zijn.

TCS_418 De bedrijfskaart moet de onderstaande gegevensstructuur hebben:

Bestand/gegevenselement	Aantal registraties	Grootte (Bytes) Min	Grootte (Bytes) Max	Standaardwaarden
MF		*11147*	*24487*	
╠═EF ICC		*25*	*25*	
╚═CardIccIdentification		*25*	*25*	
├─clockStop		1	1	{00}
├─cardExtendedSerialNumber		8	8	{00..00}
├─cardApprovalNumber		8	8	{20..20}
├─cardPersonaliserID		1	1	{00}
├─embedderIcAssemblerId		5	5	{00..00}
└─IcIdentifier		2	2	{00 00}
╠═EF IC		*8*	*8*	
╚═CardChipIdentification		*8*	*8*	
├─IcSerialNumber		4	4	{00..00}
└─IcManufacturingReferences		4	4	{00..00}
╚═DF Tachograph		*11114*	*24454*	
╠═EF Application_Identification		*5*	*5*	
╚═CompanyCardApplicationIdentification		*5*	*5*	
├─typeOfTachographCardId		1	1	{00}
├─cardStructureVersion		2	2	{00 00}
└─noOfCompanyActivityRecords		2	2	{00 00}
╠═EF Card_Certificate		*194*	*194*	
╚═CardCertificate		194	194	{00..00}
╠═EF CA_Certificate		*194*	*194*	
╚═MemberStateCertificate		194	194	{00..00}
╠═EF Identification		*139*	*139*	
├─CardIdentification		*65*	*65*	
├─cardIssuingMemberState		1	1	{00}
├─cardNumber		16	16	{20..20}
├─cardIssuingAuthorityName		36	36	{00, 20..20}
├─cardIssueDate		4	4	{00..00}
├─cardValidityBegin		4	4	{00..00}
└─cardExpiryDate		4	4	{00..00}
└─CompanyCardHolderIdentification		*74*	*74*	
├─companyName		36	36	{00, 20..20}
├─companyAddress		36	36	{00, 20..20}
└─cardHolderPreferredLanguage		2	2	{20 20}
╚═EF Company_Activity_Data		*10582*	*23922*	
└─CompanyActivityData		*10582*	*23922*	
├─companyPointerNewestRecord		2	2	{00 00}
└─companyActivityRecords		*10580*	*23920*	
└─companyActivityRecord	n_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}

├─cardNumberInformation			
│ ├─cardType	1	1	{00}
│ ├─cardIssuingMemberState	1	1	{00}
│ └─cardNumber	16	16	{20..20}
├─downloadPeriodBegin	4	4	{00..00}
└─downloadPeriodEnd	4	4	{00..00}

TCS_419 De onderstaande waarden, die worden gebruikt om de grootte in de bovenstaande tabel aan te geven, zijn de laagste en hoogste waarden van het aantal registraties dat de gegevensstructuur van de bedrijfskaart moet gebruiken:

		Min	Max
ng	NoOfCompanyActivityRecords	230	520

Appendix 3

PICTOGRAMMEN

PIC_001 Het controleapparaat kan de onderstaande pictogrammen en pictogramcombinaties gebruiken:

1. BASISPICTOGRAMMEN

	Mensen	**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	Rijtijdperiode
	Rusten	Lopende rustperiode
	Werken	Lopende werkperiode
	Onderbreking	Cumulatieve periode van onderbreking
?	Onbekend	

	Inrichting	**Functies**
1	Lezer van de bestuurder	
2	Lezer van de bijrijder	
	Kaart	
	Uurwerk	
	Leesvenster	Visuele weergave
	Externe opslag	Overdracht
	Stroomvoorziening	
	Printer/afdruk	Afdrukken
	Opnemer	
	Bandenmaat	
	Voertuig/voertuigunit	

	Specifieke omstandigheden
OUT	Niet verplicht
	Vervoer per veerboot/trein

	Diversen		
!	Voorvallen		Fouten
	Begin van de dagelijkse werkperiode		Einde van de dagelijkse werkperiode
	Plaats	M	Handmatige invoer van werkzaamheden van de bestuurder
	Beveiliging		Snelheid
	Tijdsaanduiding	Σ	Totaal/overzicht

	Kwalificerende elementen
24h	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+	Begin Niet verplicht	+OUT	Einde buiten bereik

Kaarten

Bestuurderskaart
Bedrijfskaart
Controlekaart
Werkplaatskaart
Geen kaart

Rijden

Rijden met een ploeg
Rijtijd van een week
Rijtijd van twee weken

Afdrukken

Dagelijkse afdruk van de kaart van de activiteiten van de bestuurder
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
Afdruk van technische gegevens
Afdruk van snelheidsoverschrijding

Voorvallen

Inbrengen van een ongeldige kaart
Kaartconflict
Tijdsoverlapping
Rijden zonder geschikte kaart
Inbrengen van kaart tijdens het rijden
Laatste kaartsessie niet correct afgesloten
Snelheidsoverschrijding
Onderbreking in stroomvoorziening
Fout in de bewegingsgegevens
Poging tot inbreuk op de beveiliging
Tijdafstelling (door werkplaats)
Controle op snelheidsoverschrijding

Fouten

Kaartfout (lezer van de bestuurder)
Kaartfout (lezer van de bijrijder)
Leesvensterfout
Overbrengingsfout
Printerfout
Fout in de opnemer
Interne fout in de VU

Procedure bij handmatige invoer

Nog steeds 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: Additionele pictogramcombinaties voor het vormen van een afdrukblok of registratie-identificatiemiddelen worden in appendix 4 gedefinieerd.

Appendix 4

AFDRUKKEN

INHOUD

1. Algemeen 131
2. Specificatie van gegevensblokken 131
3. Afdrukspecificaties 137
3.1. Dagelijkse afdruk van de de kaart met de activiteiten van de bestuurder 138
3.2. Dagelijkse afdruk van de VU met de activiteiten van de bestuurder 138
3.3. Afdruk van de kaart met voorvallen en fouten 139
3.4. Afdruk van de VU met voorvallen en fouten 139
3.5. Afdruk van technische gegevens 140
3.6. Afdruk van snelheidsoverschrijding 140

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 record-identificatiesymbool.

PRT_001 Wanneer een blokidentificatiesymbool onmiddellijk voorafgaat aan een record-identificatiesymbool, wordt het record-identificatiesymbool niet afgedrukt.

PRT_002 Als een gegevensbestanddeel onbekend is, of niet afgedrukt moet worden uit hoofde van gegevenstoegangsrechten, worden in plaats daarvan spaties afgedrukt.

PRT_003 Indien de inhoud van een volledige regel onbekend is, of niet afgedrukt hoeft te worden, dan 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).

2. SPECIFICATIE VAN GEGEVENSBLOKKEN

In dit hoofdstuk worden de onderstaande opmaakcriteria gehanteerd:

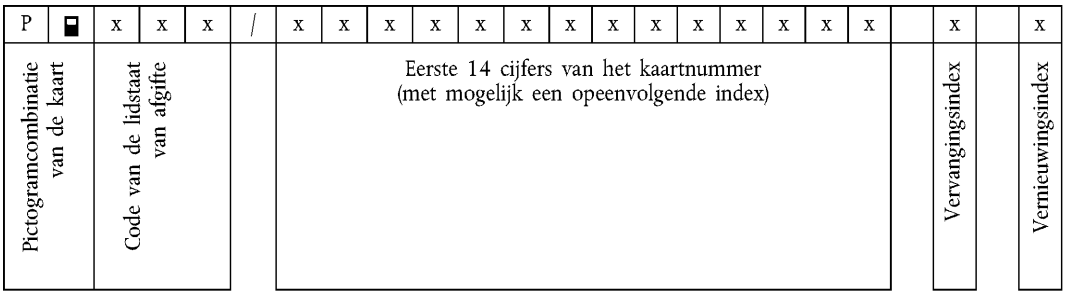
— **vet** gedrukte letters geven standaardtekst aan die afgedrukt moet worden (afdrukken geschiedt in standaardletters);

— standaardletters geven variabelen aan (pictogrammen of gegevens) die door hun afdrukwaarden moeten worden vervangen;

— namen van variabelen zijn onderstreept om de lengte van het gegevenbestanddeel die voor de variabele ter beschikking is, te tonen;

— data worden in de vorm van „dd/mm/jjjj" (dag, maand, jaar) gespecificeerd. 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:



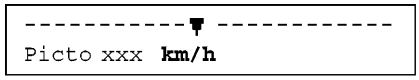
PRT_006 Afdrukken moeten de onderstaande gegevensblokken en/of gegevensrecords overeenkomstig de onderstaande betekenissen en opmaak gebruiken:

Blok- of recordnummer Betekenis	Data Format
1 **Datum en tijd waarop het document wordt afgedrukt**	dd/mm/jjjj hh:mm **(UTC)**

2 **Soort afdruk**

Blokidentificatiesymbool

Afdruk pictogramcombinatie (zie appendix 3), instelling snelheidsbegrenzer (alleen afdruk snelheidsoverschrijding)



3 **Identificatie van de kaarthouder**

Blokidentificatiesymbool. P = pictogram voor personen

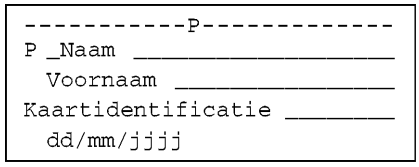
Naam van de kaarthouder

Voornaam van de kaarthouder (indien van toepassing)

Kaartidentificatie

Vervaldatum van de kaart (indien van toepassing)

Als de kaart geen persoonlijke kaart is en de achternaam van de kaarthouder niet hoeft te worden vermeld, moet de naam van het bedrijf of de werkplaats of die van de controle-instantie worden afgedrukt.

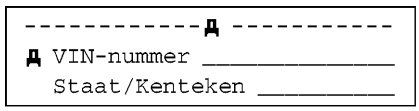


4 **Voertuigidentificatie**

Blokidentificatiesymbool

VIN-nummer

Lidstaat van registratie en kenteken

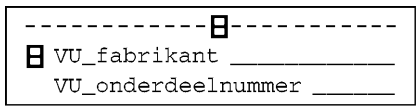


5 **VU-identificatie**

Blokidentificatiesymbool

Naam van fabrikant van VU

Onderdeelnummer van VU



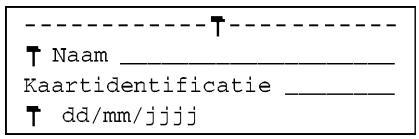
6 **Laatste kalibrering van het controleapparaat**

Blokidentificatiesymbool

Naam van de werkplaats

Identificatie van de werkplaatskaart

Datum van de kalibrering



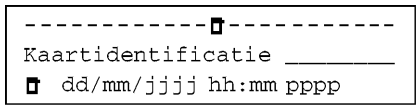
7 **Laatste controle (door een controleur)**

Blokidentificatiesymbool

Identificatie van de controleurskaart

Datum, tijd en type van de controle

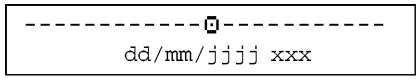
Type controle: Maximaal vier pictogrammen. Het type controle kan (een combinatie) zijn (van):
: Kaartoverdacht, : VU-overdracht, : Afdrukken, : Visuele weergave



8 **Activiteiten van de bestuurder die in volgorde van optreden op een kaart opgeslagen zijn**

Blokidentificatiesymbool

Onderzoeksdatum (kalenderdag van de afdruk) + Dagelijkse aanwezigheidsteller van de kaart



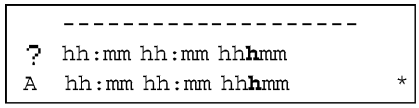
8.1 *Periode waarin de kaart niet ingebracht was*

8.1a Record-identificatiesymbool (begin van de periode)

8.1b *Onbekende periode*. Begin- en eindtijd, duur

8.1c *Handmatig ingevoerde activiteit*

Pictogram van de activiteit, begin- en eindtijd (inclusief), duur, rusttijden van ten minste een uur worden gelabeld met een sterretje.



8.2 *Kaartinbrenging in lezer S*

Record-identificatiesymbool; S = Lezerpictogram

Registerende lidstaat van het voertuig en kenteken

Kilometerstand van het voertuig bij kaartinbrenging

```
----------S----------
Staat/Kenteken _______
x xxx xxx km
```

8.3 *Activiteit (terwijl de kaart ingebracht was)*

Pictogram van de activiteit, begin- en eindtijd (inclusief), duur, status van de bemanning (bemanningspictogram bij PLOEG, spaties bij ALLEEN), rusttijden van ten minste een uur worden gelabeld met een sterretje.

```
A hh:mm hh:mm hhhmm OO      *
```

8.3a *Specifieke omstandigheid*. Tijd van invoer, pictogram van specifieke omstandigheid (of pictogramcombinatie).

```
hh:mm ----- pppp -----
```

8.4 *Kaartuitneming*

Kilometerstand van het voertuig en afgelegde afstand sinds de laatste inbrenging waarvan de kilometerstand bekend is

```
x xxx xxx km; x xxx km
```

9 **Activiteiten van de bestuurder in chronologische volgorde opgeslagen in een VU per lezer**

Blokidentificatiesymbool

Onderzoeksdatum (kalenderdag van de afdruk)

Kilometerstand van het voertuig om 00:00 en 24:00

```
-----------O-----------
        dd/mm/jjjj
x xxx xxx - x xxx xxx km
```

10 **Activiteiten overgedragen naar lezer S**

Blokidentificatiesymbool

```
---------- S ----------
```

10.1 *Periode waarin geen kaart in lezer S ingebracht is*

Record-identificatiesymbool

Geen kaart ingebracht

Kilometerstand van het voertuig aan het begin van de periode

```
--------------------
O --
x xxx xxx km
```

10.2 *Kaartinbrenging*

Record-identificatiesymbool van kaartinbrenging

Naam van de bestuurder

Voornaam van de bestuurder

Identificatie van de bestuurderskaart

Vervaldatum van de bestuurderskaart

Lidstaat van registratie en kenteken van het vorige gebruikte voertuig

Datum en tijd van kaartuitneming bij het vorige voertuig

Witregel

Kilometerstand van het voertuig bij kaartinbrenging, handmatige invoer van label van activiteiten van de bestuurder (M indien ja, spatie indien nee).

```
--------------------
O Naam _____________________
  Voornaam _________________
Kaartidentificatie _________
  dd/mm/jjjj
Staat/Kenteken _____________

  dd/mm/jjjj hh:mm


  x xxx xxx km              M
```

10.3 *Activiteit*

Activiteitspictogram, begin- en eindtijd (inclusief), duur, status van de bemanning (ploegpictogram indien met een PLOEG, spatie indien ALLEEN), rusttijden van ten minste een uur worden gelabeld met een sterretje.

```
A hh:mm hh:mm hhhmm OO      *
```

10.3a *Specifieke omstandigheid*. Tijd van invoer, pictogram van specifieke omstandigheid (of pictogramcombinatie).

```
hh:mm ----- pppp -----
```

10.4 *Kaartuitneming of einde van een „geen kaart"-periode*

Kilometerstand van het voertuig bij kaartuitneming of aan het einde van een „geen kaart"-periode en afgelegde afstand sinds inbrenging, of sinds het begin van de „geen kaart"-periode.

```
x xxx xxx km; x xxx km
```

11 **Dagelijks overzicht**

Blokidentificatiesymbool

```
----------Σ ---------
```

11.1 *VU-overzicht van perioden zonder kaart in de lezer van de bestuurder*

Blokidentificatiesymbool

```
10■ - - -
```

11.2 *VU-overzicht van perioden zonder kaart in de lezer van de bijrijder*

Blokidentificatiesymbool

```
20■ - - -
```

11.3 *Dagelijks overzicht van de VU per bestuurder*

Record-identificatiesymbool

Naam van de bestuurder

Voornaam van de bestuurder

Identificatie van de bestuurderskaart

```
--------------------
0 Naam _____________________
  Voornaam _________________
Kaartidentificatie ________
```

11.4 *Invoer van de plaats waar de dagelijkse werkperiode begint en/of eindigt*

pi = begin/einde-plaatspictogram, tijd, land, regio,

Kilometerstand

```
pihh:mm  Cou  Reg
  x xxx  xxx  km
```

11.5 *Totaal van de activiteiten (van een kaart)*

Totale rijtijd, afgelegde afstand

Totale duur van werken en beschikbaarheid

Totale duur van rusttijden en onbekende perioden

Totale duur van activiteiten van de bemanning

```
0 hhhmm x xxx km
⚒ hhhmm ⧈ hhhmm
⊢ hhhmm ? hhhmm
00 hhhmm
```

11.6 *Totaal van de activiteiten (perioden zonder kaart in de lezer van de bestuurder)*

Totale rijtijd, afgelegde afstand

Totale duur van werken en beschikbaarheid

Totale duur van rusttijden

```
0 hhhmm x xxx km
⚒ hhhmm ⧈ hhhmm
⊢ hhhmm
```

11.7 *Totaal van de activiteiten (perioden zonder kaart in de lezer van de bijrijder)*

Totale duur van werken en beschikbaarheid

Totale duur van rusttijden

```
⚒ hhhmm ⧈ hhhmm
⊢ hhhmm
```

11.8 *Totaal van de activiteiten (per bestuurder van beide lezers)*

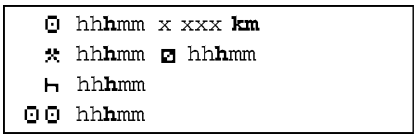
Totale rijtijd, afgelegde afstand

Totale duur van werken en beschikbaarheid

Totale duur van rusttijden

Totale duur van activiteiten van de bemanning

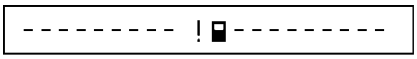
Wanneer een dagelijkse afdruk voor de lopende dag vereist is, wordt de dagelijkse overzichtsinformatie aan de hand van de beschikbare gegevens op het tijdstip van afdrukken berekend.



12 **Op een kaart opgeslagen voorvallen en/of fouten**

12.1 Blokidentificatiesymbool laatste 5 „Voorvallen en Fouten" van een kaart

12.2 Blokidentificatiesymbool alle geregistreerde „Voorvallen" op een kaart



12.3 Blokidentificatiesymbool alle geregistreerde „Fouten" op een kaart

12.4 *Voorval-record en/of fout-record*

Record-identificatiesymbool

Voorval/foutpictogram, doel van het record, datum en tijd van begin

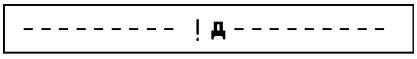
(eventuele) Additionele voorval/foutcode, duur

Lidstaat van registratie en kentekennummer van het voertuig waarin het voorval of de fout optrad

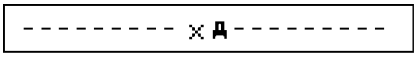
13 **In een VU opgeslagen of aanhoudende voorvallen en/of fouten**

13.1 Blokidentificatiesymbool laatste 5 „Voorvallen en Fouten" van een VU

13.2 Blokidentificatiesymbool alle geregistreerde of aanhoudende „Voorvallen" in een VU



13.3 Blokidentificatiesymbool alle geregistreerde of aanhoudende „Fouten" in een VU



13.4 *Voorval-record en/of fout-record*

Record-identificatiesymbool

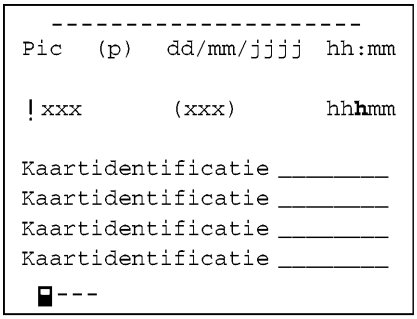
Voorval-/foutpictogram, doel van het record, datum en tijd van begin

(eventuele) Additionele voorval-/foutcode, aantal vergelijkbare voorvallen op die dag, duur

Identificatie van de kaarten die bij begin en einde van het voorval of de fout ingebracht zijn (maximaal 4 regels zonder hetzelfde kaartnummer te herhalen)

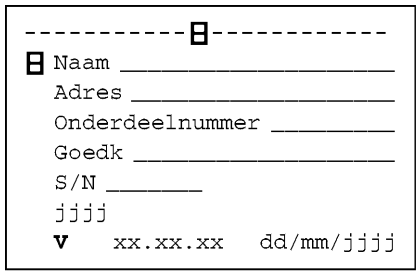
Geval waarin geen kaart ingebracht was

Het doel van het record (p) is een numerieke code die verklaart waarom het voorval of de fout geregistreerd werd, gecodeerd overeenkomstig het gegevensbestanddeel `VoorvalFoutRecordDoel`.



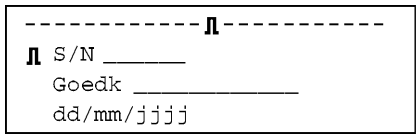
14 **VU-identificatie**

Blokidentificatiesymbool
Naam van de fabrikant van de VU
Adres van de fabrikant van de VU
Onderdeelnummer VU
Goedkeuringsnummer VU
Serienummer VU
Bouwjaar van de VU
Softwareversie van de VU en installatiedatum



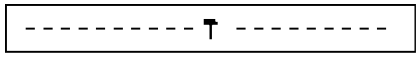
15 **Identificatie van de opnemer**

Blokidentificatiesymbool
Serienummer van de opnemer
Goedkeuringsnummer van de opnemer
Datum van eerste installatie van de opnemer



16 **Kalibreringsgegevens**

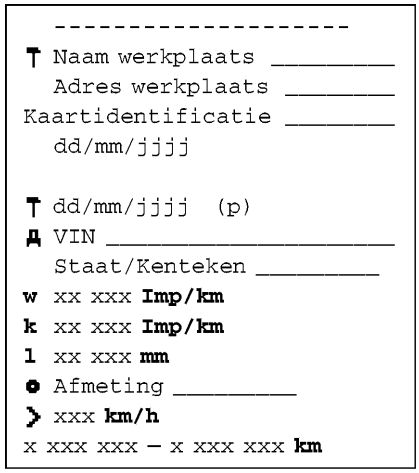
Blokidentificatiesymbool



16.1 *Kalibreringsrecord*

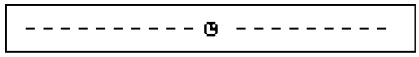
Record-identificatiesymbool
Werkplaats die de kalibrering heeft uitgevoerd
Adres van de werkplaats
Identificatie van de werkplaatskaart
Vervaldatum van de werkplaatskaart
Witregel
Kalibreringsdatum + kalibreringsdoel
VIN-nummer
Lidstaat van registratie en kenteken
Kenmerkende coëfficiënt van het voertuig
Constante van het controleapparaat
Effectieve omtrek van de wielbanden
Maat van gemonteerde banden
Instelling van de snelheidsbegrenzer
Oude en nieuwe kilometerstand

Het kalibreringsdoel (p) is een numerieke code die verklaart waarom deze kalibreringsparameters geregistreerd werden, gecodeerd overeenkomstig het gegevensbestanddeel `KalibreringDoel`.



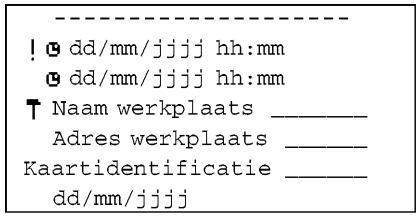
17 **Tijdafstelling**

Blokidentificatiesymbool



17.1 *Tijdafstellingsrecord*

Record-identificatiesymbool
Oude datum en tijd
Nieuwe datum en tijd
Werkplaats die de tijdafstelling heeft uitgevoerd
Adres van de werkplaats
Identificatie van de werkplaatskaart
Vervaldatum van de werkplaatskaart



18 **Meest recent(e) in de VU geregistreerd(e) voorval en fout**

Blokidentificatiesymbool

Datum en tijd meest recent voorval

Datum en tijd meest recente fout

```
----------!×A----------
!  dd/mm/jjjj  hh:mm
×  dd/mm/jjjj  hh:mm
```

19 **Informatie over controle snelheidsoverschrijding**

Blokidentificatiesymbool

Datum en tijd laatste CONTROLE SNELHEIDSOVERSCHRIJDING

Datum/tijd van eerste snelheidsoverschrijving en aantal snelheidsoverschrijdingen sindsdien

```
-----------›› ----------
›▯ dd/mm/jjjj  hh:mm
›› dd/mm/jjjj hh:mm (nnn)
```

20 **Snelheidsoverschrijdingsrecord**

20.1 Blokidentificatiesymbool „Eerste snelheidsoverschrijding na de laatste kalibrering”

```
-------- ››T --------
```

20.2 Blokidentificatiesymbool „De 5 grootste gedurende de afgelopen 365 dagen”

```
------- ››(365)-------
```

20.3 Blokidentificatiesymbool „De grootste voor elk van de laatste 10 dagen waarop snelheidsoverschrijding plaatsvond”

```
------- ››(10) -------
```

20.4 Record-identificatiesymbool

Datum, tijd en duur

Gemiddelde en maximumsnelheid, aantal vergelijkbare voorvallen op die dag

Naam van de bestuurder

Voorna(a)m(en) van de bestuurder

Identificatie van de bestuurderskaart

```
   ------------------
›› dd/mm/jjjj hh:mm hhhmm
   xxx km/h xxx km/h (xxx)
⊙  Naam _____________________
   Voornaam _________________
Kaartidentificatie ________
```

20.5 Indien geen snelheidsoverschrijdingsrecord in een blok aanwezig is

```
›› - - -
```

21 **Geschreven informatie**

Blokidentificatiesymbool

21.1 Plaats van controle

21.2 Handtekening van de controleur

21.3 Van tijdstip

21.4 Tot tijdstip

21.5 Handtekening van de bestuurder

„Geschreven informatie”; Voeg voldoende witregels boven een geschreven rubriek in om de vereiste informatie te kunnen noteren of een handtekening te kunnen zetten.

```
------------------------
▯●  ....................
▯   ....................
◷+  ....................
+◷  ....................
⊙   ....................
```

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 activiteiten van de bestuurder**

PRT_007 De dagelijkse afdruk van de kaart met de activiteiten van de bestuurder moet in overeenstemming zijn met onderstaande opmaak:

1	Datum en tijd waarop het document wordt afgedrukt
2	Soort afdruk
3	Identificatie van de controleur (indien een controlekaart in de VU ingebracht is)
3	Identificatie van de bestuurder (van de kaart waarvan de afdruk gemaakt wordt)
4	VIN-nummer (voertuig waarvan de afdruk gemaakt wordt)
5	VU-identificatie (VU waarvan de afdruk gemaakt wordt)
6	Laatste kalibrering van deze VU
7	Laatste controle waaraan de gecontroleerde bestuurder werd onderworpen
8	Begrenzer van de activiteiten van de bestuurder
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Activiteiten van de bestuurder in volgorde van uitvoering
11	Begrenzer van dagelijkse overzichten
11.4	Plaatsen ingevoerd in chronologische volgorde
11.5	Totaal van de activiteiten
12.1	Voorvallen of fouten van de begrenzer van de kaart
12.4	Voorval-records/fout-records (de 5 laatste op de kaart opgeslagen voorvallen of fouten)
13.1	Voorvallen of fouten van de begrenzer van de VU
13.4	Voorval-records/fout-records (de laatste 5 in de VU opgeslagen of aanhoudende voorvallen of fouten)
21.1	Controleplaats
21.2	Handtekening van de controleur
21.5	Handtekening van de bestuurder

3.2. **Dagelijkse afdruk van de VU met de activiteiten van de bestuurder**

PRT_008 De dagelijkse afdruk van de VU van de activiteiten van de bestuurder moet in overeenstemming zijn met onderstaande opmaak:

1	Datum en tijd waarop het document afgedrukt wordt
2	Soort afdruk
3	Identificatie van de kaarthouder (voor alle in de VU ingebrachte kaarten)
4	VIN-nummer (voertuig waarvan de afdruk gemaakt wordt)
5	VU-identificatie (VU waarvan de afdruk wordt gemaakt)
6	Laatste kalibrering van deze VU
7	Laatste controle van dit controleapparaat
9	Begrenzer van de activiteiten van de bestuurder
10	Begrenzer van de lezer van de bestuurder (lezer 1)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Activiteiten in chronologische volgorde (lezer van de bestuurder)
10	Begrenzer van de lezer van de bijrijder (lezer 2)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Activiteiten in chronologische volgorde (lezer van de bijrijder)
11	Begrenzer van dagelijkse overzichten
11.1	Overzicht van perioden zonder kaart in de lezer van de bestuurder
11.4	Plaatsen ingevoerd in chronologische volgorde
11.6	Totaal van de activiteiten

11.2	Overzicht van perioden zonder kaart in de lezer van de bijrijder	
11.4	Plaatsen ingevoerd in chronologische volgorde	
11.7	Totaal van de activiteiten	
11.3	Overzicht van activiteiten van een bestuurder van beide lezers	
11.4	Plaatsen ingevoerd door deze bestuurder in chronologische volgorde	
11.7	Totaal van de activiteiten van deze bestuurder	
13.1	Begrenzer voorvallen fouten	
13.4	Voorval-records/fout-records (de laatste 5 in de VU opgeslagen of aanhoudende voorvallen of fouten)	
21.1	Controleplaats	
21.2	Handtekening van de controleur	
21.3	Van tijdstip	(ruimte waarin een bestuurder die geen kaart heeft, kan aangeven welke perioden op hem betrekking hebben)
21.4	Tot tijdstip	
21.5	Handtekening van de bestuurder	

3.3. **Afdruk van de kaart met voorvallen en fouten**

PRT_009 De afdruk van de kaart met voorvallen en fouten moet in overeenstemming zijn met onderstaande opmaak:

1	Datum en tijd waarop het document afgedrukt wordt
2	Soort afdruk
3	Identificatie van de controleur (indien een controlekaart in de VU ingebracht is)
3	Identificatie van de bestuurder (van de kaart waarvan de afdruk gemaakt wordt)
4	VIN-nummer (voertuig waarvan de afdruk gemaakt wordt)
12.2	Begrenzer van voorvallen
12.4	Voorval-records (alle op de kaart opgeslagen voorvallen)
12.3	Foutenbegrenzer
12.4	Fout-records (alle op de kaart opgeslagen fouten)
21.1	Controleplaats
21.2	Handtekening van de controleur
21.5	Handtekening van de bestuurder

3.4. **Afdruk van de VU met voorvallen en fouten**

PRT_010 De afdruk van de VU met voorvallen en fouten moet in overeenstemming zijn met onderstaande opmaak:

1	Datum en tijd waarop het document afgedrukt wordt
2	Soort afdruk
3	Identificatie van de kaarthouder (voor alle in de VU ingebrachte kaarten)
4	VIN-nummer (voertuig waarvan de afdruk gemaakt wordt)
13.2	Begrenzer van voorvallen
13.4	Voorval-records (alle in de VU opgeslagen of aanhoudende voorvallen)
13.3	Begrenzer van fouten
13.4	Fout-records (alle in de VU opgeslagen of aanhoudende fouten)
21.1	Controleplaats
21.2	Handtekening van de controleur
21.5	Handtekening van de bestuurder

3.5. **Afdruk van technische gegevens**

PRT_011 De afdruk van technische gegevens moet in overeenstemming zijn met onderstaande opmaak:

1	Datum en tijd waarop het document afgedrukt wordt
2	Soort afdruk
3	Identificatie van de kaarthouder (voor alle in de VU ingebrachte kaarten)
4	VIN-nummer (voertuig waarvan de afdruk gemaakt wordt)
14	VU-identificatie
15	Identificatie van de opnemer
16	Begrenzer van kalibreringsgegevens
16.1	Kalibreringsrecords (alle records in chronologische volgorde)
17	Begrenzer van de tijdafstelling
17.1	Tijdafstellingsrecords (alle records van tijdafstelling en kalibreringsgegevens)
18	Meest recent(e) door de VU geregistreerd(e) voorval en fout

3.6. **Afdruk van snelheidsoverschrijding**

PRT_012 De afdruk van snelheidsoverschrijding moet in overeenstemming zijn met onderstaande opmaak:

1	Datum en tijd waarop het document afgedrukt wordt
2	Soort afdruk
3	Identificatie van de kaarthouder (voor alle in de VU ingebrachte kaarten)
4	VIN-nummer (voertuig waarvan de afdruk gemaakt wordt)
19	Informatie over controle snelheidsoverschrijding
20.1	Identificatiesymbool snelheidsoverschrijdingsgegevens
20.4 / 20.5	Eerste snelheidsoverschrijding na de laatste kalibrering
20.2	Identificatiesymbool snelheidsoverschrijdingsgegevens
20.4 / 20.5	De 5 grootste snelheidsoverschrijdingen gedurende de afgelopen 365 dagen
20.3	Identificatiesymbool snelheidsoverschrijdingsgegevens
20.4 / 20.5	De grootste snelheidsoverschrijding gedurende van de laatste 10 dagen waarop snelheidsoverschrijding plaatsvond
21.1	Controleplaats
21.2	Handtekening van de controleur
21.5	Handtekening van de bestuurder

Appendix 5

LEESVENSTER

In deze appendix worden de onderstaande opmaakcriteria gehanteerd:

— **vet** gedrukte letters geven standaardtekst aan die getoond moet worden (leesvenster blijft in standaardletters);

— standaardletters geven variabelen aan (pictogrammen of gegevens) die bij het tonen ervan door hun waarden moeten worden vervangen:

dd mm jjjj:	dag, maand, jaar,
hh:	uren,
mm:	minuten,
D:	duurpictogram,
EF:	pictogramcombinatie van voorvallen en fouten,
O:	pictogram van de werkingsmodus.

DIS_001 Het controleapparaat moet de gegevens met gebruikmaking van onderstaande opmaak tonen:

Gegevens	Opmaak
Standaardleesvenster	
Plaatselijke tijd	hh:mm
Werkingsmodus	O
Informatie betreffende de bestuurder	1 Dhh**h**mm ▮▮hh**h**mm
Informatie betreffende de bijrijder	2 Dhh**h**mm
„Niet verplicht" -omstandigheid geopend	OUT
Waarschuwingsleesvenster	
Overschrijden van de rijtijdperiode	10 hh**h**mm ▮▮hh**h**mm
Voorval of fout	EF
Overige leesvensters	
UTC-datum Tijd	UTC dd/mm/jjjj of UTC dd.mm.jjjj hh:mm
Rijtijdperiode en cumulatieve rusttijd van de bestuurder	10 hh**h**mm ▮▮hh**h**mm
Rijtijdperiode en cumulatieve rusttijd van de bijrijder	20 hh**h**mm ▮▮hh**h**mm
Cumulatieve rijtijdperiode van de bestuurder in de voorafgaande en de lopende week	10 ▮ hhh**h**mm
Cumulatieve rijtijdperiode van de bijrijder in de voorafgaande en de lopende week	20 ▮ hhh**h**mm

Apendix 6

EXTERNE INTERFACES

INHOUD

1. Hardware 144

1.1. Connector 144

1.2. Contacttoewijzing 146

1.3. Blokschema 146

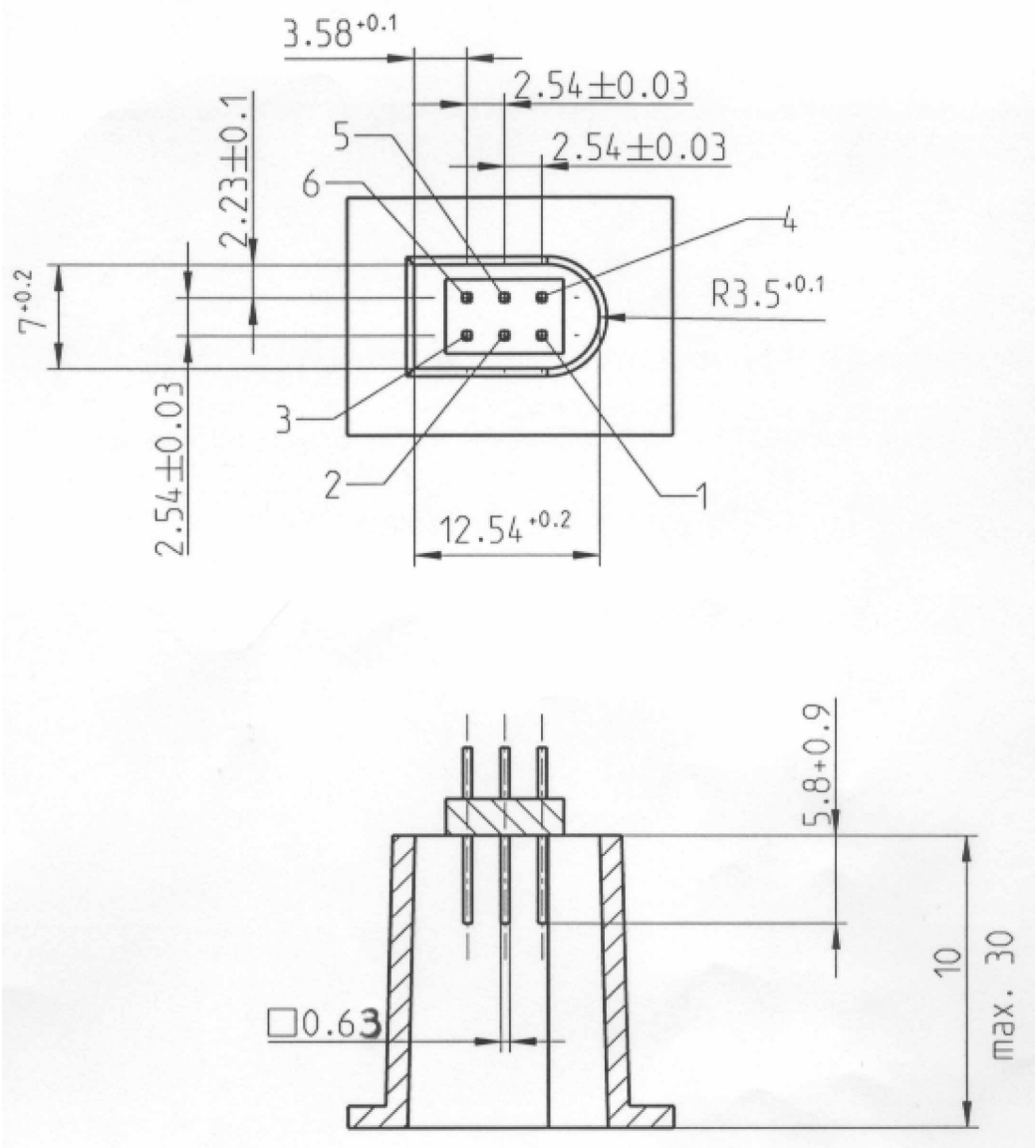
2. Overbrengingsinterface 146

3. Kalibreringsinterface 147

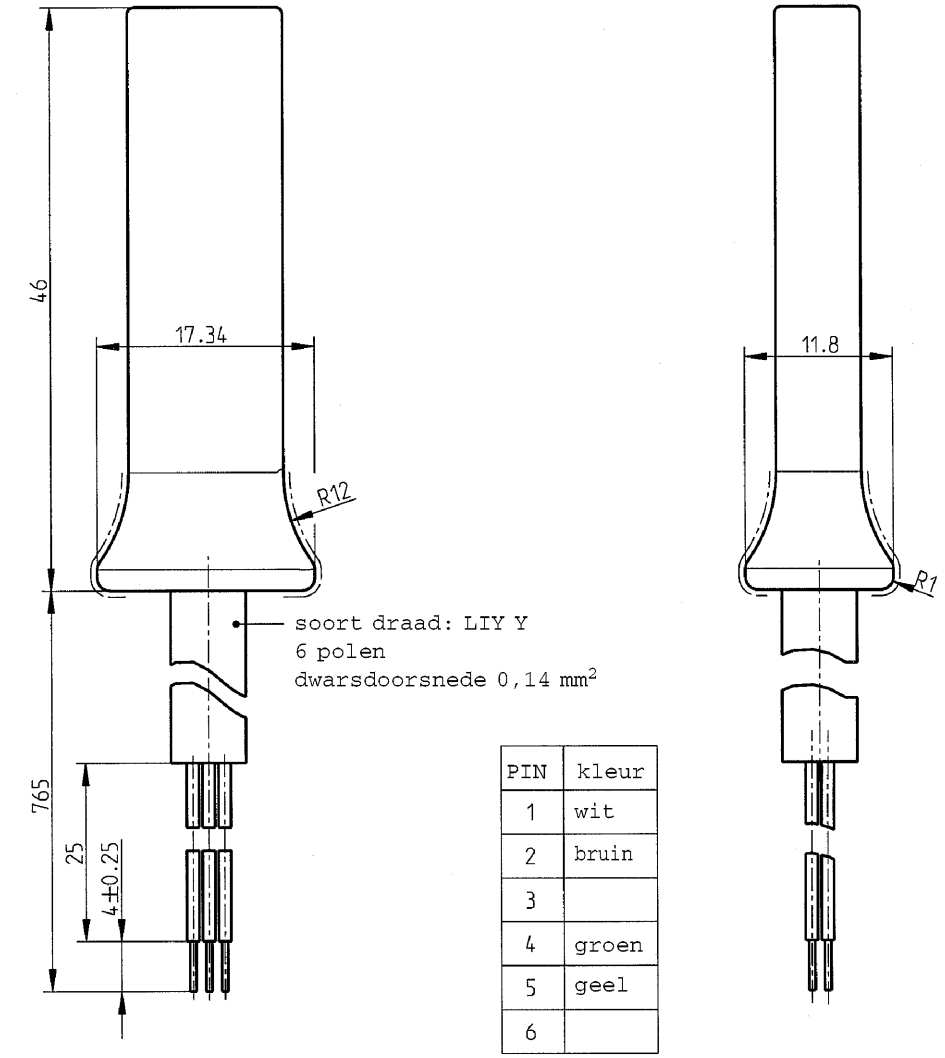
1. HARDWARE

1.1. **Connector**

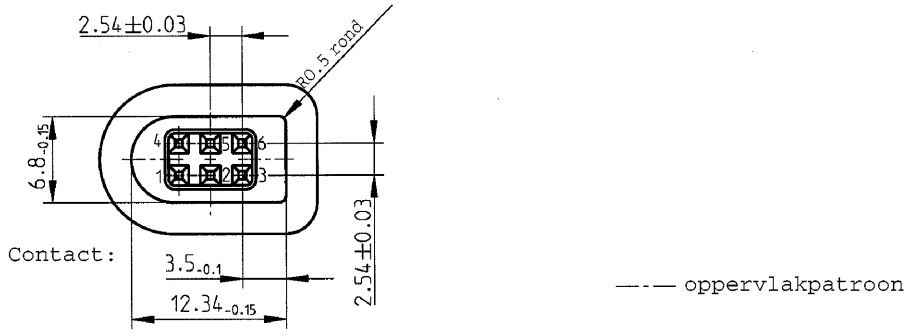
INT_001 De overbrengings-/kalibreringsconnector moet een 6 pins connector zijn die via het frontpaneel toegankelijk is, zonder dat daarvoor delen van het controleapparaat losgekoppeld moeten worden. De connector moet voldoen aan de onderstaande tekening (alle maten in millimeters):



Het onderstaande schema toont een normale 6 pins contrasteker:



PIN	kleur
1	wit
2	bruin
3	
4	groen
5	geel
6	



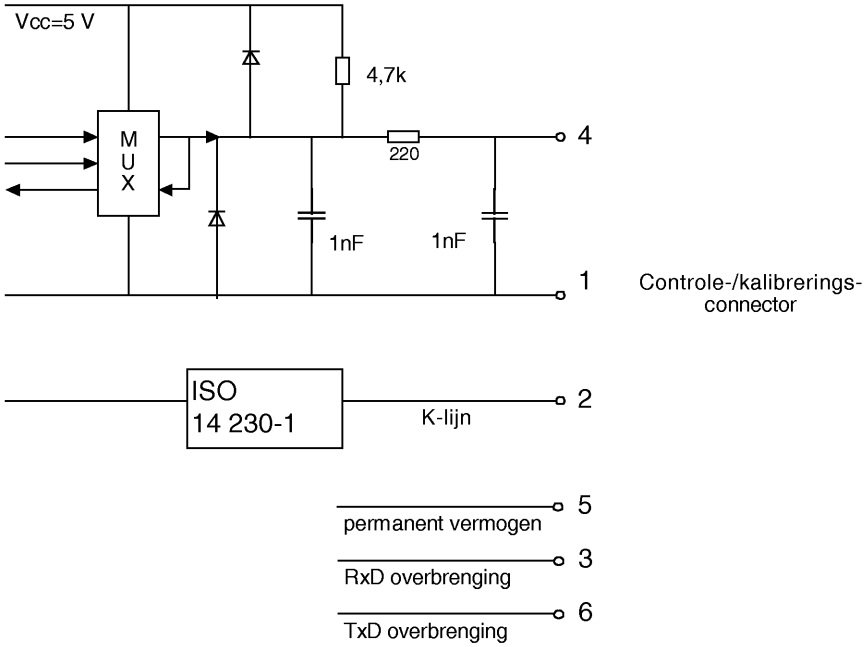
1.2. **Contacttoewijzing**

INT_002 Contacten moeten overeenkomstig de onderstaande tabel worden toegewezen:

Pin	Omschrijving	Opmerking
1	Minpool	Verbonden met de minpool van het voertuig
2	Gegevensoverdracht	K-lijn (ISO 14230-1)
3	RxD — Overbrenging	Gegevensinvoer naar controleapparaat
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 — Overbrenging	Gegevensuitvoer van controleapparaat

1.3. **Blokschema**

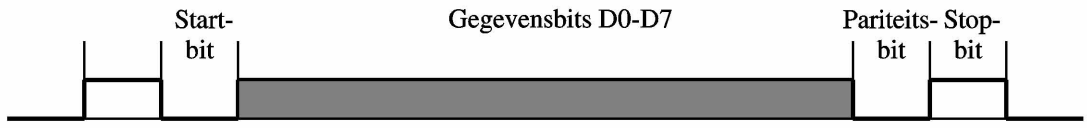
INT_003 Het blokschema moet aan het onderstaande voldoen:



2. OVERBRENGINGSINTERFACE

INT_004 De overbrengingsinterface moet voldoen aan RS232 specificaties.

INT_005 De overbrengingsinterface 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 die uit meer dan een byte bestaan, verzonden worden, wordt de meest significante 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 een communicatiebegin op 9 600 bps moet worden gezet.

3. KALIBRERINGSINTERFACE

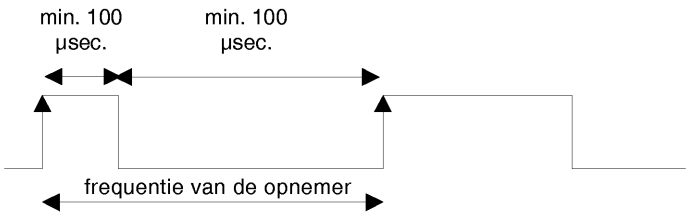
INT_007 De gegevensoverdacht moet voldoen aan ISO 14230-1 Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part 1: Physical layer, First edition: 1999.

INT_008 Het invoer-/uitvoersignaal moet voldoen aan de onderstaande elektrische specificatie:

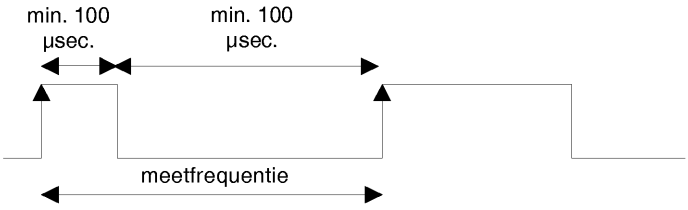
Parameter	Minimum	Normaal	Maximum	Opmerking
U_{laag} (in)			1,0 V	I = 750 µA
U_{hoog} (in)	4 V			I = 200 µA
Frequentie			4 kHz	
U_{laag} (uit)			1,0 V	I = 1 mA
U_{hoog} (uit)	4 V			I = 1 mA

INT_009 Het invoer-/uitvoersignaal moet voldoen aan de onderstaande tijdschema's:

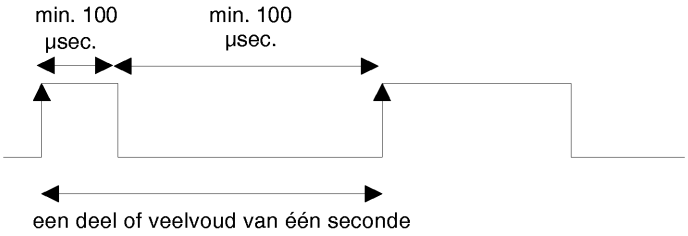
signaal van de opnemer (uit)



meetsignaal (in)



UTC kloksignaal (uit)



Appendix 7

PROTOCOLLEN VOOR GEGEVENSOVERDRACHT

INHOUD

1.	Inleiding	150
1.1.	Toepassingsgebied	150
1.2.	Acroniemen en notaties	150
2.	Gegevensoverdracht van de VU	151
2.1.	Overdrachtprocedure	151
2.2.	Protocol voor gegevensoverdracht	151
2.2.1.	Berichtenstructuur	151
2.2.2.	Berichtensoorten	152
2.2.3.	Berichtenstroom	156
2.2.4.	Timing	157
2.2.5.	Behandeling van fouten	157
2.2.6.	Inhoud van het antwoordbericht	160
2.3.	ESM bestandsopslag	164
3.	Protocol van overdracht van tachograafkaarten	164
3.1.	Toepassingsgebied	164
3.2.	Definities	164
3.3.	Overdracht van de kaart	164
3.3.1.	Initialisatiesequentie	165
3.3.2.	Sequentie voor niet-getekende gegevensbestanden	165
3.3.3.	Sequentie voor getekende gegevensbestanden	165
3.3.4.	Sequentie voor het terugstellen van de kalibreringsteller	166

3.4. Opmaak gegevensopslag 166
3.4.1. Inleiding 166
3.4.2. Bestandsopmaak 166
4. Overbrengen van een tachograafkaart via een voertuigunit 167

1. INLEIDING

Deze appendix specificeert de te volgen procedures voor het uitvoeren van de verschillende soorten gegevensoverdracht 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 worden overgebracht naar een ESM:

— vanuit een voertuigunit door een met de VU verbonden intelligente toepassingsgerichte inrichting (IDE);

— vanaf een tachograafkaart door een met een kaartinterface-inrichting (IFD) uitgeruste IDE;

— vanaf een tachograafkaart via een voertuigunit door een met de VU verbonden IDE.

Teneinde de authenticiteit en integriteit van de overgebrachte, op een ESM opgeslagen gegevens te kunnen verifiëren, worden gegevens met een toegevoegde handtekening overeenkomstig appendix 11 (Algemene beveiligingsinrichtingen) overgebracht. De identificatie van de broninrichting (VU of kaart) en de beveiligingscertificaten (lidstaat en inrichting) worden ook overgebracht. De controleur van de gegevens moet zelf een betrouwbare Europese openbare sleutel in zijn bezit hebben.

DDP_001 De tijdens een overdrachtssessie overgebrachte gegevens moeten in het EMS in één bestand worden opgeslagen.

1.2. **Acroniemen en notaties**

De onderstaande acroniemen worden in deze appendix gebruikt:

AID	Toepassingsidentificatiesymbool
ATR	Antwoord op terugstellen
CS	Controlesombyte
DF	Toepassingsgericht bestand
DS	Diagnostische sessie
EF	Hoofdbestand
ESM	Extern opslagmedium
FID	Bestandsidentificatiesymbool (bestands-ID)
FMT	Opmaakbyte (eerste byte van de koptitel van het bericht)
ICC	IC-kaart
IDE	Intelligente toepassingsgerichte inrichting: de inrichting die wordt gebruikt voor het overbrengen van gegevens naar het ESM (bijv. personal computer)
IFD	Interface-inrichting
KWP	Sleutelwoordprotocol 2000
LEN	Lengtebyte (laatste byte van de koptitel van het bericht)
PPS	Protocol parameterselectie
PSO	Voer beveiligingsoperatie uit
SID	Identificatiesymbool van de dienst
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. **Overdrachtprocedure**

Om een gegevensoverdracht van een VU uit te voeren, moet de operator de onderstaande operaties verrichten:

— zijn tachograafkaart in een kaartlezer van de VU ([1]) inbrengen;

— de IDE met de overdrachtsconnector 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 overdrachtssessie 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, versie 6 van 22 februari 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:

— koptitel bestaande uit een opmaakbyte (FMT), een doelbyte (TGT), een bronbyte (SRC) en mogelijk 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).

Koptitel				Gegevensveld					Controle-som
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 bytes				Max. 255 bytes					1 byte

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.

([1]) De ingebrachte kaart zal de vereiste toegangsrechten met betrekking tot de overdrachtsfunctie en met betrekking tot de gegevens opstarten.

DDP_003 Indien 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 koptitel, hetzelfde SID en 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 foutencontrole 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 voortijdig beëindigen.

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:

Koptitel	SID	TREP	Bericht	CS
4 bytes	Langer dan 255 bytes			

Wordt overgebracht als:

Koptitel	SID	TREP	00	01	Subbericht 1	CS
4 bytes	255 bytes					

Koptitel	SID	TREP	00	02	Subbericht 2	CS
4 bytes	255 bytes					

…

Koptitel	SID	TREP	xx	yy	Subbericht n	CS
4 bytes	Minder dan 255 bytes					

of als:

Koptitel	SID	TREP	00	01	Subbericht 1	CS
4 bytes	255 bytes					

Koptitel	SID	TREP	00	02	Subbericht 2	CS
4 bytes	255 bytes					

…

Koptitel	SID	TREP	xx	yy	Subbericht n	CS
4 bytes	255 bytes					

Koptitel	SID	TREP	xx	yy+1	CS
4 bytes	4 bytes				

2.2.2. ***Berichtensoorten***

Het overdrachtsprotocol voor de gegevensoverdracht tussen de VU en de IDE vereist de uitwisseling van 8 verschillende berichtensoorten.

De onderstaande tabel vat deze berichten samen.

Berichtenstructuur	Max. 4 bytes Koptitel				Max. 255 bytes Gegevens			1 byte Controlesom
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		8F,EA	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	ED
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
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
Transfer Data Request								
Overzicht	80	EE	F0	02	36	01		97
Activiteiten	80	EE	F0	06	36	02	Datum	CS
Voorvallen en fouten	80	EE	F0	02	36	03		99
Gedetailleerde snelheid	80	EE	F0	02	36	04		9A
Technische gegevens	80	EE	F0	02	36	05		9B
Kaartoverbrenging	80	EE	F0	02	36	06		9C
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Gegevens	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Transfer Exit	80	F0	EE	01	77			D6
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Communication	80	F0	EE	01	C2			21
Bevestig subbericht	80	EE	F0	Len	83		Gegevens	CS
Negatieve antwoorden								
Algemene verwerping	80	F0	EE	03	7F	Sid Reg	10	CS
Service niet ondersteund	80	F0	EE	03	7F	Sid Reg	11	CS
Subfunctie niet ondersteund	80	F0	EE	03	7F	Sid Reg	12	CS
Onjuiste berichtlengte	80	F0	EE	03	7F	Sid Reg	13	CS
Voorwaarden niet correct of Verzoeksequentiefout	80	F0	EE	03	7F	Sid Reg	22	CS
Verzoek buiten bereik	80	F0	EE	03	7F	Sid Reg	31	CS
Overbrenging niet geaccepteerd	80	F0	EE	03	7F	Sid Reg	50	CS
Antwoord in behandeling	80	F0	EE	03	7F	Sid Reg	78	CS
Gegevens niet beschikbaar	80	F0	EE	03	7F	Sid Reg	FA	CS

Aantekeningen:
— 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 (overbrenging) (vanaf de IDE) wordt gebruikt voor compatibiliteit met ISO 14229. Het betekent hetzelfde als download (overdracht) (vanaf de VU).
— Potentiële tellers van 2 bytes voor het tellen van subberichten worden in deze tabel niet getoond.

2.2.2.1. *Start Communication Request (Verzoek Start Overdracht) (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 (Positief Antwoord Start Overdracht) (SID C1)*

DDP_006 Dit bericht wordt door de VU verstrekt om positief op een verzoek om de start van de overdracht te antwoorden. Het bevat de 2 sleutelbytes '8F' en 'EA', die aangeven dat de unit het protocol met koptitel inclusief informatie over doel, bron en lengte ondersteunt.

2.2.2.3. *Start Diagnostic Session Request (Verzoek Start Diagnostische Sessie) (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 (Positief Antwoord Start Diagnose) (SID 50)*

DDP_008 Het bericht Positive Response Start Diagnostic wordt door de VU gezonden om positief op Diagnostic Session Request te antwoorden.

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. Dit vindt in twee stappen plaats. 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 (Positief Antwoord Link Control) (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 (Verzoek Overbrenging) (SID 35)*

DDP_009 Het bericht Request Upload wordt door de IDE verstrekt om aan de VU te melden dat een overbrengingsoperatie 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 voor 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 (Positief Antwoord Verzoek Overbrenging) (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 over te brengen. Om aan het vereiste in ISO 14229 te voldoen, worden in dit positieve antwoordbericht gegevens opgenomen die de IDE aangeven dat verdere Positive Response Transfer Data-berichten maximaal 00FF hex bytes zullen bevatten.

2.2.2.9. *Transfer Data Request (Verzoek Gegevensoverdracht) (SID 36)*

DDP_011 Het Transfer Data Request wordt door de IDE gezonden om de VU de soort over te brengen gegevens mede te delen. 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),

— kaartoverbrenging (TRTP 06).

DDP_054 De IDE is verplicht gedurende een overbrengingssessie de overdracht van overzichtsgegevens (TRTP 01) aan te vragen, daar alleen dit garandeert dat de VU-certificaten in het overgebrachte 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 over te brengen kalenderdag (`TimeReal` opmaak).

2.2.2.10. *Positive Response Transfer Data (Positief Antwoord Gegevensoverdracht) (SID 76)*

DDP_012 Het Positive Response Transfer Data wordt door de VU in antwoord op het Transfer Data Request gezonden. Het bericht bevat de gevraagde gegevens met een Transfer Response Parameter (TREP) die correspondeert met de TRTP van het verzoek.

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

— beveiligingscertificaten,

— voertuigidentificatie,

— huidige datum en tijd van de VU,

— min. en max. opvraagbare datum (VU-gegevens),

— indicatie van in de VU aanwezige kaarten,

— vorige overbrenging naar een bedrijf,

— bedrijfsvergrendelingen,

— vorige controles.

2.2.2.11. *Request Transfer Exit (Verzoek Overdrachtsexit) (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 (Positief Antwoord Verzoek Overdrachtsexit) (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 (Verzoek Beëindiging Overdracht) (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 (Positief Antwoord Beëindiging Overdracht) (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 (Bevestig Subbericht) (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 overgebracht wordt. 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 subbericht opnieuw te zenden.

— FFFF verzoekt 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 (Negatief Antwoord) (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. Het gegevensveld van het bericht bevat 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 overbrenging 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 ingebracht is).

2.2.3. ***Berichtenstroom***

Een typische berichtenstroom tijdens een normale gegevensoverdrachtsprocedure ziet er als volgt uit:

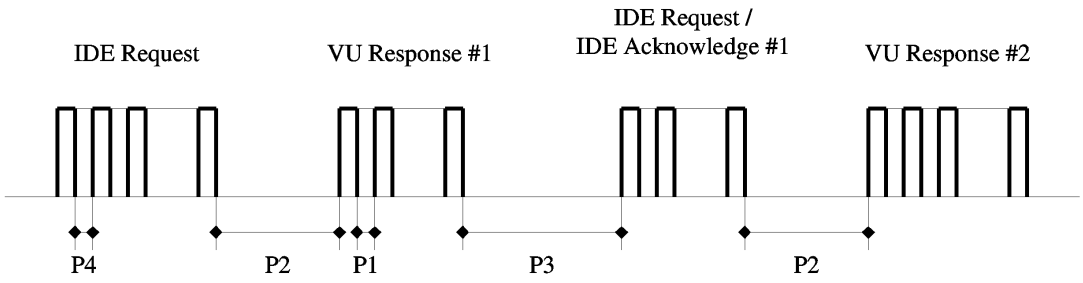
IDE		VU
Start Communication Request	⇨	
	⇦	Positive Response
Start Diagnostic Service Request	⇨	
	⇦	Positive Response
Request Upload	⇨	
	⇦	Positive Response
Transfer Data Request Overview	⇨	
	⇦	Positive Response
Transfer Data Request #2	⇨	
	⇦	Positive Response #1
Acknowledge Sub Message #1	⇨	
	⇦	Positive 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. ***Timing***

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 kaartoverbrenging.

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).

Timingparameter	Laagste waarde (ms)	Hoogste waarde (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 aan dezelfde hoogste waarde van P3 toebedeeld.

2.2.5. ***Behandeling van fouten***

Indien tijdens de uitwisseling van berichten een fout optreedt, wordt het berichtenstroomschema afhankelijk van de inrichting die de fout heeft opgespoord of van het bericht dat de fout heeft veroorzaakt, gewijzigd.

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 Communication Phase*

DDP_020 Indien de IDE tijdens de Start Communicatie Phase, 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, dan dient de VU geen antwoord te zenden, maar te wachten op een ander Start Communication Request-bericht binnen een P3max-periode.

2.2.5.2. *Communication Phase*

Twee verschillende gebieden voor de behandeling van fouten kunnen gedefinieerd worden:

1. De VU spoort een IDE overbrengingsfout op.

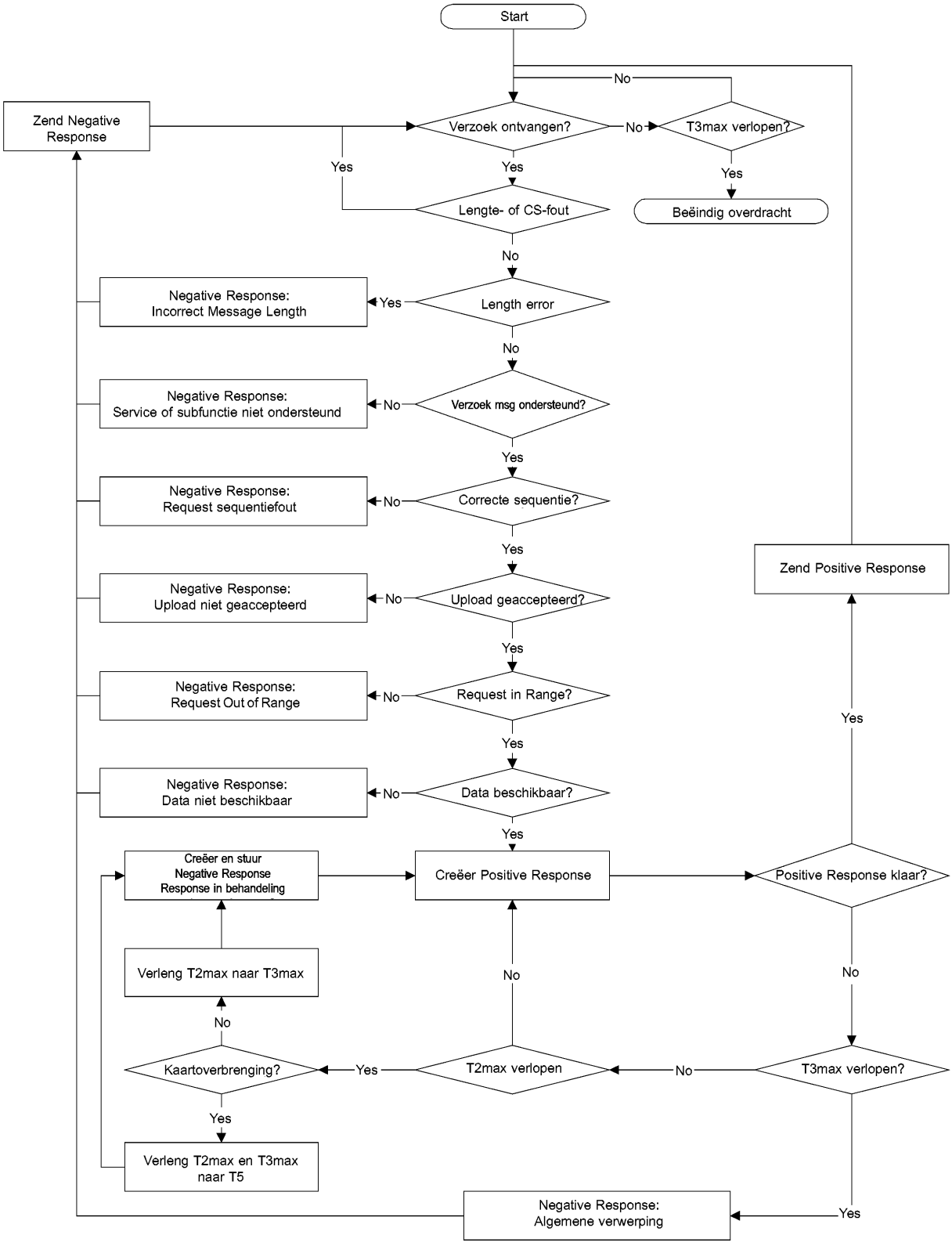
DDP_022 Voor elk ontvangen bericht moet de VU timingfouten, byteopmaakfouten (bijv. foutieve start- en stopbits) en frame errors (verkeerd aantal bytes ontvangen, foutieve controlesombyte) opsporen.

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 dit geval moet de VU aan de IDE met een Negative Response-bericht antwoorden dat de aard van de fout specificeert.

Figuur 2

VU behandeling van fouten



2. De IDE spoort een VU overbrengingsfout 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.

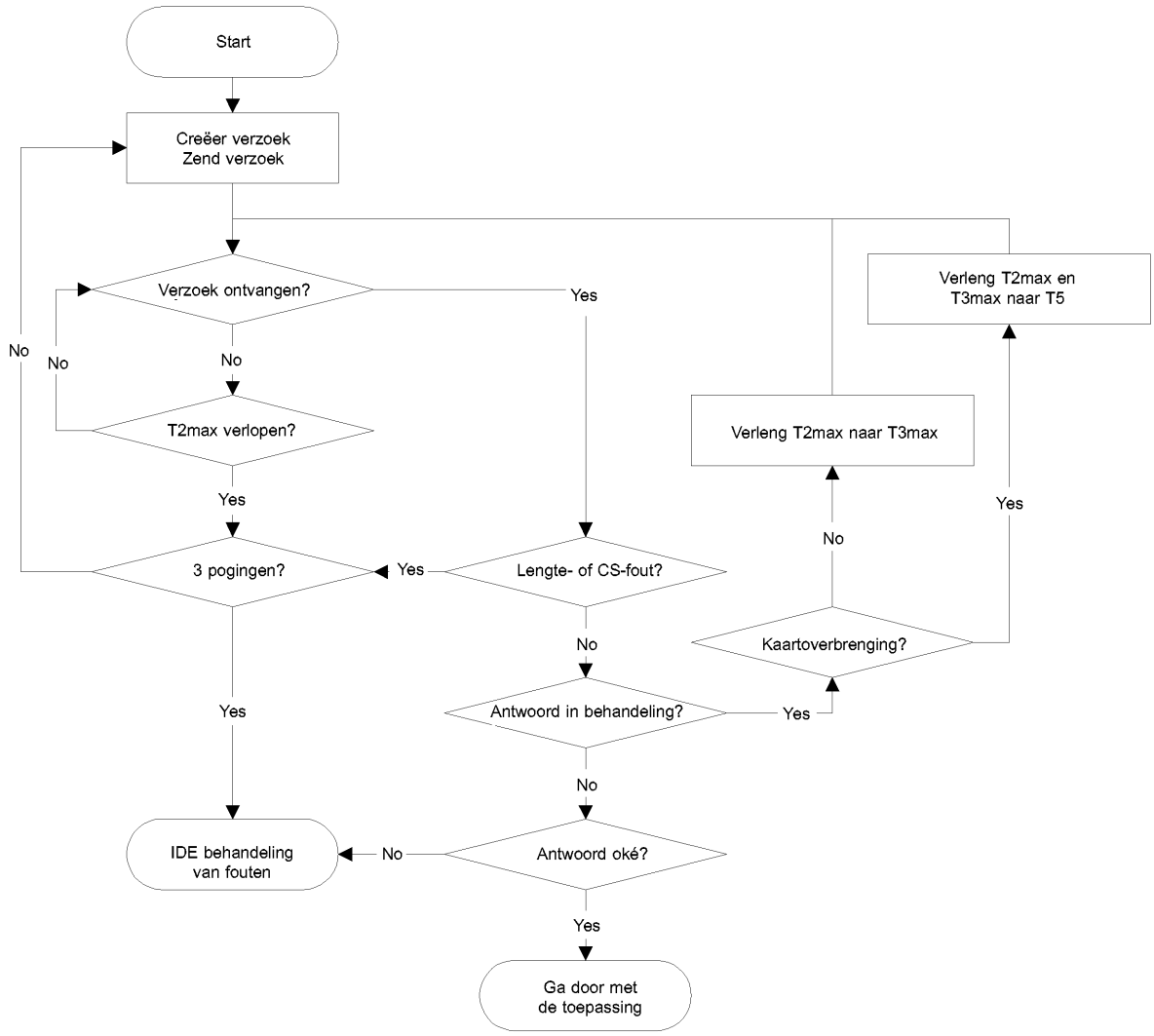
DDP_026 De IDE moet sequentiefouten opsporen, bijv. niet correcte standverhogingen bij de teller van de subberichten bij na elkaar ontvangen berichten.

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 behandeling van fouten



2.2.6. ***Inhoud van het antwoordbericht***

Dit punt specificeert de inhoud van de gegevensvelden van de verschillende positieve antwoordberichten.

Gegevenselementen worden in appendix 1 (Verklarende woordenlijst van de gegevens) gedefinieerd.

2.2.6.1. *Positive Response Transfer Data Overview (Positief antwoord gegevensoverdracht-overzicht)*

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:

Gegevenselement	Lengte (Bytes)	Opmerking
MemberStateCertificate	194	VU beveiligingscertificaten
VUCertificate	194	
VehicleIdentificationNumber	17	VIN-nummer
VehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
CurrentDateTime	4	VU huidige datum en tijd
VuDownloadablePeriod		Over te brengen periode
minDownloadableTime	4	
maxDownloadableTime	4	
CardSlotsStatus	1	Soort in de VU ingebrachte kaarten
VuDownloadActivityData		Vorige overbrenging van de VU
downloadingTime	4	
fullCardNumber	18	
companyOrWorkshopName	36	
VuCompanyLocksData		Alle opgeslagen bedrijfsvergrendelingen. Indien de sectie leeg is, wordt alleen noOfLocks = 0 gezonden
noOfLocks	1	
...	(98)	
VuCompanyLocksRecord		
lockInTime	4	
lockOutTime	4	
companyName	36	
companyAddress	36	
companyCardNumber	18	
...		
VuControlActivityData		Alle in de VU opgeslagen controleregistraties. Indien de sectie leeg is, wordt alleen noOfControls = 0 gezonden
noOfControls	1	
...	(31)	
VuControlActivityRecord		
controlType	1	
controlTime	4	
controlCardNumber	18	
downloadPeriodBeginTime	4	
downloadPeriodEndTime	4	
...		
Signature	128	RSA-handtekening van alle gegevens (met uitzondering van certificaten) beginnend met het VehicleIdentificationNumber tot de laatste byte van de laatste VuControlActivityRecord

2.2.6.2. *Positive Response Transfer Data Activities (Positief antwoord gegevensoverdrachtactiviteiten)*

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:

Gegevenselement	Lengte (Bytes)	Opmerking
TimeReal	4	Datum van overgebrachte dag
OdometerValueMidnight	3	Kilometerstand aan het einde van de overgebrachte dag
VuCardIWData		Gegevens over cycli van inbrengen en uitnemen van kaarten. — Indien deze sectie geen beschikbare gegevens bevat, wordt alleen noOfVuCardIWRecords = 0 gezonden. — Wanneer een VuCardIWRecord doorloopt na 00:00 uur (kaartinbrenging op de vorige dag) of na 24:00 uur (kaartuitneming op de volgende dag) moet de registratie op de twee betreffende dagen volledig worden getoond.
NoOfVuCardIWRecords	2	
...	(129)	
VuCardIWRecord		
cardHolderName		
holderSurname	36	
holderFirstNames	36	
fullCardNumber	18	
cardExpiryDate	4	
cardInsertionTime	4	
vehicleOdometerValueAtInsertion	3	
cardSlotNumber	1	
cardWithdrawalTime	4	
vehicleOdometerValueAtWithdrawal	3	
previousVehicleInfo		
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
cardWithdrawalTime	4	
manualInputFlag	1	
...		
VuActivityDailyData		Lezerstatus op 00:00 en voor de overgebrachte dag geregistreerde veranderingen van activiteiten.
noOfActivityChanges	2	
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData		Plaatsen met betrekking tot de geregistreerde gegevens voor de overgebrachte dag. Indien de sectie leeg is, wordt alleen noOfPlaceRecords = 0 gezonden.
noOfPlaceRecords	1	
...	(28)	
VuPlaceDailyWorkPeriodRecord		
fullCardNumber	18	
placeRecord		
entryTime	4	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		
VuSpecificConditionData		Geregistreerde gegevens over specifieke omstandigheden voor de overgebrachte dag. Indien de sectie leeg is, wordt alleen noOfSpecificConditionRecords = 0 gezonden.
noOfSpecificConditionRecords	2	
...	(5)	
SpecificConditionRecord		
EntryTime	4	
specificConditionType	1	
...		
Signature	128	RSA-handtekening van alle gegevens beginnend met TimeReal tot de laatste byte van de laatste registratie van een specifieke omstandigheid.

2.2.6.3. *Positive Response Transfer Data Events and Faults (Positief antwoord gegevensoverdracht voorvallen en fouten)*

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 02 Hex en de passende splitsing en telling van de subberichten verstrekken:

Gegevenselement	Lengte (Bytes)	Opmerking
VuFaultData		Alle in de VU opgeslagen of aan de gang zijnde fouten. Indien de sectie leeg is, wordt alleen noOfVuFaults = 0 gezonden.
NoOfVuFaults	1	
...	(82)	
VuFaultRecord: FaultType	1	
VuFaultRecord: FaultRecordPurpose	1	
VuFaultRecord: FaultBeginTime	4	
VuFaultRecord: FaultEndTime	4	
VuFaultRecord: CardNumberDriverSlotBegin	18	
VuFaultRecord: cardNumberCodriverSlotBegin	18	
VuFaultRecord: CardNumberDriverSlotEnd	18	
VuFaultRecord: CardNumberCodriverSlotEnd	18	
...		
VuEventData		Alle in de VU opgeslagen of aan de gang zijnde voorvallen (met uitzondering van snelheidsoverschrijdingen). Indien de sectie leeg is, wordt alleen noOfVuEvents = 0 gezonden.
NoOfVuEvents	1	
...	(83)	
VuEventRecord: EventType	1	
VuEventRecord: EventRecordPurpose	1	
VuEventRecord: EventBeginTime	4	
VuEventRecord: EventEndTime	4	
VuEventRecord: CardNumberDriverSlotBegin	18	
VuEventRecord: cardNumberCodriverSlotBegin	18	
VuEventRecord: CardNumberDriverSlotEnd	18	
VuEventRecord: CardNumberCodriverSlotEnd	18	
VuEventRecord: SimilarEventsNumber	1	
...		
VuOverSpeedingControlData		Gegevens met betrekking tot de laatste controle van snelheidsoverschrijdingen (standaardwaarde bij ontbreken van gegevens)
LastOverspeedControlTime	4	
FirstOverspeedSince	4	
NumberOfOverspeedSince	1	
VuOverSpeedingEventData		Alle in de VU opgeslagen gevallen van snelheidsoverschrijding. Indien de sectie leeg is, wordt alleen noOfVuOverSpeedingEvents = 0 gezonden.
NoOfVuOverSpeedingEvents	1	
...	(31)	
VuOverSpeedingEventRecord: EventType	1	
VuOverSpeedingEventRecord: EventRecordPurpose	1	
VuOverSpeedingEventRecord: EventBeginTime	4	
VuOverSpeedingEventRecord: EventEndTime	4	
VuOverSpeedingEventRecord: MaxSpeedValue	1	
VuOverSpeedingEventRecord: AverageSpeedValue	1	
VuOverSpeedingEventRecord: CardNumberDriverSlotBegin	18	
VuOverSpeedingEventRecord: SimilarEventsNumber	1	
...		
VuTimeAdjustmentData		Alle in de VU opgeslagen voorvallen van tijdafstelling (buiten het kader van een volledige kalibrering). Indien de sectie leeg is, wordt alleen noOfVuTimeAdjRecords = 0 gezonden.
NoOfVuTimeAdjRecords	1	
...	(98)	
VuTimeAdjustmentRecord: OldTimeValue	4	
VuTimeAdjustmentRecord: NewTimeValue	4	
VuTimeAdjustmentRecord: WorkshopName	36	
VuTimeAdjustmentRecord: WorkshopAddress	36	
VuTimeAdjustmentRecord: WorkshopCardNumber	18	
...		
Signature	128	RSA-handtekening van alle gegevens beginnend met noOfVuFaults tot de laatste byte van de laatste tijdafstellingsregistratie

2.2.6.4. *Positive Response Transfer Data Detailed Speed (Positief antwoord gegevensoverdracht gedetailleerde snelheid)*

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:

Gegevenselement	Lengte (Bytes)	Opmerking
VuDetailedSpeedData		
NoOfSpeedBlocks	2	Alle in de VU opgeslagen gedetailleerde snelheden (één snelheidsblok per minuut waarin het voertuig rijdt). 60 snelheidswaarden per minuut (een per seconde).
...		
VuDetailedSpeedBlock		
SpeedBlockBeginDate	4	
speedsPerSecond	60	
...		
Signature	128	RSA-handtekening van alle gegevens beginnend met noOfSpeedBlocks tot en met de laatste byte van het laatste snelheidsblok.

2.2.6.5. *Positive Response Transfer Data Technical Data (Positief antwoord gegevensoverdracht technische gegevens)*

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 04 Hex en de passende splitsing en telling van de subberichten verstrekken:

Gegevenselement	Lengte (Bytes)	Opmerking
VuIdentification		
vuManufacturerName	36	
vuManufacturerAddress	36	
vuPartNumber	16	
vuSerialNumber	8	
vuSoftwareIdentification		
vuSoftwareVersion	4	
vuSoftInstallationDate	4	
vuManufacturingDate	4	
vuApprovalNumber	8	
SensorPaired		
sensorSerialNumber	8	
sensorApprovalNumber	8	
sensorPairingDateFirst	4	
VuCalibrationData		Alle in de VU opgeslagen kalibreringsregistraties
noOfVuCalibrationRecords	1	
...	(164)	
VuCalibrationRecord		
calibrationPurpose	1	
workshopName	36	
workshopAddress	36	
workshopCardNumber	18	
workshopCardExpiryDate	4	
vehicleIdentificationNumber	17	
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
wVehicleCharacteristicConstant	2	
kConstantOfRecordingEquipment	2	
lTyreCircumference	2	
tyreSize	15	
authorisedSpeed	1	
oldOdometerValue	3	
newOdometerValue	3	
oldTimeValue	4	
newTimeValue	4	
nextCalibrationDate	4	
...		
Signature	128	RSA-handtekening van alle gegevens beginnend met vuManufacturerName tot de laatste byte van de laatste Vu CalibrationRecord

2.3. **ESM bestandsopslag**

DDP_034 Wanneer tijdens een overdrachtsessie een gegevensoverdracht van een VU heeft plaatsgevonden, moet de IDE alle tijdens de overdrachtsessie van de VU ontvangen gegevens in de berichten Positive Response Transfer Data in één fysiek veld opslaan. Opgeslagen gegevens zijn exclusief koptitels 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. PROTOCOL VAN OVERDRACHT 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 beveiligingsomgeving; daarom vindt er geen authentificatie tussen de kaart en de IDE plaats.

3.2. **Definities**

Overdrachtssessie: Elke keer dat er een gegevensoverdracht van de ICC wordt uitgevoerd. De sessie omvat de volledige procedure vanaf het terugstellen van de ICC door een IFD tot de inactivering van de ICC (uitnemen van de kaart of volgende reset).

Getekend gegevensbestand: Een bestand van de ICC. Het bestand wordt ongecodeerd naar de IFD overgebracht. Op de ICC wordt het bestand gehashed en getekend; de handtekening wordt naar de IFD overgebracht.

3.3. **Overdracht van de kaart**

DDP_035 De overdracht van een tachograafkaart omvat de onderstaande stappen:

— Overdracht van de algemene informatie van de kaart naar de `ICC` en `IC` van het EF. Deze informatie is facultatief en wordt niet met een digitale handtekening beveiligd.

— Overdracht van het `Card_Certificate` en `CA_Certificate` van het EF. Deze informatie wordt niet met een digitale handtekening beveiligd.

  Het is verplicht om deze bestanden voor elke overdrachtssessie over te brengen.

— Overdracht van de andere toepassingsgegevens van de EF's (in `Tachograph` DF) 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 overdrachtssessie over te brengen.

  — Bij de overdracht van een bestuurderskaart is het ook verplicht de onderstaande EF's over te brengen:

    — `Events_Data`,

    — `Faults_Data`,

    — `Driver_Activity_Data`,

    — `Vehicles_Used`,

    — `Places`,

    — `Control_Activity_Data`,

    — `Specific_Conditions`.

— Bij de overdracht van een bestuurderskaart moet de datum van de `LastCardDownload` in `Card_Download` van het EF worden aangepast.

— Bij de overdracht van een werkplaatskaart moet de kalibreringsteller in `Card_Download` van het EF worden teruggesteld.

3.3.1. ***Initialisatiesequentie***

DDP_036 De IDE moet de sequentie als volgt initiëren:

Kaart	Richting	IDE/IFD	Betekenis/Opmerkingen
	⇦	Hardware terugstellen	
ATR	⇨		

Het gebruik van PPS om over te schakelen op een hogere baudsnelheid, is facultatief zolang de ICC dit ondersteunt.

3.3.2. ***Sequentie voor niet-getekende gegevensbestanden***

DDP_037 De sequentie voor overdracht van de `ICC`, `IC`, `Card_Certificate` 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

Opmerking: Voor het selecteren van het `Card_Certificate`-EF, moet de tachograaftoepassing worden geselecteerd (selectie met AID).

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 overgebracht moeten worden:

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 appendix 11. Dit commando is geen ISO-commando
Bereken hash van bestand 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 vasthouden, moet het commando worden herhaald totdat het volledige bestand is gelezen
Bestandsgegevens OK	⇨	Sla ontvangen gegevens in ESM op	Overeenkomstig 3.4, Opmaak gegevensopslag
	⇦	PSO: COMPUTE DIGITAL SIGNATURE	
Voer beveiligingsoperatie uit „Bereken digitale handtekening” met de tijdelijk opgeslagen hashwaarde			
Handtekening OK	⇨	Koppel gegevens aan de vorige in het ESM opgeslagen gegevens	Overeenkomstig 3.4, Opmaak gegevensopslag

3.3.4. ***Sequentie voor het terugstellen van de kalibreringsteller***

DDP_039 De sequentie voor het terugstellen 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 bestands-identificatiesymbolen
OK	⇨		
	⇦	UPDATE BINARY `NoOfCalibrations SinceDownload` = '00 00'	
Stelt het volgnummer van kaartoverbrenging terug			
OK	⇨		

3.4. **Opmaak gegevensopslag**

3.4.1. ***Inleiding***

DDP_040 De overgebrachte gegevens moeten overeenkomstig de onderstaande voorwaarden worden opgeslagen:

— De gegevens moeten transparant worden opgeslagen. Dit 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 overdrachtssessie overgebrachte bestanden van de kaart worden in een 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 overgebracht, 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”	Label 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. OVERBRENGEN VAN EEN TACHOGRAAFKAART VIA EEN VOERTUIGUNIT

DDP_047 De VU moet het overbrengen van de inhoud van een bestuurderkaart die in een met de VU verbonden IDE is ingebracht mogelijk maken.

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 de hele kaart overbrengen, bestand voor bestand, overeenkomstig het in punt 3 gedefinieerde protocol van kaartoverdracht en alle van de kaart ontvangen gegevens in de vereiste TLV-bestandsopmaak (zie 3.4.2) naar de IDE zenden en ingekapseld in een „Positive Response Transfer Data"-bericht naar de IDE zenden.

DDP_050 De IDE moet kaartgegevens van het „Positive Response Transfer Data"-bericht lezen (alle koptitels, SID's, TREP's, tellers van subberichten en controlesommen verwijderen) en deze gegevens in een fysiek bestand zoals beschreven in punt 2.3 opslaan.

DDP_051 De VU moet vervolgens, naar gelang van het geval, het bestand `Control_Activity_Data` of `Card_Download` van de bestuurderskaart bijwerken.

Appendix 8

KALIBRERINGSPROTOCOL

INHOUD

1.	Inleiding	170
2.	Termen, definities en referenties	170
3.	Overzicht van diensten	170
3.1.	Beschikbare diensten	170
3.2.	Antwoordcodes	171
4.	Overdrachtsdiensten	171
4.1.	StartCommunication-dienst (Start overdracht)	171
4.2.	StopCommunication-dienst (Beëindig overdracht)	173
4.2.1.	Omschrijving van het bericht	173
4.2.2.	Berichtformaat	174
4.2.3.	Parameterdefinitie	175
4.3.	TesterPresent-dienst (Testapparaat actief)	175
4.3.1.	Omschrijving van het bericht	175
4.3.2.	Berichtformaat	175
5.	Beheerdiensten	176
5.1.	StartDiagnosticSession-dienst (Start diagnostische sessie)	176
5.1.1.	Omschrijving van het bericht	176
5.1.2.	Berichtformaat	177
5.1.3.	Parameterdefinitie	178
5.2.	SecurityAccess-dienst (Veiligheidstoegang)	178
5.2.1.	Omschrijving van het bericht	178
5.2.2.	Berichtformaat — SecurityAccess — requestSeed	179
5.2.3.	Berichtformaat — SecurityAccess — sendKey	180
6.	Gegevensoverbrengingsdiensten	181
6.1.	ReadDataByIdentifier-dienst (Lees gegevens met identificatiesymbool)	181
6.1.1.	Omschrijving van het bericht	181
6.1.2.	Berichtformaat	181
6.1.3.	Parameterdefinitie	182
6.2.	WriteDataByIdentifier-dienst (Schrijf gegevens met identificatiesymbool)	183
6.2.1	Omschrijving van het bericht	183
6.2.2.	Berichtformaat	183
6.2.3.	Parameterdefinitie	184
7.	Controle van testimpulsen — Invoer-/uitvoercontrole functionele eenheid	184
7.1.	InputOutputControlByIdentifier-dienst (Invoer-/uitvoercontrole door identificatiesymbool)	184

7.1.1. Omschrijving van het bericht 184
7.1.2. Berichtformaat 185
7.1.3. Parameterdefinitie 186
8. Formaten van dataRecords (Gegevensregistraties) 187
8.1. Overgebrachte parameterreeksen 187
8.2. Formaten van dataRecords 188

1. INLEIDING

Deze appendix beschrijft hoe gegevens worden uitgewisseld tussen een voertuigunit en een testapparaat via de K-lijn die deel uitmaakt van de in appendix 6 beschreven kalibreringsinterface. Hij beschrijft ook de controle van de signaallijn van de invoer/uitvoer op de kalibreringsconnector.

Het tot stand brengen van overdracht van de K-lijn wordt beschreven in punt 4 „Overdrachtsdiensten".

Deze appendix gebruikt het idee van diagnostische „sessies" om het toepassingsgebied van K-lijncontrole onder verschillende omstandigheden vast te stellen. De standaardsessie is de „StandardDiagnosticSession" waarin alle gegevens van een voertuigunit kunnen worden gelezen maar waarin geen gegevens naar een voertuigunit kunnen worden geschreven.

Selectie van de diagnostische sessie wordt beschreven in punt 4.3 „Beheerdiensten".

CPR_001 Met de „ECUProgrammingSession" kunnen gegevens in de voertuigunit worden ingevoerd. In het geval van invoer van kalibreringsgegevens (voorschriften 097 en 098) moet de voertuigunit bovendien in de werkingsmodus CALIBRATION zijn.

Gegevensoverdracht via K-lijn wordt beschreven in punt 6 „Gegevensoverbrengingsdiensten". Formaten van overgebrachte gegevens worden nader beschreven in punt 8 „Formaten van gegevensregistraties".

CPR_002 Met de „ECUAdjustmentSession" kan de I/O-modus van de I/O-signaallijn voor kalibrering via de K-lijninterface worden geselecteerd. Controle van de kalibrerings-I/O-signaallijn wordt beschreven in punt 7 „Controle van testpulsen — Invoer-/uitvoercontrole functionele unit".

CPR_003 In dit document wordt aan het testapparaat gerefereerd 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 het meest recente ontwerp van ISO 14229-1 (Road vehicles — Diagnostic systems — Part 1: Diagnostic services, version 6 of 22 February 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: ISO 14230-2: Road Vehicles — Diagnostic Systems — Keyword Protocol 2000 — Part 2: Data Link Layer. First edition: 1999. Voertuigen — Diagnostische systemen.

3. OVERZICHT VAN DIENSTEN

3.1. **Beschikbare diensten**

De onderstaande tabel geeft een overzicht van de in het controleapparaat 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 1e kolom vermeldt de beschikbare diensten.

— De 2e kolom bevat het nummer van het punt in deze appendix, waarin de dienst nader wordt gedefinieerd.

— De 3e kolom kent de waarden van het dienstidentificatiesymbool toe voor verzoekberichten.

— De 4e kolom specificeert de diensten van de „StandardDiagnosticSession" (SD) (standaard diagnostische sessie) die in elke VU geïmplementeerd moeten worden.

— De 5e 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 6e kolom specificeert de diensten van de „ECUProgrammingSession" (ECUPS) (ECU-programmeersessie) die geïmplementeerd moeten worden om programmering van de parameters in de VU mogelijk te maken.

Tabel 1

Verzameltabel waarden dienstidentificatiesymbolen

			Diagnostische sessies		
Naam van de diagnostische dienst	Punt nr.	Sid Verzoek-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 de dienst verplicht is in deze diagnostische sessie.
Geen symbool geeft aan dat deze dienst in deze diagnostische sessie niet toegestaan is.

3.2. **Antwoordcodes**

Voor elke dienst zijn antwoordcodes bepaald.

4. OVERDRACHTSDIENSTEN

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

Overdrachtsdiensten

Naam van de dienst	Omschrijving
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 een activiteit gaat een bus-stilstandtijd vooraf.

— Het testapparaat zendt vervolgens een initialisatiepatroon.

— Het antwoord van de VU bevat alle noodzakelijk informatie om de overdracht tot stand te brengen.

CPR_012 Na voltooiing van de initialisatie:

— Alle overdrachtparameters worden overeenkomstig de sleutelbytes op in tabel 5 bepaalde waarden gezet.

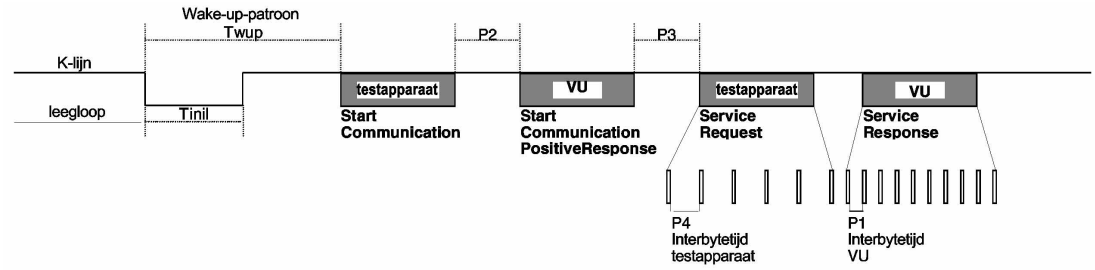
— De VU wacht op het eerste verzoek van het testapparaat.

— De VU is in de standaard diagnostische modus, d.w.z. StandardDiagnosticSession.

— De kalibrerings-I/O-signaallijn is 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 leegloop op de K-lijn met een lage tijd van Tinil. 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 leegloop:

— 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		Min.-waarde	Max.-waarde
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	5000
P4	Interbytetijd voor verzoek van het testapparaat	5	20

CPR_018 Het berichtenformaat voor snelle initialisatie wordt omschreven in de onderstaande tabellen.

Tabel 5

StartCommunication Request-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	81	FMT
nr. 2	Byte van het doeladres	EE	TGT
nr. 3	Byte van het bronadres	tt	SRC
nr. 4	StartCommunication Request Service Id	81	SCR
nr. 5	Controlesom	00-FF	CS

Tabel 6

StartCommunication Positive Response-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	03	LEN
nr. 5	StartCommunication Positive Response Service Id	C1	SCRPR
nr. 6	Sleutelbyte 1	EA	KB1
nr. 7	Sleutelbyte 2	8F	KB2
nr. 8	Controlesom	00-FF	CS

CPR_019 Er is geen negatief antwoord op het bericht StartCommunication Request. Indien er geen bericht van positief antwoord gezonden hoeft te worden, dan wordt de VU niet geïnitialiseerd. Er wordt niets gezonden en de VU blijft in zijn normale werking.

4.2. **StopCommunication-dienst (Beëindig overdracht)**

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 afgegeven 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 afgegeven.

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-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	EE	TGT
nr. 3	Byte van het bronadres	tt	SRC
nr. 4	Additionele lengtebyte	01	LEN
nr. 5	StopCommunication Request Service Id	82	SPR
nr. 6	Controlesom	00-FF	CS

Tabel 8

StopCommunication Positive Response-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	01	LEN
nr. 5	StopCommunication Positive Response Service	C2	SPRPR
nr. 6	Controlesom	00-FF	CS

Tabel 9

StopCommunication Negative Response-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	03	LEN
nr. 5	Negative Response Service Id	7F	NR
nr. 6	StopCommunication Request Service Identification	82	SPR
nr. 7	ResponseCode = generalReject	10	RC_GR
nr. 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 gezonden, 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-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	EE	TGT
nr. 3	Byte van het bronadres	tt	SRC
nr. 4	Additionele lengtebyte	02	LEN
nr. 5	TesterPresent Request Service Id	3E	TP
nr. 6	Subfunctie = responseRequired (antwoord vereist) = [ja	01	RESPREQ_Y
	nee]	02	RESPREQ_NO
nr. 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-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	01	LEN
nr. 5	TesterPresent Positive Response Service Id	7E	TPPR
nr. 6	Controlesom	00-FF	CS

CPR_081 De dienst ondersteunt de volgende negatieve-antwoordencodes:

Tabel 12

TesterPresent Negative Response-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	03	LEN
nr. 5	Negative Response Service Id	7F	NR
nr. 6	TesterPresent Request Service Identification	3E	TP
nr. 7	ResponseCode = [SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
	incorrectMessageLength]	13	RC_IML
nr. 8	Controlesom 00-FF CS	00-FF	CS

5. BEHEERDIENSTEN

De beschikbare diensten worden omschreven in de onderstaande tabel:

Tabel 13

Beheerdiensten

Naam van de dienst	Omschrijving
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, dan moet de StandardDiagnosticSession actief blijven zolang de VU wordt aangedreven.

— Indien een diagnostische sessie die reeds actief is, door het testapparaat wordt aangevraagd, dan 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, dan 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 5 moeten actief zijn na een succesvolle StartDiagnosticSession waarbij de diagnostic-Session-parameter in het verzoekbericht ingesteld is op „StandardDiagnosticSession" indien een andere diagnostische sessie voorheen 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-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	EE	TGT
nr. 3	Byte van het bronadres	tt	SRC
nr. 4	Additionele lengtebyte	02	LEN
nr. 5	StartDiagnosticSession Request Service Id	10	STDS
nr. 6	DiagnosticSession = [een waarde uit tabel 17]	xx	DS_…
nr. 7	Controlesom	00-FF	CS

Tabel 15

StartDiagnosticSession Positive Response-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	02	LEN
nr. 5	StartDiagnosticSession Positive Response Service Id	50	STDSPR
nr. 6	DiagnosticSession = [zelfde waarde als in Byte-nr. 6 tabel 14]	xx	DS_…
nr. 7	Controlesom	00-FF	CS

Tabel 16

StartDiagnosticSession Negative Response-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	03	LEN
nr. 5	Negative Response Service Id	7F	NR
nr. 6	StartDiagnosticSession Request Service Id	10	STDS
nr. 7	ResponseCode = [subFunctionNotSupported ([a])	12	RC_SFNS
	incorrectMessageLength ([b])	13	RC_IML
	conditionsNotCorrect ([c])]	22	RC_CNC
nr. 8	Controlesom	00-FF	CS

([a]) De in Byte-nr. 6 van het verzoekbericht ingebrachte waarde wordt niet ondersteund, d.w.z. niet in tabel 17.
([b]) De lengte van het bericht is fout.
([c]) Aan de criteria voor het verzoek StartDiagnosticSession is niet voldaan.

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	Omschrijving	Mnemonisch
81	StandardDiagnosticSession Deze diagnostische sessie maakt alle in tabel 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 afgesloten is. 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, 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, 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 of toegang tot de invoer-/uitvoerlijn van de kalibrering is niet mogelijk tenzij de VU in de CALIBRATION-modus is. Naast het inbrengen van een geldige werkplaatskaart moet de juiste PIN-code worden ingevoerd voordat toegang tot de CALIBRATION-modus wordt verkregen.

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 is.

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 kaartauthentificatieproces 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 vijf 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 met gebruikmaking van de dienst SecurityAccess Positive Response alleen beantwoorden wanneer hij in CALIBRATION-modus is.

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 authentificatie 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-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	EE	TGT
nr. 3	Byte van het bronadres	tt	SRC
nr. 4	Additionele lengtebyte	02	LEN
nr. 5	SecurityAccess Request Service Id	27	SA
nr. 6	AccessType — requestSeed	7D	AT_RSD
nr. 7	Controlesom	00-FF	CS

Tabel 19

SecurityAccess — requestSeed Positive Response-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	04	LEN
nr. 5	SecurityAccess Positive Response Service Id	67	SAPR
nr. 6	AccessType — requestSeed	7D	AT_RSD
nr. 7	Seed High	00-FF	SEEDH
nr. 8	Seed Low	00-FF	SEEDL
nr. 9	Controlesom	00-FF	CS

Tabel 20

SecurityAccess Negative Response-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	03	LEN
nr. 5	Negative Response Service Id	7F	NR
nr. 6	SecurityAccess Request Service Id	27	SA
nr. 7	ResponseCode = [conditionsNotCorrectOrRequestSequenceError incorrectMessageLength]	22 13	RC_CNC RC_IML
nr. 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-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	EE	TGT
nr. 3	Byte van het bronadres	tt	SRC
nr. 4	Additionele lengtebyte	m+2	LEN
nr. 5	SecurityAccess Request Service Id	27	SA
nr. 6	AccessType — sendKey	7E	AT_SK
nr. 7 tot nr. m+6	Key #1 (High) … Key # m (low, m moet minimaal 4 en maximaal 8 zijn)	xx … xx	KEY
nr. m+7	Controlesom	00-FF	CS

Tabel 22

SecurityAccess — sendKey Positive Response-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	02	LEN
nr. 5	SecurityAccess Positive Response Service Id	67	SAPR
nr. 6	AccessType — sendKey	7E	AT_SK
nr. 7	Controlesom	00-FF	CS

Tabel 23

SecurityAccess Negative Response-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	03	LEN
nr. 5	Negative Response Service Id	7F	NR
nr. 6	SecurityAccess Request Service Id	27	SA
nr. 7	ResponseCode = [generalReject	10	RC_GR
	subFunctionNotSupported	12	RC_SFNS
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	invalidKey	35	RC_IK
	exceededNumberOfAttempts	36	RC_ENA
	requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
nr. 8	Controlesom	00-FF	CS

6. GEGEVENSOVERBRENGINGSDIENSTEN

De beschikbare diensten worden omschreven in de onderstaande tabel:

Tabel 24

Gegevensoverbrengingsdiensten

Naam van de dienst	Omschrijving
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 Response-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	EE	TGT
nr. 3	Byte van het bronadres	tt	SRC
nr. 4	Additionele lengtebyte	03	LEN
nr. 5	ReadDataByIdentifier Request Service Id	22	RDBI
nr. 6 tot nr. 7	RecordDataIdentifier = [een waarde uit tabel 28]	xxxx	RDI_…
nr. 8	Controlesom	00-FF	CS

Tabel 26

ReadDataByIdentifier Positive Response-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	m+3	LEN
nr. 5	ReadDataByIdentifier Positive Response Service Id	62	RDBIPR
nr. 6 en nr. 7	recordDataIdentifier = [zelfde waarde als byte-nrs. 6 en 7 tabel 25]	xxxx	RDI_…
nr. 8 tot nr. m+7	DataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
nr. m+8	Controlesom	00-FF	CS

Tabel 27

ReadDataByIdentifier Negative Response-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	03	LEN
nr. 5	Negative Response Service Id	7F	NR
nr. 6	ReadDataByIdentifier Request Service Id	22	RDBI
nr. 7	ResponseCode = [requestOutOfRange incorrectMessageLength conditionsNotCorrect]	31 13 22	RC_ROOR RC_IML RC_CNC
nr. 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 toegekend is.

— De 2e kolom (Gegevenselement) specificeert het gegevenselement van appendix 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 de waarden van de recordDataIdentifier

Hex	Gegevenselement	recordDataIdentifier-naam (zie formaat in punt 8.2)	Mnemonisch
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	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 aangegeven. 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-dienst (Schrijf gegevens met identificatiesymbool)**

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 fabrikant van de VU dat tijdens het uitvoeren van deze dienst aan de voorwaarden van de server wordt voldaan. Om de parameters van tabel 28 bij te werken moet de VU in CALIBRATION-modus zijn

6.2.2. ***Berichtformaat***

CPR_057 De berichtformaten voor de WriteDataByIdentifier-primitieven worden omschreven in de onderstaande tabellen.

Tabel 29

WriteDataByIdentifier Request-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	EE	TGT
nr. 3	Byte van het bronadres	tt	SRC
nr. 4	Additionele lengtebyte	m+3	LEN
nr. 5	WriteDataByIdentifier Request Service Id	2E	WDBI
nr. 6 tot 7	RecordDataIdentifier = [een waarde uit tabel 28]	xxxx	RDI_…
nr. 8 tot nr. m+7	DataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
nr. m+8	Controlesom	00-FF	CS

Tabel 30

WriteDataByIdentifier Positive Response-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	03	LEN
nr. 5	WriteDataByIdentifier Request Service Id	6E	WDBIPR
nr. 6 tot nr. 7	RecordDataIdentifier = [zelfde waarde als byte-nrs. 6 en 7 tabel 29]	xxxx	RDI_…
nr. 8	Controlesom	00-FF	CS

Tabel 31

WriteDataByIdentifier Negative Response-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	03	LEN
nr. 5	NegativeResponse Service Id	7F	NR
nr. 6	WriteDataByIdentifier Request Service Id	2E	WDBI
nr. 7	ResponseCode = [requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect]	22	RC_CNC
nr. 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 aangegeven.

7. CONTROLE VAN TESTIMPULSEN — INVOER-/UITVOERCONTROLE FUNCTIONELE EENHEID

De beschikbare diensten worden omschreven in de onderstaande tabel:

Tabel 32

Invoer-/uitvoercontrole functionele eenheid

Naam van de dienst	Omschrijving
InputOutputControlByIdentifier	De cliënt verzoekt om controle van een voor de server specifieke invoer/uitvoer

7.1. **InputOutputControlByIdentifier-dienst (Invoer-/uitvoercontrole door identificatiesymbool)**

7.1.1. ***Omschrijving van het bericht***

Er is een verbinding via de frontconnector waarmee testpulsen met gebruikmaking van een geschikt testapparaat geregeld of gecontroleerd kunnen worden.

CPR_058 Deze kalibrerings-I/O-signaallijn kan door het K-lijncommando met gebruikmaking van de dienst InputOutputControlByIdentifier geconfigureerd worden 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,

— 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.

CPR_059 De voertuigunit moet een afstellingssessie ingevoerd hebben en in CALIBRATION-modus zijn om de instelling van de lijn te configureren. Bij het verlaten van de afstellingssessie of van de CALIBRATION-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, dan moet de kalibrerings-I/O-signaallijn op uitvoer worden gezet of 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-werkingsmodus (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-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	EE	TGT
nr. 3	Byte van het bronadres	tt	SRC
nr. 4	Additionele lengtebyte	xx	LEN
nr. 5	InputOutputControlByIdentifier Request Sid	2F	IOCBI
nr. 6 en nr. 7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
nr. 8 of nr. 8 tot nr. 9	ControlOptionRecord = [		COR_…
	inputOutputControlParameter — een waarde uit tabel 36	xx	IOCP_…
	controlState — een waarde uit tabel 38 (zie onderstaande opmerking)]	xx	CS_…
nr. 9 of nr. 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-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	xx	LEN
nr. 5	InputOutputControlByIdentifier Positive Response SId	6F	IOCBIPR
nr. 6 en nr. 7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
nr. 8 of nr. 8 tot nr. 9	ControlStatusRecord = [		CSR_
	inputOutputControlParameter (zelfde waarde als byte-nr. 8 tabel 33)	xx	IOCP_…
	controlState (zelfde waarde als byte-nr. 9 tabel 33)] indien van toepassing	xx	CS_…
nr. 9 of nr. 10	Controlesom	00-FF	CS

Tabel 35

InputOutputControlByIdentifier Negative Response-bericht

Byte-nr.	Parameternaam	Hex-waarde	Mnemonisch
nr. 1	Formaatbyte — fysieke adressering	80	FMT
nr. 2	Byte van het doeladres	tt	TGT
nr. 3	Byte van het bronadres	EE	SRC
nr. 4	Additionele lengtebyte	03	LEN
nr. 5	Negative Response Service Id	7F	NR
nr. 6	InputOutputControlByIdentifier Request SId	2F	IOCBI
nr. 7	ResponseCode = [		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
nr. 8	Controlesom	00-FF	CS

7.1.3. ***Parameterdefinitie***

CPR_064 De parameter inputOutputControlParameter (IOCP_) wordt omschreven in de onderstaande tabel.

Tabel 36

Omschrijving van de waarden van de inputOutputControlParameter

Hex	Omschrijving	Mnemonisch
01	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

Omschrijving van de waarden van de controlState

Modus	Hex-waarde	Omschrijving
Disable	00	I/O-lijn is geblokkeerd (standaardinstelling)
Enable	01	Kalibrerings-I/O-lijn kan worden gebruikt als speedSignalInput
Enable	02	Kalibrerings-I/O-lijn kan worden gebruikt als realTimeSpeedSignalOutputSensor
Enable	03	Kalibrerings-I/O-lijn kan worden gebruikt als RTCOutput

8. FORMATEN VAN DATARECORDS (GEGEVENSREGISTRATIES)

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 De reeksen die worden gebruikt om de geldigheid van een overgebrachte parameter te bepalen, zijn in tabel 38 gedefinieerd.

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 registratieapparatuur.

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 component 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

dataRecords reeksen

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 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**

Tabel 39 tot en met tabel 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 details 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
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Zie details 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 details 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 # F00B)

Byte	Parameterdefinitie	Resolutie	Bedrijfsreeks
1	Seconden	0,25 s/bit, toename, 0 s comp.	0 tot 59,75 s
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 # F022)

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 dag
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.
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 bevat bijzonderheden betreffende de formaten van de verschillende bytes van de VehicleRegistrationNumber-parameter:

Tabel 42

Gedetailleerd formaat van VehicleRegistrationNumber (recordDataIdentifier-waarde # F07E)

Byte	Parameterdefinitie	Resolutie	Bedrijfsreeks
1	Code Page (zoals gedefinieerd in appendix 1)	ASCII	01 tot 0A
2 tot 14	Vehicle Registration Number (zoals gedefinieerd in appendix 1)	ASCII	ASCII

Appendix 9

TYPEGOEDKEURING — LIJST VAN MINIMAAL VEREISTE BEPROEVINGEN

INHOUD

1. Inleiding 191

1.1. Typekoedkeuring 191

1.2. Referentienormen 191

2. Functiebeproevingen van de voertuigunit 192

3. Functiebeproevingen van de bewegingsopnemer 195

4. Functiebeproevingen van tachograafkaarten 197

5. Interoperabiliteitsbeproevingen 198

1. INLEIDING

1.1. **Typegoedkeuring**

De EG-goedkeuring van een controleapparaat (of component) of van een tachograafkaart is gebaseerd op:

— een veiligheidscertificatie uitgevoerd door een autoriteit van de ITSEC, met een veiligheidsdoelstelling die volledig voldoet aan appendix 10 bij deze bijlage;

— een functiecertificatie uitgevoerd door een autoriteit van de lidstaat die certificeert dat het beproefde item voldoet aan de voorschriften van deze bijlage met betrekking tot uitgevoerde functies, nauwkeurigheid van de metingen en milieukenmerken;

— een interoperabiliteitscertificatie uitgevoerd door de bevoegde instantie die certificeert dat het controleapparaat (of de tachograafkaart) volledig interoperabel is met de vereiste modellen tachograafkaarten (of controleapparatuur) (zie hoofdstuk VIII van deze bijlage).

Deze appendix specificeert welke beproevingen minimaal door een autoriteit van de lidstaat tijdens functiebeproevingen moeten worden uitgevoerd, en welke beproevingen minimaal door de bevoegde instantie tijdens de interoperabiliteitsbeproevingen moeten worden uitgevoerd. Te volgen procedures voor het uitvoeren van de beproevingen of het soort beproevingen worden niet nader gespecificeerd.

De aspecten van de veiligheidscertificatie zijn niet in deze appendix opgenomen. Indien een aantal voor goedkeuring vereiste beproevingen tijdens de veiligheidscertificatie en het certificatieproces uitgevoerd zijn, dan hoeven deze beproevingen niet opnieuw uitgevoerd te worden. In dat geval moeten alleen de resultaten van deze veiligheidsbeproevingen worden gecontroleerd. Ter informatie worden de voorschriften die naar verwachting tijdens de veiligheidscertificatie worden beproefd (of die nauw verband houden met de beproevingen die naar verwachting worden uitgevoerd) in deze appendix met een „*” aangeduid.

Deze appendix behandelt afzonderlijk de goedkeuring van de bewegingsopnemer en van de voertuigunit als samenstellende delen van het controleapparaat. Interoperabiliteit tussen elk model bewegingsopnemer en elk model voertuigunit is niet vereist, daarom kan de goedkeuring van een bewegingsopnemer alleen in combinatie met de goedkeuring van een voertuigunit en vice versa worden verleend.

1.2. **Referentienormen**

De onderstaande referentienormen worden in deze appendix gebruikt:

IEC 68-2-1	Environmental testing — Part 2: Tests — Tests A: Cold. 1990 + Amendment 2: 1994.
IEC 68-2-2	Environmental testing — Part 2: Tests — Tests B: Dry heat. 1974 + Amendment 2: 1994.
IEC 68-2-6	Basic environmental testing procedures — Test methods — Test Fc and guidance: Vibrations (sinusoidal). 6th edition: 1985.
IEC 68-2-14	Basic environmental testing procedures — Test methods — Test N: Change of temperature. Modification 1: 1986.
IEC 68-2-27	Basic environmental testing procedures — Test methods — Test Ea and guidance: Shock. Edition 3: 1987.
IEC 68-2-30	Basic environmental testing procedures — Test methods — Test Db and guidance: Damp heat, cyclic (12 + 12 — hour cycle). Modification 1: 1985.
IEC 68-2-35	Basic environmental testing procedure — Test methods — Test Fda: Random Vibrations wide band — Reproducibility High. Modification 1: 1983.
IEC 529	Degrees of protection provided by enclosures (IP code). Edition 2: 1989.
IEC 61000-4-2	Electromagnetic Compatibility (EMC) — Testing and measurement techniques — Electrostatic discharge immunity test: 1995/Amendment 1: 1998.
ISO 7637-1	Road vehicles — Electrical disturbance by conduction and coupling — Part 1: Passenger cars and light commercial vehicles with nominal 12 V supply voltage — Electrical transient conduction along supply lines only. Edition 2: 1990.

ISO 7637-2 Road vehicles — Electrical disturbance by conduction and coupling — Part 2: Commercial vehicles with nominal 24 V supply voltage — Electrical transient conduction along supply lines only. First edition: 1990.

ISO 7637-3 Road vehicles — Electrical disturbance by conduction and coupling — Part 3: Vehicles with 12 V or 24 V supply voltage — Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines. First Edition: 1995 + Cor 1: 1995.

ISO/IEC 7816-1 Identification cards — Integrated circuit(s) cards with contacts — Part 1: Physical characteristics. First edition: 1998.

ISO/IEC 7816-2 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts. First edition: 1999.

ISO/IEC 7816-3 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocol. Edition 2: 1997.

ISO/IEC 10373 Identification cards — Test methods. First edition: 1993.

2. FUNCTIEBEPROEVINGEN VAN DE VOERTUIGUNIT

Nr.	Beproeving	Omschrijving	Gerelateerde voorschriften
1.	**Administratieve controle**		
1.1.	Documentatie	Juistheid van de documentatie	
1.2.	Beproevingsresultaten van de fabrikant	Resultaten van de beproeving door de fabrikant uitgevoerd tijdens integratie. Papierdemonstraties	070, 071, 073
2.	**Visuele inspectie**		
2.1.	Naleving van documentatie		
2.2.	Identificatie / opschriften		168, 169
2.3.	Materialen		163 tot en met 167
2.4	Verzegeling		251
2.5.	Externe interfaces		
3.	**Functiebeproevingen**		
3.1.	Aanwezige functies		002, 004, 244
3.2.	Werkingsmodi		006*, 007*, 008*, 009*, 106, 107
3.3.	Functies en gegevenstoegangsrechten		010*, 011*, 240, 246, 247
3.4.	Controle op het inbrengen en uitnemen van kaarten		013, 014, 015*, 016*, 106
3.5.	Meting van snelheid en afstand		017 tot en met 026
3.6.	Tijdmeting (beproeving uitgevoerd bij 20 °C)		027 tot en met 032
3.7.	Controle op activiteiten van de bestuurder		033 tot en met 043, 106
3.8.	Controle op de status van de bestuurders		044, 045, 106
3.9.	Handmatige invoer		046 tot en met 050b
3.10.	Beheer van bedrijfsvergrendelingen		051 tot en met 055
3.11.	Bewaken van controleactiviteiten		056, 057
3.12.	Opsporing van voorvallen en/of fouten		059 tot en met 069, 16

Nr.	Beproeving	Omschrijving	Gerelateerde voorschriften
3.13.	Identificatiegegevens van de inrichting		075*, 076*, 079
3.14.	Gegevens over inbrengen en uitnemen van de bestuurderskaart		081* tot en met 083*
3.15.	Gegevens over activiteiten van de bestuurder		084* tot en met 086*
3.16.	Gegevens over plaatsen		087* tot en met 089*
3.17.	Gegevens over de kilometerstand		090* tot en met 092*
3.18.	Gedetailleerde gegevens over snelheid		093*
3.19.	Gegevens over voorvallen		094*, 095
3.20.	Gegevens over fouten		096*
3.21.	Kalibreringsgegevens		097*, 098*
3.22.	Tijdafstellingsgegevens		100*, 101*
3.23.	Gegevens over controleactiviteiten		102*, 103*
3.24.	Gegevens over bedrijfsvergrendelingen		104*
3.25.	Gegevens over overbrengingsactiviteiten		105*
3.26.	Gegevens over specifieke omstandigheden		105a*, 105b*
3.27.	Registreren en opslaan op tachograafkaarten		108, 109*, 109a*, 110*, 111, 112
3.28.	Visuele weergave		072, 106, 113 tot en met 128, PIC_001, DIS_001
3.29.	Afdrukken		072, 106, 129 tot en met 138, PIC_001, PRT_001 tot en met PRT_012
3.30.	Waarschuwingssignalen		106, 139 tot en met 148, PIC_001
3.31.	Overbrengen van gegevens naar externe media		072, 106, 149 tot en met 151
3.32.	Uitvoergegevens naar additionele externe inrichtingen		152, 153
3.33.	Kalibrering		154*, 155*, 156*, 245
3.34.	Tijdafstelling		157*, 158*
3.35.	Geen interferentie van additionele functies		003, 269

Nr.	Beproeving	Omschrijving	Gerelateerde voorschriften
4.	**Milieubeproevingen**		
4.1.	Temperatuur	Controleer functionaliteit aan de hand van: — IEC 68-2-1, test Ad, met een beproevingsduur van 72 uur bij de laagste temperatuur (– 20 °C), 1 uur ingeschakeld, 1 uur uitgeschakeld; — IEC 68-2-2, test Bd, met een beproevingsduur van 72 uur bij de hoogste temperatuur (+ 70 °C), 1 uur ingeschakeld, 1 uur uitgeschakeld Temperatuurwisselproef: controleer de bestandheid van de voertuigunit tegen snelle wisselingen in de omgevingstemperatuur aan de hand van IEC 68-2-14, test Na, met 20 wisselingen, elk met een temperatuur variërend van de laagste temperatuur (– 20 °C) tot de hoogste temperatuur (+ 70 °C), bij een verblijf gedurende 2 uur bij de laagste en de hoogste temperatuur Een kleiner aantal beproevingen (zoals gedefinieerd in sectie 3 van deze tabel) kan bij de laagste temperatuur, de hoogste temperatuur en tijdens de temperatuurwisselingen worden uitgevoerd	159
4.2.	Vochtigheid	Controleer de bestandheid van de voertuigunit tegen een cyclische vochtigheid (warmteproef) aan de hand van IEC 68-2-30, 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	160
4.3.	Vibratie	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 68-2-6, test Fc, met een minimale beproevingsduur van 3 × 12 uur (12 uur per as) 2. Willekeurige vibraties: Controleer de bestandheid van de voertuigunit tegen willekeurige vibraties bij onderstaande kenmerken: frequentie 5-150 Hz, niveau 0,02 g^2/Hz Dit voorschrift wordt gecontroleerd aan de hand van IEC 68-2-35, test Ffda, met een minimale beproevingsduur van 3 × 12 uur (12 uur per as), 1 uur ingeschakeld, 1 uur uitgeschakeld De twee bovengenoemde beproevingen worden op twee verschillende modellen van de te beproeven inrichting uitgevoerd	163
4.4.	Bescherming tegen water en vreemde lichamen	Controleer of de beveiligingsindex van de voertuigunit volgens IEC 529 ten minste IP 40 is, wanneer deze in bedrijfsomstandigheden in een voertuig wordt geplaatst	164, 165
4.5.	Beveiliging tegen te hoge spanning	Controleer of de voertuigunit bestand is tegen een stroomvoorziening van: 24 V-uitvoeringen: 34 V bij + 40 °C 1 uur 12 V-uitvoeringen: 17 V bij + 40 °C 1 uur	161
4.6.	Beveiliging tegen ompolen	Controleer of de voertuigunit bestand is tegen een omkering in de stroomvoorziening	161
4.7.	Beveiliging tegen kortsluiting	Controleer of invoer-/uitvoersignalen beveiligd zijn tegen kortsluiting in de stroomvoorziening en tegen aardsluiting	161

Nr.	Beproeving	Omschrijving	Gerelateerde voorschriften
5.	**EMC-beproevingen**		
5.1.	Stralingen en gevoeligheid	Overeenkomstig Richtlijn 95/54/EG	162
5.2.	Elektrostatische ontlading	Overeenkomstig IEC 61000-4-2, ± 2 kV (niveau 1)	162
5.3.	Transiënte geleidingsverschijnselen in de stroomvoorziening	voor 24 V-uitvoeringen: overeenkomstig ISO 7637-2 puls 1a: Vs = – 100 V, Ri = 10 ohm puls 2: Vs = + 100 V, Ri = 10 ohm puls 3a: Vs = – 100 V, Ri = 50 ohm puls 3b: Vs = + 100 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 12 V-uitvoeringen: overeenkomstig ISO 7637-1 puls 1: Vs = - 100 V, Ri = 10 ohm puls 2: Vs = + 100 V, Ri = 10 ohm puls 3a: Vs = – 100 V, Ri = 50 ohm puls 3b: Vs = + 100 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 bij voertuigunits worden beproefd die in voertuigen worden geïnstalleerd waarvoor geen externe gewone beveiliging tegen een plotselinge spanningsverlaging geïmplementeerd is	162

3. FUNCTIEBEPROEVINGEN VAN DE BEWEGINGSOPNEMER

Nr.	Beproeving	Omschrijving	Gerelateerde voorschriften
1.	**Administratieve controle**		
1.1.	Documentatie	Juistheid van de documentatie	
2.	**Visuele inspectie**		
2.1.	Inachtneming van documentatie		
2.2.	Identificatie/opschriften		169, 170
2.3.	Materialen		163 tot en met 167
2.4.	Verzegeling		251
3.	**Functiebeproevingen**		
3.1.	Identificatiegegevens van de opnemer		077*
3.2.	Verbinding bewegingsopnemer — voertuigunit		099*, 155
3.3.	Bewegingsdetectie Juistheid van bewegingsmeting		 022 tot en met 026

Nr.	Beproeving	Omschrijving	Gerelateerde voorschriften
4.	**Milieubeproevingen**		
4.1.	Bedrijfstemperatuur	Controleer functionaliteit (zoals gedefinieerd in beproeving nr. 3.3) in temperatuurbereik [– 40 °C; + 135 °C] aan de hand van: — IEC 68-2-1, test Ad, met een beproevingsduur van 96 uur bij de laagste temperatuur To_{min} — IEC 68-2-2, test Bd, met een beproevingsduur van 96 uur bij de hoogste temperatuur To_{max}	159
4.2.	Temperatuurwisselproef	Controleer functionaliteit (zoals gedefinieerd in beproeving nr. 3.3) aan de hand van IEC 68-2-14, test Na, 20 wisselingen, elk met een temperatuur variërend van de laagste temperatuur (– 40 °C) tot de hoogste temperatuur (+135 °C) en met een verblijf van 2 uur bij de laagste en de hoogste temperatuur Een kleiner aantal beproevingen (zoals gedefinieerd in beproeving nr. 3.3) kan bij de laagste temperatuur, de hoogste temperatuur en tijdens temperatuurwisselingen worden uitgevoerd	159
4.3.	Vochtigheidscycli	Controleer functionaliteit (zoals gedefinieerd in beproeving nr. 3.3) aan de hand van IEC 68-2-30, 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	160
4.4.	Vibratie	Controleer functionaliteit (zoals gedefinieerd in beproeving nr. 3.3) aan de hand van IEC 68-2-6, test Fc, met een beproevingsduur van 100 frequenctiecycli: constante verplaatsing tussen 10 en 57 Hz: 1,5 mm piek constante acceleratie tussen 57 en 500 Hz: 20 g	163
4.5.	Mechanische schok	Controleer functionaliteit (zoals gedefinieerd in beproeving nr. 3.3) met de IEC 68-2-27, test Ea, 3 schokken in beide richtingen van de 3 loodrechte assen	163
4.6.	Bescherming tegen water en vreemde lichamen	Controleer of de beveiligingsindex van de bewegingsopnemer volgens IEC 529 ten minste IP 64 is, wanneer deze in bedrijfsomstandigheden in een voertuig geplaatst is	165
4.7.	Beveiliging tegen ompolen	Controleer of de bewegingsopnemer bestand is tegen een omkering in de stroomvoorziening	161
4.8.	Beveiliging tegen kortsluiting	Controleer of de invoer-/uitvoersignalen beveiligd zijn tegen kortsluiting in de stroomvoorziening en tegen aardsluiting	161
5.	**EMC-beproevingen**		
5.1.	Stralingen en gevoeligheid	Overeenkomstig Richtlijn 95/54/EEC	162
5.2.	Elektrostatische ontlading	Overeenkomstig IEC 61000-4-2, ± 2 kV (niveau 1)	162
5.3.	Transiënte geleidingsverschijnselen in datatransmissielijnen	Overeenkomstig ISO 7637-3 (niveau III)	162

4. FUNCTIEBEPROEVINGEN VAN TACHOGRAAFKAARTEN

Nr.	Beproeving	Omschrijving	Gerelateerde voorschriften
1.	**Administratieve controle**		
1.1.	Documentatie	Juistheid van de documentatie	
2.	**Visuele inspectie**		
2.1.		Controleer of alle beveiligingskenmerken en zichtbare gegevens naar behoren en conform de regels op de kaart zijn afgedrukt	171 tot en met 181
3.	**Fysieke beproevingen**		
3.1.	Controleer de afmeting van de kaart en de plaats van de contacten		184 ISO/IEC 7816-1 ISO/IEC 7816-2
4.	**Protocolbeproevingen**		
4.1.	ATR	Controleer of de ATR voldoet	ISO/IEC 7816-3 TCS 304, 307, 308
4.2.	T=0	Controleer of het protocol T=0 voldoet	ISO/IEC 7816-3 TCS 302, 303, 305
4.3.	PTS	Controleer of de PTS-opdracht voldoet door T=0 op T=1 te zetten	ISO/IEC 7816-3 TCS 309 tot en met 311
4.4.	T=1	Controleer of het protocol T=1 voldoet	ISO/IEC 7816-3 TCS 303, 306
5.	**Kaartstructuur**		
5.1.		Ga na of de bestandsstructuur van de kaart voldoet door de kaart te controleren op de aanwezigheid van verplichte bestanden en hun toegangscondities	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	**Functiebeproevingen**		
6.1.	Normale verwerking	Controleer ten minste een keer het toegestane gebruik van elke opdracht (bijv.: test de UPDATE BINARY-opdracht met CLA = '00', CLA = '0C' en met verschillende P1-, P2- en Lc-parameters)	TCS 313 tot en met TCS 379
6.2.	Foutmeldingen	Beproef ten minste een keer elke algemene fout (met uitzondering van '6400' integriteitsfouten gecontroleerd tijdens de veiligheidscertificatie)	
7.	**Milieubeproevingen**		
7.1.		Controleer of de kaarten werken binnen de vastgestelde grenswaarden overeenkomstig ISO/IEC 10373	185 tot en met 188 ISO/IEC 7816-1

5. INTEROPERABILITEITSBEPROEVINGEN

Nr.	Beproeving	Omschrijving
1.	Wederzijdse authenticatie	Controleer of de wederzijdse authenticatie tussen de voertuigunit en de tachograafkaart normaal functioneert
2.	Lees-/schrijf-beproevingen	Voer een typisch functiescenario in de voertuigunit uit. Het scenario moet aan de soort te beproeven kaart worden aangepast en schrijfopdrachten in zoveel mogelijk EF's op de kaart bevatten Controleer door middel van een kaartoverbrenging of alle corresponderende registraties correct ingevoerd zijn Controleer door middel van een dagelijkse afdruk van de kaart of alle corresponderende registraties correct gelezen kunnen worden

Appendix 10

ALGEMENE BEVEILIGINGSDOELSTELLINGEN

Deze appendix specificeert de minimaal vereiste beveiligingsdoelstellingen voor de bewegingsopnemer, voertuigunit en tachograafkaart.

Teneinde de doelstellingen te formuleren op basis waarvan een verzoek om veiligheidscertificatie wordt ingediend, moeten de fabrikanten de documenten waar nodig verbeteren en completeren en mogen zij bestaande bedreigingen, doelstellingen, procedurele middelen alsmede uitvoeringsspecificaties voor beveiligingsfuncties wijzigen noch verwijderen.

INHOUD

Algemene beveilingsdoelstelling van de bewegingsopnemer

1. Inleiding ... 204
2. Afkortingen, definities en referenties ... 204
2.1. Afkortingen ... 204
2.2. Definities ... 204
2.3. Referentienormen ... 205
3. Productratio ... 205
3.1. Beschrijving van de bewegingsopnemer en gebruiksaanwijzing ... 205
3.2. Levenscyclus van de bewegingsopnemer ... 206
3.3. Bedreigingen ... 206
3.3.1. Bedreigingen voor de toegangsbewaking ... 206
3.3.2. Ontwerpgerelateerde bedreigingen ... 207
3.3.3. Werkingsgerelateerde bedreigingen ... 207
3.4. Beveiligingsdoelstellingen ... 207
3.5. Informatietechnologische beveiligingsdoelstellingen ... 207
3.6. Fysieke, personele of procedurele middelen ... 208
3.6.1. Ontwerp van de inrichting ... 208
3.6.2. Levering van de inrichting ... 208
3.6.3. Ontwikkeling van beveiligingsgegevens en overdracht ... 208
3.6.4. Installatie, kalibrering en controle van het controleapparaat ... 208
3.6.5. Controle op de naleving van de wet ... 208
3.6.6. Softwareaanpassing ... 208
4. Beveiligingsfuncties ... 208
4.1. Identificatie en authenticatie ... 208
4.2. Toegangscontrole ... 209
4.2.1. Toegangscontrolebeleid ... 209
4.2.2. Toegangsrechten tot gegevens ... 209
4.2.3. Bestandsstructuur en toegangscondities ... 209
4.3. Verantwoording ... 209

4.4. Audit . . . 210
4.5. Nauwkeurigheid . . . 210
4.5.1. Controlebeleid met betrekking tot de informatiestroom . . . 210
4.5.2. Overdracht van interne gegevens . . . 210
4.5.3. Integriteit van opgeslagen gegevens . . . 210
4.6. Betrouwbaarheid van de werking . . . 210
4.6.1. Beproevingen . . . 210
4.6.2. Software . . . 211
4.6.3. Fysieke bescherming . . . 211
4.6.4. Onderbrekingen in de stroomvoorziening . . . 211
4.6.5. Terugstelvoorwaarden . . . 211
4.6.6. Beschikbaarheid van gegevens . . . 211
4.6.7. Meervoudige toepassingen . . . 211
4.7. Gegevensuitwisseling . . . 211
4.8. Cryptografische ondersteuning . . . 211
5. Definitie van beveiligingsmechanismen . . . 212
6. Minimumsterkte van beveiligingsmechanismen . . . 212
7. Garantieniveau . . . 212
8. Ratio . . . 212

Algemene beveiligingsdoelstelling van de voertuigunit

1. Inleiding . . . 214
2. Afkortingen, definities en referenties . . . 214
2.1. Afkortingen . . . 214
2.2. Definities . . . 214
2.3. Referentienormen . . . 214
3. Productratio . . . 214
3.1. Beschrijving van de voertuigunit en gebruiksaanwijzing . . . 214
3.2. Levenscyclus van de voertuigunit . . . 216
3.3. Bedreigingen . . . 216
3.3.1. Bedreigingen voor identificatie en toegangsbewaking . . . 216
3.3.2. Ontwerpgerelateerde bedreigingen . . . 217
3.3.3. Werkingsgerelateerde bedreigingen . . . 217
3.4. Beveiligingsdoelstellingen . . . 217
3.5. Informatietechnologische beveiligingsdoelstellingen . . . 218
3.6. Fysieke, personele of procedurele middelen . . . 218
3.6.1. Ontwerp van de apparatuur . . . 218
3.6.2. Levering en activering van de apparatuur . . . 218
3.6.3. Ontwikkeling van beveiligingsgegevens en overdracht . . . 218

3.6.4. Levering van kaarten . . . 219
3.6.5. Installatie, kalibrering en controle van het controleapparaat . . . 219
3.6.6. Bediening van de apparatuur . . . 219
3.6.7. Controle op de naleving van de wet . . . 219
3.6.8. Softwareaanpassing . . . 219
4. Beveiligingsfuncties . . . 219
4.1. Identificatie en authenticatie . . . 219
4.1.1. Identificatie en authenticatie van de bewegingsopnemer . . . 219
4.1.2. Identificatie en authenticatie van de gebruiker . . . 220
4.1.3. Identificatie en authenticatie van een op afstand aangesloten bedrijf . . . 221
4.1.4. Identificatie en authenticatie van de beheersinrichting . . . 221
4.2. Toegangscontrole . . . 221
4.2.1. Toegangscontrolebeleid . . . 221
4.2.2. Toegangsrechten tot functies . . . 221
4.2.3. Toegangsrechten tot gegevens . . . 221
4.2.4. Bestandsstructuur en toegangscondities . . . 222
4.3. Verantwoording . . . 222
4.4. Audit . . . 222
4.5. Hergebruik van objecten . . . 223
4.6. Nauwkeurigheid . . . 223
4.6.1. Controlebeleid met betrekking tot de informatiestroom . . . 223
4.6.2. Overdracht van interne gegevens . . . 223
4.6.3. Integriteit van opgeslagen gegevens . . . 223
4.7. Betrouwbaarheid van de werking . . . 223
4.7.1. Beproevingen . . . 223
4.7.2. Software . . . 224
4.7.3. Fysieke bescherming . . . 224
4.7.4. Onderbrekingen in de stroomvoorziening . . . 224
4.7.5. Terugstelvoorwaarden . . . 224
4.7.6. Beschikbaarheid van gegevens . . . 224
4.7.7. Meervoudige toepassingen . . . 224
4.8. Gegevensuitwisseling . . . 224
4.8.1. Gegevensuitwisseling met de bewegingsopnemer . . . 224
4.8.2. Gegevensuitwisseling met tachograafkaarten . . . 225
4.8.3. Gegevensuitwisseling met externe opslagmedia (overbrengingsfunctie) . . . 225
4.9. Cryptografische ondersteuning . . . 225

5. Definitie van beveiligingsmechanismen ... 225
6. Minimumsterkte van beveiligingsmechanismen ... 225
7. Garantieniveau ... 225
8. Ratio ... 226

Algemene beveiligingsdoelstelling van de tachograafkaart

1. Inleiding ... 230
2. Afkortingen, definities en referentienormen ... 230
2.1. Afkortingen ... 230
2.2. Definities ... 230
2.3. Referentienormen ... 231
3. Productratio ... 231
3.1. Beschrijving van de tachograafkaart en gebruikaanwijzing ... 231
3.2. Levenscyclus van een tachograafkaart ... 231
3.3. Bedreigingen ... 232
3.3.1. Einddoelen ... 232
3.3.2. Aanvalspaden ... 232
3.4. Beveiligingsdoelstellingen ... 232
3.5. Informatietechnologische beveiligingsdoelstellingen ... 232
3.6. Fysieke, personele of procedurele middelen ... 232
4. Beveiligingsfuncties ... 233
4.1. Overeenstemming met beschermingsprofielen ... 233
4.2. Identificatie en authenticatie van de gebruiker ... 233
4.2.1. Identificatie van de gebruiker ... 233
4.2.2. Authenticatie van de gebruiker ... 233
4.2.3. Authenticatiefouten ... 233
4.3. Toegangscontrole ... 234
4.3.1. Toegangscontrolebeleid ... 234
4.3.2. Toegangscontrolefuncties ... 234
4.4. Verantwoording ... 234
4.5. Audit ... 234
4.6. Nauwkeurigheid ... 234
4.6.1. Integriteit van opgeslagen gegevens ... 234
4.6.2. Authenticatie van basisgegevens ... 234
4.7. Betrouwbaarheid van de werking ... 235
4.7.1. Beproevingen ... 235
4.7.2. Software ... 235
4.7.3. Stroomvoorziening ... 235

4.7.4. Terugstelvoorwaarden 235
4.8. Gegevensuitwisseling 235
4.8.1. Gegevensuitwisseling met een voertuigunit 235
4.8.2. Uitvoer van gegevens naar een niet-voertuigunit (overbrengingsfunctie) 235
4.9. Cryptografische ondersteuning 235
5. Definitie van beveiligingsmechanismen 235
6. Opgegeven minimumsterkte van mechanismen 236
7. Garantieniveau 236
8. Ratio 236

ALGEMENE BEVEILIGINGSDOELSTELLING VAN DE BEWEGINGSOPNEMER

1. **Inleiding**

Dit document bevat een beschrijving van de bewegingsopnemer, van de door de bewegingsopnemer te neutraliseren bedreigingen en van de te realiseren beveiligingsdoelstellingen. Het specificeert de vereiste beveiligingsfuncties. Het document vermeldt verder de vereiste minimumsterkte van beveiligingsmechanismen en het vereiste garantieniveau voor de ontwikkeling en de evaluatie.

De voorschriften waarnaar in het document wordt verwezen, staan in de tekst van bijlage I B. Voor de duidelijkheid treedt er soms herhaling op tussen de voorschriften in de tekst van bijlage I B en de voorschriften van de beveiligingsdoelstelling. In het geval van onduidelijkheid tussen een voorschrift van de beveiligingsdoelstelling en een voorschrift van bijlage I B waarnaar in dit document wordt verwezen, geldt het voorschrift van bijlage I B.

Voorschriften van bijlage I B die in de beveiligingsdoelstellingen niet worden genoemd, zijn geen onderwerp van de beveiligingsfuncties.

Er zijn unieke labels toegewezen aan bedreigingen, doelstellingen, procedurele middelen en SEF-specificaties, zodat deze gemakkelijk in ontwikkelings- en beproevingsdocumentatie terug te vinden zijn.

2. **Afkortingen, definities en referenties**

2.1. ***Afkortingen***

ROM	Read only memory (ROM-geheugen)
SEF	Security enforcing function (beveiligingsfunctie)
TBD	To be defined (nog te bepalen)
TOE	Target of evaluation (doel van de evaluatie)
VU	Vehicle unit (voertuigunit)

2.2. ***Definities***

Digitale tachograaf	Controleapparaat
Unit	Een met de bewegingsopnemer verbonden inrichting
Bewegingsgegevens	De met de VU uitgewisselde gegevens betreffende snelheid en afgelegde afstand
Fysiek gescheiden delen	Fysieke componenten van de bewegingsopnemer die zich op verschillende plaatsen in het voertuig bevinden, in tegenstelling met fysieke, in de behuizing van de bewegingsopnemer ondergebrachte componenten
Beveiligingsgegevens	De specifieke gegevens ter ondersteuning van beveiligingsfuncties (bijv. cryptosleutels)
Systeem	Inrichtingen, mensen of organisaties die op de een of andere manier bij de controleapparatuur betrokken zijn
Gebruiker	Een menselijke gebruiker van de bewegingsopnemer (wanneer niet gebruikt in de uitdrukking „gebruikersgegevens")
Gebruikersgegevens	Door de bewegingsopnemer geregistreerde of opgeslagen gegevens, anders dan bewegings- of beveiligingsgegevens

2.3. ***Referentienormen***

ITSEC ITSEC Information Technology Security Evaluation Criteria 1991

3. **Productratio**

3.1. ***Beschrijving van de bewegingsopnemer en gebruiksaanwijzing***

De bewegingsopnemer is bedoeld voor installatie in voertuigen voor het wegvervoer. Het doel ervan is beveiligde bewegingsgegevens betreffende de snelheid en afgelegde afstand van het voertuig aan de VU te leveren.

De bewegingsopnemer wordt op mechanische wijze verbonden met een bewegend deel van het voertuig. Deze beweging kan representatief zijn voor de snelheid of de afgelegde afstand van het voertuig. De inrichting kan in de versnellingsbak of in een ander deel van het voertuig worden geplaatst.

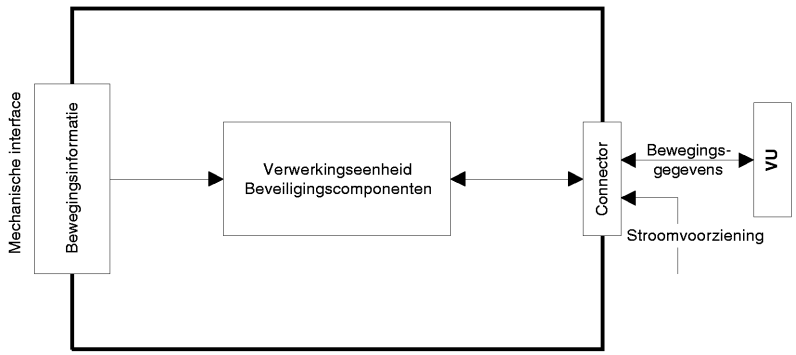
In de operationele modus is de bewegingsopnemer met een VU verbonden.

De opnemer kan ook met een specifieke inrichting voor beheersdoeleinden worden verbonden (TBD door de fabrikant)

De standaardbewegingsopnemer wordt weergegeven in de onderstaande figuur:

Figuur 1

Standaardbewegingsopnemer

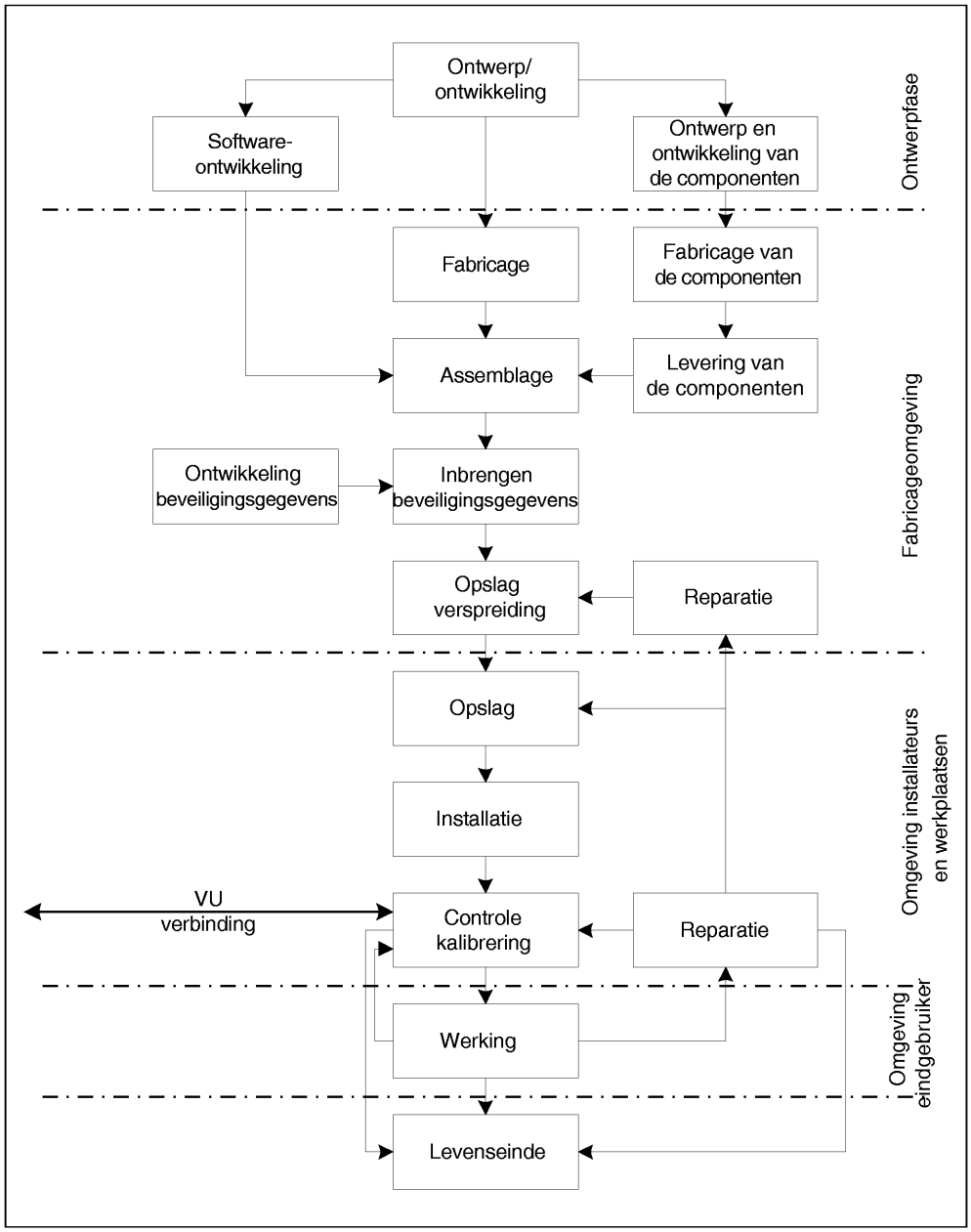


3.2. ***Levenscyclus van de bewegingsopnemer***

De typische levenscyclus van de bewegingsopnemer wordt weergegeven in de onderstaande figuur:

Figuur 2

Typische levenscyclus van de bewegingsopnemer



3.3. ***Bedreigingen***

Dit punt beschrijft de bedreigingen waarmee de bewegingsopnemer geconfronteerd kan worden.

3.3.1. *Bedreigingen voor de toegangsbewaking*

T.Toegang Gebruikers kunnen proberen toegang te krijgen tot niet aan hen toegewezen functies

3.3.2. *Ontwerpgerelateerde bedreigingen*

T.Fouten	Fouten in hardware, software en communicatieprocedures kunnen voor de bewegingsopnemer onvoorziene omstandigheden veroorzaken waardoor de beveiliging in gevaar wordt gebracht
T.Beproevingen	Het gebruik van niet-gevalideerde beproevingsmethoden of van bestaande achterdeurtjes kan de beveiliging van de bewegingsopnemer in gevaar brengen
T.Ontwerp	Gebruikers kunnen illegaal kennis verkrijgen van het ontwerp via het materiaal van de fabrikant (door diefstal, omkoping, enz.) of door ontsleutelen

3.3.3. *Werkingsgerelateerde bedreigingen*

T.Milieu	Gebruikers kunnen de bewegingsopnemer door blootstelling aan omgevingsinvloeden (thermisch, elektromagnetisch, optisch, chemisch, mechanisch, enz.) in gevaar brengen
T.Hardware	Gebruikers kunnen de hardware van de bewegingsopnemer wijzigen
T.Mechanische_Oorsprong	Gebruikers kunnen de invoer van de bewegingsopnemer manipuleren (bijv. de opnemer losschroeven van de versnellingsbak, enz.)
T.Bewegingsgegevens	Gebruikers kunnen de bewegingsgegevens van het voertuig wijzigen (toevoeging, wijziging, verwijdering, signaalherhaling)
T.Stroomvoorziening	Gebruikers kunnen de beveiligingsdoelstellingen van de bewegingsopnemer dwarsbomen door het wijzigen (onderbreken, verminderen, verhogen) van de stroomvoorziening
T.Beveiligingsgegevens	Gebruikers kunnen illegaal kennis verkrijgen van beveiligingsgegevens tijdens het genereren van de beveiligingsgegevens of tijdens transport of opslag in de inrichting
T.Software	Gebruikers kunnen de software van de bewegingsopnemer wijzigen
T.Opgeslagen_gegevens	Gebruikers kunnen opgeslagen gegevens (beveiligings- of gebruikersgegevens) wijzigen

3.4. ***Beveiligingsdoelstellingen***

De belangrijkste beveiligingsdoelstelling van het digitale tachograafsysteem is de volgende:

O.Belangrijkste	De door de controleautoriteiten te controleren gegevens moeten beschikbaar zijn en de activiteiten van de gecontroleerde bestuurders en voertuigen met betrekking tot rijden, werken, beschikbaarheid en rusttijden alsmede de gegevens met betrekking tot de snelheid van het voertuig volledig en nauwkeurig weergeven

De beveiligingsdoelstelling van de bewegingsopnemer, die tot de totale beveiligingsdoelstelling bijdraagt, is derhalve:

O.Opnemer_Belangrijkste	De door de bewegingsopnemer overgebrachte gegevens moeten beschikbaar zijn voor de VU zodat de VU de beweging van het voertuig met betrekking tot snelheid en afgelegde afstand volledig en nauwkeurig kan bepalen

3.5. ***Informatietechnologische beveiligingsdoelstellingen***

De specifieke IT-beveiligingsdoelstellingen van de bewegingsopnemer die tot de belangrijkste beveiligingsdoelstelling bijdragen, zijn de volgende:

O.Toegang	De bewegingsopnemer moet de toegang van aangesloten units tot functies en gegevens controleren
O.Audit	De bewegingsopnemer moet pogingen om de beveiliging te ondermijnen controleren en deze traceren naar aangesloten units
O.Authenticatie	De bewegingsopnemer moet de authenticiteit van aangesloten units vaststellen

O.Verwerking	De bewegingsopnemer moet de nauwkeurige verwerking waarborgen van invoergegevens waarvan bewegingsgegevens worden afgeleid
O.Betrouwbaarheid	De bewegingsopnemer moet betrouwbaar zijn
O.Beveiligde_gegevensuitwisseling	De bewegingsopnemer moet de gegevensuitwisseling met de VU beveiligen

3.6. ***Fysieke, personele of procedurele middelen***

Dit punt beschrijft de fysieke, personele of procedurele voorschriften die tot de beveiliging van de bewegingsopnemer bijdragen.

3.6.1. *Ontwerp van de inrichting*

M.Ontwikkeling	Ontwikkelaars van bewegingsopnemers moeten erop toezien dat bij de toewijzing van verantwoordelijkheden tijdens de ontwikkeling de IT-beveiliging gehandhaafd blijft
M.Fabricage	Fabrikanten van bewegingsopnemers moeten erop toezien dat bij de toewijzing van verantwoordelijkheden tijdens de fabricage de IT-beveiliging gehandhaafd blijft en dat de bewegingsopnemer tijdens het fabricageproces beschermd wordt tegen fysieke agressie die de IT-beveiliging in gevaar kan brengen

3.6.2. *Levering van de inrichting*

M.Levering	Fabrikanten van bewegingsopnemers, voertuigfabrikanten en installateurs of werkplaatsen moeten erop toezien dat bij de behandeling van de bewegingsopnemer de IT-beveiliging gehandhaafd blijft

3.6.3. *Ontwikkeling van beveiligingsgegevens en overdracht*

M.Ontwikkeling_beveiligingsgegevens	Algoritmen voor de ontwikkeling van beveiligingsgegevens moeten uitsluitend voor bevoegde en betrouwbare personen toegankelijk zijn
M.Transport_beveiligingsgegevens	Beveiligingsgegevens moeten zodanig worden gegenereerd, getransporteerd en in de bewegingsopnemer ingebracht dat de vereiste vertrouwelijkheid en integriteit gehandhaafd blijven

3.6.4. *Installatie, kalibrering en controle van het controleapparaat*

M.Erkende_werkplaatsen	Installatie, kalibrering en reparatie van het controleapparaat moeten door betrouwbare en erkende installateurs of werkplaatsen worden uitgevoerd
M.Mechanische_interface	Er moet worden voorzien in middelen om fysieke manipulatie met de mechanische interface op te sporen (bijv. verzegelingen)
M.Regelmatige_controle	Het controleapparaat moet periodiek gecontroleerd en gekalibreerd worden

3.6.5. *Controle op de naleving van de wet*

M.Controles	Controles op naleving van de wet moeten regelmatig en willekeurig worden uitgevoerd en dienen beveiligingsaudits te omvatten

3.6.6. *Softwareaanpassing*

M.Softwareaanpassing	Softwarerevisies moeten een veiligheidscertificatie hebben gekregen voordat ze in een bewegingsopnemer geïmplementeerd kunnen worden

4. **Beveiligingsfuncties**

4.1. ***Identificatie en authenticatie***

UIA_101 De bewegingsopnemer moet voor iedere interactie de identiteit van de aangesloten unit kunnen vaststellen.

UIA_102 De identiteit van een aangesloten unit moet bestaan uit:

— een unitgroep:

— VU,

— beheersinrichting,

— anders,

een unit-ID (alleen bij de VU).

UIA_103 De unit-ID van een aangesloten VU moet uit het goedkeuringsnummer en serienummer van de VU bestaan.

UIA_104 De bewegingsopnemer moet de authenticiteit van iedere aangesloten VU of beheersinrichting kunnen vaststellen:

— bij verbinding van de unit,

— bij herstel van de stroomvoorziening.

UIA_105 De bewegingsopnemer moet de authenticiteit van de aangesloten VU periodiek opnieuw kunnen vaststellen.

UIA_106 De bewegingsopnemer moet het gebruik van gekopieerde en weergegeven authenticatiegegevens kunnen detecteren en verhinderen.

UIA_107 Nadat (TBD door de fabrikant en niet meer dan 20) opeenvolgende niet succesvolle authenticatiepogingen gedetecteerd zijn, moet de SEF:

— een auditregistratie van het voorval genereren;

— de unit waarschuwen;

— bewegingsgegevens in een niet-beveiligde modus blijven exporteren.

4.2. ***Toegangscontrole***

Toegangscontroles garanderen dat uitsluitend bevoegde personen informatie in het TOE kunnen lezen, aanmaken of wijzigen.

4.2.1. *Toegangscontrolebeleid*

ACC_101 De bewegingsopnemer moet toegangsrechten tot functies en gegevens controleren.

4.2.2. *Toegangsrechten tot gegevens*

ACC_102 De bewegingsopnemer moet garanderen dat identificatiegegevens van de bewegingsopnemer slechts eenmaal geschreven kunnen worden (voorschrift 078).

ACC_103 De bewegingsopnemer moet uitsluitend gebruikersgegevens van geauthentiseerde units accepteren en/of opslaan.

ACC_104 De bewegingsopnemer moet de vereiste toegangsrechten betreffende lezen en schrijven van beveiligingsgegevens toepassen.

4.2.3. *Bestandsstructuur en toegangscondities*

ACC_105 De structuur en toegangscondities van toepassings- en gegevensbestanden moeten tijdens het fabricageproces worden aangemaakt en vervolgens voor toekomstige wijzigingen of verwijderingen worden vergrendeld.

4.3. ***Verantwoording***

ACT_101 De bewegingsopnemer moet in zijn geheugen de identificatiegegevens van de bewegingsopnemer opslaan (voorschrift 077).

ACT_102 De bewegingsopnemer moet in zijn geheugen de installatiegegevens opslaan (voorschrift 099).

ACT_103 De bewegingsopnemer moet de mogelijkheid hebben om op verzoek verantwoordingsgegevens naar geauthentiseerde units uit te voeren.

4.4. ***Audit***

AUD_101 De bewegingsopnemer moet bij voorvallen die zijn beveiliging in gevaar brengen, auditregistraties van de voorvallen genereren.

AUD_102 De voorvallen die van invloed zijn op de beveiliging van de bewegingsopnemer, zijn de volgende:

— pogingen tot inbreuk op de beveiliging:

  — authenticatiefout;

  — integriteitsfout in opgeslagen gegevens;

  — overdrachtsfout in interne gegevens;

  — niet-geautoriseerde opening van de behuizing;

  — sabotage van de hardware;

— fout in de opnemer.

AUD_103 Auditregistraties moeten de onderstaande gegevens bevatten:

— datum en tijd van het voorval;

— soort voorval;

— identiteit van de aangesloten unit.

Wanneer de vereiste gegevens niet beschikbaar zijn, wordt een geschikte standaardindicatie gegeven (TBD door de fabrikant).

AUD_104 De bewegingsopnemer moet de gegenereerde auditregistraties zodra deze worden gegenereerd naar de VU sturen en kan deze ook in zijn geheugen opslaan.

AUD_105 Als de bewegingsopnemer auditregistraties opslaat, moet deze ervoor zorgen dat 20 auditregistraties onafhankelijk van het vol raken van de auditgeheugen kunnen worden bewaard en moet de opnemer de mogelijkheid hebben om — op verzoek — opgeslagen auditregistraties naar geauthentiseerde units uit te voeren.

4.5. ***Nauwkeurigheid***

4.5.1. *Controlebeleid met betrekking tot de informatiestroom*

ACR_101 De bewegingsopnemer moet ervoor zorgen dat bewegingsgegevens uitsluitend kunnen worden verwerkt en afgeleid van de mechanische invoer van de opnemer.

4.5.2. *Overdracht van interne gegevens*

De voorschriften van dit punt zijn alleen van toepassing indien de bewegingsopnemer gebruik maakt van fysiek afzonderlijke delen.

ACR_102 Indien gegevens tussen de fysiek afzonderlijke delen van de bewegingsopnemer worden overdragen, moeten de gegevens tegen wijzigingen worden beveiligd.

ACR_103 Na detectie van een gegevensoverdrachtsfout tijdens een interne overdracht moet de overbrenging worden weergegeven en moet de SEF een auditregistratie van het voorval genereren.

4.5.3. *Integriteit van opgeslagen gegevens*

ACR_104 De bewegingsopnemer moet de in het geheugen opgeslagen gebruikersgegevens op integriteitsfouten controleren.

ACR_105 Na detectie van een integriteitsfout in de opgeslagen gebruikersgegevens moet de SEF een auditregistratie genereren.

4.6. ***Betrouwbaarheid van de werking***

4.6.1 *Beproevingen*

RLB_101 Alle opdrachten, acties, of testpunten, die specifiek zijn voor de beproevingen in de fabricagefase, moeten voor het einde van de fabricagefase worden geblokkeerd of verwijderd. Het is niet mogelijk om deze voor toekomstig gebruik terug te zetten.

RLB_102 De bewegingsopnemer moet tijdens de eerste start en tijdens normaal bedrijf zelfbeproevingen uitvoeren om de juiste werking te verifiëren. De zelfbeproevingen van de bewegingsopnemer moeten een verificatie van de integriteit van de beveiligingsgegevens en een verificatie van de integriteit van de opgeslagen uitvoercode (indien niet in ROM) bevatten.

RLB_103 Na detectie van een interne fout tijdens een zelfbeproeving moet de SEF een auditregistratie genereren (fout in de opnemer).

4.6.2. *Software*

RLB_104 Het analyseren of debuggen van de software van de bewegingsopnemer in het veld is niet mogelijk.

RLB_105 Invoergegevens afkomstig uit externe bronnen worden niet als uitvoerbare code geaccepteerd.

4.6.3. *Fysieke bescherming*

RLB_106 Indien de bewegingsopnemer zodanig ontworpen is dat hij geopend kan worden, moet de bewegingsopnemer elke opening van de behuizing detecteren, zelfs zonder externe stroomvoorziening gedurende ten minste 6 maanden. In dit geval moet de SEF een auditregistratie van het voorval genereren (de auditregistratie kan na herstel van de stroomvoorziening gegenereerd en opgeslagen worden).

Indien de bewegingsopnemer zodanig ontworpen is dat hij niet geopend kan worden, moet hij zodanig geconstrueerd zijn dat fysieke manipulatiepogingen gemakkelijk gedetecteerd kunnen worden (bijv. door visuele inspectie).

RLB_107 De bewegingsopnemer moet gespecificeerde (TBD door de fabrikant) hardwaresabotage detecteren.

RLB_108 In het bovengenoemde geval moet de SEF een auditregistratie genereren en moet de bewegingsopnemer: (TBD door de fabrikant).

4.6.4. *Onderbrekingen in de stroomvoorziening*

RLB_109 De bewegingsopnemer moet tijdens een onderbreking van of schommelingen in de stroomvoorziening in een veilige toestand blijven.

4.6.5. *Terugstelvoorwaarden*

RLB_110 In het geval van onderbreking van de stroomvoorziening, of wanneer een transactie voor de voltooiing wordt afgebroken, of bij andere terugstelvoorwaarden, moet de bewegingsopnemer correct worden teruggesteld.

4.6.6. *Beschikbaarheid van gegevens*

RLB_111 De bewegingsopnemer moet ervoor zorgen dat — indien vereist — toegang tot systeemelementen wordt verkregen en dat systeemelementen niet onnodig worden opgevraagd of vastgehouden.

4.6.7. *Meervoudige toepassingen*

RLB_112 Indien de bewegingsopnemer andere toepassingen dan de tachograaftoepassing levert, moeten alle toepassingen fysiek en/of logisch onderscheidbaar zijn. Deze toepassingen delen geen beveiligingsgegevens. Er is maar een taak tegelijk actief.

4.7. ***Gegevensuitwisseling***

DEX_101 De bewegingsopnemer moet bewegingsgegevens met de bijbehorende beveiligingskenmerken naar de VU uitvoeren, zodat de VU de integriteit en authenticiteit kan verifiëren.

4.8. ***Cryptografische ondersteuning***

De voorschriften van dit punt zijn alleen waar nodig van toepassing, afhankelijk van de gebruikte beveiligingsmechanismen en de oplossingen van de fabrikant.

CSP_101 Elke cryptografische door de bewegingsopnemer uitgevoerde bewerking moet in overeenstemming zijn met een gespecificeerde algoritme en een gespecificeerd sleutelformaat.

CSP_102 Indien de bewegingsopnemer cryptografische sleutels genereert, moet dit in overeenstemming zijn met gespecificeerde ontwikkelingsalgoritmen van cryptografische sleutels en met gespecificeerde formaten van cryptografische sleutels.

CSP_103 Indien de bewegingsopnemer cryptografische sleutels verspreidt, moet dit in overeenstemming zijn met gespecificeerde verspreidingsmethoden voor dergelijke sleutels.

CSP_104 Indien de bewegingssensor toegang heeft tot cryptografische sleutels, moet dit in overeenstemming zijn met gespecificeerde toegangsmethoden voor dergelijke sleutels.

CSP_105 Indien de bewegingsopnemer cryptografische sleutels vernietigt, moet dit in overeenstemming zijn met gespecificeerde vernietigingsmethoden voor dergelijke sleutels.

5. **Definitie van beveiligingsmechanismen**

De beveiligingsmechanismen die de beveiligingsfuncties van de bewegingsopnemer uitvoeren worden gedefinieerd door de fabrikanten van de bewegingsopnemers.

6. **Minimumsterkte van beveiligingsmechanismen**

De minimumsterkte van de beveiligingsmechanismen van de bewegingsopnemer is Hoog, zoals gedefinieerd in referentienorm ITSEC.

7. **Garantieniveau**

Het nagestreefde garantieniveau voor de bewegingsopnemer is ITSEC niveau E3, zoals gedefinieerd in referentienorm ITSEC.

8. **Ratio**

De onderstaande tabellen geven een ratio voor de SEF's aan:

— welke SEF's of middelen welke bedreigingen tegengaan;

— welke SEF's aan welke IT-beveiligingsdoelstellingen voldoen.

	Bedreigingen												IT-doelstellingen					
	T.Toegang	T.Fouten	T.Beproevingen	T.Ontwerp	T.Milieu	T.Hardware	T.Mechanische_Oorsprong	T.Bewegingsgegevens	T.Stroomvoorziening	T.Beveiligingsgegevens	T.Software	T.Opgeslagen_gegevens	O.Toegang	O.Audit	O.Authenticatie	O.Verwerking	O.Betrouwbaarheid	O.Beveiligde_gegevens-uitwisseling
Fysieke personele procedurele middelen																		
Ontwikkeling		x	x	x														
Fabricage			x	x														
Levering						x					x	x						
Ontwikkeling beveiligingsgegevens										x								
Transport beveiligingsgegevens										x								
Erkende werkplaatsen							x											
Mechanische interface							x											
Regelmatige controle						x	x		x		x							
Controles op naleving van de wet					x	x	x		x	x	x							
Softwareaanpassing											x							
Beveiligingsfuncties																		
Identificatie en authenticatie																		
UIA_101 Unit-identificatie	x							x					x		x			x
UIA_102 Unit-identiteit	x												x		x			
UIA_103 VU-identiteit														x				
UIA_104 Unit-authenticatie	x							x					x		x			x
UIA_105 Herauthenticatie	x							x					x		x			x
UIA_106 Onvervalsbare authenticatie	x							x					x		x			
UIA_107 Authenticatiefout								x						x			x	
Toegangscontrole																		
ACC_101 Beleid toegangscontrole	x									x		x	x					
ACC_102 ID bewegingsopnemer												x	x					

	Bedreigingen												IT-doelstellingen					
	T.Toegang	T.Fouten	T.Beproevingen	T.Ontwerp	T.Milieu	T.Hardware	T.Mechanische_Oorsprong	T.Bewegingsgegevens	T.Stroomvoorziening	T.Beveiligingsgegevens	T.Software	T.Opgeslagen_gegevens	O.Toegang	O.Audit	O.Authenticatie	O.Verwerking	O.Betrouwbaarheid	O.Beveiligde_gegevens-uitwisseling
ACC_103 Gebruikersgegevens												x	x					
ACC_104 Beveiligingsgegevens										x		x	x					
ACC_105 Bestandsstructuur en toegangscondities	x									x		x	x					
Verantwoording																		
ACT_101 ID-gegevens bewegingsopnemer														x				
ACT_102 Verbindingsgegevens														x				
ACT_103 Verantwoordingsgegevens														x				
Audit																		
AUD_101 Auditregistraties														x				
AUD_102 Voorvallenlijst audit	x				x	x						x		x				
AUD_103 Auditgegevens														x				
AUD_104 Audit-instrumenten														x				
AUD_105 Opslag auditregistraties														x				
Nauwkeurigheid																		
ACR_101 Controlebeleid informatiestroom								x								x	x	
ACR_102 Interne overdracht																x	x	
ACR_103 Interne overdracht														x				
ACR_104 Integriteit opgeslagen gegevens												x					x	
ACR_105 Integriteit opgeslagen gegevens												x		x				
Betrouwbaarheid																		
RLB_101 Fabricagebeproevingen			x	x													x	
RLB_102 Zelfbeproevingen		x				x			x		x						x	
RLB_103 Zelfbeproevingen						x			x		x			x				
RLB_104 Softwareanalyse				x							x						x	
RLB_105 Software-invoer											x					x	x	
RLB_106 Opening behuizing				x	x	x				x	x	x					x	
RLB_107 Hardwaresabotage						x											x	
RLB_108 Hardwaresabotage						x								x				
RLB_109 Onderbreking stroomvoorziening									x								x	
RLB_110 Terugstellen		x															x	
RLB_111 Beschikbaarheid gegevens																x	x	
RLB_112 Meervoudige toepassingen																	x	
Gegevensuitwisseling																		
DEX_101 Beveiligde uitvoer bewegingsgegevens								x										x
Cryptografische ondersteuning																		
CSP_101 Algoritmen																	x	x
CSP_102 Ontwikkeling sleutel																	x	x
CSP_103 Verspreiding sleutel																	x	x
CSP_104 Toegang sleutel																	x	x
CSP_105 Vernietiging sleutel																	x	x

ALGEMENE BEVEILIGINGSDOELSTELLING VAN DE VOERTUIGUNIT

1. **Inleiding**

Dit document bevat een beschrijving van de voertuigunit, van de door de VU te neutraliseren bedreigingen en van de te realiseren beveiligingsdoelstellingen. Het specificeert de vereiste beveiligingsfuncties. Het stelt de vereiste minimumsterkte van beveiligingsmechanismen en het vereiste garantieniveau voor de ontwikkeling en beproeving vast.

De voorschriften waarnaar in het document wordt verwezen, staan in de tekst van bijlage I B. Voor de duidelijkheid treedt er soms herhaling op tussen de voorschriften in de tekst van bijlage I B en de voorschriften van de beveiligingsdoelstelling. In geval van onduidelijkheid tussen een voorschrift van de beveiligingsdoelstelling en een voorschrift van bijlage I B waarnaar in dit document wordt verwezen, geldt het voorschrift van bijlage I B.

Voorschriften van bijlage I B die in de beveiligingsdoelstellingen niet worden genoemd zijn geen onderwerp van de beveiligingsfuncties.

Er zijn unieke labels toegewezen aan bedreigingen, doelstellingen, procedurele middelen en SEF-specificaties zodat deze gemakkelijk in ontwikkelings- en evaluatiedocumentatie terug te vinden zijn.

2. **Afkortingen, definities en referenties**

2.1. ***Afkortingen***

PIN	Personal identification number (PIN-code)
ROM	Read only memory (ROM-geheugen)
SEF	Security enforcing function (beveiligingsfunctie)
TBD	To be defined (nog te bepalen)
TOE	Target of evaluation (doel van de evaluatie)
VU	Vehicle unit (voertuigunit)

2.2. ***Definities***

Digitale tachograaf	Controleapparaat
Bewegingsgegevens	De gegevens betreffende snelheid en afgelegde afstand die met de bewegingsopnemer worden uitgewisseld
Fysiek gescheiden delen	Fysieke componenten van de bewegingsopnemer die zich op verschillende plaatsen in het voertuig bevinden, in tegenstelling met fysieke, in de behuizing van de bewegingsopnemer ondergebrachte componenten
Beveiligingsgegevens	De specifieke gegevens ter ondersteuning van de beveiligingsfuncties (bijv. cryptosleutels)
Systeem	Inrichtingen, mensen of organisaties die op de een of andere manier bij het controleapparaat betrokken zijn
Gebruiker	Menselijke gebruikers van de apparatuur. Normale gebruikers van de VU zijn bestuurders, controleurs, werkplaatsen en bedrijven
Gebruikersgegevens	Door de VU geregistreerde en opgeslagen gegevens, anders dan beveiligingsgegevens, zoals omschreven in hoofdstuk III.12

2.3. ***Referentienormen***

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991

3. **Productratio**

3.1. ***Beschrijving van de voertuigunit en gebruiksaanwijzing***

De VU is bedoeld voor installatie in voertuigen voor het wegvervoer. Het doel ervan is het registreren, opslaan, zichtbaar maken, afdrukken en uitvoeren van gegevens betreffende de activiteiten van de bestuurder.

De VU is verbonden met een bewegingsopnemer, waarmee de unit bewegingsgegevens van het voertuig uitwisselt.

Gebruikers identificeren zich met een tachograafkaart bij de VU.

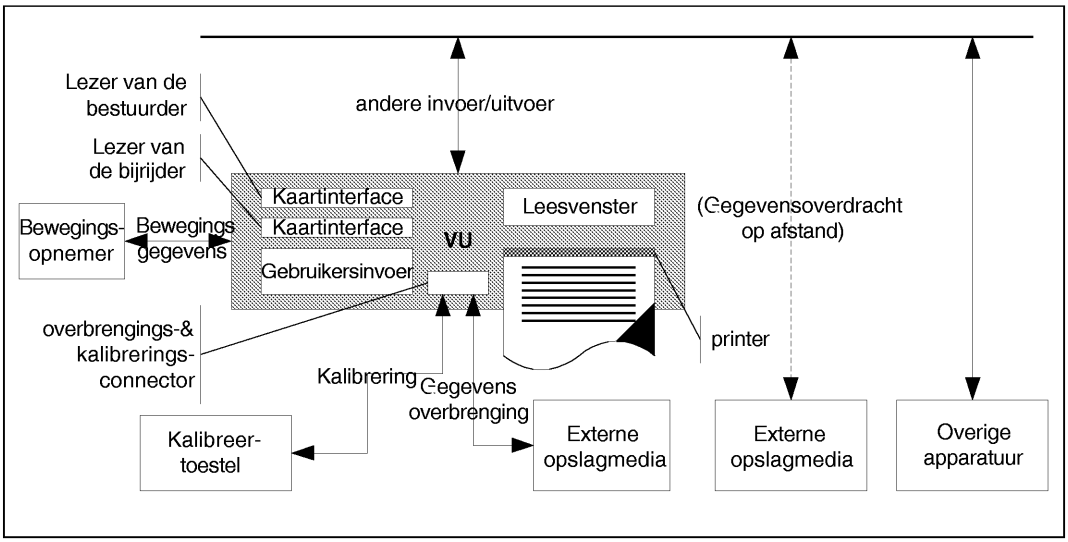
De VU registreert gegevens over de activiteiten van de gebruiker en slaat deze in zijn geheugen op. Hij registreert ook gegevens over de activiteiten van de gebruiker op de tachograafkaarten.

De VU voert gegevens uit naar leesvenster, printer en externe inrichtingen.

De operationele omgeving van de in een voertuig geïnstalleerde voertuigunit is weergegeven in de onderstaande figuur:

Figuur 2

Operationele omgeving van VU



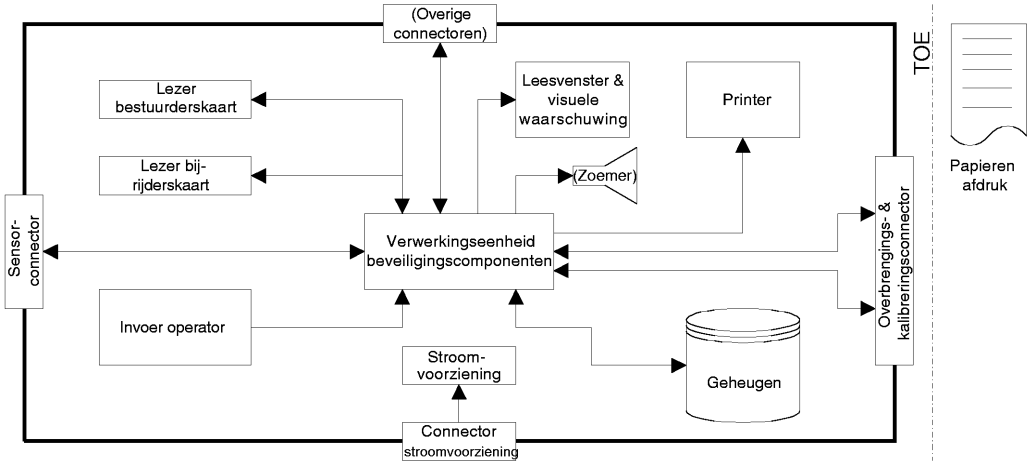
De algemene kenmerken, functies en werkingsmodi worden beschreven in hoofdstuk II van bijlage I B.

De functionele voorschriften van de VU worden beschreven in hoofdstuk III van bijlage I B.

De standaard-VU wordt weergegeven in de onderstaande figuur:

Figuur 3

Standaard-VU (…) facultatief



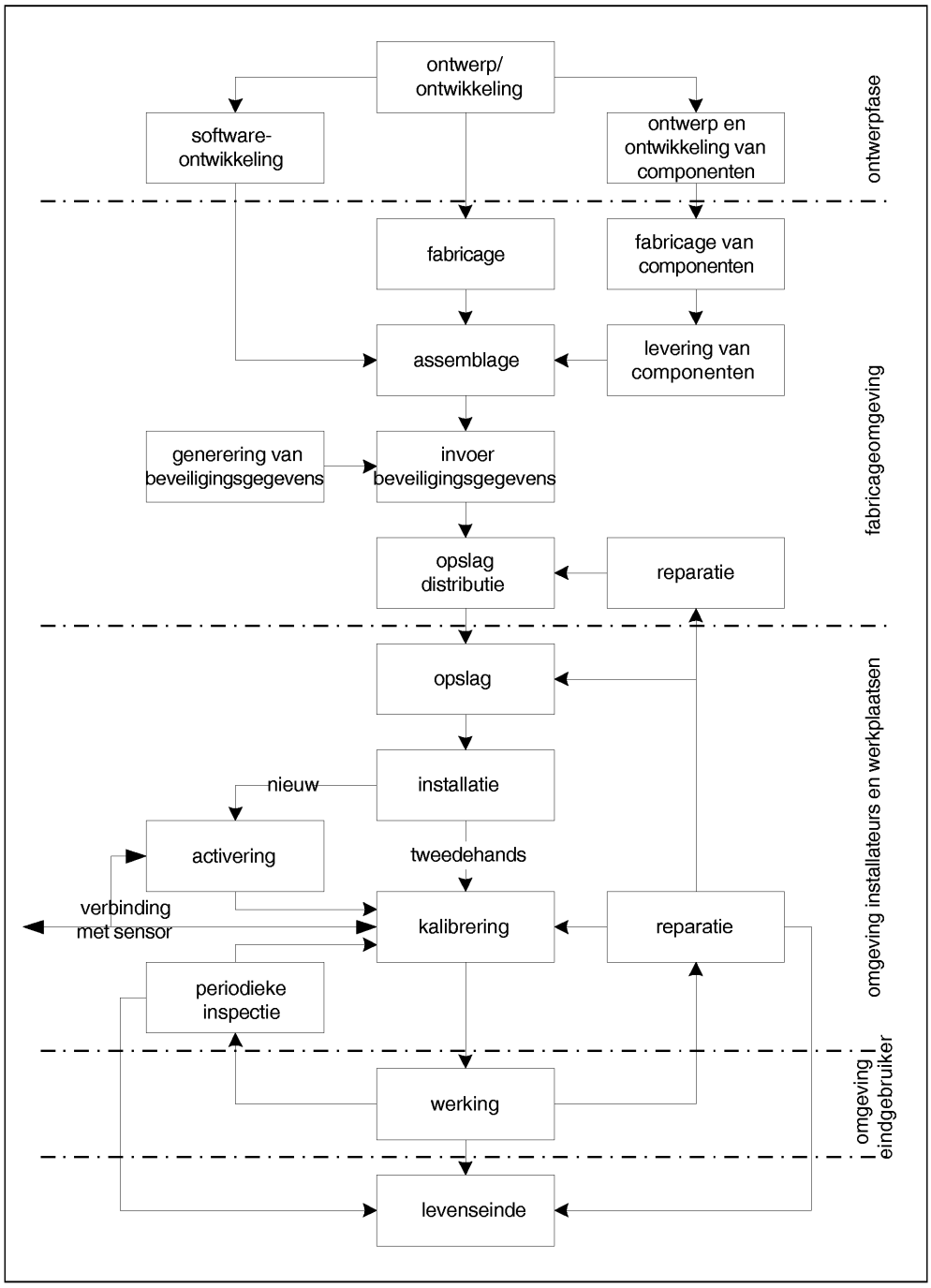
Opgemerkt wordt dat de printerinrichting deel uitmaakt van het TOE, maar dat het eenmaal geproduceerde papieren document hier geen deel van uitmaakt.

3.2. ***Levenscyclus van de voertuigunit***

De typische levenscyclus van de VU wordt weergegeven in de onderstaande figuur:

Figuur 4

Typische levenscyclus van de VU



3.3. ***Bedreigingen***

Dit punt beschrijft de bedreigingen waarmee de VU geconfronteerd kan worden.

3.3.1. *Bedreigingen voor identificatie en toegangsbewaking*

T.Toegang	Gebruikers kunnen toegang krijgen tot niet aan hen toegewezen functies (bijv. bestuurders krijgen toegang tot de kalibreringsfunctie)
T.Identificatie	Gebruikers kunnen verscheidene identificaties of geen identificatie gebruiken

3.3.2. *Ontwerpgerelateerde bedreigingen*

T.Fouten	Fouten in hardware, software en communicatieprocedures kunnen voor de VU onvoorziene omstandigheden veroorzaken waardoor de beveiliging in gevaar wordt gebracht
T.Beproevingen	Het gebruik van niet-gevalideerde beproevingsmethoden of van bestaande achterdeurtjes kan de beveiliging van de VU in gevaar brengen
T.Ontwerp	Gebruikers kunnen illegaal kennis verkrijgen van het ontwerp via het materiaal van de fabrikant (door diefstal, omkoping, enz.) of door ontsleuteling

3.3.3. *Werkingsgerelateerde bedreigingen*

T.Kalibreringsparameters	Gebruikers kunnen onjuist gekalibreerde inrichtingen gebruiken (door wijziging van de kalibreringsgegevens of door organisatorisch zwakke punten)
T.Gegevensuitwisseling_van_de_kaart	Gebruikers kunnen gegevens wijzigen terwijl deze tussen de VU en de tachograafkaart worden uitgewisseld (toevoeging, wijziging, verwijdering, signaalherhaling)
T.Klok	Gebruikers kunnen de interne klok manipuleren
T.Milieu	Gebruikers kunnen de beveiliging van de VU door blootstelling aan omgevingsinvloeden (thermisch, elektromagnetisch, optisch, chemisch, mechanisch, enz.) in gevaar brengen
T.Valse_inrichtingen	Gebruikers kunnen valse inrichtingen (bewegingsopnemer, smartcards) met de VU verbinden
T.Hardware	Gebruikers kunnen de hardware van de VU wijzigen
T.Bewegingsgegevens	Gebruikers kunnen de bewegingsgegevens van het voertuig wijzigen (toevoeging, wijziging, verwijdering, signaalherhaling)
T.Niet-geactiveerd	Gebruikers kunnen niet-geactiveerde inrichtingen gebruiken
T.Uitvoergegevens	Gebruikers kunnen uitvoergegevens wijzigen (afdrukken, tonen of overbrengen)
T.Stroomvoorziening	Gebruikers kunnen de beveiligingsdoelstellingen van de VU dwarsbomen door het wijzigen (onderbreken, verminderen, verhogen) van de stroomvoorziening
T.Beveiligingsgegevens	Gebruikers kunnen illegaal kennis verkrijgen van beveiligingsgegevens tijdens het genereren van de beveiligingsgegevens of tijdens transport of opslag in de inrichting
T.Software	Gebruikers kunnen de software van de VU wijzigen
T.Opgeslagen_gegevens	Gebruikers kunnen opgeslagen gegevens (beveiligings- of gebruikersgegevens) wijzigen

3.4. ***Beveiligingsdoelstellingen***

De belangrijkste beveiligingsdoelstelling van het digitale tachograafsysteem is de volgende:

O.Belangrijkste	De door de controleautoriteiten te controleren gegevens moeten beschikbaar zijn en de activiteiten van de gecontroleerde bestuurders en voertuigen met betrekking tot rijden, werken, beschikbaarheid en rusttijden alsmede de gegevens met betrekking tot de snelheid van het voertuig volledig en nauwkeurig weergeven

De beveiligingsdoelstellingen van de VU die tot de totale beveiligingsdoelstelling bijdragen, zijn derhalve:

O.VU_Belangrijkste	De te meten en te registreren en vervolgens door de controleautoriteiten te controleren gegevens moeten beschikbaar zijn en de activiteiten van de gecontroleerde bestuurders en voertuigen met betrekking tot rijden, werken, beschikbaarheid en rusttijden alsmede de gegevens met betrekking tot de snelheid van het voertuig nauwkeurig weergeven
O.VU_Uitvoer	De VU moet gegevens zodanig naar externe opslagmedia uitvoeren dat de integriteit en authenticiteit geverifieerd kunnen worden

3.5. ***Informatietechnologische beveiligingsdoelstellingen***

De specifieke IT-beveiligingsdoelstellingen van de VU die tot de belangrijkste beveiligingsdoelstellingen bijdragen, zijn de volgende:

O.Toegang	De VU moet de toegang van de gebruiker tot functies en gegevens controleren
O.Verantwoording	De VU moet nauwkeurige verantwoordingsgegevens verzamelen
O.Audit	De VU moet pogingen om de systeemveiligheid te ondermijnen controleren en deze traceren naar aangesloten gebruikers
O.Authenticatie	De VU moet de authenticiteit van gebruikers en aangesloten units vaststellen (wanneer een betrouwbaar pad tussen units ontwikkeld moet worden)
O.Integriteit	De VU moet de integriteit van opgeslagen gegevens handhaven
O.Uitvoer	De VU moet ervoor zorgen dat de gegevensuitvoer de gemeten en opgeslagen gegevens nauwkeurig weergeeft
O.Verwerking	De VU moet ervoor zorgen dat de verwerking van invoergegevens ter verkrijging van gebruikersgegevens nauwkeurig is
O.Betrouwbaarheid	De VU moet betrouwbaar zijn
O.Beveiligde_gegevensuitwisseling	De VU moet de gegevensuitwisseling met de bewegingsopnemer en met de tachograafkaarten beveiligen

3.6. ***Fysieke, personele of procedurele middelen***

Dit punt beschrijft de fysieke, personele of procedurele voorschriften die tot de beveiliging van de VU bijdragen.

3.6.1. *Ontwerp van de apparatuur*

M.Ontwikkeling	Ontwikkelaars van VU's moeten erop toezien dat bij de toewijzing van verantwoordelijkheden tijdens de ontwikkeling de IT-beveiliging gehandhaafd blijft
M.Fabricage	Fabrikanten van VU's moeten erop toezien dat bij de toewijzing van verantwoordelijkheden tijdens de fabricage de IT-beveiliging gehandhaafd blijft en dat de VU tijdens het fabricageproces tegen fysieke agressie, die de IT-beveiliging in gevaar kan brengen, wordt beschermd

3.6.2. *Levering en activering van de apparatuur*

M.Levering	Fabrikanten van VU's, voertuigfabrikanten en installateurs of werkplaatsen moeten erop toezien dat bij de behandeling van een niet-geactiveerde VU de beveiliging van de VU gehandhaafd blijft
M.Activering	Voertuigfabrikanten en installateurs of werkplaatsen moeten de VU na de installatie activeren voordat het voertuig het bedrijf verlaat waar de installatie plaatsvond

3.6.3. *Ontwikkeling van beveiligingsgegevens en overdracht*

M.Ontwikkeling_beveiligingsgegevens	Algoritmen voor de ontwikkeling van beveiligingsgegevens moeten uitsluitend voor bevoegde en betrouwbare personen toegankelijk zijn
M.Transport_beveiligingsgegevens	Beveiligingsgegevens moeten zodanig gegenereerd, getransporteerd en in de VU ingebracht worden dat de vereiste vertrouwelijkheid en integriteit gehandhaafd blijft

3.6.4. *Levering van kaarten*

M.Beschikbaarheid	Tachograafkaarten moeten uitsluitend voor bevoegde personen beschikbaar zijn
M.Een_enkele_bestuurderskaart	Bestuurders mogen maar één geldige bestuurderskaart in hun bezit hebben
M.Traceerbaarheid_van_de_kaart	Levering van de kaart moet traceerbaar zijn (witte lijsten, zwarte lijsten) en zwarte lijsten moeten tijdens beveiligingsaudits worden gebruikt

3.6.5. *Installatie, kalibrering en controle van het controleapparaat*

M.Erkende_werkplaatsen	Installatie, kalibrering en reparatie van het controleapparaat moeten door betrouwbare en erkende installateurs of werkplaatsen worden uitgevoerd
M.Regelmatige_controle	Het controleapparaat moet periodiek gecontroleerd en gekalibreerd worden
M.Nauwkeurige_kalibrering	Erkende installateurs en werkplaatsen moeten tijdens de kalibrering de juiste voertuigparameters in het controleapparaat invoeren

3.6.6. *Bediening van de apparatuur*

M.Betrouwbare_bestuurders	Bestuurders moeten volgens de regels en verantwoordelijk te werk gaan (bijv. hun bestuurderskaart gebruiken, handmatig te selecteren activiteiten correct selecteren, enz.)

3.6.7. *Controle op de naleving van de wet*

M.Controles	Controles op naleving van de wet moeten regelmatig en willekeurig worden uitgevoerd en dienen beveiligingsaudits te omvatten

3.6.8. *Softwareaanpassing*

M.Softwareaanpassing	Softwarerevisies moeten een veiligheidscertificatie hebben gekregen voordat ze in een VU geïmplementeerd kunnen worden

4. **Beveiligingsfuncties**

4.1. ***Identificatie en authenticatie***

4.1.1. *Identificatie en authenticatie van de bewegingsopnemer*

UIA_201 De VU moet voor iedere interactie de identiteit van de aangesloten bewegingsopnemer kunnen vaststellen.

UIA_202 De identiteit van de bewegingsopnemer moet uit het goedkeuringsnummer en het serienummer van de opnemer bestaan.

UIA_203 De VU moet de authenticiteit vaststellen van de bewegingsopnemer waarmee de VU verbonden is:

— bij de aansluiting met bewegingsopnemer;

— bij elke kalibrering van het controleapparaat;

— bij herstel van de stroomvoorziening.

Authenticatie moet wederzijds zijn en door de VU worden gestart.

UIA_204 De VU moet periodiek (periode TBD door de fabrikant en meer dan een keer per uur) de identiteit en authenticiteit van de aangesloten bewegingsopnemer opnieuw vaststellen en controleren of de tijdens de laatste kalibrering geïdentificeerde bewegingsopnemer van het controleapparaat niet werd omgewisseld.

UIA_205 De VU moet gekopieerde en weergegeven authenticatiegegevens detecteren en het gebruik ervan verhinderen.

UIA_206 Nadat (TBD door de fabrikant en niet meer dan 20) opeenvolgende niet succesvolle authenticatiepogingen gedetecteerd worden en/of na de ontdekking dat de identiteit van de bewegingsopnemer ongeautoriseerd veranderd is (d.w.z. niet tijdens kalibrering van het controleapparaat), moet de SEF:

— een auditregistratie van het voorval genereren;

— de gebruiker waarschuwen;

— niet-beveiligde door de bewegingsopnemer gestuurde gegevens blijven accepteren en gebruiken.

4.1.2. *Identificatie en authenticatie van de gebruiker*

UIA_207 De VU moet permanent en selectief de identiteit van twee gebruikers traceren door middel van het controleren van de tachograafkaarten die respectievelijk in de lezer van de bestuurder en de lezer van de bijrijder van de inrichting ingebracht zijn.

UIA_208 De identiteit van de gebruiker moet bestaan uit:

— een gebruikersgroep:

  — BESTUURDER (bestuurderskaart),

  — CONTROLEUR (controlekaart),

  — WERKPLAATS (werkplaatskaart),

  — BEDRIJF (bedrijfskaart),

  — ONBEKEND (geen kaart ingebracht),

  een gebruikers-ID, bestaande uit:

  — de code van de lidstaat die de kaart afgeeft en het kaartnummer,

  — ONBEKEND wanneer de gebruikersgroep ONBEKEND is.

ONBEKENDE identiteiten kunnen impliciet of expliciet bekend zijn.

UIA_209 De VU moet de authenticiteit van de gebruikers bij kaartinbrenging vaststellen.

UIA_210 De VU moet de authenticiteit van de gebruikers opnieuw vaststellen:

— bij herstel van de stroomvoorziening;

— periodiek of na het optreden van specifieke voorvallen (TBD door de fabrikant en vaker dan één keer per dag).

UIA_211 Authenticatie van een geldige kaart moet worden uitgevoerd door middel van verificatie van de ingebrachte tachograafkaart met beveiligingsgegevens die alleen door het systeem kunnen worden doorgegeven. Authenticatie moet wederzijds zijn en door de VU worden gestart.

UIA_212 Bovendien moet de authenticiteit van werkplaatsen door controle van een PIN-code succesvol worden bevestigd. PIN-codes moeten ten minste 4 tekens bevatten.

Opmerking: als de PIN-code door een externe, in de nabijheid van de VU gelegen inrichting naar de VU wordt overgezonden, hoeft de vertrouwelijkheid van de PIN-code tijdens de overzending niet beschermd te worden.

UIA_213 De VU moet het gebruik van gekopieerde en weergegeven authenticatiegegevens detecteren en verhinderen.

UIA_214 Nadat 5 opeenvolgende niet-succesvolle authenticatiepogingen gedetecteerd zijn, moet de SEF:

— een auditregistratie van het voorval genereren;

— de gebruiker waarschuwen;

— aannemen dat de gebruiker ONBEKEND is en dat de kaart ongeldig is (definitie z en voorschrift 007).

4.1.3. *Identificatie en authenticatie van een op afstand aangesloten bedrijf*

Verbinding met een bedrijf op afstand is optioneel. Dit punt is derhalve alleen van toepassing indien deze voorziening geïmplementeerd is.

UIA_215 Voor elke interactie met een op afstand aangesloten bedrijf moet de VU de identiteit van het bedrijf kunnen vaststellen.

UIA_216 De identiteit van een op afstand aangesloten bedrijf moet bestaan uit de code van de lidstaat van afgifte van de bedrijfskaart en het bedrijfskaartnummer.

UIA_217 De VU moet voor de gegevensoverdracht de authenticiteit van het op afstand aangesloten bedrijf succesvol vaststellen.

UIA_218 Authenticatie moet worden uitgevoerd door middel van verificatie of het bedrijf een geldige bedrijfskaart heeft met beveiligingsgegevens die alleen door het systeem kunnen worden doorgegeven.

UIA_219 De VU moet het gebruik van gekopieerde en weergegeven authenticatiegegevens detecteren en verhinderen.

UIA_220 Nadat 5 opeenvolgende niet-succesvolle authenticatiepogingen gedetecteerd zijn, moet de VU:

— het op afstand aangesloten bedrijf waarschuwen.

4.1.4. *Identificatie en authenticatie van de beheersinrichting*

VU-fabrikanten kunnen toepassingsgerichte inrichtingen voor additionele beheersfuncties van de VU (bijv. softwareaanpassing, opnieuw laden van beveiligingsgegevens, enz.) installeren. Dit punt is derhalve alleen van toepassing indien deze voorziening geïmplementeerd is.

UIA_221 Bij iedere interactie met een beheersinrichting moet de VU de identiteit van de inrichting vaststellen.

UIA_222 Voor iedere volgende interactie moet de VU de authenticiteit van de beheersinrichting succesvol vaststellen.

UIA_223 De VU moet het gebruik van gekopieerde en weergegeven authenticatiegegevens detecteren en verhinderen.

4.2. ***Toegangscontrole***

Toegangscontroles garanderen dat uitsluitend bevoegde personen informatie in het TOE kunnen lezen, aanmaken of wijzigen.

Opgemerkt wordt dat de door de VU geregistreerde gebruikersgegevens, hoewel deze privacyaspecten of commercieel gevoelige aspecten kunnen bevatten, niet vertrouwelijk zijn. Het functionele voorschrift betreffende toegangsrechten voor het lezen van gegevens (voorschrift 011) is derhalve niet van toepassing op een beveiligingsfunctie.

4.2.1. *Toegangscontrolebeleid*

ACC_201 De VU moet toegangsrechten tot functies en gegevens beheren en controleren.

4.2.2. *Toegangsrechten tot functies*

ACC_202 De VU moet de selectieregels voor werkingsmodi (voorschriften 006 tot 009) toepassen.

ACC_203 De VU moet de werkingsmodus gebruiken om de regels voor toegangsrechten tot functies (voorschrift 010) toe te passen.

4.2.3. *Toegangsrechten tot gegevens*

ACC_204 De VU moet de toegangsregels voor het schrijven van de identificatiegegevens van de VU (voorschrift 076) toepassen.

ACC_205 De VU moet de toegangsregels voor het schrijven van identificatiegegevens van de gekoppelde bewegingsopnemer (voorschrift 079 en 155) toepassen.

ACC_206 Na activering van de VU moet de VU ervoor zorgen dat gegevens alleen in de kalibereringsmodus in de VU ingevoerd en in het geheugen daarvan opgeslagen kunnen worden (voorschrift 154 en 156).

ACC_207 Na activering van de VU moet de VU toegangsregels voor het schrijven en wissen van kalibreringsgegevens (voorschrift 097) toepassen.

ACC_208 Na activering van de VU moet de VU ervoor zorgen dat tijdafstellingsgegevens alleen in de kalibreringsmodus in de VU ingevoerd en in het geheugen daarvan opgeslagen kunnen worden (dit voorschrift is niet van toepassing op kleine tijdafstellingen overeenkomstig voorschrift 157 en 158).

ACC_209 Na activering van de VU moet de VU toegangsregels voor het schrijven en wissen van tijdafstellingsgegevens (voorschrift 100) toepassen.

ACC_210 De VU moet de vereiste toegangsregels voor het lezen en schrijven van beveiligingsgegevens (voorschrift 080) toepassen.

4.2.4. *Bestandsstructuur en toegangscondities*

ACC_211 De structuur en toegangscondities van toepassings- en gegevensbestanden moeten tijdens het fabricageproces worden aangemaakt en vervolgens voor toekomstige wijzigingen of verwijderingen worden vergrendeld.

4.3. ***Verantwoording***

ACT_201 De VU moet ervoor zorgen dat bestuurders verantwoording kunnen afleggen over hun activiteiten (voorschrift 081, 084, 087, 105a, 105b, 109 en 109a).

ACT_202 De VU moet permanent identificatiegegevens (voorschrift 075) vasthouden.

ACT_203 De VU moet ervoor zorgen dat werkplaatsen verantwoording kunnen afleggen over hun activiteiten (voorschrift 098, 101 en 109).

ACT_204 De VU moet ervoor zorgen dat controleurs verantwoording kunnen afleggen over hun activiteiten (voorschrift 102, 103 en 109).

ACT_205 De VU moet gegevens over de kilometerstand (voorschrift 090) en gedetailleerde snelheidsgegevens (voorschrift 093) registreren.

ACT_206 De VU moet ervoor zorgen dat geregistreerde gebruikersgegevens met betrekking tot voorschriften 081 tot en met 093 en 102 tot en met 105b niet worden gewijzigd behalve wanneer nieuwe gegevens de oudste moeten vervangen.

ACT_207 De VU moet ervoor zorgen dat de op een tachograafkaart opgeslagen gegevens niet worden gewijzigd (voorschrift 109 en 109a) behalve wanneer nieuwe gegevens de oudste moeten vervangen (voorschrift 110) of in het geval zoals beschreven in appendix 1, punt 2.1, opmerking.

4.4. ***Audit***

Mogelijkheden tot het uitvoeren van een audit zijn uitsluitend vereist bij voorvallen die mogelijk duiden op misbruik of een poging tot inbreuk op de beveiliging. Het is niet vereist bij de normale uitoefening van rechten, zelfs indien relevant voor de beveiliging.

AUD_201 De VU moet voorvallen die de beveiliging van de VU in gevaar brengen, registreren inclusief de betreffende gegevens (voorschrift 094, 096 en 109).

AUD_202 De voorvallen die van invloed zijn op de beveiliging van de VU, zijn de volgende:

— pogingen tot inbreuk op de beveiliging:

  — authenticatiefout van de bewegingsopnemer;

  — authenticatiefout van de tachograafkaart;

  — niet-geautoriseerde wijziging van de bewegingsopnemer;

  — integriteitsfout bij de gegevensinvoer op de kaart;

  — integriteitsfout in opgeslagen gebruikersgegevens;

  — overdrachtsfout in interne gegevens;

  — niet-geautoriseerde opening van de behuizing;

  — sabotage van de hardware;

— laatste kaartsessie niet correct afgesloten;

— fout in de bewegingsgegevens;

— onderbreking in de stroomvoorziening;

— interne fout in de VU.

AUD_203 De VU moet opslagregels voor auditregistraties (voorschrift 094 en 096) toepassen.

AUD_204 De VU moet door de bewegingsopnemer gegenereerde auditregistraties in zijn geheugen opslaan.

AUD_205 Auditregistraties moeten afgedrukt, getoond en overgebracht kunnen worden.

4.5. ***Hergebruik van objecten***

REU_201 De VU moet ervoor zorgen dat tijdelijk opgeslagen objecten hergebruikt kunnen worden zonder dat dit een ontoelaatbare informatiestroom betekent.

4.6. ***Nauwkeurigheid***

4.6.1. *Controlebeleid met betrekking tot de informatiestroom*

ACR_201 De VU moet ervoor zorgen dat gebruikersgegevens met betrekking tot de voorschriften 081, 084, 087, 090, 093, 102, 104, 105, 105a en 109 alleen verwerkt worden wanneer ze afkomstig zijn van de juiste invoerbronnen:

— bewegingsgegevens van het voertuig;

— de tijdklok van de VU;

— kalibreringsparameters van het controleapparaat;

— tachograafkaarten;

— invoer door de gebruiker.

ACR_201a De VU moet ervoor zorgen dat gebruikersgegevens met betrekking tot voorschrift 109a uitsluitend voor de periode „laatste kaartuitneming — huidige inbrenging" (voorschrift 050a) kunnen worden ingevoerd.

4.6.2. *Overdracht van interne gegevens*

De voorschriften van dit punt zijn alleen van toepassing indien de VU gebruik maakt van fysiek gescheiden delen.

ACR_202 Indien gegevens tussen de fysiek gescheiden delen van de VU worden overgedragen, moeten de gegevens tegen wijzigingen worden beveiligd.

ACR_203 Na detectie van een gegevensoverdrachtsfout tijdens een interne overdracht moet de overbrenging worden weergegeven en moet de SEF een auditregistratie van het voorval genereren.

4.6.3. *Integriteit van opgeslagen gegevens*

ACR_204 De VU moet de in het geheugen opgeslagen gebruikersgegevens op integriteitsfouten controleren.

ACR_205 Na detectie van een integriteitsfout in de opgeslagen gebruikersgegevens moet de SEF een auditregistratie genereren.

4.7. ***Betrouwbaarheid van de werking***

4.7.1. *Beproevingen*

RLB_201 Alle opdrachten, acties of testpunten die specifiek zijn voor de beproevingen van de VU in de fabricagefase, moeten vóór activering van de VU worden geblokkeerd of verwijderd. Het is niet mogelijk om deze voor toekomstig gebruik terug te zetten.

RLB_202 De VU moet tijdens het voor de eerste keer opstarten en tijdens normaal bedrijf zelfbeproevingen uitvoeren om de juiste werking te verifiëren. De zelfbeproevingen van de VU moeten een verificatie van de integriteit van de beveiligingsgegevens en een verificatie van de integriteit van de opgeslagen uitvoercode (indien niet in ROM) omvatten.

RLB_203 Na detectie van een interne fout tijdens een zelfbeproeving, moet de SEF:

— een auditregistratie genereren (behalve in de kalibreringsmodus) (interne fout in de VU);

— de integriteit van de opgeslagen gegevens handhaven.

4.7.2. *Software*

RLB_204 Het in het veld analyseren of debuggen van de software na activering van de VU is niet mogelijk.

RLB_205 Invoergegevens afkomstig uit externe bronnen worden niet als uitvoerbare code geaccepteerd.

4.7.3. *Fysieke bescherming*

RLB_206 Indien de VU zodanig ontworpen is dat deze geopend kan worden, moet de VU elke opening van de behuizing detecteren, zelfs zonder externe stroomvoorziening gedurende ten minste 6 maanden, behalve in de kalibreringsmodus. In dit geval moet de SEF een auditregistratie genereren (het is acceptabel wanneer de auditregistratie na herstel van de stroomvoorziening gegenereerd en opgeslagen wordt).

Indien de VU zodanig ontworpen is dat deze niet geopend kan worden, moet hij zodanig geconstrueerd worden dat fysieke manipulatiepogingen gemakkelijk gedetecteerd kunnen worden (bijv. door visuele inspectie).

RLB_207 Na activering moet de VU gespecificeerde (TBD door de fabrikant) sabotage van de hardware detecteren.

RLB_208 In het bovengenoemde geval moet de SEF een auditregistratie genereren en moet de VU: (TBD door de fabrikant).

4.7.4. *Onderbrekingen in de stroomvoorziening*

RLB_209 De VU moet afwijkingen in de gespecificeerde waarden van de stroomvoorziening detecteren, waaronder afsluiting.

RLB_210 In het bovengenoemde geval moet de SEF:

— een auditregistratie genereren (behalve in de kalibreringsmodus);

— de veilige toestand van de VU handhaven;

— de beveiligingsfuncties met betrekking tot componenten of processen die nog operationeel zijn, handhaven;

— de integriteit van de opgeslagen gegevens handhaven.

4.7.5. *Terugstelvoorwaarden*

RLB_211 In geval van onderbreking in de stroomvoorziening of wanneer een transactie vóór de voltooiing afgebroken wordt, of bij andere terugstelvoorwaarden, moet de VU correct worden teruggesteld.

4.7.6. *Beschikbaarheid van gegevens*

RLB_212 De VU moet ervoor zorgen dat — indien vereist — toegang tot systeemelementen wordt verkregen en dat systeemelementen niet onnodig worden opgevraagd of vastgehouden.

RLB_213 De VU moet ervoor zorgen dat kaarten niet kunnen worden uitgenomen voordat relevante gegevens opgeslagen zijn (voorschrift 015 en 016).

RLB_214 In het bovengenoemde geval moet de SEF een auditregistratie van het voorval genereren.

4.7.7. *Meervoudige toepassingen*

RLB_215 Indien de VU andere toepassingen dan de tachograaftoepassing levert, moeten alle toepassingen fysiek en/of logisch scheidbaar zijn. Deze toepassingen mogen geen beveiligingsgegevens delen. Er is maar een taak tegelijk actief.

4.8. ***Gegevensuitwisseling***

Dit punt behandelt de gegevensuitwisseling tussen de VU en aangesloten inrichtingen.

4.8.1. *Gegevensuitwisseling met de bewegingsopnemer*

DEX_201 De VU moet de integriteit en authenticiteit van de door de bewegingsopnemer ingevoerde bewegingsgegevens verifiëren.

DEX_202 Na detectie van een integriteits- of authenticiteitsfout in de bewegingsgegevens moet de SEF:

— een auditregistratie genereren,

— ingevoerde gegevens blijven gebruiken.

4.8.2. *Gegevensuitwisseling met tachograafkaarten*

DEX_203 De VU moet de integriteit en authenticiteit van de vanaf de tachograafkaarten ingevoerde gegevens verifiëren.

DEX_204 Na detectie van een integriteits- of authenticiteitsfout in de kaartgegevens dient de VU:

— een auditregistratie te genereren,

— de gegevens niet te gebruiken.

DEX_205 De VU moet gegevens naar tachograaf-smartcards met de betreffende beveiligingskenmerken uitvoeren zodat de kaart de integriteit en authenticiteit van de gegevens kan verifiëren.

4.8.3. *Gegevensuitwisseling met externe opslagmedia (overbrengingsfunctie)*

DEX_206 De VU moet een bewijs van oorsprong voor de naar externe media overgebrachte gegevens genereren.

DEX_207 De VU moet de mogelijkheid bieden het bewijs van oorsprong van de naar de ontvanger overgebrachte gegevens te verifiëren.

DEX_208 De VU moet gegevens naar externe opslagmedia met de betreffende beveiligingskenmerken uitvoeren zodat de integriteit en authenticiteit van de overgebrachte gegevens geverifieerd kunnen worden.

4.9. ***Cryptografische ondersteuning***

De voorschriften van dit punt zijn alleen waar nodig van toepassing, afhankelijk van de gebruikte beveiligingsmechanismen en de oplossingen van de fabrikant.

CSP_201 Elke door de VU uitgevoerde cryptografische bewerking moet in overeenstemming zijn met een gespecificeerde algoritme en een gespecificeerd sleutelformaat.

CSP_202 Indien de VU cryptografische sleutels genereert, moet dit in overeenstemming zijn met gespecificeerde ontwikkelingsalgoritmen van cryptografische sleutels en met gespecificeerde formaten van dergelijke sleutels.

CSP_203 Indien de VU cryptografische sleutels verspreidt, moet dit in overeenstemming zijn met gespecificeerde verspreidingsmethoden van dergelijke sleutels.

CSP_204 Indien de VU toegang heeft tot cryptografische sleutels, moet dit in overeenstemming zijn met gespecificeerde toegangsmethoden tot dergelijke sleutels.

CSP_205 Indien de VU cryptografische sleutels vernietigt, moet dit in overeenstemming zijn met gespecificeerde vernietigingsmethoden van dergelijke sleutels.

5. **Definitie van beveiligingsmechanismen**

De vereiste beveiligingsmechanismen worden gespecificeerd in appendix 11.

Alle andere beveiligingsmechanismen moeten door de fabrikanten gedefinieerd worden.

6. **Minimumsterkte van beveiligingsmechanismen**

De minimumsterkte van de beveiligingsmechanismen van de voertuigunit is Hoog, zoals gedefinieerd in referentienorm ITSEC.

7. **Garantieniveau**

Het streefniveau van garantie voor de voertuigunit is ITSEC niveau E3, zoals gedefinieerd in referentienorm ITSEC.

8. **Ratio**

De onderstaande tabellen geven een ratio voor de SEF's aan:

— welke SEF's of middelen welke bedreigingen tegengaan;

— welke SEF's aan welke IT-beveiligingsdoelstellingen voldoen.

	Bedreigingen																	IT-doelstellingen								
	T.Toegang	T.Identificatie	T.Fouten	T.Beproevingen	T.Ontwerp	T.Kalibreringsparameters	T.Uitwisseling kaartgegevens	T.Uurwerk	T.Milieu	T.Valse_inrichtingen	T.Hardware	T.Bewegingsgegevens	T.Niet-geactiveerd	T.Uitvoergegevens	T.Stroomvoorziening		T.Beveiligingsgegevens	T.Software	T.Opgeslagen_gegevens	O.Toegang	O.Verantwoording	O.Audit	O.Authenticatie	O.Integriteit	O.Uitvoer	O.Verwerking	O.Betrouwbaarheid	O.Bev._gegevensuitwisseling
Fysieke personele procedurele middelen																												
Ontwikkeling			x	x	x																							
Fabricage				x	x																							
Levering												x																
Activering	x											x																
Ontwikkeling beveiligingsgegevens																	x											
Transport beveiligingsgegevens																	x											
Beschikbaarheid kaart		x																										
Eén bestuurderskaart		x																										
Traceerbaarheid kaart		x																										
Erkende werkplaatsen						x		x																				
Regelmatige controle kalibrering						x		x				x	x			x												
Betrouwbare werkplaatsen						x		x																				
Betrouwbare bestuurders		x																										
Controles op naleving van de wet		x				x		x	x		x		x		x			x	x									
Softwareaanpassing																			x									
Beveiligingsfuncties																												
Identificatie en authenticatie																												
UIA_201 Identificatie opnemer										x		x											x					x
UIA_202 Identiteit opnemer										x		x											x					x
UIA_203 Authenticatie opnemer										x		x											x					x
UIA_204 Heridentificatie en herauthenticatie opnemer										x		x											x					x
UIA_205 Onvervalsbare authenticatie										x		x											x					
UIA_206 Authenticatiefout										x		x										x					x	
UIA_207 Gebruikersidentificatie	x	x								x										x			x					x
UIA_208 Gebruikersidentiteit	x	x								x										x			x					x
UIA_209 Gebruikersauthenticatie	x	x								x										x			x					x
UIA_210 Herauthenticatie van de gebruiker	x	x								x										x			x					x
UIA_211 Authenticatiemiddelen	x	x								x										x			x					
UIA_212 PIN-controles	x	x				x		x												x			x					
UIA_213 Onvervalsbare authenticatie	x	x								x										x			x					

	Bedreigingen																			IT-doelstellingen								
	T.Toegang	T.Identificatie	T.Fouten	T.Beproevingen	T.Ontwerp	T.Kalibreringsparameters	T.Uitwisseling kaartgegevens	T.Uurwerk	T.Milieu	T.Valse_inrichtingen	T.Hardware	T.Bewegingsgegevens	T.Niet-geactiveerd	T.Uitvoergegevens	T.Stroomvoorziening		T.Beveiligingsgegevens	T.Software	T.Opgeslagen_gegevens	O.Toegang	O.Verantwoording	O.Audit	O.Authenticatie	O.Integriteit	O.Uitvoer	O.Verwerking	O.Betrouwbaarheid	O.Bev._gegevensuitwisseling
UIA_214 Authenticatiefout	x	x								x												x						
UIA_215 Gebruikersidentificatie op afstand	x	x																		x			x					x
UIA_216 Gebruikersidentiteit op afstand	x	x																		x			x					
UIA_217 Gebruikersauthenticatie op afstand	x	x																		x			x					x
UIA_218 Authenticatiemiddelen	x	x																		x			x					
UIA_219 Onvervalsbare authenticatie	x	x																		x			x					
UIA_220 Authenticatiefout	x	x																										
UIA_221 Identificatie beheersinrichting	x	x																		x			x					
UIA_222 Authenticatie beheersinrichting	x	x																		x			x					
UIA_223 Onvervalsbare authenticatie	x	x																		x			x					
Toegangscontrole																												
ACC_201 Beleid toegangscontrole	x					x		x									x		x	x								
ACC_202 Toegangsrechten tot functies	x					x		x												x								
ACC_203 Toegangsrechten tot functies	x					x		x												x								
ACC_204 VU-ID																			x	x								
ACC_205 ID aangesloten opnemer										x									x	x								
ACC_206 Kalibreringsgegevens	x					x													x	x								
ACC_207 Kalibreringsgegevens						x													x	x								
ACC_208 Tijdafstellingsgegevens								x											x	x								
ACC_209 Tijdafstellingsgegevens								x											x	x								
ACC_210 Beveiligingsgegevens																	x		x	x								
ACC_211 Bestandsstructuur en toegangscondities	x					x											x		x	x								
Verantwoording																												
ACT_201 Verantwoording bestuurders																					x							
ACT_202 VU-ID gegevens																					x	x						
ACT_203 Verantwoording werkplaatsen																					x							
ACT_204 Verantwoording controleurs																					x							
ACT_205 Verantwoording voertuigbewegingen																					x							
ACT_206 Wijziging verantwoordingsgegevens																			x					x			x	
ACT_207 Wijziging verantwoordingsgegevens																			x					x			x	

	Bedreigingen																		IT-doelstellingen							
	T.Toegang	T.Identificatie	T.Fouten	T.Beproevingen	T.Ontwerp	T.Kalibreringsparameters	T.Uitwisseling kaartgegevens	T.Uurwerk	T.Milieu	T.Valse_inrichtingen	T.Hardware	T.Bewegingsgegevens	T.Niet-geactiveerd	T.Uitvoergegevens	T.Stroomvoorziening		T.Beveiligingsgegevens	T.Software	T.Opgeslagen_gegevens	O.Toegang	O.Verantwoording	O.Audit	O.Authenticatie	O.Integriteit	O.Uitvoer	O.Verwerking	O.Betrouwbaarheid	O.Bev._gegevensuitwisseling
Audit																												
AUD_201 Auditregistraties																						x						
AUD_202 Audit voorvallenlijst	x						x				x	x		x	x				x			x						
AUD_203 Opslagregels auditregistraties																						x						
AUD_204 Auditregistraties opnemer																						x						
AUD_205 Auditinstrumenten																						x						
REU_201 Hergebruik																	x									x	x	
Nauwkeurigheid																												
ACR_201 Controlebeleid Informatiestroom						x			x		x															x	x	
ACR_202 Interne overdracht														x											x	x	x	
ACR_203 Interne overdracht														x								x						
ACR_204 Integriteit opgeslagen gegevens																		x					x				x	
ACR_205 Integriteit opgeslagen gegevens																		x				x						
RLB_201 Fabricagebeproevingen				x	x																						x	
RLB_202 Zelfbeproevingen			x								x				x			x									x	
RLB_203 Zelfbeproevingen											x				x			x				x						
RLB_204 Softwareanalyse					x													x									x	
RLB_205 Software-invoer																		x							x	x	x	
RLB_206 Opening omhulsel					x				x		x			x			x	x	x						x		x	
RLB_207 Hardwaresabotage											x																x	
RLB_208 Hardwaresabotage											x											x						
RLB_209 Onderbrekingen stroomvoorziening															x												x	
RLB_210 Onderbrekingen stroomvoorziening															x							x						
RLB_211 Terugstellen			x																								x	
RLB_212 Beschikbaarheid gegevens																										x	x	
RLB_213 Kaartuitneming																											x	
RLB_214 Kaartsessie niet correct afgesloten																							x					
RLB_215 Meervoudige toepassingen																											x	
DEX_201 Beveiligde invoer bewegingsgegevens												x																x
DEX_202 Beveiligde invoer bewegingsgegevens												x							x									
DEX_203 Beveiligde invoer kaartgegevens							x																					x

	Bedreigingen																			IT-doelstellingen								
	T.Toegang	T.Identificatie	T.Fouten	T.Beproevingen	T.Ontwerp	T.Kalibreringsparameters	T.Uitwisseling kaartgegevens	T.Uurwerk	T.Milieu	T.Valse_inrichtingen	T.Hardware	T.Bewegingsgegevens	T.Niet-geactiveerd	T.Uitvoergegevens	T.Stroomvoorziening		T.Beveiligingsgegevens	T.Software	T.Opgeslagen_gegevens	O.Toegang	O.Verantwoording	O.Audit	O.Authenticatie	O.Integriteit	O.Uitvoer	O.Verwerking	O.Betrouwbaarheid	O.Bev._gegevensuitwisseling
DEX_204 Beveiligde invoer kaartgegevens							x															x						
DEX_205 Beveiligde uitvoer gegevens naar kaart							x																					x
DEX_206 Bewijs van oorsprong																								x	x			
DEX_207 Bewijs van oorsprong																								x	x			
DEX_208 Beveiligde uitvoer naar externe media																								x	x			
IT-doelstellingen																												
CSP_201 Algoritmen																											x	x
CSP_202 Ontwikkeling sleutel																											x	x
CSP_203 Verspreiding sleutel																											x	x
CSP_204 Toegang sleutel																											x	x
CSP_205 Vernietiging sleutel																											x	x

ALGEMENE BEVEILIGINGSDOELSTELLING VAN DE TACHOGRAAFKAART

1. **Inleiding**

Dit document bevat een beschrijving van de tachograafkaart, van de door de tachograafkaart te neutraliseren bedreigingen en van de te realiseren beveiligingsdoelstellingen. Het specificeert de vereiste beveiligingsfuncties. Het document stelt de vereiste minimumsterkte van beveiligingsmechanismen en het vereiste garantieniveau voor de ontwikkeling en beproeving vast.

De voorschriften waarnaar in dit document wordt verwezen, staan in de tekst van bijlage I B. Voor de duidelijkheid treedt er soms herhaling op tussen de voorschriften in bijlage I B en de voorschriften van de beveiligingsdoelstelling. In geval van onduidelijkheid tussen een voorschrift van de beveiligingsdoelstelling en een voorschrift van bijlage I B waarnaar in dit document wordt verwezen, geldt het voorschrift van bijlage I B.

Voorschriften van bijlage I B die in de beveiligingsdoelstellingen niet worden genoemd, zijn geen onderwerp van de beveiligingsfuncties.

Een tachograafkaart is een standaardsmartcard met een toepassingsgerichte tachograaftoepassing en moet aan de meest recente voor smartcards geldende beveiligingsvoorschriften betreffende functies en garanties voldoen. In deze beveiligingsdoelstelling zijn derhalve uitsluitend de bijkomende beveiligingsvoorschriften voor de tachograaftoepassing opgenomen.

Er zijn unieke labels toegewezen aan bedreigingen, doelstellingen, procedurele middelen en SEF-specificaties zodat deze gemakkelijk in ontwikkelings- en beproevingsdocumentatie terug te vinden zijn.

2. **Afkortingen, definities en referentienormen**

2.1. ***Afkortingen***

IC	Integrated circuit (Elektronische component voor het uitvoeren van verwerkings- en/of geheugenfuncties),
OS	Operating system (besturingssysteem)
PIN	Personal identification number (PIN-code)
ROM	Read only memory (ROM-geheugen)
SFP	Security functions policy (beleid t.a.v. beveiligingsfuncties)
TBD	To be defined (nog te bepalen)
TOE	Target of evaluation (doel van de evaluatie)
TSF	TOE security function (TOE-beveiligingsfunctie)
VU	Vehicle unit (voertuigunit)

2.2. ***Definities***

Digitale tachograaf	Controleapparaat
Gevoelige gegevens	Op de tachograafkaart opgeslagen gegevens die in verband met integriteit, onbevoegde wijziging en vertrouwelijkheid beveiligd moeten worden (waar toepasbaar op beveiligingsgegevens). Gevoelige gegevens bestaan uit beveiligingsgegevens en gebruikersgegevens
Beveiligingsgegevens	De specifieke gegevens ter ondersteuning van de beveiligingsfuncties (bijv. cryptosleutels)
Systeem	Inrichtingen, mensen of organisaties die op de een of andere manier bij het controleapparaat betrokken zijn
Gebruiker	Een unit (menselijke gebruiker of externe IT-unit) buiten het TOE die met het TOE in wisselwerking staat (wanneer niet gebruikt in de uitdrukking „gebruikersgegevens”)

Gebruikersgegevens	Gevoelige, op de tachograafkaart opgeslagen gegevens, anders dan beveiligingsgegevens. Gebruikersgegevens bestaan uit identificatiegegevens en gegevens over activiteiten
Identificatiegegevens	Identificatiegegevens bestaan uit kaartidentificatiegegevens en identificatiegegevens m.b.t. de kaarthouder
Kaartidentificatiegegevens	Gebruikersgegevens met betrekking tot de kaartidentificatie zoals gedefinieerd in voorschrift 190, 191, 192, 194, 215, 231 en 235
Identificatiegegevens m.b.t. de kaarthouder	Gebruikersgegevens met betrekking tot de identificatie van de kaarthouder zoals gedefinieerd in voorschrift 195, 196, 216, 232 en 236
Gegevens over activiteiten	Gegevens over activiteiten bestaan uit gegevens over de activiteiten van de kaarthouder, gegevens over voorvallen en fouten en gegevens over controleactiviteiten
Gegevens over activiteiten van de kaarthouder	Gebruikersgegevens met betrekking tot de activiteiten van de kaarthouder zoals gedefinieerd in voorschrift 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 en 237
Gegevens over voorvallen en fouten	Gebruikersgegevens met betrekking tot voorvallen en fouten zoals gedefinieerd in voorschrift 204, 205, 207, 208 en 223
Gegevens over controleactiviteiten	Gebruikersgegevens met betrekking tot wettelijke controles zoals gedefinieerd in voorschrift 210 en 225

2.3. ***Referentienormen***

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991
IC PP	Smartcard Integrated Circuit Protection Profile — versie 2.0 — uitgave september 1998. Geregistreerd door de Franse certificeringsinstantie onder nummer PP/9806
ES PP	Smart Card Integrated Circuit With Embedded Software Protection Profile — versie 2.0 - uitgave juni 1999. Geregistreerd door de Franse certificeringsinstantie onder nummer PP/9911

3. **Productratio**

3.1. ***Beschrijving van de tachograafkaart en gebruiksaanwijzing***

Een tachograafkaart is een smartcard, zoals gedefinieerd in referentienorm IC PP en referentienorm ES PP en bedoeld voor gebruik in het controleapparaat.

De basisfuncties van de tachograafkaart zijn:

— opslaan van kaartidentificatiegegevens en gegevens over de kaarthouder. Deze gegevens worden door de voertuigunit gebruikt om de kaarthouder te identificeren, dienovereenkomstig toegangsrechten tot gegevens en functies te leveren en de verantwoording van de kaarthouder voor zijn activiteiten te waarborgen;

— het opslaan van gegevens over de activiteiten van de kaarthouder, gegevens over voorvallen en fouten en gegevens over controleactiviteiten met betrekking tot de kaarthouder.

Een tachograafkaart is derhalve bedoeld voor gebruik in een kaartinterface-inrichting van een voertuigunit. De kaart kan ook in een andere kaartlezer (bijv. van een personal computer) met volledige toegangsrechten voor het lezen van gebruikersgegevens worden gebruikt.

Tijdens de eindgebruiksfase van de levenscyclus van een tachograafkaart (fase 7 van de levenscyclus zoals gedefinieerd in referentienorm ES PP) kunnen voertuigunits uitsluitend gegevens naar de kaart schrijven.

De functionele voorschriften voor een tachograafkaart worden gespecificeerd in bijlage I B en appendix 2.

3.2. ***Levenscyclus van een tachograafkaart***

De levenscyclus van een tachograafkaart komt overeen met de levenscyclus van een smartcard zoals gedefinieerd in referentienorm ES PP.

3.3. ***Bedreigingen***

Naast de algemene bedreigingen van de smartcard zoals vermeld in referentienorm ES PP en referentienorm IC PP, kan de tachograafkaart met de onderstaande bedreigingen geconfronteerd worden:

3.3.1. *Einddoelen*

Het einddoel van aanvallers is het wijzigen van in het TOE opgeslagen gebruikersgegevens.

T.Identificatiegegevens	Een succesvolle wijziging van de identificatiegegevens van het TOE (bijv. kaartsoort of vervaldatum van de kaart of de identificatiegegevens van de kaarthouder) kan een frauduleus gebruik van het TOE mogelijk maken en een belangrijke bedreiging voor de algemene beveiligingsdoelstelling van het systeem vormen.
T.Gegevens_over_activiteiten	Een succesvolle wijziging van de in het TOE opgeslagen gegevens over activiteiten vormt een bedreiging voor de beveiliging van het TOE.
T.Gegevensuitwisseling	Een succesvolle wijziging van de gegevens over activiteiten (toevoeging, verwijdering, wijziging) tijdens de invoer of uitvoer vormt een bedreiging voor de beveiliging van het TOE.

3.3.2. *Aanvalspaden*

De elementen van het TOE kunnen worden aangevallen door:

— pogingen tot het verkrijgen van illegale kennis van de hardware en software van het TOE en in het bijzonder van de beveiligingsfuncties of beveiligingsgegevens. Illegale kennis kan worden verkregen door middel van misbruik van het materiaal van de ontwerper of fabrikant (diefstal, omkoping, enz.) of door rechtstreeks onderzoek van het TOE (fysiek onderzoek, inferentieanalyse, enz.).

— misbruik maken van de zwakke punten in het ontwerp of de uitvoering van het TOE (gebruikmaken van fouten in de hardware, fouten in de software, overbrengingsfouten, fouten in het TOE ten gevolge van milieubelasting, gebruikmaken van de zwakke punten van beveiligingsfuncties zoals authenticatieprocedures, gegevenstoegangscontrole, cryptografische functies, enz.).

— wijzigen van het TOE of zijn beveiligingsfuncties door middel van fysieke, elektrische of logische aanvallen of een combinatie daarvan.

3.4. ***Beveiligingsdoelstellingen***

De belangrijkste beveiligingsdoelstelling van het gehele digitale tachograafsysteem is de volgende:

O.Belangrijkste	De door de controleautoriteiten te controleren gegevens moeten beschikbaar zijn en de activiteiten van de gecontroleerde bestuurders en voertuigen met betrekking tot rijden, werken, beschikbaarheid en rusttijden alsmede de gegevens met betrekking tot de snelheid van het voertuig volledig en nauwkeurig weergeven.

De belangrijkste beveiligingsdoelstellingen van het TOE die aan de totale beveiligingsdoelstelling bijdraagt, zijn derhalve:

O.Kaartidentificatiegegevens	Het TOE moet de tijdens het personalisatieproces van de kaart opgeslagen kaartidentificatiegegevens en identificatiegegevens van de kaarthouder bewaren.
O.Opslag_van_activiteiten_op_de_kaart	Het TOE moet door de voertuigunits op de kaart opgeslagen gebruikersgegevens bewaren.

3.5. ***Informatietechnologische beveiligingsdoelstellingen***

Naast de algemene beveiligingsdoelstellingen van de smartcard zoals vermeld in referentienorm ES PP en referentienorm IC PP zijn de specifieke IT-beveiligingsdoelstellingen van het TOE die aan de belangrijkste beveiligingsdoelstellingen tijdens de eindgebruiksfase van de levenscyclus bijdragen, de volgende:

O.Gegevenstoegang	Het TOE moet de toegangsrechten voor de invoer van gebruikersgegevens in geauthentiseerde voertuigunits beperken.
O.Veilige_Communicatie	Het TOE moet, wanneer de toepassing dit vereist, veilige communicatieprotocollen en -procedures tussen de kaart en de kaartinterface-inrichting kunnen ondersteunen.

3.6. ***Fysieke, personele of procedurele middelen***

De fysieke, personele of procedurele voorschriften die tot de beveiliging van het TOE bijdragen, worden vermeld in referentienorm ES PP en referentienorm IC PP (hoofdstukken over beveiligingsdoelstellingen voor de omgeving).

4. **Beveiligingsfuncties**

Dit punt werkt een aantal toegestane operaties uit zoals toewijzing of selectie van referentienorm ES PP en levert additionele functievoorschriften voor de SEF.

4.1. ***Overeenstemming met beschermingsprofielen***

CPP_301 Het TOE moet voldoen aan referentienorm IC PP.

CPP_302 Het TOE moet voldoen aan de verder uitgewerkte referentienorm ES PP.

4.2. ***Identificatie en authenticatie van de gebruiker***

De kaart moet de unit identificeren waarin hij wordt ingebracht, en herkennen of het een geauthentiseerde voertuigunit is. De kaart kan gebruikersgegevens van de unit waarmee hij verbonden is uitvoeren, met uitzondering van de controlekaart die identificatiegegevens van de kaarthouder uitsluitend naar geauthentiseerde voertuigunits kan uitvoeren (op zodanige wijze dat de controleur ervan verzekerd kan zijn dat de voertuigunit geen vervalsing is, doordat hij zijn naam in het leesvenster of op de afdrukken kan zien).

4.2.1. *Identificatie van de gebruiker*

Opdracht (FIA_UID.1.1) *Lijst met door TSF overgebrachte acties*: geen.

Opdracht (FIA_ATD.1.1) *Lijst met beveiligingskenmerken*:

GEBRUIKERSGROEP: VOERTUIGUNIT, NIET_VOERTUIGUNIT,

GEBRUIKERS_ID: Registratienummer van het voertuig (VRN) en code van de registerende lidstaat (GEBRUIKERS_ID is alleen bekend voor GEBRUIKERSGROEP = VOERTUIGUNIT).

4.2.2. *Authenticatie van de gebruiker*

Opdracht (FIA_UAU.1.1) *Lijst met door TSF overgebrachte acties*:

— Bestuurders- en werkplaatskaart: uitvoer van gebruikersgegevens met beveiligingskenmerken (overdrachtsfunctie van kaartgegevens);

— Controlekaart: uitvoer van gebruikersgegevens zonder beveiligingskenmerken met uitzondering van identificatiegegevens van de kaarthouder.

UIA_301 Authenticatie van een voertuigunit moet geschieden door aan te tonen dat de unit beveiligingsgegevens bezit die alleen door het systeem kunnen worden verspreid.

Selectie (FIA_UAU.3.1 en FIA_UAU.3.2): verhinderen.

Opdracht (FIA_UAU.4.1) *Geïdentificeerde authenticatiemechanisme(n)*: elk authenticatiemechanisme.

UIA_302 De werkplaatskaart moet voorzien in een additioneel authenticatiemechanisme door het controleren van een PIN-code (met dit mechanisme moet de voertuigunit de identiteit van de kaarthouder vaststellen, het is niet bedoeld om de inhoud van de werkplaatskaart te beveiligen).

4.2.3. *Authenticatiefouten*

De onderstaande opdrachten beschrijven de reactie van de kaart bij elke afzonderlijke gebruikersauthenticatiefout.

Opdracht (FIA_AFL.1.1) *Nummer: 1, lijst met authenticatievoorvallen:* authenticatie van een kaartinterface-inrichting.

Opdracht (FIA_AFL.1.2) *Lijst met acties*:

— de aangesloten unit waarschuwen;

— aannemen dat de gebruiker NIET_VOERTUIGUNIT is.

De onderstaande opdrachten beschrijven de reactie van de kaart in het geval van een storing van het in UIA_302 vereiste additionele authenticatiemechanisme.

Opdracht (FIA_AFL.1.1) *Nummer: 5, lijst met authenticatievoorvallen:* controles PIN-code (werkplaatskaart).

Opdracht (FIA_AFL.1.2) *Lijst met acties*:

— de aangesloten unit waarschuwen;

— de controleprocedure van de PIN-code blokkeren zodat elke volgende controle van de PIN-code mislukt;

— aan volgende gebruikers de reden van de blokkering opgeven.

4.3. ***Toegangscontrole***

4.3.1. *Toegangscontrolebeleid*

Tijdens de eindgebruiksfase van zijn levenscyclus wordt de tachograafkaart onderworpen aan een enkele toegangscontrole van de beveiligingsfuncties (SFP), AC_SFP genoemd.

Opdracht (FDP_ACC.2.1) *Toegangscontrole SFP*: AC_SFP.

4.3.2. *Toegangscontrolefuncties*

Opdracht (FDP_ACF.1.1) *Toegangscontrole SFP*: AC_SFP.

Opdracht (FDP_ACF.1.1) *Genoemde groep beveiligingskenmerken*: GEBRUIKERSGROEP.

Opdracht (FDP_ACF.1.2) *Regels die de toegang tussen gecontroleerde subjecten en gecontroleerde objecten regelen met behulp van gecontroleerde operaties op gecontroleerde objecten*:

ALGEMEEN_LEZEN	Gebruikersgegevens kunnen door elke gebruiker vanaf het TOE worden gelezen, met uitzondering van identificatiegegevens van de kaarthouder die uitsluitend door de VOERTUIGUNIT afgelezen kunnen worden van controlekaarten.
IDENTIF_SCHRIJVEN	Identificatiegegevens mogen slechts eenmaal en vóór het einde van fase 6 van de levenscyclus van de kaart worden geschreven. Gebruikers mogen tijdens de eindgebruiksfase van de levenscyclus van de kaart geen identificatiegegevens schrijven of wijzigen
ACTIVITEIT_SCHRIJVEN	Gegevens over activiteiten kunnen alleen door de VOERTUIGUNIT naar het TOE worden geschreven.
SOFT_AANPASSING	Gebruikers mogen de software van het TOE niet aanpassen.
BESTANDSSTRUCTUUR	Bestandsstructuur en toegangscondities moeten voor het einde van fase 6 van de levenscyclus van het TOE worden aangemaakt en vervolgens vergrendeld worden ter voorkoming van toekomstige wijziging of verwijdering door een gebruiker.

4.4. ***Verantwoording***

ACT_301 Het TOE moet permanent identificatiegegevens vasthouden.

ACT_302 Er moet een indicatie zijn van de tijd en datum van de personalisatie van het TOE. Deze indicatie mag niet gewijzigd worden.

4.5. ***Audit***

Het TOE moet controleren of voorvallen plaatsvinden die duiden op een potentiële inbreuk op de beveiliging.

Opdracht (FAU_SAA.1.2) *Deelverzameling van gedefinieerde te controleren voorvallen*:

— authenticatiefout van de kaarthouder (5 opeenvolgende niet-succesvolle controles van de PIN-code);

— fout bij de zelfbeproeving;

— integriteitsfout in de opgeslagen gegevens;

— integriteitsfout bij de invoer van gegevens over activiteiten.

4.6. ***Nauwkeurigheid***

4.6.1. *Integriteit van opgeslagen gegevens*

Opdracht (FDP_SDI.2.2) *Te ondernemen acties*: de aangesloten unit waarschuwen.

4.6.2. *Authenticatie van basisgegevens*

Opdracht (FDP_DAU.1.1) *Lijst met objecten of informatiesoorten*: gegevens over activiteiten.

Opdracht (FDP_DAU.1.2) *Lijst met subjecten*: geen.

4.7. ***Betrouwbaarheid van de werking***

4.7.1. *Beproevingen*

Selectie (FPT_TST.1.1): tijdens het voor de eerste keer opstarten, periodiek tijdens normaal bedrijf.

Opmerking: Tijdens het voor de eerste keer opstarten betekent voordat de code wordt uitgevoerd (en niet per definitie tijdens de Answer To Reset procedure).

RLB_301 De zelfbeproevingen van het TOE moeten de verificatie van de integriteit van een niet in ROM opgeslagen softwarecode bevatten.

RLB_302 Na detectie van een zelfbeproevingsfout moet de TSF de aangesloten unit waarschuwen.

RLB_303 Nadat de OS-beproeving voltooid is, moeten alle beproevingsspecifieke opdrachten en acties geblokkeerd of verwijderd worden. Het is niet mogelijk deze controles op te heffen en voor gebruik terug te zetten. Opdrachten die uitsluitend op één fase van de levenscyclus toepasbaar zijn, zijn tijdens een andere fase niet toegankelijk.

4.7.2. *Software*

RLB_304 Het is niet mogelijk de software van het TOE in het veld te analyseren, te debuggen of te wijzigen.

RLB_305 Invoergegevens afkomstig uit externe bronnen worden niet als uitvoerbare code geaccepteerd.

4.7.3. *Stroomvoorziening*

RLB_306 Het TOE moet tijdens een onderbreking van of schommelingen in de stroomvoorziening in een veilige toestand blijven.

4.7.4. *Terugstelvoorwaarden*

RLB_307 In geval van onderbreking van de stroomvoorziening van het TOE (of wanneer schommelingen in de stroomvoorziening optreden), of wanneer een transactie vóór de voltooiing afgebroken wordt, of bij andere terugstelvoorwaarden, moet het TOE correct worden teruggesteld.

4.8. ***Gegevensuitwisseling***

4.8.1. *Gegevensuitwisseling met een voertuigunit*

DEX_301 Het TOE moet de integriteit en authenticiteit van de door een voertuigunit ingevoerde gegevens verifiëren.

DEX_302 Na detectie van een integriteitsfout in de ingevoerde gegevens moet het TOE:

— de unit die de gegevens heeft gezonden waarschuwen;

— de gegevens niet gebruiken.

DEX_303 Het TOE moet gebruikersgegevens met de bijbehorende beveiligingskenmerken naar de voertuigunit uitvoeren zodat deze unit de integriteit en authenticiteit van de ontvangen gegevens kan verifiëren.

4.8.2. *Uitvoer van gegevens naar een niet-voertuigunit (overbrengingsfunctie)*

DEX_304 Het TOE moet een bewijs van oorsprong voor de naar externe media overgebrachte gegevens kunnen genereren.

DEX_305 Het TOE moet de mogelijkheid kunnen bieden het bewijs van oorsprong van naar de ontvanger overgebrachte gegevens te verifiëren.

DEX_306 Het TOE moet gegevens met bijbehorende beveiligingskenmerken naar externe opslagmedia kunnen uitvoeren zodat de integriteit van de overgebrachte gegevens geverifieerd kan worden.

4.9. ***Cryptografische ondersteuning***

CSP_301 Indien de TSF cryptografische sleutels genereert, moet dit in overeenstemming zijn met gespecificeerde ontwikkelingsalgoritmen van cryptografische sleutels en met gespecificeerde formaten van dergelijke sleutels. Gegenereerde sleutels voor cryptografische sessies moeten een beperkt (TBD door de fabrikant en niet meer dan 240) aantal keren gebruikt kunnen worden.

CSP_302 Indien de TSF cryptografische sleutels verspreidt, moet dit in overeenstemming zijn met gespecificeerde verspreidingsmethoden van dergelijke sleutels.

5. **Definitie van beveiligingsmechanismen**

De vereiste beveiligingsmechanismen worden gespecificeerd in appendix 11.

Alle andere beveiligingsmechanismen worden door de fabrikant van het TOE gedefinieerd.

6. **Opgegeven minimumsterkte van mechanismen**
De minimumsterkte van mechanismen voor de tachograafkaart is Hoog, zoals gedefinieerd in referentienorm ITSEC.

7. **Garantieniveau**
Het nagestreefde garantieniveau voor de tachograafkaart is ITSEC niveau E3, zoals gedefinieerd in referentienorm ITSEC.

8. **Ratio**
De onderstaande tabel geeft een ratio voor de additionele SEF's aan:

— welke SEF's welke bedreigingen tegengaan;

— welke SEF's aan welke IT-beveiligingsdoelstellingen voldoen.

	Bedreigingen											IT-doelstellingen								
	T.CLON*	T.DIS_ES2	T.T_ES	T.T_CMD	T.MOD_SOFT*	T.MOD_LOAD	T.MOD_EXE	T.MOD_SHARE	T.Ident_Gegevens	T.Gegevens_activiteiten	T.Gegevensuitwisseling	O.TAMPER_ES	O.CLON*	O.OPERATE*	O.FLAW*	O.DIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	O.Gegevenstoegang	O.Beveiligde_Communicatie
UIA_301 Authenticatiemiddelen																			x	
UIA_302 Controles PIN-code																			x	
ACT_301 Identificatiegegevens																				
ACT_302 Personalisatiegegevens																				
RLB_301 Software-integriteit												x		x						
RLB_302 Zelfbeproevingen												x		x						
RLB_303 Fabricagebeproevingen					x	x						x		x						
RLB_304 Softwareanalyse					x		x	x				x		x						
RLB_305 Software-invoer					x	x		x				x		x						
RLB_306 Stroomvoorziening									x	x		x		x						
RLB_307 Terugstellen												x		x						
DEX_301 Invoer beveiligde gegevens											x									x
DEX_302 Invoer beveiligde gegevens											x									x
DEX_303 Uitvoer beveiligde gegevens naar VU											x									x
DEX_304 Bewijs van oorsprong											x									x
DEX_305 Bewijs van oorsprong											x									x
DEX_306 Beveiligde uitvoer naar externe media											x									x
CSP_301 Sleutelontwikkeling												x								x
CSP_302 Sleutelverspreiding												x								x

Appendix 11

ALGEMENE VEILIGHEIDSMECHANISMEN

INHOUD

1.	Algemeen	238
1.1.	Referentienormen	238
1.2.	Begrippen en afkortingen	239
2.	Cryptografische systemen en algoritmen	240
2.1.	Cryptografische systemen	240
2.2.	Cryptografische algoritmen	240
2.2.1.	RSA-algoritme	240
2.2.2.	Hash-algoritme	240
2.2.3.	Algoritme voor gegevenscodering	240
3.	Sleutels en certificaten	240
3.1.	Ontwikkeling en verspreiding van sleutels	240
3.1.1.	Ontwikkeling en verspreiding van RSA-sleutels	240
3.1.2.	RSA-beproevingssleutels	242
3.1.3.	Sleutels bewegingsopnemer	242
3.1.4.	Ontwikkeling en verspreiding van T-DES-sessiesleutels	242
3.2.	Sleutels	242
3.3.	Certificaten	242
3.3.1.	Inhoud van de certificaten	243
3.3.2.	Afgegeven certificaten	244
3.3.3.	Certificaatverificatie en uitpakken	245
4.	Mechanisme voor wederzijdse authenticatie	245
5.	Vertrouwelijkheids-, integriteits- en authenticatieapparatuur voor gegevensoverdracht van VU-kaarten	248
5.1.	Veilige transmissie	248
5.2.	Behandeling van fouten bij de beveiligde transmissie	249
5.3.	Algoritme voor het berekenen van cryptografische controlesommen	250
5.4.	Algoritme voor het berekenen van cryptogrammen voor vertrouwelijkheid DO's	250
6.	Digitale handtekeningapparatuur voor gegevensoverbrenging	251
6.1.	Ontwikkeling van de handtekening	251
6.2.	Handtekeningverificatie	251

1. ALGEMEEN

Deze appendix specificeert de veiligheidsmechanismen die het volgende waarborgen:

— de wederzijdse authenticatie tussen de VU en de tachograafkaart, inclusief sleutelovereenstemming tijdens de sessie;

— de vertrouwelijkheid, integriteit en authenticatie van de tussen de VU en de tachograafkaart overgebrachte gegevens;

— de integriteit en authenticatie van de van de VU naar externe opslagmedia overgebrachte gegevens;

— de integriteit en authenticatie van gegevens die van de tachograafkaart naar externe opslagmedia overgebracht worden.

1.1. **Referentienormen**

De onderstaande referentienormen worden in deze appendix 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 deze appendix gebruikt:

(K_a, K_b, K_c)	Een sleutelbos voor gebruik door het drievoudige algoritme voor gegevenscodering
CA	Certificeringsinstantie
CAR	Referentie van de certificeringsinstantie
CC	Cryptografische controlesom
CG	Cryptogram
CH	Opdracht-koptitel
CHA	Autorisatie van de certificaathouder
CHR	Referentie van de certificaathouder
D()	Decodering met DES
DE	Gegevenselement
DO	Gegevensobject
d	RSA particuliere sleutel, particuliere exponent
e	RSA openbare sleutel, openbare exponent
E()	Codering met DES
EQT	Apparatuur
Hash()	Hashwaarde, een uitvoer van *Hash*
Hash	Hashing
KID	Sleutel-identificatiesymbool
Km	TDES-sleutel. Master Key, gedefinieerd in ISO 16844-3
Km_{VU}	TDES-sleutel, ingebracht in voertuigunits
Km_{WC}	TDES-sleutel ingebracht in werkplaatskaarten
m	Berichtsymbool, een eenheid tussen 0 en *n*-1
n	RSA-sleutels, modulus
PB	Padding bytes
PI	Padding indicatorbyte (voor gebruik bij cryptogram voor vertrouwelijkheid DO)
PV	Ongecodeerde waarde
s	Handtekeningsymbool, een eenheid tussen 0 en *n*-1
SSC	Zendsequentieteller
SM	Beveiligde overbrenging
TCBC	TDEA-modus cipher block chaining
TDEA	Drievoudig algoritme voor gegevenscodering
TLV	Waarde labellengte
VU	Voertuigunit
X.C	Certificaat van gebruiker X afgegeven door een certificeringsinstantie
X.CA	Certificeringsinstantie van gebruiker X
$X.CA.PK_oX.C$	Handeling van uitpakken van een certificaat om een openbare sleutel te selecteren. Het is een infix-operator; de linker operand is de openbare sleutel van een certificeringsinstantie en de rechter operand is het door die certificeringsinstantie afgegeven certificaat. Het resultaat is de openbare sleutel van gebruiker X wiens certificaat de rechter operand is

X.PK	RSA-openbare 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
||	Verbindingsoperator

2. CRYPTOGRAFISCHE SYSTEMEN EN ALGORITMEN

2.1. **Cryptografische systemen**

CSM_001 Voertuigunits en tachograafkaarten moeten een standaard RSA cryptografisch systeem van openbare sleutels gebruiken om de onderstaande veiligheidsmechanismen te leveren:

— authenticatie tussen voertuigunit en kaart,

— transport van drievoudige DES-sessiesleutels tussen voertuigunit en tachograafkaart,

— digitale handtekening van overgebrachte gegevens van de voertuigunit of tachograafkaart naar externe media.

CSM_002 Voertuigunits en tachograafkaarten moeten een drievoudig DES symmetrisch cryptografisch systeem gebruiken om een mechanisme te bieden voor de integriteit van de gegevens tijdens de uitwisseling van gebruikersgegevens tussen de voertuigunit en de tachograafkaart en, waar van toepassing, te zorgen voor vertrouwelijkheid van de gegevensuitwisseling tussen voertuigunit en tachograafkaart.

2.2. **Cryptografische algoritmen**

2.2.1. ***RSA-algoritme***

CSM_003 Het RSA-algoritme wordt door de onderstaande vergelijkingen volledig gedefinieerd:

$$\text{X.SK}[m] = s = m^d \bmod n$$

$$\text{X.PK}[s] = m = s^e \bmod n$$

Een uitgebreidere beschrijving van de RSA-functie staat in referentienorm PKCS1. De in het RSA-algoritme gebruikte openbare exponent e moet in alle gegenereerde RSA-sleutels verschillend zijn van 2.

2.2.2. ***Hash-algoritme***

CSM_004 De apparatuur voor digitale handtekeningen moet het in referentienorm SHA-1 gedefinieerde SHA-1 hash-algoritme gebruiken.

2.2.3. ***Algoritme voor gegevenscodering***

CSM_005 Op DES gebaseerde algoritmen moeten in de cipher block chaining modus worden gebruikt.

3. SLEUTELS EN CERTIFICATEN

3.1. **Ontwikkeling en verspreiding van sleutels**

3.1.1. ***Ontwikkeling en verspreiding van RSA-sleutels***

CSM_006 RSA-sleutels moeten via drie functionele hiërarchische niveaus gegenereerd worden:

— Europees niveau,

— niveau van de lidstaat,

— niveau van de apparatuur.

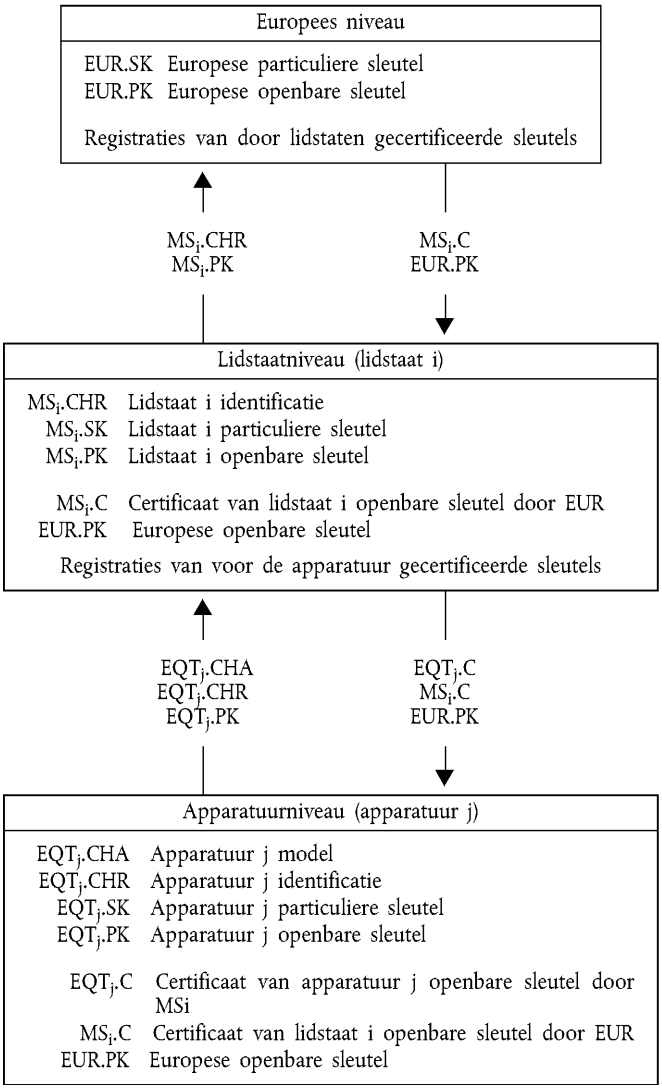
CSM_007 Op Europees niveau moet een enkel Europees sleutelpaar (EUR.SK en EUR.PK) gegenereerd worden. De Europese particuliere sleutel moet worden gebruikt om de openbare sleutels van de lidstaten te certificeren. Registraties van alle gecertificeerde sleutels moeten worden bijgehouden. Deze taken moeten door een Europese certificeringsinstantie, in opdracht en onder verantwoordelijkheid van de Europese Commissie, worden uitgevoerd.

CSM_008 Op lidstaatniveau moet een lidstaat-sleutelpaar (MS.SK en MS.PK) gegenereerd worden. Openbare sleutels van lidstaten moeten door de Europese certificeringsinstantie gecertificeerd worden. De particuliere sleutel van de lidstaten moet worden gebruikt om de openbare, in apparatuur (voertuigunit of tachograafkaart) in te brengen openbare sleutels te certificeren. Registraties van alle gecertificeerde openbare sleutels met de identificatie van de betreffende apparatuur moeten worden bijgehouden. Deze taken moeten door een certificeringsinstantie van een lidstaat worden uitgevoerd. Een lidstaat kan zijn sleutelpaar regelmatig wijzigen.

CSM_009 Op apparatuurniveau moet een enkel sleutelpaar (EQT.SK en EQT.PK) gegenereerd en in alle apparatuur ingebracht worden. Openbare sleutels van de apparatuur moeten door een certificeringsinstantie van de lidstaat gecertificeerd worden. Deze taken kunnen door de fabrikanten van de apparatuur, installateurs van de apparatuur of instanties van de lidstaat worden uitgevoerd. Dit sleutelpaar wordt gebruikt voor authenticatie, digitale handtekeningen en codering.

CSM_010 De vertrouwelijkheid van particuliere sleutels moet tijdens de ontwikkeling, het transport (indien van toepassing) en de opslag gehandhaafd blijven.

Het onderstaande schema vat de gegevensstroom van dit proces samen:



3.1.2. ***RSA-beproevingssleutels***

CSM_011 Voor beproevingsdoeleinden van de apparatuur (inclusief interoperabiliteitsbeproevingen) moet de Europese certificeringsinstantie een afzonderlijke Europese beproevingssleutel en ten minste twee beproevingssleutels voor de lidstaten genereren. De openbare sleutels van deze beproevingssleutels moeten met de Europese particuliere beproevingssleutel gecertificeerd worden. Bij beproevingen in verband met de goedkeuring van apparatuur moeten fabrikanten beproevingssleutels inbrengen die door een van deze beproevingssleutels van de lidstaten gecertificeerd zijn.

3.1.3. ***Sleutels bewegingsopnemer***

De vertrouwelijkheid van de drie hieronder beschreven TDES-sleutels moet tijdens de ontwikkeling, het transport (indien van toepassing) en de opslag op adequate wijze worden gehandhaafd.

Teneinde met ISO 16844 in overeenstemming zijnde controleapparaten te ondersteunen, zorgen de Europese certificeringsinstantie en de certificeringsinstanties van de lidstaten bovendien voor het volgende:

CSM_036 De Europese certificeringsinstantie ontwikkelt Km_{VU} en Km_{WC}, twee onafhankelijke en unieke Triple DES-sleutels, en ontwikkelen Km als:

$$Km = Km_{VU} \text{ XOR } Km_{WC}$$

De Europese certificeringsinstantie zendt deze sleutels op verzoek toe aan de certificeringsinstanties van de lidstaten, via adequaat beveiligde procedures.

CSM_037 De certificeringsinstanties van de lidstaten:

— gebruiken Km om door de fabrikanten van bewegingsopnemers gevraagde gegevens van de bewegingsopnemer te coderen (de met Km te coderen data zijn gedefinieerd in ISO 16844-3),

— zenden Km_{VU} toe aan fabrikanten van voertuigunits, via adequaat beveiligde procedures, voor gebruik in voertuigunits,

— zorgen ervoor dat Km_{WC} wordt ingebracht in alle werkplaatskaarten (`SensorInstallationSecData` in basisbestand `Sensor_Installation_Data`) bij de personalisering van de kaart.

3.1.4. ***Ontwikkeling en verspreiding van T-DES-sessiesleutels***

CSM_012 Voertuigunits en tachograafkaarten moeten als onderdeel van het wederzijds authenticatieproces de vereiste gegevens genereren en uitwisselen om een gemeenschappelijke drievoudige DES-sessiesleutel te ontwikkelen. Met het oog op de vertrouwelijkheid moet deze gegevensuitwisseling door een RSA-crypto-apparatuur worden beveiligd.

CSM_013 Deze sleutel moet bij alle volgende cryptografische operaties met veilige overbrenging worden gebruikt. De geldigheid vervalt aan het einde van de sessie (kaartuitneming of kaartterugstelling) en/of na 240 toepassingen (een toepassing van de sleutel = een met veilige overdracht naar de kaart gezonden opdracht en het bijbehorende antwoord).

3.2. **Sleutels**

CSM_014 RSA-sleutels moeten (ongeacht het niveau) de volgende lengte hebben: modulus *n* 1024 bits, openbare exponent *e* maximaal 64 bits, particuliere exponent *d* 1024 bits.

CSM_015 Drievoudige DES-sleutels moeten de vorm (K_a, K_b, K_a), hebben, waarbij K_a en K_b onafhankelijke sleutels van 64 bits zijn. Er worden geen bits ingesteld die pariteitsfouten ontdekken.

3.3. **Certificaten**

CSM_016 Certificaten van openbare RSA-sleutels moeten „niet-zelfbeschrijvende" „kaartverifieerbare" certificaten (Ref.: ISO/IEC 7816-8) zijn.

3.3.1. ***Inhoud van de certificaten***

CSM_017 Certificaten van openbare RSA-sleutels bevatten de onderstaande gegevens in de onderstaande volgorde:

Gegevens	Formaat	Bytes	Obs
CPI	INTEGER	1	Certificaatprofiel identificatiesymbool (′01′ voor deze versie)
CAR	OCTET STRING	8	Referentienorm van certificeringsinstantie
CHA	OCTET STRING	7	Autorisatie van certificaathouder
EOV	TimeReal	4	Vervaldatum van certificaat. Facultatief, ′FF′ opgevuld indien niet gebruikt
CHR	OCTET STRING	8	Referentienorm van certificaathouder
n	OCTET STRING	128	Openbare sleutel (modulus)
e	OCTET STRING	8	Openbare sleutel (openbare exponent)
		164	

Opmerkingen:

1. Het „Certificaatprofiel identificatiesymbool" (CPI) geeft de exacte structuur van een authenticatiecertificaat aan. Het kan worden gebruikt als een intern identificatiesymbool van een apparaat op een relevante lijst koptitels die de verbinding van gegevenselementen in het certificaat beschrijft.

   De koptitels met betrekking tot de inhoud van dit certificaat zijn de volgende:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Toegevoegde koptitellabel	Lengte van koptitellijst	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 van opeenvolgende DO's	Label van de modulus	Lengte van de modulus	Label van de openbare exponent	Lengte van de openbare exponent

2. Het doel van de „referentienorm van de certificeringsinstantie" (CAR) is het identificeren van de CA die het certificaat afgeeft, zodanig dat het gegevenselement tegelijkertijd met een sleutel-identificatiesymbool van de instantie kan worden gebruikt ter verwijzing naar de openbare sleutel van de certificeringsinstantie (zie onderstaand sleutel-identificatiesymbool voor codering).

3. De „autorisatie van de certificaathouder" (CHA) wordt gebruikt om de rechten van de certificaathouder te identificeren. Het bestaat uit de ID van de tachograaftoepassing en uit het model van de apparatuur waarvoor het certificaat bedoeld is (overeenkomstig het `ApparatuurModel` gegevenselement, „00" voor een lidstaat).

4. Het doel van de „referentienorm van de certificaathouder" (CHR) is het op een unieke manier identificeren van de certificaathouder, zodanig dat het gegevenselement tegelijkertijd met een sleutel-identificatiesymbool van het subject kan worden gebruikt ter verwijzing naar de openbare sleutel van de certificaathouder.

5. Sleutel-identificatiesymbolen identificeren op een unieke manier de certificaathouder of de certificeringsinstanties. Ze worden als volgt gecodeerd:

   5.1. Apparatuur (VU of kaart):

Gegevens	Serienummer van de apparatuur	Datum	Model	Fabrikant
Lengte	4 bytes	2 bytes	1 byte	1 byte
Waarde	Eenheid	Mm yy BCD-codering	Specifiek kenmerk fabrikant	Code fabrikant

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 stuurt de fabrikant de identificatie van de apparatuur met de openbare sleutel ter certificatie naar de instantie van zijn lidstaat. Het certificaat bevat dan de identificatie van de apparatuur en de fabrikant moet garanderen dat sleutels en certificaat in de betreffende apparatuur worden ingebracht. Het sleutel-identificatiesymbool heeft de bovenstaande vorm.

In het tweede geval moet de fabrikant ieder verzoek om een certificaat op een unieke manier identificeren en deze identificatie met de openbare sleutel ter certificering naar de instantie van zijn lidstaat sturen. Het certificaat moet het identificatieverzoek bevatten. De fabrikant moet aan de instantie van zijn lidstaat de toewijzing van de sleutel in de apparatuur (d.w.z. identificatie van het verzoek om een certificaat, identificatie van de apparatuur) na installatie van de sleutel in de apparatuur doorgeven. Het sleutel-identificatiesymbool heeft de onderstaande vorm:

Gegevens	Seriennummer certificaatverzoek	Datum	Model	Fabrikant
Lengte	4 bytes	2 bytes	1 byte	1 byte
Waarde	BCD-codering	mm yy BCD-codering	'FF'	Code fabrikant

5.2. Certificeringsinstantie:

Gegevens	Identificatie instantie	Serienummer van de sleutel	Additionele info	Identificatiesymbool
Lengte	4 bytes	1 byte	2 bytes	1 byte
Waarde	1 byte numerieke code van de staat 3 bytes alfanumerieke code van de staat	Eenheid	additionele codering (specifiek voor certificerings-instantie) 'FF FF' indien niet gebruikt	'01'

Het serienummer van de sleutel wordt gebruikt om de verschillende sleutels van een lidstaat te onderscheiden wanneer de sleutel gewijzigd wordt.

6. Certificaatverificateurs moeten impliciet weten dat de gecertificeerde openbare sleutel een RSA-sleutel is die van belang is voor de authenticatie, verificatie van de digitale handtekening en codering voor vertrouwelijke diensten (het certificaat bevat geen object-identificatiesymbool om het te specificeren).

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, waarbij de „referentienorm van de certificeringsinstantie" toegevoegd is.

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, \mathit{Hash}(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

Met inhoud van het certificaat $= Cc = \underset{106\ \text{bytes}}{C_r} \,||\, \underset{58\ \text{bytes}}{C_n}$

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 certificeringsinstantie ter verificatie van het certificaat geselecteerd kan worden.

3. Ter ondertekening van het certificaat moet de certificaatverificateur het door de certificeringsinstantie gebruikte algoritme impliciet kennen.

4. De koptitels met betrekking tot dit afgegeven certificaat zijn de volgende:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
CV certificaat label (Geconstrueerd)	Lengte van opeenvolgende DO's	Label handtekening	Lengte handtekening	Restlabel	Restlengte	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 moeten de volgende stappen worden genomen:

Verifieer handtekening en zoek inhoud:

— van X.C zoek Teken, C_n' en CAR′: X.C = teken (128 Bytes) || C_n' (58 Bytes) || CAR' (8 Bytes)

— van CAR′ selecteer de vereiste openbare sleutel van de certificeringsinstantie (indien dit nog niet met andere middelen gedaan is)

— open Teken met CA Openbare Sleutel: Sr′ = X.CA.PK [Teken],

— controleer of Sr′ begint met ′6A′ en eindigt met ′BC′

— bereken Cr′ en H′ van: Sr' = '6A' || C_r' (106 Bytes) || H' (20 Bytes) || 'BC'

— vind inhoud van het certificaat C′ = C_r' || C_n',

— controleer *Hash*(C′) = H′

Indien de controles o.k. zijn, is het certificaat authentiek, de inhoud ervan is C′.

Verifieer geldigheid. Van C′:

— indien van toepassing, controleer einde van de geldigheidsdatum,

Zoek en sla openbare sleutel, sleutel-identificatiesymbool, autorisatie van de certificaathouder en einde van de geldigheid van het certificaat van C′ op:

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MECHANISME VOOR WEDERZIJDSE AUTHENTICATIE

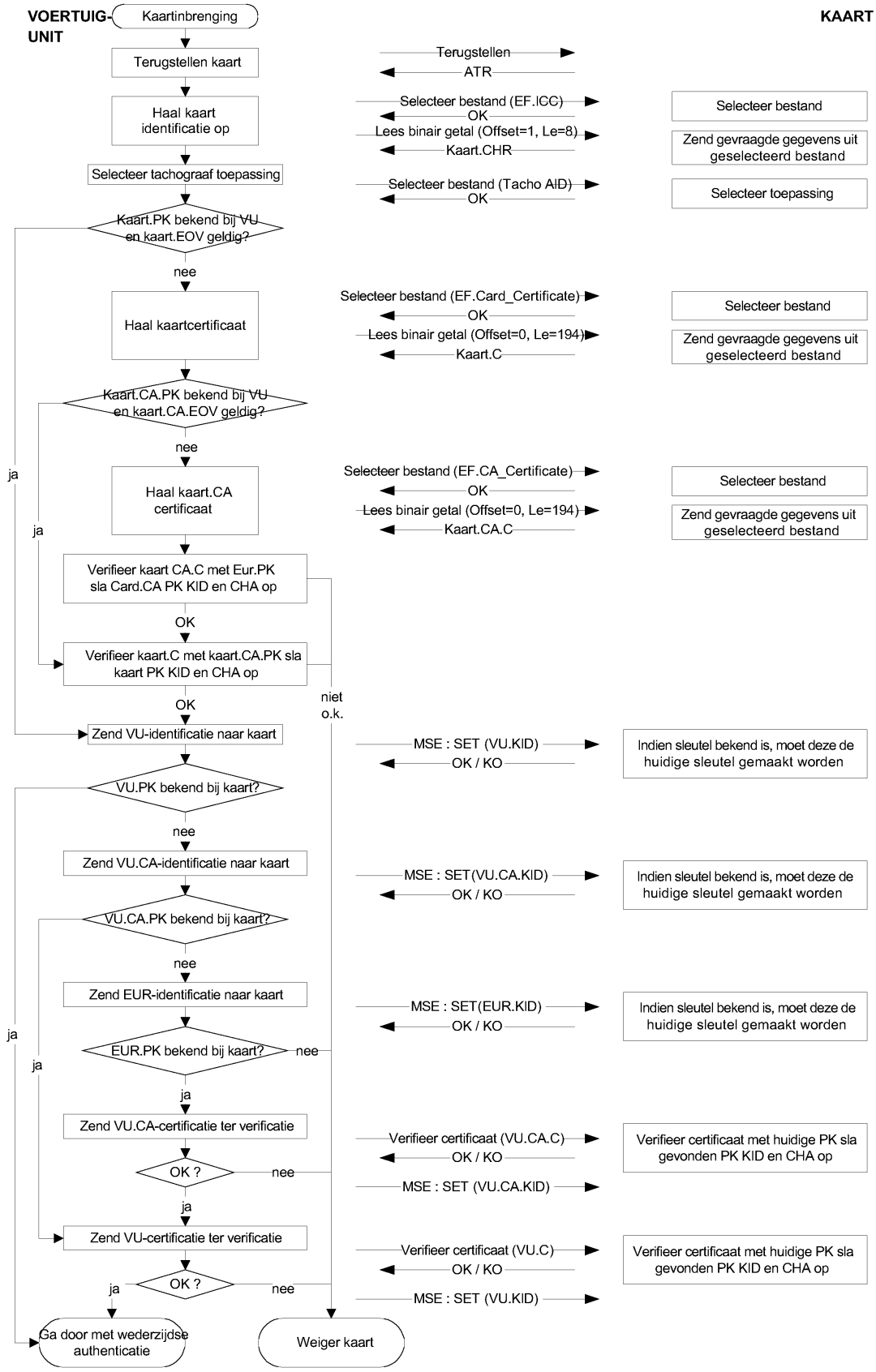
Wederzijdse authenticatie tussen kaarten en VU is gebaseerd op het volgende principe:

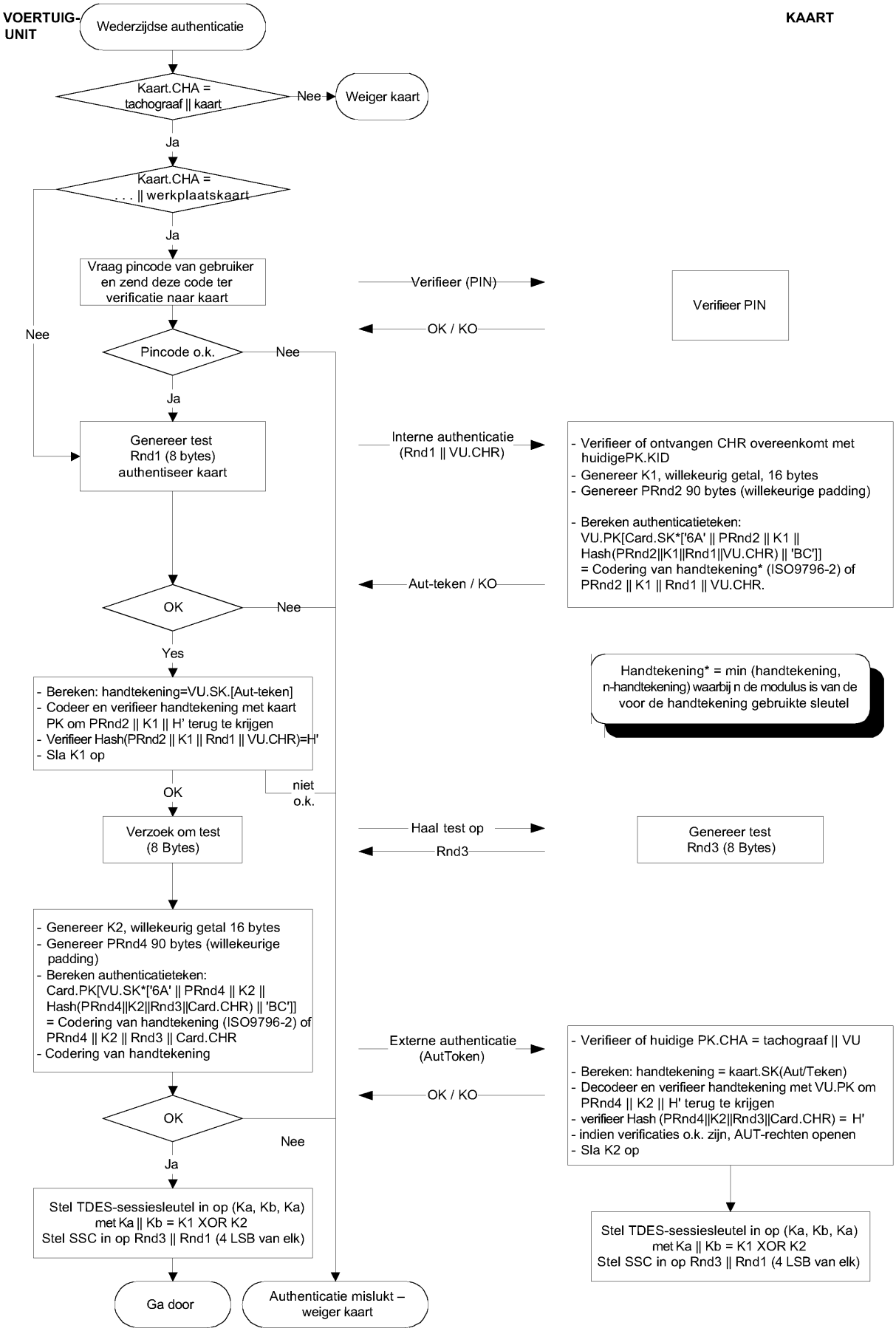
Elke partij moet aan de ander aantonen dat hij een geldig sleutelpaar heeft, waarvan de openbare sleutel gecertificeerd is door een certificeringsinstantie van een lidstaat, die zelf weer gecertificeerd is door de Europese certificeringsinstantie.

Het bewijs wordt geleverd door ondertekening met de particuliere sleutel van een willekeurig, door de andere partij gezonden nummer, die het gezonden willekeurige nummer bij de verificatie van deze handtekening moet terugvinden.

Het mechanisme wordt door de VU bij kaartinbrenging gestart. 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 moet worden gebruikt (pijltjes geven opdrachten en uitgewisselde gegevens aan (zie appendix 2)):




VOERTUIG-UNIT
KAART
Wederzijdse authenticatie
Kaart.CHA = tachograaf || kaart
Nee
Weiger kaart
Ja
Kaart.CHA = . . . || werkplaatskaart
Ja
Vraag pincode van gebruiker en zend deze code ter verificatie naar kaart
Verifieer (PIN)
Verifieer PIN
OK / KO
Nee
Pincode o.k.
Nee
Ja
Genereer test Rnd1 (8 bytes) authentiseer kaart
Interne authenticatie (Rnd1 || VU.CHR)
- Verifieer of ontvangen CHR overeenkomt met huidigePK.KID
- Genereer K1, willekeurig getal, 16 bytes
- Genereer PRnd2 90 bytes (willekeurige padding)
- Bereken authenticatieteken: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Codering van handtekening* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
Aut-teken / KO
OK
Nee
Yes
Handtekening* = min (handtekening, n-handtekening) waarbij n de modulus is van de voor de handtekening gebruikte sleutel
- Bereken: handtekening=VU.SK.[Aut-teken]
- Codeer en verifieer handtekening met kaart PK om PRnd2 || K1 || H' terug te krijgen
- Verifieer Hash(PRnd2 || K1 || Rnd1 || VU.CHR)=H'
- Sla K1 op
niet o.k.
OK
Verzoek om test (8 Bytes)
Haal test op
Rnd3
Genereer test Rnd3 (8 Bytes)
- Genereer K2, willekeurig getal 16 bytes
- Genereer PRnd4 90 bytes (willekeurige padding)
- Bereken authenticatieteken: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Codering van handtekening (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Codering van handtekening
Externe authenticatie (AutToken)
- Verifieer of huidige PK.CHA = tachograaf || VU
- Bereken: handtekening = kaart.SK(Aut/Teken)
- Decodeer en verifieer handtekening met VU.PK om PRnd4 || K2 || H' terug te krijgen
- verifieer Hash (PRnd4||K2||Rnd3||Card.CHR) = H'
- indien verificaties o.k. zijn, AUT-rechten openen
- Sla K2 op
OK / KO
OK
Nee
Ja
Stel TDES-sessiesleutel in op (Ka, Kb, Ka) met Ka || Kb = K1 XOR K2
Stel SSC in op Rnd3 || Rnd1 (4 LSB van elk)
Stel TDES-sessiesleutel in op (Ka, Kb, Ka) met Ka || Kb = K1 XOR K2
Stel SSC in op Rnd3 || Rnd1 (4 LSB van elk)
Ga door
Authenticatie mislukt – weiger kaart

5. VERTROUWELIJKHEIDS-, INTEGRITEITS- EN AUTHENTICATIEAPPARATUUR VOOR GEGEVENSOVERDRACHT VAN VU-KAARTEN

5.1. **Veilige transmissie**

CSM_021 De integriteit van de gegevensoverdracht van VU-kaarten moet door beveiligde transmissie overeenkomstig de referentienormen ISO/IEC 7816-4 en ISO/IEC 7816-8 beschermd worden.

CSM_022 Wanneer gegevens tijdens de overdracht beveiligd moeten worden, moet een cryptografische controlesom gegevensobject aan de binnen de opdracht of het antwoord gezonden gegevensobjecten worden toegevoegd. De cryptografische controlesom moet door de ontvanger geverifieerd worden.

CSM_023 De cryptografische controlesom van binnen een opdracht gezonden gegevens moet de opdracht-koptitel en alle gezonden gegevensobjecten integreren (= > CLA = ′0C′, en alle gegevensobjecten moeten worden ingekapseld met labels waarin b 1= 1).

CSM_024 De bytes van de statusinformatie van het antwoord moeten door een cryptografische controlesom worden beveiligd wanneer het antwoord geen gegevensveld bevat.

CSM_025 Cryptografische controlesommen moeten 4 bytes lang zijn.

De structuur van opdrachten en antwoorden bij gebruik van veilige transmissie is derhalve de volgende:

De gebruikte DO's zijn een deelverzameling van de veilige transmissie-DO's beschreven in ISO/IEC 7816-4:

Label	Mnemoniek	Betekenis
′81′	T_{PV}	Ongecodeerde waarde van niet met BER-TLV gecodeerde gegevens (te beschermen door CC)
′97′	T_{LE}	Waarde van Le in de onbeveiligde opdracht (te beschermen door CC)
′99′	T_{SW}	Statusinformatie (te beschermen door CC)
′8E′	T_{CC}	Cryptografische controlesom
′87′	$T_{PI\ CG}$	Padding aanwijsbyte || Cryptogram (Ongecodeerde waarde niet in BER-TLV gecodeerd)

Gegeven een onbeveiligd opdracht-antwoordpaar:

Opdracht-koptitel	Opdracht-object
CLA INS P1 P2	[L_c veld] [Gegevensveld] [L_e veld]
Vier bytes	L bytes, aangeduid als B_1tot B_L

Antwoordobject	Staartlabel antwoord
[Gegevensveld]	SW1 SW2
L_r gegevensbytes	Twee bytes

Het corresponderende beveiligde opdracht-antwoordpaar is:

Beveiligde opdracht:

Opdracht-koptitel (CH)	Opdracht-object										
CLA INS P1 P2	[Nieuw L_c veld]	[Nieuw gegevensveld]									[Nieuw L_e veld]
′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 = Padding bytes (80 .. 00) overeenkomstig ISO-IEC 7816-4 en ISO 9797, methode 2.

DO's, PV en LE zijn alleen aanwezig wanneer er corresponderende gegevens in de onbeveiligde opdracht zijn.

Beveiligd antwoord:

1. Geval waarin het gegevensveld van het antwoord niet leeg is en niet beveiligd hoeft te worden in verband met vertrouwelijkheid:

Antwoordobject						Staartlabel antwoord
[Nieuw gegevensveld]						Nieuw SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	Gege-vensveld	'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 voor vertrouwelijkheid beveiligd moet worden:

Antwoordobject						Staartlabel 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 padding bytes.

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:

Antwoordobject						Staartlabel antwoord
[Nieuw gegevensveld]						Nieuwe SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	Nieuw SW1 SW2	'8E'	'04'	CC	

In de controlesom te integreren gegevens = T_{SW} || L_{SW} || SW || PB

5.2. **Behandeling van fouten bij de beveiligde transmissie**

CSM_026 Wanneer de tachograafkaart tijdens het vertalen van een opdracht een SM-fout ontdekt, dan moeten de statusbytes zonder SM teruggezonden worden. Overeenkomstig ISO/IEC 7816-4 moeten de onderstaande statusbytes gedefinieerd worden om SM-fouten aan te geven:

'66 88' Verificatie van cryptografische controlesom mislukt,

'69 87' Verwachte SM-gegevensobjecten ontbreken,

'69 88' SM-gegevensobjecten onjuist.

CSM_027 Wanneer de tachograafkaart statusbytes zonder SM DO's of met een foutieve SM DO terugzendt, moet de sessie door de VU afgebroken worden.

5.3. **Algoritme voor het berekenen van cryptografische controlesommen**

CSM_028 Cryptografische controlesommen worden opgebouwd in een retail MAC overeenkomstig ANSI X9.19 met DES:

— 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.

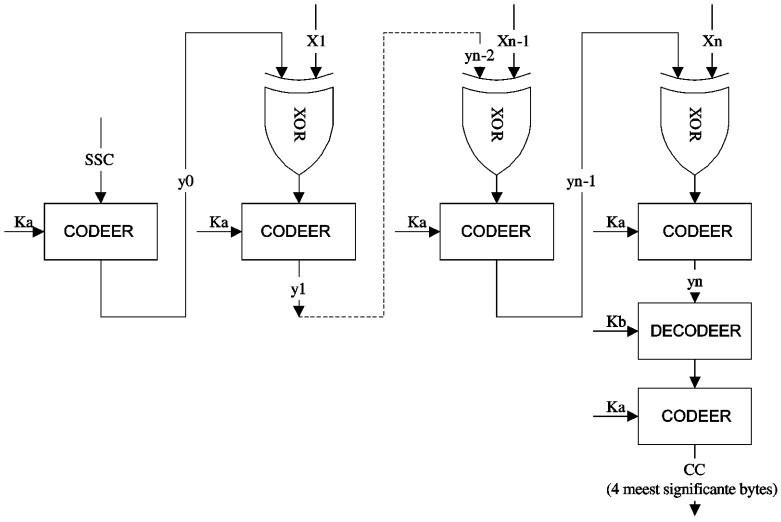
De vier meest significante bytes van de cryptografische controlesom worden overgedragen.

CSM_029 De zendsequentieteller (SSC) moet tijdens de goedkeuringsprocedure van de sleutel geïnitieerd worden:

Begin SSC : Rnd3 (4 laatste significante bytes) || Rnd1 (4 laatste significante bytes).

CSM_030 De zendsequentieteller moet elke keer voordat een MAC wordt berekend, met 1 worden verhoogd (d.w.z. de SSC voor de eerste opdracht is Begin SSC + 1, de SSC voor het eerste antwoord is Begin SSC + 2).

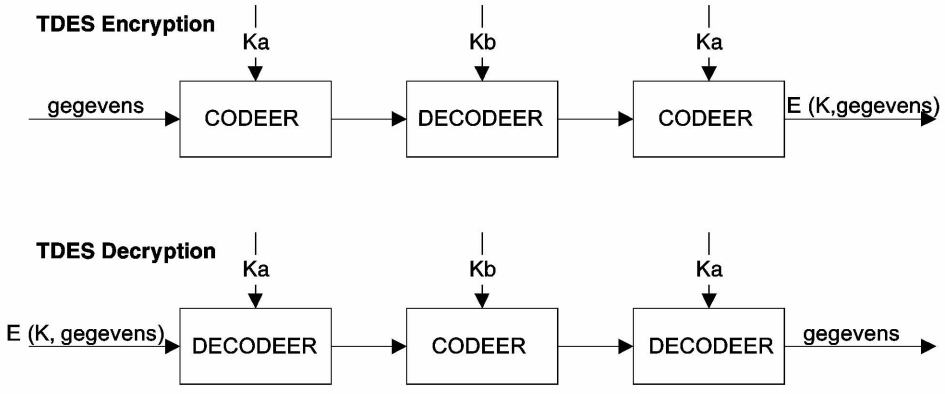
De onderstaande figuur toont de berekening van de retail MAC:



5.4. **Algoritme voor het berekenen van cryptogrammen voor vertrouwelijkheid DO's**

CSM_031 Cryptogrammen worden met TDEA in de TCBC-werkingsmodus berekend overeenkomstig referentienorm TDES en TDES-OP en met de lege vector als beginwaardeblok.

De onderstaande figuur toont de toepassing van sleutels in TDES:



6. DIGITALE HANDTEKENINGAPPARATUUR VOOR GEGEVENSOVERBRENGING

CSM_032 De intelligente toepassingsgerichte apparatuur (IDE) slaat de van een apparaat (VU of kaart) tijdens een overbrengingssessie 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 appendix 7 (Gegevensoverbrengingsprotocollen).

CSM_033 Digitale handtekeningen van overgebrachte gegevens moeten een digitaal handtekeningschema met aanhangsel gebruiken zodat overgebrachte gegevens indien gewenst zonder decodering gelezen kunnen worden.

6.1. **Ontwikkeling van de handtekening**

CSM_034 De ontwikkeling van de gegevenshandtekening door de apparatuur moet het handtekeningschema met aanhangsel zoals gedefinieerd in referentienorm PKCS1 met de SHA-1 hashing-functie volgen:

$$\text{Handtekening} = \text{EQT.SK}[\text{'00'} \,||\, \text{'01'} \,||\, PS \,||\, \text{'00'} \,||\, \text{DER(SHA-1(Gegevens))}]$$

PS = Padding string van achtbits bytes met waarde 'FF' zodat de lengte 128 is.

DER(SHA-1(M)) is de codering van de ID van het algoritme voor de hashing-functie en de hashwaarde in een ASN.1-waarde van het type `OntsluitInfo` (kenmerkende coderingsregels):

'30'||'21'||'30'||'09'||'06'||'05'||'2B'||'0E'||'03'||'02'||'1A'||'05'||'00'||'04'||'14'||Hashwaarde.

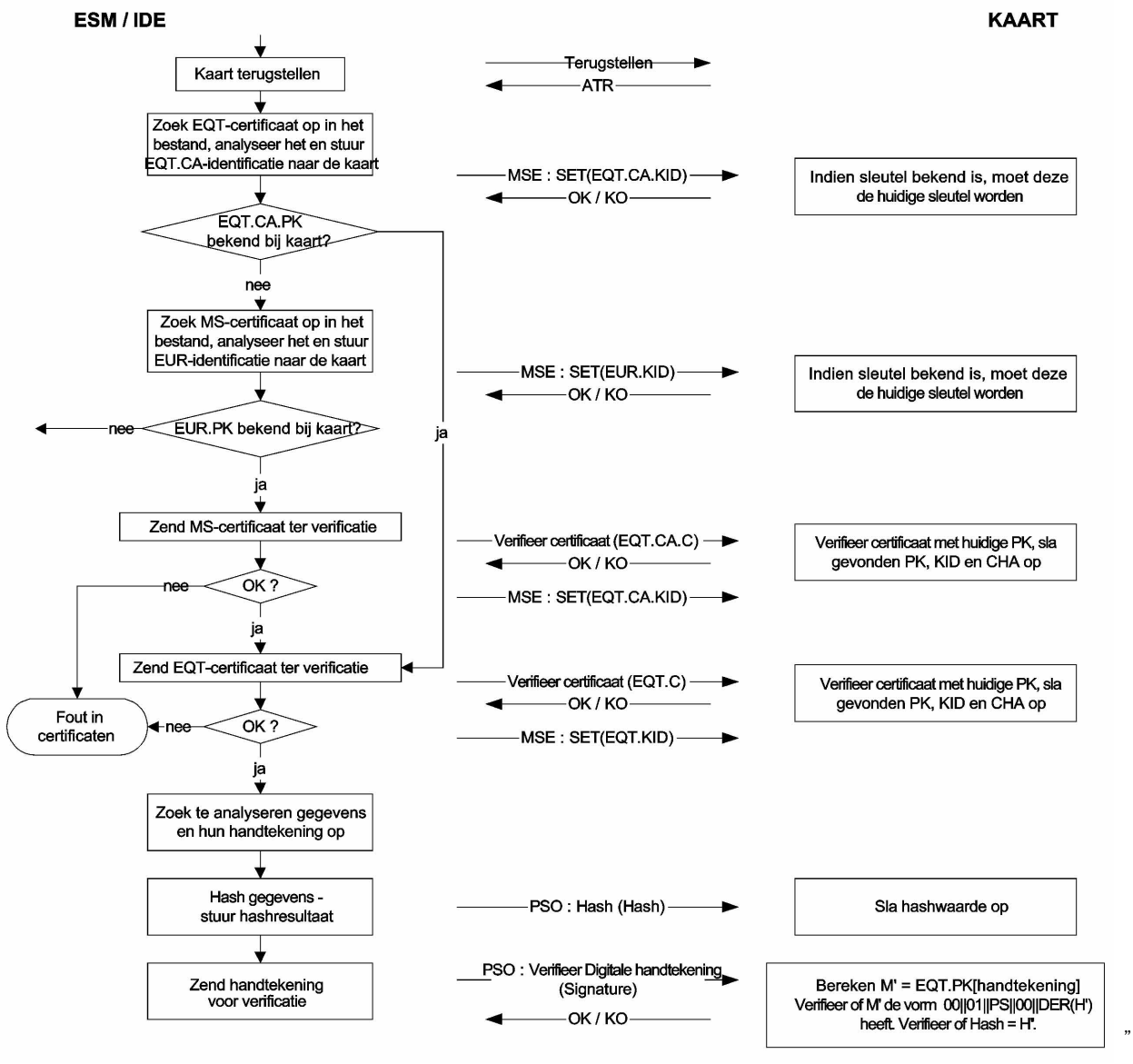
6.2. **Handtekeningverificatie**

CSM_035 Verificatie van de gegevenshandtekening op overgebrachte gegevens moet het handtekeningschema met aanhangsel zoals gedefinieerd in referentienorm PKCS1 met de SHA-1 hashing-functie volgen.

De verificateur moet de Europese openbare sleutel EUR.PK zelf kennen (en vertrouwen).

De onderstaande tabel illustreert het protocol dat een controlekaart dragende IDE kan volgen om de integriteit van de overgebrachte en op de ESM (externe opslagmedia) opgeslagen gegevens te verifiëren. De controlekaart wordt gebruikt voor de decodering van digitale handtekeningen. Deze functie mag in dit geval niet in de IDE geïmplementeerd worden.

De apparatuur die de te analyseren gegevens heeft overgebracht en ondertekend, wordt met EQT aangeduid.


ESM / IDE
KAART
Kaart terugstellen
Terugstellen
ATR
Zoek EQT-certificaat op in het bestand, analyseer het en stuur EQT.CA-identificatie naar de kaart
MSE : SET(EQT.CA.KID)
OK / KO
Indien sleutel bekend is, moet deze de huidige sleutel worden
EQT.CA.PK bekend bij kaart?
nee
Zoek MS-certificaat op in het bestand, analyseer het en stuur EUR-identificatie naar de kaart
MSE : SET(EUR.KID)
OK / KO
Indien sleutel bekend is, moet deze de huidige sleutel worden
nee
EUR.PK bekend bij kaart?
ja
ja
Zend MS-certificaat ter verificatie
Verifieer certificaat (EQT.CA.C)
OK / KO
Verifieer certificaat met huidige PK, sla gevonden PK, KID en CHA op
nee
OK ?
MSE : SET(EQT.CA.KID)
ja
Zend EQT-certificaat ter verificatie
Verifieer certificaat (EQT.C)
OK / KO
Verifieer certificaat met huidige PK, sla gevonden PK, KID en CHA op
Fout in certificaten
nee
OK ?
MSE : SET(EQT.KID)
ja
Zoek te analyseren gegevens en hun handtekening op
Hash gegevens - stuur hashresultaat
PSO : Hash (Hash)
Sla hashwaarde op
Zend handtekening voor verificatie
PSO : Verifieer Digitale handtekening (Signature)
OK / KO
Bereken M' = EQT.PK[handtekening]
Verifieer of M' de vorm 00||01||PS||00||DER(H') heeft. Verifieer of Hash = H'.

"