STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 9656
9 april
2015

Regeling van de Staatssecretaris van Infrastructuur en Milieu, van 20 maart 2015, nr. IENM/BSK-2015/35270, houdende wijziging van de Regeling specificaties en typegoedkeuring boordcomputer taxi en de Regeling erkenning werkplaatsen boordcomputer taxi

De Staatssecretaris van Infrastructuur en Milieu,

Gelet op artikel 22, eerste lid, van de Wegenverkeerswet 1994 en artikel 79, zevende en achtste lid, van het Besluit personenvervoer 2000;

BESLUIT:

ARTIKEL I

De Regeling specificaties en typegoedkeuring boordcomputer taxi wordt als volgt gewijzigd:

A

Artikel 1 wordt als volgt gewijzigd:

1. De definitie van activering komt te luiden:

activering: handeling waarmee de boordcomputer in geactiveerde toestand wordt gebracht;

2. In de alfabetische rangschikking worden de volgende definities ingevoegd:

– *boordcomputereenheid:* boordcomputer zonder systeemkaart;
– *deactivering:* handeling waarmee de boordcomputer in niet-geactiveerde toe stand wordt gebracht;
– *eerste systeemkaart:* voor een boordcomputer met een bepaald typegoedkeuringsnummer aan diens fabrikant afgegeven processorkaart waarvan de functie voor het genereren van elektronische handtekeningen nog niet actief is;
– *programmatuur:* de combinatie van uitvoerbare code van de boordcomputer en bijbehorende programmatuurgegevens;
– *programmatuurgegevens:* vaste attributen van programmatuur of een programmatuurrevisie;
– *programmatuurrevisie:* nieuwere versie van programmatuur;
– *programmatuurversienummer:* vast attribuut van programmatuur of programmatuurrevisie, zijnde een nummer waarmee de versie van programmatuur respectievelijk de programmatuurrevisie uniek geïdentificeerd kan worden;
– *vervangende systeemkaart:* door de minister voor de vervanging van de systeemkaart van een specifieke boordcomputer aan de fabrikant of werkplaats afgegeven nieuwe processorkaart waarvan de functie voor het genereren van elektronische handtekeningen nog niet actief is;
– *werkplaats:* werkplaats als bedoeld in artikel 1 van de Regeling erkenning werk plaatsen boordcomputer taxi;.

B

Artikel 2, vierde lid, komt te luiden:

4. De boordcomputer voldoet aan de bij deze regeling behorende bijlagen.

C

In artikel 7, vijfde lid, wordt ‘drie procent’ vervangen door: vijf procent.

D

Aan artikel 9, zevende lid, wordt een zin toegevoegd, luidende: Deze omvatten ten minste de totalen van de aan de in het eerste lid bedoelde activiteiten bestede tijd.

E

Artikel 13 wordt als volgt gewijzigd:

1. Onder vervanging van de punt na het eerste lid door een komma, wordt toegevoegd: dan wel een opdracht voor het overbrengen van gegevens aan de boordcomputer te verzenden buiten een fysieke verbinding tussen ondernemerskaart en boordcomputer.

2. Onder vernummering van het tweede lid tot vierde lid, worden twee leden ingevoegd, luidende:

2. Ingeval van verzending buiten een fysieke verbinding tussen ondernemerskaart en boordcomputer kan de boordcomputer zelfstandig vaststellen dat de opdracht door een daartoe geautoriseerde ondernemerskaart is gegeven in de bedrijfsmodus en door de ondernemerskaart is voorzien van een elektronische handtekening.
3. De in het tweede lid bedoelde autorisatie heeft een door de ondernemer in te stellen geldigheidsduur, die echter door de boordcomputer moet worden beëindigd bij verandering van de bedrijfsvergrendeling.

F

In artikel 14 wordt, onder vernummering van het derde lid tot vierde lid, een lid ingevoegd, luidende:

3. De boordcomputer wordt uitsluitend automatisch uitgeschakeld indien:
   a. zij zich bevindt in het werkingsniveau, bedoeld in artikel 4, tweede lid, onder a;
   b. het contact is uitgeschakeld;
   c. er gedurende meer dan twee uur geen activiteit is geweest van de kaartinterface en van het invoerscherm, en
   d. gedurende meer dan twee uur geen toestand rijden of verplaatsen is gedetecteerd.

G

Artikel 17 komt te luiden:

Artikel 17

1. De boordcomputer:
   a. detecteert het inbrengen en uitnemen van boordcomputerkaarten en de aanwezigheid van een boordcomputerkaart in de kaartinterface;
   b. negeert ingebrachte ongeldige boordcomputerkaarten;
   c. leest bij het inbrengen van een boordcomputerkaart binnen vijf seconden de noodzakelijke gegevens af om het kaarttype, de kaarthouder en de geldigheid van de kaart vast te stellen en registreert deze gegevens onmiddellijk;
   d. leest van de chauffeurskaart binnen vijf seconden de noodzakelijke gegevens af om de eerder gebruikte auto, de datum en het tijdstip van het einde van de laatste kaartsessie en de op dat moment geselecteerde activiteit te identificeren en om te controleren of de laatste kaartsessie correct is afgesloten en registreert deze gegevens onmiddellijk;
   e. authenticeert de houder van de boordcomputerkaart direct bij het inbrengen van de boordcomputerkaart op basis van een persoonlijk identificatie nummer;
   f. geeft selectieve toegangsrechten tot gegevens en functies op basis van het type boordcomputerkaart dat wordt ingevoerd, zoals beschreven in bijlage 1;
   g. blokkeert een kaartsessie als bedoeld in artikel 6.2 van bijlage 1 indien een boordcomputerkaart wordt uitgenomen zonder dat door de gebruiker is aangegeven dat de sessie beëindigd dient te worden;
   h. werkt op het moment van optreden de gegevens die op een geldige chauffeurskaart zijn opgeslagen bij met de gegevens, bedoeld in artikel 9, eerste lid;
   i. stelt de bestuurder in staat de op de chauffeurskaart opgeslagen gegevens, bedoeld in artikel 9, eerste lid, over te brengen naar de boordcomputer conform artikel 8 van bijlage 2;
   j. selecteert, leest en schrijft gegevens op de chauffeurskaart op de wijze zoals gespecificeerd in de hoofdstukken 5 en 6 en de paragrafen 8.9 tot en met 8.16 en 8.19 tot en met 8.21 van bijlage 4;
   k. onderhoudt kaartsessies met chauffeurskaarten op de wijze zoals gespecificeerd in hoofdstuk 7 van bijlage 4;
   l. laat een chauffeurs- of inspectiekaart elektronische handtekeningen genereren op de wijze zoals gespecificeerd in paragraaf 8.5 van bijlage 4;
   m. laat een boordcomputerkaart authenticiteit handtekeningen genereren op de wijze zoals gespecificeerd in paragraaf 8.7 van bijlage 4;

n. laat een boordcomputerkaart zich aan de boordcomputer authenticiteren op de wijze zoals gespecificeerd in paragraaf 8.8 van bijlage 4;
o. controleert op de chauffeurskaart geregistreerde gegevens en verwijdert gecorrumpeerde delen daarvan op de wijze zoals gespecificeerd in paragrafen 8.17 en 8.18 van bijlage 4;
p. onderhoudt het op de chauffeurskaart aanwezige logboek van de door de bestuurder uitgevoerde gegevensleveringen van chauffeurskaartdata (zoals gedefinieerd in artikel 8 van bijlage 2) op de wijze zoals gespecificeerd in de paragrafen 8.22 en 8.23 van bijlage 4;
q. functioneert op correcte wijze met de systeemkaart;
r. gaat tijdens de inschakeling na of het serienummer, bedoeld in artikel 22, tweede lid, onderdeel b, overeenkomt met het serienummer van de boordcomputer, zoals vastgelegd op de chip van de systeemkaart;
s. koppelt zich, onder verantwoordelijkheid van de fabrikant en in diens productiefaciliteit, aan een vervangende systeemkaart op de wijze zoals gespecificeerd in hoofdstuk 3, in het bijzonder overeenkomstig het in paragraaf 3.1.2 gestelde, en overeenkomstig paragraaf 8.2 van bijlage 4;
t. communiceert met zijn systeemkaart op de wijze zoals gespecificeerd in hoofdstuk 4 van bijlage 4;
u. laat zijn systeemkaart elektronische handtekeningen genereren op de wijze zoals gespecificeerd in paragraaf 8.6 van bijlage 4;
v. koppelt zich, onder verantwoordelijkheid van de fabrikant en in diens productiefaciliteit, aan een eerste systeemkaart op de wijze zoals gespecificeerd in hoofdstuk 3, in het bijzonder overeenkomstig het in paragraaf 3.1.1 gestelde, en overeenkomstig paragraaf 8.2 van bijlage 4.

2. Voor het vaststellen van de geldigheid van de boordcomputerkaart, als bedoeld in het eerste lid, onder c, verifieert de boordcomputer dat het boordcomputerkaartcertificaat is uitgegeven door een certificatieautoriteit die daarvoor door de minister is geautoriseerd en valideert de boordcomputer daarbij de geldigheid van het volledige certificeringspad tot en met het relevante stamcertificaat van de Staat der Nederlanden.

3. Indien zich een fout voordoet bij het lezen of het schrijven van gegevens naar de boordcomputerkaart, voert de boordcomputer dezelfde leesopdracht onderscheidenlijk schrijfopdracht maximaal drie keer uit.

4. Nadat een kaartsessie is gestart werkt de boordcomputer de gegevens die op een geldige chauffeurskaart zijn opgeslagen bij met de volgende gegevens:
a. het kenteken van de auto, en
b. het nummer van de ondernemerskaart van de vervoerder zoals vastgelegd in de ingeschakelde bedrijfsvergrendeling.

H

Artikel 18 komt te luiden:

Artikel 18

1. Voordat een kaart wordt uitgenomen zorgt de boordcomputer ervoor dat de kaartsessie volledig en succesvol wordt beëindigd.

2. Het beëindigen van de kaartsessie vereist de aanwezigheid van de boordcomputerkaart in de kaartlezer en is alleen mogelijk indien de auto niet rijdt.

3. Na het beëindigen van een kaartsessie schakelt de boordcomputer automatisch over naar de operationele modus, werkingsniveau basis.

4. De handelingen, bedoeld in het eerste en derde lid, nemen maximaal vijf seconden in beslag.

I

Artikel 20 wordt als volgt gewijzigd:

1. Het tweede lid komt te luiden:

2. Het geheugen houdt bij normaal gebruik alle geregistreerde gegevens ten minste 26 weken vast, met uitzondering van de gegevens, bedoeld in de artikelen 22, tweede en vijfde lid, en 25, zesde lid.

2. Het derde lid vervalt.

3. Het vierde tot en met zesde lid worden vernummerd tot onderscheidenlijk derde tot en met vijfde lid.

J

In artikel 21, tweede lid, wordt ‘gegevens’ vervangen door: actuele waarden van de gegevens.

K

Artikel 22 wordt als volgt gewijzigd:

1. Het eerste lid komt te luiden:

1. In niet-geactiveerde toestand registreert de boordcomputer, uitgezonderd de gegevens, bedoeld in het tweede lid, geen gegevens en kan de boordcomputer uitsluitend de functies voor activering danwel deactivering uitvoeren.

2. Na het zesde lid wordt een lid toegevoegd, luidende:

7. Na activering is de boordcomputer volledig operationeel en kan deze, uitgezonderd activering zelf, alle functies uitvoeren.

L

Aan artikel 23 wordt een lid toegevoegd, luidende:

5. De boordcomputer geraakt na deactivering in inactieve toestand en kan van daaruit uitsluitend de activeringsmodus en de keuringsmodus aannemen.

M

In artikel 27, zevende lid, wordt ‘artikel 1’ vervangen door: artikel 12.

N

In artikel 28, vijfde lid, wordt ‘artikel 26, tweede lid, onderdeel j,’ vervangen door: artikel 26, tweede lid, onderdeel j of k,.

O

Artikel 29 wordt als volgt gewijzigd:

1. Het vierde lid, tweede volzin, komt te luiden: Behoudens het vijfde lid blijft de waarschuwing zichtbaar zo lang de fout of gebeurtenis voortduurt met een maximum van dertig seconden na het optreden daarvan.

2. Er wordt een lid toegevoegd, luidende:

5. De waarschuwing, bedoeld in het vierde lid, blijft zichtbaar totdat de gebruiker handmatig bevestigt de waarschuwing te hebben opgemerkt:
   a. ingeval van een storing;
   b. na de tweede, vierde, zesde en achtste onderbreking van ten minste vijf seconden in de stroomvoorziening van de boordcomputer;
   c. na het verstrijken van het zesd^{e}, twaalfd^{e} en achttiend^{e} uur na detectie van een fout in de bewegingsensor of de positiebepalingsensor; en
   d. na de vijfentwintigste, vijftigste en vijfenzeventigste detectie binnen een kalenderdag van een fout in de bewegingsensor of de positiebepalingsensor.

P

Artikel 30, eerste tot en met derde lid, komt te luiden:

1. De boordcomputer voldoet aan de eisen die zijn neergelegd in NEN-ISO 10605 Severity level III.

Met ESD contact ontladingen met 7 kV, ESD lucht ontladingen met 14 kV en Functional Status Classification A.

2. De boordcomputer voldoet aan de eisen die zijn neergelegd in NEN-EN-IEC 60068-2-1 en NEN-EN-IEC 60068-2-2 en functioneert naar behoren binnen het temperatuurbereik van -20 °C tot +70 °C waarbij:
   a. Conformiteit aan IEC 60068-2-1 wordt aangetoond volgens testtype Ad gedurende 16 uur, en
   b. Conformiteit aan IEC 60068-2-2 wordt aangetoond volgens testtype Bd gedurende 16 uur.

3. De boordcomputer voldoet aan de eisen die zijn neergelegd in NEN-EN-IEC 60068-2-30 en functioneert naar behoren binnen het vochtigheidsbereik van 10% tot 90% relatieve vochtigheid, aangetoond volgens testtype Db gedurende 24 uur met 6 cycli.

Q

In artikel 31 worden, onder vernummering van het vierde en vijfde lid tot zesde en zevende lid, twee leden ingevoegd, luidende:

4. De boordcomputer vereist activerings- en keuringsmodus voor het implementeren van programmatuurrevisies die op aangeven van de fabrikant door de Dienst Wegverkeer zijn aangemerkt als revisies die werkzaamheden vereisen als bedoeld in artikel 13, onder b van de Regeling erkenning werkplaatsen boordcomputer taxi.

5. Implementeren van programmatuurrevisies als bedoeld in het vierde lid vindt uitsluitend in een erkende werkplaats plaats.

R

Na artikel 31 wordt in § 2.8 een artikel ingevoegd, luidende:

Artikel 31a

De fabrikant voorziet erin dat de pin-code van de boordcomputerkaart gedeblokkeerd en gewijzigd kan worden op de wijze zoals gespecificeerd in de paragrafen 8.1, 8.3 en 8.4 van bijlage 4.

S

Artikel 35 komt te luiden:

Artikel 35

1. Artikel 3.16, eerste lid, van de Regeling voertuigen is van overeenkomstige toepassing op wijzigingen ten aanzien van de boordcomputer.

2. In de bij de programmatuur behorende programmatuurgegevens neemt de fabrikant ten minste de volgende gegevens op:
   a. een programmatuurversienummer waarmee de combinatie van programmatuur en bijbehorende progammatuurgegevens uniek identificeerbaar is, en
   b. de certificaten of publieke sleutels van alle certificatieautoriteiten waarmee de authenticiteit en geldigheid van de certificaten van boordcomputerkaarten en systeemkaarten kan worden geverifieerd.

3. In de bij een programmatuurrevisie behorende programmatuurgegevens neemt de fabrikant ten minste de volgende gegevens op:
   a. een programmatuurversienummer waarmee de combinatie van programmatuurrevisie en bijbehorende progammatuurgegevens uniek identificeerbaar is,
   b. eventuele aanvullende of vervangende certificaten of publieke sleutels als bedoeld in het tweede lid onder b, en
   c. een attribuut dat aanduidt of implementeren van de betreffende programmatuurrevisie al dan niet gevolgd moet worden door werkzaamheden als bedoeld in artikel 13, onder b, van de Regeling erkenning werkplaatsen boordcomputer taxi.

4. De fabrikant distribueert de programmatuurrevisie inclusief de bijbehorende programmatuurgegevens niet eerder dan na een positieve beoordeling door de Dienst Wegverkeer.

5. De boordcomputer vervangt de programmatuur met een programmatuurrevisie uitsluitend nadat de authenticiteit van de programmatuurrevisie is geverifieerd en uitsluitend in een van de volgende twee situaties:
   a. indien de boordcomputer zich in de operationele modus, werkingsniveau basis, bevindt en het attribuut, bedoeld in het derde lid, onder c, aanduidt dat het implementeren van de programmatuurrevisie niet gevolgd hoeft te worden door werkzaamheden als bedoeld in artikel 13, onder b, van de Regeling erkenning werkplaatsen boordcomputer taxi;
   b. indien de boordcomputer zich in de activerings- en keuringsmodus bevindt.

6. Na vervanging van de programmatuur met een programmatuurrevisie neemt de boordcomputer het programmatuurversienummer van de programmatuurrevisie over als het programmatuurversienummer van de programmatuur.

T

De bijlagen 1 en 2 bij de Regeling specificaties en typegoedkeuring boordcomputer taxi worden vervangen door de bij deze regeling gevoegde bijlagen 1 en 2.

U

Bijlage 4 wordt vastgesteld overeenkomstig de als bijlage 4 bij deze regeling gevoegde bijlage.

ARTIKEL II

De Regeling erkenning werkplaatsen boordcomputer taxi wordt als volgt gewijzigd:

A

In artikel 6, eerste lid, vervalt ‘voor een werkplaats’.

B

In artikel 8, eerste lid, wordt ‘artikel 3, derde lid’ vervangen door: artikel 3, eerste en derde lid.

C

In artikel 14, eerste lid, wordt na ‘deactivering van de boordcomputer’ ingevoegd: , als bedoeld in de Regeling specificaties en typegoedkeuring boordcomputer taxi.

D

Artikel 17 wordt als volgt gewijzigd:

1. In het eerste lid, aanhef, wordt ‘Nadat er werkzaamheden aan de boordcomputer zijn verricht,’ vervangen door: Nadat er werkzaamheden aan de boordcomputer zijn verricht ingeval van toepassing van artikel 31, vijfde lid, van de Regeling specificaties en typegoedkeuring boordcomputer taxi,.

2. In het derde lid wordt na ‘aanwijzingen’ ingevoegd: met betrekking tot de levering van de in het eerste en tweede lid bedoelde gegevens.

E

In artikel 19, vijfde lid, wordt na ‘In de gegevens, bedoeld in het eerste en tweede lid,’ ingevoegd: en in de documenten, bedoeld in het derde lid,.

ARTIKEL III

1. Deze regeling treedt in werking met ingang van 1 april 2015.

2. De boordcomputer, bedoeld in de Regeling specificaties en typegoedkeuring boordcomputer taxi, die niet voldoet aan genoemde regeling, zoals die luidt met ingang van het tijdstip van inwerkingtreding van deze regeling, wordt tot 1 juli 2016 aangemerkt als functionerend op correcte wijze als bedoeld in artikel 79, eerste lid, van het Besluit personenvervoer 2000, indien deze boordcomputer voldoet aan genoemde regeling, zoals die luidde tot bedoeld tijdstip van inwerkingtreding.

3. Een typegoedkeuring voor een boordcomputer die is afgegeven op basis van de eisen die golden

voor inwerkingtreding van deze regeling kan worden aangepast tot 1 juli 2016, waarbij de eisen van toepassing zijn zoals die luidden voor de inwerkingtreding van deze regeling.

Deze regeling zal met de bijlagen en de toelichting in de Staatscourant worden geplaatst.

De Staatssecretaris van Infrastructuur en Milieu,
W.J. Mansveld

BIJLAGE 1 BIJ DE REGELING BOORDCOMPUTER TAXI

Beveiligingsprofiel Boordcomputer Taxi (PP-BCT)

Versie 1.8

Datum 6 februari 205
Status Defnitief

Inhoud

Artikel 1 Introductie

Deze bijlage is een beveiligingsprofiel (Protection Profile) voor de voertuigcomponenten van de boordcomputer in overeenstemming met de Common Criteria versie 3.1. Het beveiligingsprofiel geeft een beschrijving van het door de boordcomputer te implementeren beleid, de te realiseren beveiligingsdoelstellingen, en de te behalen beveiligingseisen, alsmede het vereiste garantieniveau voor de boordcomputer, zoals afgeleid is bij een eerdere afhankelijkheids- en kwetsbaarheidsanalyse.

Dit beveiligingsprofiel voor de boordcomputer is opgesteld voor de Inspectie Leefomgeving en Transport van het Ministerie van Infrastructuur en Milieu.

Artikel 2 Afkortingen, acroniemen, definities en referenties

Artikel 2.1 PP Referentie

Dit document is het ‘Beveiligingsprofiel Boordcomputer Taxi’ (PP-BCT) Versie 1.8, 6 februari 2015.

Artikel 2.2 Claim voor voldoen aan de Common Criteria

Dit beveiligingsprofiel voldoet aan Common Criteria versie 3.1 Revisie 4. Hoewel de 'International English' versie is gebruikt voor het ontwikkelen van dit beveiligingsprofiel, is (met toestemming van het certificeringsschema) dit profiel in het Nederlands.

Dit beveiligingsprofiel:
- is CC Deel 2 conform;
- is CC Deel 3 conform;
- is EAL3 conform;
- claimt niet te voldoen aan andere beveiligingsprofielen;
- vereist strikte conformering van andere beveiligingsprofielen (PPs) of beveiligingsspecificaties (STs) die aan dit beveiligingsprofiel willen voldoen.

Artikel 2.3 Notities

Dit document volgt de naamgeving en notaties voor beveiligingsprofielen volgens de Common Criteria standaard. Er zijn unieke labels toegewezen aan entiteiten zodat deze gemakkelijk terug te vinden zijn. De labels beginnen met één van de onderstaande karakters:

A	Assumption (aanname)
O	Object (object)
OE	Security objective for the Environment (omgevingsdoelstellingen)
OT	Security objective for the TOE (beveiligingsdoelstelling)
P	Organisational Security Policy (beleid)
S	Subject (persoon, middel of een proces)

Artikel 2.4 Afkortingen en acroniemen

CA	Certificatieautoriteit
CC	Common Criteria (referentienorm)
CEN	European Committee for Standardization
CWA	CENWorkshop Agreements
EAL	Evaluation Assurance Level (garantieniveau)
EH	Elektronische handtekening
EPROM	Erasable Programmable Read Only Memory
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
GNSS	Global Navigation Satellite System
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISO	International Organisation for Standardisation
PIN	Personal identification number (PIN-code)
PP	Protection Profile (Beveiligingsprofiel)
PKI	Public Key Infrastructure (publieke sleutel methodiek)
PUB	Public
ROM	Read Only Memory (ROM-geheugen)
RFC	Request for Comments
SFP	Security Function Policy
SFR	Security Functional Requirement (Beveiligingseis)
SHA	Secure Hash Algorithm
ST	Security Target (Beveiligingsspecificatie)
TOE	Target of Evaluation (onderwerp van de evaluatie)
TS	Technical Standard
TSF	TOE Security Functionality
TSFI	TSF Interface

Artikel 2.5 Referentienormen

De TOE wordt getoetst conform het normenkader van Common Criteria for Information Technology Security Evaluation, versie 3.1, revisie 3, July 2009.

De TOE ondersteunt de volgende standaarden wanneer cryptografische bewerkingen dienen te worden uitgevoerd:
- Het SHA cryptografische algoritme voor hash functies zoals gedefinieerd in de ISO/IEC 10118-3, FIPS PUB 180-2 en ETSI TS 102 176-1 standaarden;
- ETSI TS 101 733 Electronic Signature Formats en de FIPS PUB 186-2 standaarden voor elektronische handtekeningen;

Artikel 3 Overzicht van de TOE

Artikel 3.1 Beschrijving van de TOE

De TOE is een controleapparaat bedoeld voor installatie in auto's gebruikt voor taxivervoer. Het doel is om handhavingprocessen te helpen uitvoeren door de elektronische registratie van de ritadministratie en de arbeids-, rij- en rusttijden en het op aanvraag ter beschikking stellen van deze informatie aan bevoegde personen ter controle.
De TOE kent vier werkingsmodi, te weten: operationele modus, controle modus, activering/keuringsmodus en bedrijfsmodus. De operationele modus kent drie werkingsniveaus: basis, arbeidstijd en taxivervoer. Wanneer taxivervoer wordt aangeboden of arbeidstijd plaatsheeft, selecteert de bestuurder handmatig het corresponderende werkingsniveau. In de operationele modus, werkingsniveau arbeidstijd of taxivervoer, worden gegevens geregistreerd over de uitgevoerde taxiritten en de arbeids-, rij-, en rusttijden van de bestuurder. De aanvang en het beëindigen van een rit wordt door een actieve bedieningshandeling van de bestuurder bij de TOE kenbaar gemaakt. Hierbij dient de beladingtoestand (beladen/onbeladen) te worden aangegeven.

Daarnaast draagt de TOE in alle modi zorg voor het beschikbaar stellen van de basisgegevens tijd en afgelegde afstand, en de positie van het voertuig. In het werkingsniveau basis wordt ook de registratie van gebeurtenissen gevoerd. In de operationele modus is het werkingsniveau basis een apart werkingsniveau. In de overige modi integreert de TOE de basis functionaliteit met de overige functionaliteit van de betreffende modus.

De TOE bestaat ten minste uit een verwerkingseenheid, een geheugen, een tijdklok, een ISO 7816 kaartinterface, een ISO 7810 ID-000 kaartinterface ten behoeve van de systeemkaart, een positiebepalingssensor of een interface voor de positiebepalingssensor, een verplaatsingsopnemer, een interface voor de bewegingsopnemer, een gegevensoverbrengingsinterface, een interface voor de taxameter, een leesvenster en voorzieningen voor de invoer van gebruikersgegevens.
De TOE kan door middel van additionele verbindingen aan andere inrichtingen worden gekoppeld, of daarmee geïntegreerd worden.

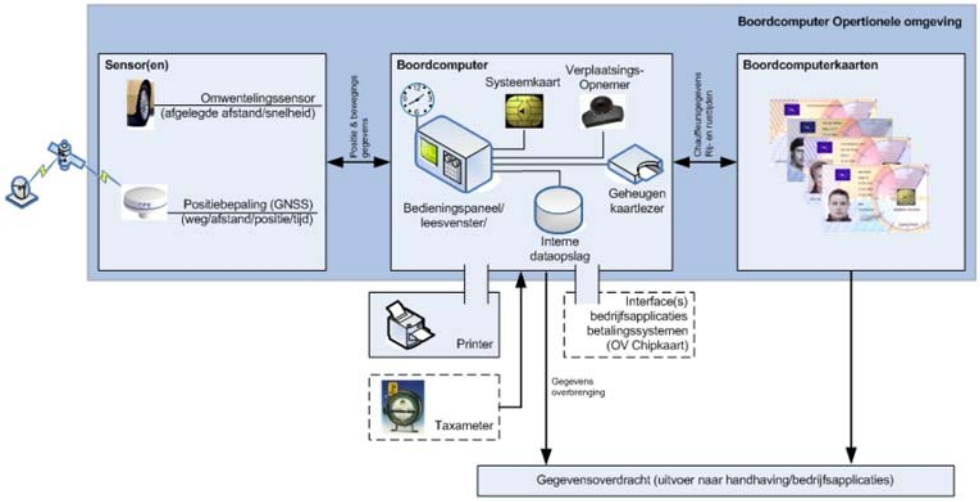
Toegang tot de TOE wordt verleend door middel van een boordcomputerkaart met PIN-code en voorzien van een (authenticatie)certificaat. Er worden vier gebruikersrollen voorzien, te weten bestuurder, toezichthouder, werkplaats en vervoerder. De omschakeling tussen werkingsmodi gebeurt door het plaatsen van de correcte boordcomputerkaart in de TOE. Er worden vier verschillende kaarten onderscheiden, te weten: chauffeurskaart, inspectiekaart, keuringskaart en ondernemerskaart. Boordcomputerkaarten maken geen onderdeel uit van de TOE.

Bij aanvang van de dienst dient een chauffeurskaart in de TOE te zijn geplaatst. De bestuurder meldt zich aan met de chauffeurskaart en een persoonlijk identificatie code (PIN-code). De TOE registreert de persoonlijke arbeids-, rij- en rusttijden van de bestuurder en slaat deze op in het interne geheugen van de TOE en op de chauffeurskaart.
In voorkomende gevallen heeft een chauffeur geen kaart en dan dient hij zijn burgerservicenummer in te voeren. Dit burgerservicenummer dient alleen voor identificatie, en wordt door de TOE verder niet gecontroleerd.

De boordcomputerkaarten voor de bestuurder zijn voorzien van een certificaat voor het elektronisch identificeren van de persoon en het ondertekenen van geregistreerde gegevens.

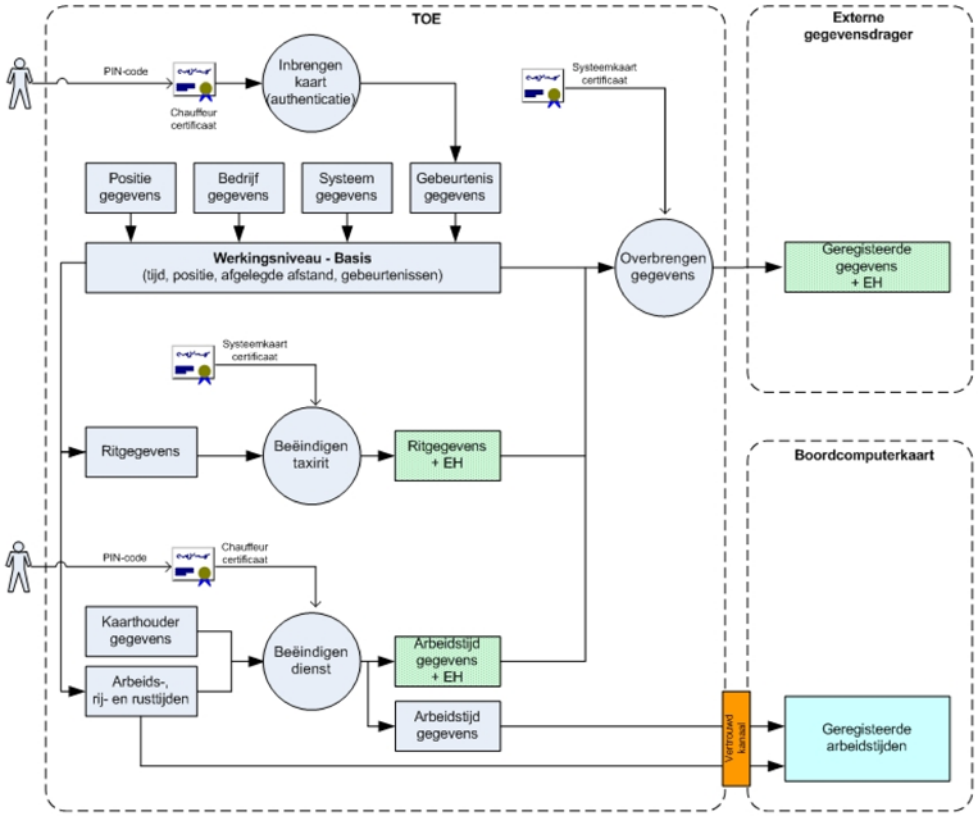
De TOE gebruikt een systeemkaart welke is voorzien van certificaten voor identificatie van de TOE en het plaatsen van elektronische handtekeningen. Het certificaat ten behoeve van de TOE wordt in de productiefase in de vorm van de systeemkaart geïmplementeerd in de TOE. Deze certificaten worden uitgegeven onder verantwoordelijkheid van de Minister van Infrastructuur en Milieu. Systeemkaarten zijn geen onderdeel van de TOE.

De TOE voert gegevens uit naar een leesvenster en kan gegevens ter beschikking stellen ten behoeve van een externe printer en externe inrichtingen.
De operationele omgeving van de TOE geïnstalleerd in de auto is weergegeven in onderstaande figuur.



Figuur 1

De systeemkaart plaatst een elektronische handtekening (EH) per uitgevoerde rit over alle ritgegevens terstond nadat de bestuurder heeft aangegeven dat de rit teneinde is.
De chauffeurskaart plaatst een elektronische handtekening bij het einde van de dienst van de bestuurder over de arbeids-, rij- en rusttijden van de bestuurder gedurende de dienst. Hiervoor wordt het persoonsgebonden certificaat van de chauffeurkaart gebruikt waarbij de bestuurder vooraf zijn goedkeuring verleent door het ingeven van de PIN-code van de chauffeurskaart.
De systeemkaart plaatst een elektronische handtekening over de geregistreerde gegevens wanneer deze worden opgeslagen en wanneer deze worden uitgevoerd naar een externe gegevensdrager.
De koppeling van bestuurder aan de geregistreerde gegevens en de waarborging van de integriteit en authenticiteit van de gegevens wordt in onderstaande figuur geïllustreerd:



Figuur 2

Artikel 3.2 Levenscyclus van de TOE

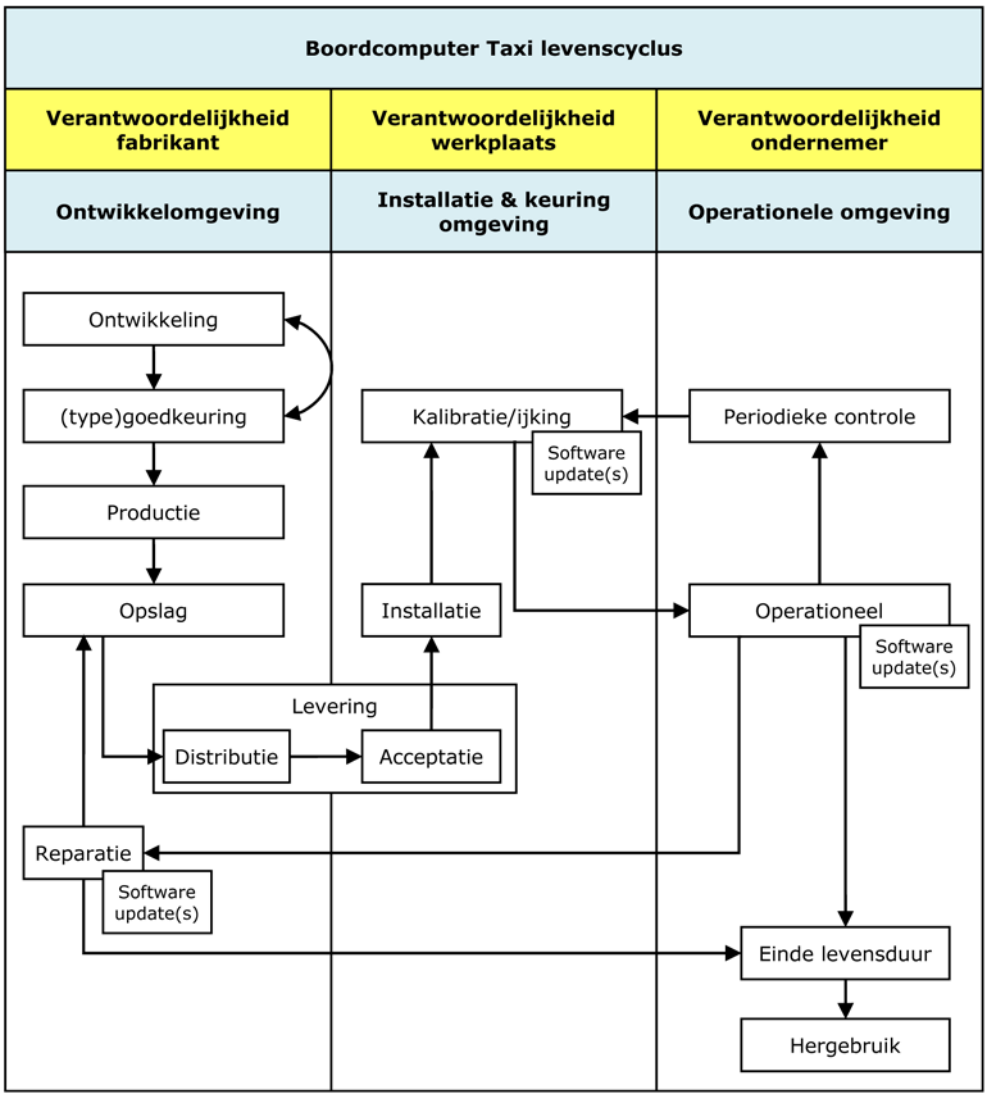
De typische levenscyclus van een TOE wordt geïllustreerd door onderstaande figuur. Het verkrijgen

van een typegoedkeuring is een verantwoordelijkheid van de fabrikant. Eventuele reparaties worden uitgevoerd door, of onder verantwoordelijkheid van, de fabrikant. Installatie van eventuele nieuwere versies van programmatuur mogen door erkende werkplaatsen met een programmatuurrevisie worden uitgevoerd na een succesvolle authenticatie met een keuringskaart.

Indien naar het oordeel van de Dienst Wegverkeer bij/na het implementeren van een bepaalde programmatuurrevisie geen kalibratie van de boordcomputer benodigd is, dan mag die programmatuurrevisie ook buiten een erkende werkplaats door eenieder op de boordcomputer geïmplementeerd worden indien deze zich in operationele modus met werkingsniveau basis bevindt en er geen gebruikerssessie actief is.

Teneinde de blijvend correcte werking van de boordcomputer te kunnen waarborgen, moet de boordcomputer ten aanzien van het implementeren van programmatuurrevisies de volgende acties uitvoeren:

- De boordcomputer moet verhinderen dat een programmatuurrevisie die wel gevolgd moet worden door kalibratie kan worden geïnstalleerd zonder een voorafgaande succesvolle authenticatie met een keuringskaart.
- De boordcomputer moet van elke aangeboden programmatuurrevisie en daarin opgenomen programmatuur vaststellen dat deze integer en authentiek is, alvorens deze te installeren.
- De boordcomputer moet van elke aangeboden programmatuurrevisie middels een door de Dienst Wegverkeer goedgekeurde op versienummers gebaseerde controle vaststellen dat de programmatuurrevisie geschikt is voor het vervangen van de op de boordcomputer operationele programmatuur, alvorens de programmatuurrevisie te installeren.
- De boordcomputer moet elke succesvol geïnstalleerde programmatuurrevisie direct na installatie in zijn geheugen registreren onder vermelding van de na installatie geldende basisgegevens, gebeurtenisgegevens en systeemgegevens.



Figuur 3

Artikel 3.3 Entiteiten

Voor de TOE zijn de volgende types van entiteiten (subjecten en objecten) relevant:

Artikel 3.3.1 Subjecten – middelen

S.BEWEGINGSOPNEMER
Het instrument, of een deel ervan, gekoppeld aan de TOE dat een signaal in de vorm van een impuls afgeeft over de beweging van de auto op basis waarvan de TOE de afgelegde afstand van de auto kan bepalen.
S.POSITIEBEPALINGSSENSOR
Het instrument, of een deel ervan, gekoppeld aan de TOE dat een signaal afgeeft aan de TOE over de locatie van de auto op basis van verkregen informatie van een satelliet positiebepalingsysteem.
S.BOORDCOMPUTERKAART
De geheugenkaart met chip voor gebruik in de TOE waarmee de TOE de identiteit van de kaarthouder kan vaststellen en waarop gegevens kunnen worden opgeslagen.
S.SYSTEEMKAART
De geheugenkaart met chip die de TOE in staat stelt een elektronische handtekening te plaatsen.
S.PRINTER
Een externe inrichting waaraan gegevens beschikbaar kunnen worden gesteld voor het afdrukken op papier.

S.TAXAMETER
De geijkte externe inrichting voor het bepalen van de ritprijs op basis van een tarievenstructuur.
S.HANDHAVINGSMIDDELEN
Fysiek aan de TOE gekoppelde hulpmiddelen, waaronder externe gegevensdragers en ook te beschouwen als externe gegevensdragers, t.b.v. toezichthouders voor het uitlezen en eventueel verwerken van gegevens.
S.KALIBRATIEMIDDELEN
Fysiek aan de TOE gekoppelde hulpmiddelen, waaronder externe gegevensdragers en ook te beschouwen als externe gegevensdragers, t.b.v. een erkende werkplaats voor het uitlezen van gegevens en/of het ijken, kalibreren, activeren en deactiveren van de TOE.
S.BEDRIJFSMIDDELEN
Fysiek of logisch aan de TOE gekoppelde hulpmiddelen, waaronder externe gegevensdragers en ook te beschouwen als externe gegevensdragers, t.b.v. de vervoerder voor de overdracht van gegevens van en naar de bedrijfsadministratie.
S.UPDATEMIDDELEN
Fysiek of logisch aan de TOE gekoppelde hulpmiddelen, waaronder externe gegevensdragers en ook te beschouwen als externe gegevensdragers, voor de overdracht van programmatuurrevisies naar de TOE.

Artikel 3.3.2 Subjecten – gebruikers

S.CHAUFFEURSKAART
Een aan de bestuurder afgegeven boordcomputerkaart waarmee de boordcomputer de identiteit van de desbetreffende bestuurder kan vaststellen, een elektronische handtekening kan plaatsen, en waarmee de operationele modus van de TOE kan worden geactiveerd.
S.INSPECTIEKAART
Een aan de met het toezicht op de naleving belaste persoon afgegeven boordcomputerkaart die de desbetreffende persoon identificeert en waarmee de controlemodus van de boordcomputer kan worden geactiveerd.
S.KEURINGSKAART
Een aan een erkende werkplaats afgegeven boordcomputerkaart die de desbetreffende werkplaats identificeert en waarmee de activerings- en keuringsmodus van de boordcomputer kan worden geactiveerd.
S.ONDERNEMERSKAART
Een aan een vervoerder afgegeven boordcomputerkaart die de desbetreffende vervoerder identificeert en waarmee de bedrijfsmodus van de boordcomputer kan worden geactiveerd.

Artikel 3.3.3 Objecten

O.BASISGEGEVENS
De tijd, afgelegde afstand en gegevens betreffende verplaatsing zoals bijgehouden door de TOE.
O.ARBEIDSTIJDGEGEVENS
De arbeids-, rij- en rusttijden gegevens van de bestuurder zijnde de rijtijd, pauze en andere werkzaamheden dan rijden geregistreerd door de TOE.
O.RITGEGEVENS
De gegevens per individuele rit bestaande uit ten minste de begin- en eindlocatie, de begin- en einddatum en tijd, afgelegde afstand, de ritprijs, de beladingstoestand en identiteit van de bestuurder geregistreerd door de TOE.
O.BEDRIJFSGEGEVENS
Gegevens over de vervoerder, waaronder autorisaties voor het gedurende een bepaalde periode onafhankelijk van een kaartsessie uitlezen van de TOE, zoals zijn vastgelegd op de TOE.
O.KAARTHOUDERGEGEVENS
Gegevens opgeslagen op de boordcomputerkaart ingebracht in de TOE.
O.POSITIEGEGEVENS
Gegevens betreffende de locatie van de auto die door de S.POSITIEBEPALINGSSENSOR aan de TOE worden aangeleverd.
O.BEWEGINGSGEGEVENS
Gegevens betreffende snelheid en afgelegde afstand die door S.BEWEGINGSOPNEMER of S.POSITIEBEPALINGSSENSOR aan de TOE worden aangeleverd.
O.GEBEURTENISGEGEVENS
Gegevens geregistreerd door de TOE met betrekking tot routinematige en uitzonderlijke gebeurtenissen op basis waarvan analyses mogelijk zijn en de verantwoordelijke gebruiker of proces kan worden bepaald.
O.SYSTEEMGEGEVENS
Specifieke gegevens ter ondersteuning of noodzakelijk voor het functioneren van de TOE of voor identificatie en instellingen van de TOE functies, bestaande uit O.VASTE_SYSTEEMGEGEVENS,

O.VARIABELE_SYSTEEMGEGEVENS en O.PROGRAMMATUURGEGEVENS.

O.VASTE_SYSTEEMGEGEVENS
Vaste gegevens van de TOE, zoals de naam van diens fabrikant, het serienummer en het bouwjaar.

O.VARIABELE_SYSTEEMGEGEVENS
Wijzigbare gegevens van de TOE, waaronder het kenteken van de auto en O.INSTELLINGSGEGEVENS.

O.INSTELLINGSGEGEVENS
Die subset van O.VARIABELE_SYSTEEMGEGEVENS die aan kalibratie onderhevig is.

O.PROGRAMMATUUR
De combinatie van TOE uitvoerbare code en gegevens zoals de CA certificaathiërarchie(ën) nodig voor het verifiëren van de geldigheid en authenticiteit van certificaten van boordcomputer- en systeemkaarten, alsmede de bij dat geheel behorende O.PROGRAMMATUURGEGEVENS.

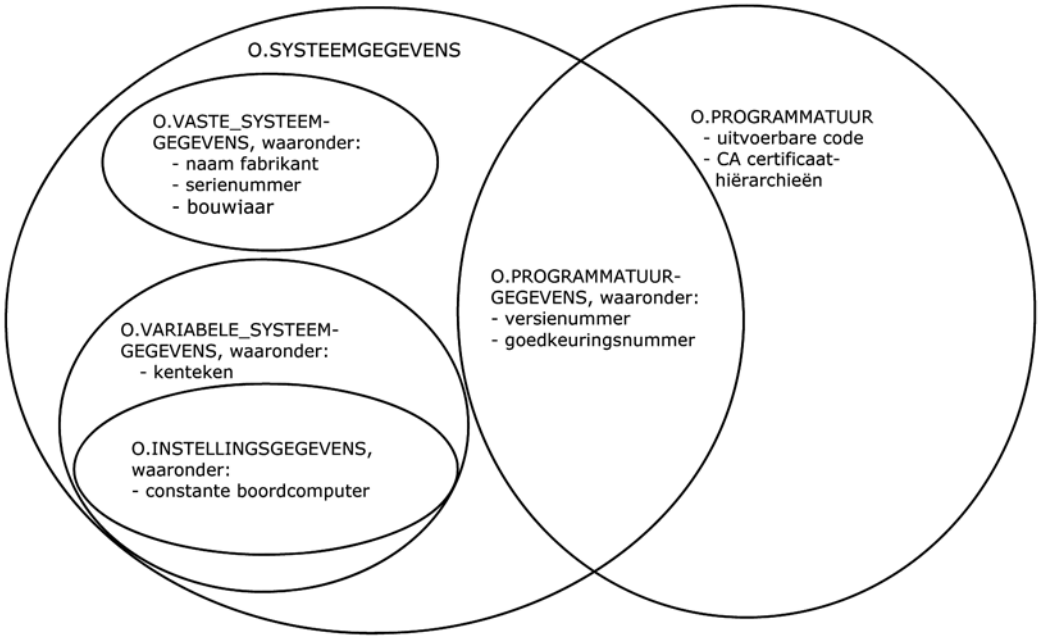
O.PROGRAMMATUURGEGEVENS
Versie-identificerende (vaste) gegevens van O.PROGRAMMATUUR, waaronder een versienummer en een goedkeuringsnummer. De O.PROGRAMMATUURGEGEVENS van de op de TOE operationele O.PROGRAMMATUUR vormen eveneens een subset van O.SYSTEEMGEGEVENS.

O.PROGRAMMATUURREVISIE
De combinatie van een versie van O.PROGRAMMATUUR die is bedoeld om de op de TOE operationele O.PROGRAMMATUUR of delen daarvan te vervangen, een O.KALIBRATIEINDICATIE en een O.VERVANGBARE_VERSIES.

O.KALIBRATIEINDICATIE
Een vast attribuut van een O.PROGRAMMATUURREVISIE dat aanduidt of het vervangen van de op de TOE operationele O.PROGRAMMATUUR met de in de O.PROGRAMMATUURREVISIE opgenomen O.PROGRAMMATUUR wel (positief) of niet (negatief) gevolgd moet worden door kalibratie van O.INSTELLINGSGEGEVENS.

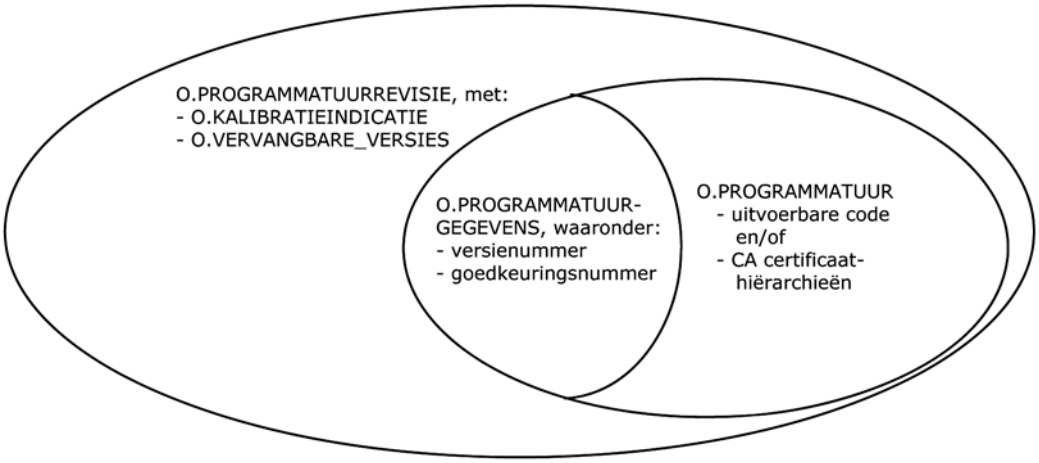
O.VERVANGBARE_VERSIES
Een in een O.PROGRAMMATUURREVISIE opgenomen criterium (zoals een lijst of wildcard) waarmee een versienummer kan worden vergeleken om te bepalen of het met dat criterium correspondeert.

Ter verduidelijking is in de onderstaande figuur de samenhang van de op de TOE aanwezige O.SYSTEEMGEGEVENS en de op de TOE operationele O.PROGRAMMATUUR en hun subobjecten / attributen grafisch weergegeven.



Figuur 4

Eveneens ter verduidelijking is in de onderstaande figuur de opbouw van een O.PROGRAMMATUURREVISIE opgenomen.

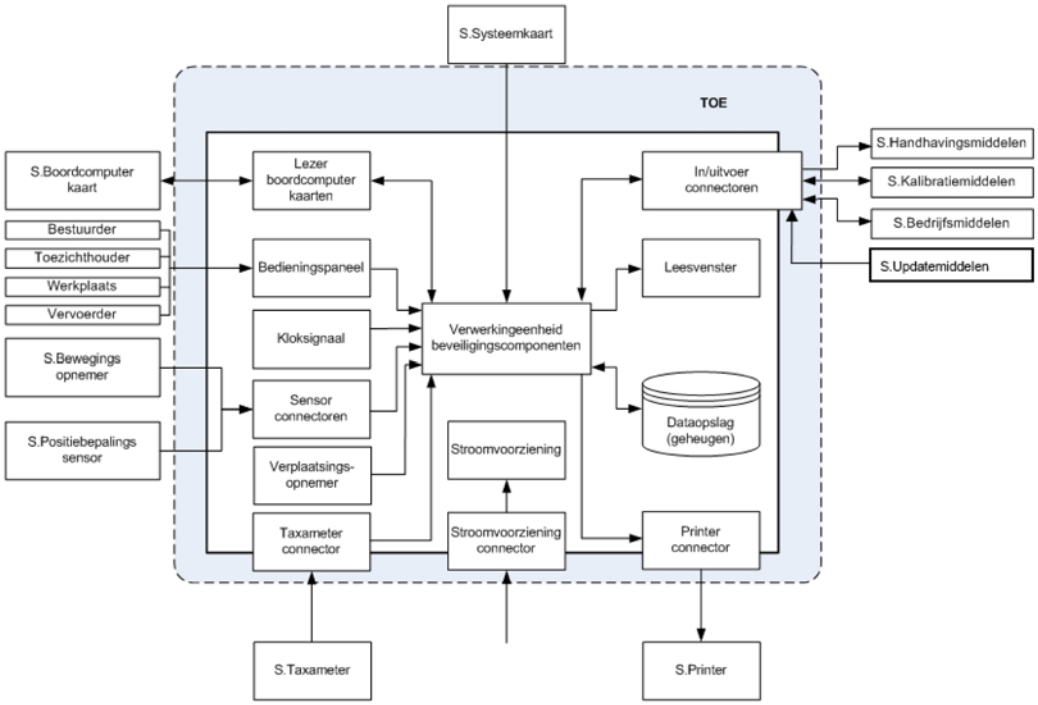


Figuur 5

Artikel 3.4 Begrenzingen van de TOE

De TOE (Target of Evaluation) is de selectie van hardware en software en bijbehorende handleidingen die uiteindelijk wordt geëvalueerd. De TOE moet alle functionaliteit omvatten die nodig is om aan de eisen in dit profiel te voldoen, maar mag daarnaast ook andere zaken bevatten, zoals een routeplanningsapplicatie.

De minimale omvang van de TOE wordt schematisch weergegeven in onderstaande figuur:



Figuur 6

Alle onderdelen die in deze afbeelding binnen de grijze omheining worden weergegeven moeten onderdeel zijn van de TOE. Dus bijvoorbeeld de (voertuig) sensor voor bewegingsgegevens (bewegingsopnemer) en de positiebepalingssensor (GNSS) hoeven geen deel uit te maken van de TOE maar de aansluiting van deze sensoren weer wel

Andere zaken die in deze figuur zijn weergegeven (zoals de taxameter en de printer), mogen onderdeel zijn van de TOE, hoewel dit niet altijd praktisch is. Ook extra software en hardware die niet in deze figuur zijn weergegeven (zoals de bovengenoemde routeplanningsapplicatie) mogen deel uitmaken van de TOE.

Daarnaast is het toegestaan om extra hardware of software binnen de fysieke behuizing van de TOE op te nemen, zonder dat deze hardware of software meteen onderdeel worden van de TOE. Het is echter niet toegestaan om tijdens de evaluatie van de TOE aan te nemen dat deze extra hardware of software vertrouwd of goedaardig is: de evaluatie van de TOE dient ondubbelzinnig aan te tonen dat de TOE nog steeds voldoet aan dit Beschermingsprofiel als deze opgenomen hardware of software niet vertrouwd of goedaardig is.

Artikel 4 Beveiligingsprobleem

Artikel 4.1 Beveiligingsbeleid

P.VASTLEGGEN
De TOE legt de volgende gegevens vast, afhankelijk van de werkingsmodus en het actieve werkingsniveau:
- Operationele modus basis: In ingeschakelde toestand registreert de TOE altijd de positie- en gebeurtenisgegevens. Direct na installatie van een programmatuurrevisie registreert de TOE de na installatie geldende basisgegevens, gebeurtenisgegevens en systeemgegevens. Indien een boordcomputerkaart is ingebracht registreert de TOE de identiteit van de kaarthouder;
- Operationele modus arbeidstijd: Na een handmatige selectie van het werkingsniveau arbeidstijd, registreert de TOE de positie- en gebeurtenisgegevens en de arbeidstijdgegevens. Het werkingsniveau arbeidstijd wordt automatisch geselecteerd door het inbrengen van de chauffeurskaart, en kan zonder chauffeurskaart handmatig geselecteerd worden na het invoeren van een burgerservicenummer. Indien een boordcomputerkaart is ingebracht registreert de TOE de identiteit van de kaarthouder, indien identificatie plaatsvindt met een burgerservicenummer, dan registreert de TOE dit burgerservicenummer;
- Operationele modus taxivervoer: Na een handmatige selectie van het werkingsniveau taxivervoer, registreert de TOE de positie- en gebeurtenisgegevens, de arbeidstijdgegevens en de ritgegevens. Indien een boordcomputerkaart is ingebracht registreert de TOE de identiteit van de kaarthouder, indien identificatie plaatsvindt met een burgerservicenummer, dan registreert de TOE dit burgerservicenummer;
- Controlemodus: De TOE registreert de positie- en gebeurtenisgegevens en de identiteit van de kaarthouder;
- Activering/keuringsmodus: De TOE registreert de positie- en gebeurtenisgegevens en de identiteit van de kaarthouder. Direct na installatie van een programmatuurrevisie registreert de TOE de na installatie geldende basisgegevens, gebeurtenisgegevens en systeemgegevens;
- Bedrijfsmodus: De TOE registreert de positie- en gebeurtenisgegevens en de identiteit van de kaarthouder.

P.BEWAREN_EN_BORGEN
De TOE bewaart de vastgelegde gegevens zodat:
- wijzigingen van de gegevens detecteerbaar zijn;
- de gegevens onweerlegbaar gekoppeld zijn aan de TOE;
- de gegevens onweerlegbaar gekoppeld zijn aan de houder van een boordcomputerkaart.

P.ACTIES
De TOE kan de volgende acties uitvoeren, afhankelijk van de werkingsmodus, het actieve werkingsniveau en de ingebrachte en geauthenticeerde boordcomputerkaart:
- Selecteren van de juiste werkingsmodus;
- Activering, deactivering en onderzoek van de TOE;
- Instellen van de bedrijfsvergrendeling;
- Detecteren en registreren van storingen[1];
- Detecteren en registeren van fouten[2];
- Detecteren en registeren van gebeurtenissen;
- Gegevens tonen op een leesvenster;
- Gegevens overbrengen van en naar een externe gegevensdrager;
- Gegevens overbrengen van de chauffeurskaart naar de TOE;
- Gegevens overbrengen naar een externe inrichting;
- Gegevens beschikbaar stellen t.b.v. een printer;
- Geven van waarschuwingssignalen
- Programmatuurrevisies overbrengen van externe updatemiddelen naar de TOE;
- Programmatuur van de TOE updaten met programmatuur uit een programmatuurrevisie.

[1] Een storing treedt op wanneer een onderbreking in de correcte werking van de boordcomputer door een gebeurtenis of fout een permanent karakter heeft.
[2] Een fout treedt op wanneer de correcte werking van de boordcomputer gedurende korte tijd wordt onderbroken.

P.UITVOEREN_GEGEVENS
De TOE kan de geregistreerde gegevens uitvoeren, afhankelijk van de ingebrachte boordcomputerkaart:
- Geen kaart, geen andere authenticatie:
  - systeemgegevens naar een leesvenster.
- Geen kaart, authenticatie op basis van burgerservicenummer:
  - systeemgegevens naar een leesvenster;
  - ritgegevens van de huidige sessie naar een leesvenster;
  - arbeids-, rij- en rusttijden van de huidige sessie naar een leesvenster;
  - ritgegevens van de huidige sessie naar een uitvoerinterface voor een printer;
  - arbeids-, rij- en rusttijden van de huidige sessie naar een uitvoerinterface voor een printer;
- Chauffeurskaart:
  - systeemgegevens naar een leesvenster;
  - eigen ritgegevens naar een leesvenster;
  - eigen arbeids-, rij- en rusttijden naar een leesvenster;
  - eigen arbeids-, rij- en rusttijden naar de chauffeurskaart;
  - eigen ritgegevens naar een uitvoerinterface voor een printer;
  - eigen arbeids-, rij- en rusttijden naar een uitvoerinterface voor een printer.
- Inspectiekaart: alle gegevens met uitzondering van positiegegevens en beveiligingsgegevens,
  - naar een leesvenster;
  - naar een uitvoerinterface voor een printer;
  - naar een extern handhavingsmiddel.
- Keuringskaart: alle gegevens met uitzondering van positiegegevens en beveiligingsgegevens,
  - naar een leesvenster;
  - naar een uitvoerinterface voor een printer;
  - naar een extern kalibratiemiddel.
- Keuringskaart, na actieve handeling gevolgd door Inspectiekaart: de positiegegevens naar een extern handhavingsmiddel.
- Ondernemerskaart: alle gegevens vastgelegd in de bedrijfsvergrendeling voor de desbetreffende vervoerder met uitzondering van positiegegevens en beveiligingsgegevens,
  - naar een leesvenster;
  - naar een uitvoerinterface voor een printer;
  - naar een extern bedrijfsmiddel.
- Ondernemerskaart: systeemgegevens
  - naar een leesvenster;
  - naar een uitvoerinterface voor een printer;
  - naar een extern bedrijfsmiddel.

De TOE kan
- de systeemgegevens en
- alle gegevens vastgelegd in de bedrijfsvergrendeling voor een bepaalde vervoerder met uitzondering van positiegegevens en beveiligingsgegevens

uitvoeren naar een extern bedrijfsmiddel (op afstand of lokaal) indien
- de TOE voor de betreffende vervoerder vergrendeld is en
- de TOE, als onderdeel van de bedrijfsgegevens, beschikt over een unieke autorisatie voor deze uitvoer die
- een nog niet verstreken geldigheidsperiode voor deze uitvoer vermeldt.

P.INVOEREN_GEGEVENS
De TOE kan gegevens invoeren, afhankelijk van de ingebrachte boordcomputerkaart:
- Keuringskaart:
  - variabele systeemgegevens van het bedieningspaneel;
  - variabele systeemgegevens van een extern kalibratiemiddel.
- Ondernemerskaart:
  - bedrijfsgegevens van het bedieningspaneel;
  - bedrijfsgegevens van een extern bedrijfsmiddel.

De TOE kan, onafhankelijk van het bestaan van een gebruikerssessie:
- Programmatuurrevisies invoeren van een extern updatemiddel;
- Bedrijfsgegevens,
  waaronder unieke autorisaties voor gegevensuitvoer zoals vermeld onder P.UITVOEREN_GEGEVENS,
  invoeren van een extern bedrijfsmiddel (op afstand of lokaal), indien
- de TOE voor de betreffende vervoerder vergrendeld is en
- de bedrijfsgegevens zijn ondertekend door een ondernemerskaart van die vervoerder.

P.VEILIG_UPDATEN
De TOE kan zijn operationele programmatuur updaten met de programmatuur uit een (van een extern updatemiddel afkomstige) programmatuurrevisie indien de TOE heeft vastgesteld dat

- de programmatuurrevisie integer en authentiek is,
- uit het corresponderen van het versienummer van de op de TOE operationele programmatuur met de door de Dienst Wegverkeer goedgekeurde invulling van O.VERVANGBARE_VERSIES blijkt dat de programmatuur uit de programmatuurrevisie geschikt is voor het updaten van de in de TOE operationele programmatuur en
- een van de volgende situaties van toepassing is:
  - op de TOE is een werkplaatssessie actief of
  - op de TOE is geen gebruikerssessie actief en uit de door de Dienst Wegverkeer goedgekeurde invulling van O.KALIBRATIEINDICATIE blijkt dat het updaten niet gevolgd hoeft te worden door kalibratie van de TOE.

P.DEACTIVERING
De TOE kan met behulp van een keuringskaart worden gedeactiveerd. Alle gegevens opgeslagen op de TOE tijdens de deactivering worden overgebracht naar een extern kalibratiemiddel met uitzondering van positiegegevens. Positiegegevens kunnen alleen worden overgebracht naar extern handhavingsmiddel als er tijdens P.DEACTIVERING op de TOE wordt aangemeld met achtereenvolgens S.KEURINGSKAART en S.INSPECTIEKAART.

Artikel 4.2 Aannames[3]

A.BEDIENING
Er wordt verondersteld dat de bestuurder van de auto de TOE juist bedient en correct het werkingsniveau, de beladingtoestand en het moment van aanvang en beëindiging van een rit selecteert.

A.SENSOREN
Er wordt verondersteld dat de gegevens aangeboden op de sensorinterface(s) correct zijn.

A.SYSTEEMKAART
Er wordt verondersteld dat de systeemkaart een certificaat bevat welk onweerlegbaar is gekoppeld met de TOE; alle gegevens die door de TOE worden aangeboden correct ondertekent; de handtekening terugstuurt naar de TOE.

A.BOORDCOMPUTERKAART
Er wordt verondersteld dat een ingebrachte boordcomputerkaart een certificaat bevat welk onweerlegbaar is gekoppeld met de boordcomputerkaarthouder; alle gegevens die door de TOE worden aangeboden correct ondertekent; de handtekening terugstuurt naar de TOE.

A.BOORDCOMPUTERKAARTHOUDER
Er wordt verondersteld dat boordcomputerkaarthouders hun boordcomputerkaart niet aan derden uitreiken en hun PIN-code geheim houden.

A.PRINTER
Er wordt verondersteld dat gegevens die worden aangeboden ten behoeve van een aangesloten printer, correct worden afgedrukt door die printer.

A.VOOR_ACTIVERING
De TOE wordt in inactieve toestand geleverd aan voertuigfabrikanten, installateurs en/of erkende werkplaatsen. Deze zullen de TOE installeren waarna een erkende werkplaats de TOE zal kalibreren en vervolgens activeren. Na activering kan de TOE door een erkende werkplaats middels deactivering weer in inactieve toestand worden teruggebracht. De cyclus van activering en deactivering door erkende werkplaatsen kan zich gedurende de levensduur van de TOE meerdere keren herhalen. Voertuigfabrikanten, installateurs en/of erkende werkplaatsen zullen de integriteit van de TOE beschermen zolang de TOE zich niet in actieve toestand bevindt.

Artikel 5 Beveiligingsdoelstellingen

Artikel 5.1 Beveiligingsdoelen voor de TOE

OT.AUDIT

[3] NB: Dit zijn zaken die in de CC worden aangenomen als zijnde waar. Ze worden niet gecontroleerd. Mochten ze in de praktijk niet waar worden gemaakt, dan is het zeer aannemelijk dat de TOE niet zijn doelen zal bereiken.

De TOE legt beveiligingsrelevante gebeurtenisgegevens vast en toont deze op het beeldscherm.

OT.AUTHENTICATIE_BOORDCOMPUTERKAART
De TOE zal een ingebrachte boordcomputerkaart authenticeren door middel van zowel:
- een door de eigenaar van de boordcomputerkaart in te brengen PIN;
- een op de boordcomputerkaart aanwezig geldig en authentiek certificaat.

OT.VASTLEGGEN
De TOE legt gegevens vast volgens de regels van P.VASTLEGGEN en zodanig dat de geregistreerde gegevens een correcte afspiegeling zijn van de waarden aangeboden op de sensorinterface(s).

OT.KOPPELEN_AAN_SYSTEEMKAART
De TOE zal gegevens die geregistreerd dienen te worden aan de systeemkaart aanbieden ter ondertekening met een elektronische handtekening.

OT.KOPPELEN_AAN_BOORDCOMPUTERKAART
De TOE zal arbeids-, rij- en rusttijden van de bestuurder die geregistreerd dienen te worden, aan de chauffeurskaart aanbieden ter ondertekening met een elektronische handtekening.

OT.OPSLAAN
De TOE zal gegevens die geregistreerd dienen te worden opslaan. De gegevens zullen gezamenlijk worden opgeslagen met de elektronische handtekeningen over deze gegevens.

OT.UITVOEREN_GEGEVENS
De TOE kan geregistreerde gegevens uitvoeren volgens de regels van P.UITVOEREN_GEGEVENS. Tenzij gegevens worden uitgevoerd naar printer of leesvenster worden de bij de gegevens opgeslagen elektronische handtekeningen eveneens uitgevoerd.

OT.INVOEREN_GEGEVENS
De TOE kan gegevens invoeren volgens de regels van P.INVOEREN_GEGEVENS.

OT.FYSIEKE_BEVEILIGING
De TOE biedt fysieke weerstand zodanig dat het openmaken van de TOE in een laboratorium kan worden vastgesteld.

OT.BEWAKING_INTEGRITEIT
De TOE zal de integriteit van de gegevens ten minste bewaken door:
- Het testen van de integriteit van opgeslagen gegevens bij het opstarten van de TOE (O.SYSTEEMGEGEVENS), op verzoek van een gebruiker of bij het overbrengen van gegevens;
- Het testen van de integriteit van de op de TOE operationele O.PROGRAMMATUUR bij het opstarten van de TOE of op verzoek van een gebruiker;
- Het testen van de correcte werking van de TOE en de S.SYSTEEMKAART bij het opstarten van de TOE of op verzoek van een gebruiker.

OT.VEILIG_UPDATEN
De TOE kan zijn operationele programmatuur updaten met de programmatuur uit een (van een extern updatemiddel afkomstige) programmatuurrevisie indien de TOE heeft vastgesteld dat
- de programmatuurrevisie integer en authentiek is,
- het versienummer van de op de TOE operationele programmatuur correspondeert met het criterium in O.VERVANGBARE_VERSIES en
- een van de volgende situaties van toepassing is:
  - op de TOE is een werkplaatssessie actief of
  - op de TOE is geen gebruikerssessie actief en O.KALIBRATIEINDICATIE is negatief.

Artikel 5.2 Beveiligingsdoelen voor de omgeving

OE.VOOR_ACTIVERING
De TOE wordt in inactieve toestand geleverd aan voertuigfabrikanten, installateurs en/of erkende werkplaatsen. Deze zullen de TOE installeren waarna een erkende werkplaats de TOE zal kalibreren en vervolgens activeren. Na activering kan de TOE door een erkende werkplaats middels deactivering weer in inactieve toestand worden teruggebracht. De cyclus van activering en deactivering door erkende werkplaatsen kan zich gedurende de levensduur van de TOE meerdere keren herhalen. Voertuigfabrikanten, installateurs en/of erkende werkplaatsen zullen de integriteit van de TOE beschermen zolang de TOE zich niet in actieve toestand bevindt.

OE.SENSOREN

De omgeving van de TOE dient ervoor zorg te dragen dat de gegevens die worden aangeboden op de sensorinterface(s) correct zijn. Dit kan bijvoorbeeld door:
- correcte installatie van TOE en sensoren in het voertuig;
- controle van het voertuig op manipulatie van sensoren en/of aansluiting.

OE.PRINTER
De omgeving van de TOE dient ervoor zorg te dragen dat de gegevens die worden aangeboden door de TOE aan de printer correct worden afgedrukt. Dit kan bijvoorbeeld door:
- correcte installatie van TOE en printer in het voertuig;
- controle van het voertuig op manipulatie van printer en/of aansluiting.

OE.BEDIENING
De omgeving van de TOE dient ervoor zorg te dragen dat de bestuurder van de auto correct gebruik maakt van de mogelijkheden om het werkingsniveau, de beladingtoestand, het begin en einde van een rit en de aanvang en einde van de dienst te selecteren. Dit kan bijvoorbeeld door:
- handleidingen en instructies;
- opleiding en training;
- ergonomisch ontwerp van de TOE en montage in de auto.

OE.SYSTEEMKAART
De omgeving van de TOE dient een systeemkaart te bevatten die:
- een certificaat bevat welk onweerlegbaar is gekoppeld met de TOE;
- alle gegevens die door de TOE worden aangeboden correct ondertekent;
- de handtekening terugstuurt naar de TOE.

OE.BOORDCOMPUTERKAART
De omgeving van de TOE dient boordcomputerkaarten te bevatten die:
- een certificaat bevat welk onweerlegbaar is gekoppeld met de boordcomputerkaarthouder;
- alle gegevens die door de TOE worden aangeboden correct ondertekent;
- de handtekening terugstuurt naar de TOE.

OE.BOORDCOMPUTERKAARTHOUDER
Boordcomputerkaarthouders dienen hun boordcomputerkaart niet aan derden uit te reiken en hun PIN-code geheim te houden. Bestuurders mogen maar één geldige chauffeurskaart in hun bezit hebben.

OE.DEACTIVERING
De TOE wordt buiten gebruik gesteld (deactivering) door erkende werkplaatsen. De opgeslagen gegevens worden hierbij verwijderd met uitzondering van O.SYSTEEMGEGEVENS, O.PROGRAMMATUUR en O.POSITIEGEGEVENS.

OE.VEILIG_UPDATEN
De omgeving van de TOE dient programmatuurrevisies aan te leveren waarvan, voorafgaand aan het door de fabrikant aan de programmatuurrevisie aanbrengen van enig integriteits- en authenticiteitskenmerk,
- de door de fabrikant gekozen invulling van O.VERVANGBARE_VERSIES zodanig is dat deze door de TOE wordt gebruikt om vast te stellen of de programmatuur uit de desbetreffende programmatuurrevisie geschikt is voor het updaten van de op de TOE operationele programmatuur en
- de door de fabrikant gekozen invulling van O.KALIBRATIEINDICATIE en O.VERVANGBARE_VERSIES is goedgekeurd door de Dienst Wegverkeer.

Artikel 6 Functionele beveiligingseisen

De functionele beveiligingseisen zijn verdeeld in een aantal functionele groepen. Iedere groep bevat één of meer onderling samenhangende eisen. De groepen zijn:
- Beveiligingsrollen: Deze definiëren de verschillende rollen en modi van de TOE, en hoe deze rollen worden aangenomen.
- Identificatie en Authenticatie: Deze definiëren hoe boordcomputerkaarten en andere randapparatuur worden geïdentificeerd en waar nodig geauthenticeerd.
- BCT-toegangsbeleid: Hier wordt beschreven wat wordt vastgelegd, en wie daar wat mee mag doen.
- Handtekeningen: Hier wordt beschreven hoe handtekeningen worden gevraagd aan Systeemkaart en Boordcomputerkaart
- Beveiligingsaudit: Hier wordt beschreven hoe welke systeemgebeurtenissen worden geregistreerd en hoe deze zijn beschermd

- Bescherming van de BCT: Hier wordt beschreven hoe de fysieke beveiliging van de BCT werkt en hoe de integriteit wordt gewaarborgd.

Artikel 6.1 Beveiligingsrollen

FMT_SMR.2 Restricties op gebruikersrollen
FMT_SMR.2.1 De TSF kent de volgende gebruikersrollen:
- BESTUURDER
- TOEZICHTHOUDER
- WERKPLAATS
- VERVOERDER
- ONBEKEND

FMT_SMR.2.2 De TSF kan rollen met gebruikers associëren
FMT_SMR.2.3 De TSF zal de volgende regels afdwingen:
- De rol BESTUURDER wordt aangenomen (en de werkingsmodus wordt Operationele Modus Arbeidstijd) als S.CHAUFFEURSKAART is ingebracht en geauthenticeerd, of als geen S.BOORD-COMPUTERKAART is ingebracht en de gebruiker met het burgerservicenummer is geïdentificeerd.
- De rol TOEZICHTHOUDER wordt aangenomen (en de werkingsmodus wordt Controle Modus) als S.INSPECTIEKAART is ingebracht en geauthenticeerd
- De rol WERKPLAATS wordt aangenomen (en de werkingsmodus wordt Activerings/ Keuringsmodus) als S.KEURINGSKAART is ingebracht en geauthenticeerd
- De rol VERVOERDER wordt aangenomen (en de werkingsmodus wordt Bedrijfsmodus) als S.ONDERNEMERSKAART is ingebracht en geauthenticeerd
- De rol ONBEKEND wordt aangenomen (en de werkingsmode wordt Operationele Modus Basis) als:
  - Geen kaart is ingebracht en de gebruiker heeft zich niet met burgerservicenummer geïdentificeerd
  - Wel een kaart is ingebracht maar de authenticatie faalt

Artikel 6.2 Identificatie en Authenticatie

FIA_UID.1 Tijd van identificatie (Boordcomputerkaarten)
FIA_UID.1.1 De TSF staat het registreren van de O.POSITIEGEGEVENS, en O.GEBEURTENISGEGEVENS namens de gebruikersrol ONBEKEND toe, voordat een gebruiker is geïdentificeerd.
FIA_UID.1.2 De TSF eist dat S.CHAUFFEURSKAART, S.INSPECTIEKAART, S.KEURINGSKAART, en S.ONDERNEMERSKAART succesvol zijn geïdentificeerd op basis van de identiteit weergegeven in het certificaat op die boordcomputerkaart, alvorens andere handelingen te verrichten namens de desbetreffende gebruiker.

FIA_UAU.1 Tijd van authenticatie (Boordcomputerkaarten)
FIA_UAU.1.1 De TSF staat het registreren van de O.BASISGEGEVENS, O.ARBEIDSTIJDGEGEVENS, O.RITGEGEVENS, O.POSITIEGEGEVENS, O.BEWEGINGSGEGEVENS en O.GEBEURTENISGEGEVENS namens de gebruikersrol ONBEKEND toe, voordat een gebruiker is geauthenticeerd.
FIA_UAU.1.2 De TSF eist dat S.CHAUFFEURSKAART, S.INSPECTIEKAART, S.KEURINGSKAART en S.ONDERNEMERSKAART succesvol zijn geauthenticeerd op basis van:
- Een minimaal 4 karakter lange PIN (deze authenticatie wordt door S.CHAUFFEURSKAART, S.INSPECTIEKAART, S.KEURINGSKAART en S.ONDERNEMERSKAART uitgevoerd en het resultaat wordt door deze aan de TSF gerapporteerd), en
- Verificatie dat het certificaat op de boordcomputerkaart geldig en authentiek is.

FIA_AFL.1 Falen van authenticatie (FIA_AFL)
FIA_AFL.1.1 De TSF detecteert wanneer vijf (5) opeenvolgende niet-succesvolle authenticatiepogingen plaatsvinden **gerelateerd aan het authenticeren van dezelfde S.CHAUFFEURSKAART, S.INSPECTIEKAART, S.KEURINGSKAART of** S.ONDERNEMERSKAART
FIA_AFL.1.2 Als er vijf (5) opeenvolgende niet-succesvolle authenticatiepogingen zijn gedetecteerd, dan zal de TSF:
- een gebeurtenis genereren;
- de gebruiker waarschuwen;
- aannemen dat de gebruikersrol ONBEKEND is.

FIA_UAU.6 Herauthenticeren
FIA_UAU.6.1 De TSF zal S.CHAUFFEURSKAART, S.INSPECTIEKAART, S.KEURINGSKAART en S.ONDERNEMERSKAART herauthenticeren onder de volgende condities:
- bij het plaatsen van een elektronische handtekening door een boordcomputerkaart;
- bij het invoeren van de boordcomputerkaart;
- bij het opheffen van een geblokkeerde kaartsessie;
- bij herstel van de stroomvoorziening na een onderbreking

FTA_SSL.2 Blokkeren van een sessie op initiatief van een gebruiker
FTA_SSL.2.1 De TSF zal S.BOORDCOMPUTERKAART toestaan een sessie te blokkeren door het uitnemen van S.BOORDCOMPUTERKAART zonder dat is aangegeven dat de sessie van de gebruiker is beëindigd en als de auto zich in de toestand stilstaan bevindt door middel van:
- het wissen van het scherm
- het blokkeren van alle invoerapparatuur behalve die benodigd is voor het opheffen van de blokkering

FTA_SSL.2.2 De TSF eist dat de volgende handelingen plaatsvinden alvorens de blokkering op te heffen:
- het opnieuw inbrengen van dezelfde S.CHAUFFEURSKAART waarvoor de kaartsessie is geblokkeerd.

FTA_SSL.3 Automatisch beëindigen van een sessie
FTA_SSL.3.1 De TSF beëindigt een kaartsessie:
- als een geblokkeerde S.CHAUFFEURSKAART sessie niet binnen 60 minuten wordt hervat;
- meteen als een andere S.BOORDCOMPUTERKAART wordt ingebracht dan waarvoor de TSF is geblokkeerd, tenzij
  - de TSF in de toestand P.DEACTIVERING is geplaatst door een S.KEURINGSKAART waarna een S.INSPECTIEKAART wordt aangeboden, of;
  - in de Operationele Modus Arbeidstijd of Operationele Modus Taxivervoer een S.INSPECTIEKAART wordt aangeboden;
- als in een sessie van een S.ONDERNEMERSKAART, S.INSPECTIEKAART of S.KEURINGSKAART gedurende 5 minuten geen handelingen aan de TSF verricht.

FIA_UID.2 Identificatie voor enige actie (Systeemkaart)
FIA_UID.2.1 De TSF identificeert S.SYSTEEMKAART op basis van de identiteit weergegeven in het machine-gebonden certificaat zoals vastgelegd op de systeemkaart verbonden met de TOE, alvorens handelingen te verrichten namens S.SYSTEEMKAART.

FIA_UID.2 Identificatie voor enige actie (Overigen)
FIA_UID.2.1 De TSF identificeert S.BEWEGINGSOPNEMER, S.POSITIEBEPALINGSSENSOR, S.PRINTER, S.TAXAMETER, S.HANDHAVINGSMIDDELEN, S.KALIBRATIEMIDDELEN, S.BEDRIJFSMIDDELEN en S.UPDATEMIDDELEN op basis van hun aanwezigheid op de daarvoor bestemde interface, alvorens handelingen te verrichten namens de desbetreffende subjecten.

Artikel 6.3 BCT-toegangsbeleid

FDP_ACC.2 Volledige toegangscontrole
FDP_ACC.2.1 De TSF dwingt het toepassen van het BCT-toegangsbeleid af voor alle subjecten, alle objecten en alle handelingen[4].
FDP_ACC.2.2 De TSF garandeert dat alle verrichtingen tussen een subject gecontroleerd door de TSF en een object gecontroleerd door de TSF zijn onderworpen aan een toegangscontrole SFP.

FDP_ACF.1 Toegangscontrole op basis van attributen
FDP_ACF.1.1 De TSF dwingt het toepassen van het BCT-toegangsbeleid af voor objecten voor alle subjecten en alle objecten.
FDP_ACF.1.2 De TSF dwingt de volgende regels af om te bepalen of een verrichting tussen gecontroleerde subjecten en gecontroleerde objecten is toegestaan:
- TSF zal:
  - Altijd O.BEWEGINGSGEGEVENS inlezen, samenvatten, en samen met de tijd[5] en de gegevens betreffende verplaatsing beschikbaar stellen als O. BASISGEGEVENS;
  - Altijd O.POSITIEGEGEVENS inlezen en vastleggen;
  - O.ARBEIDSTIJDGEGEVENS vastleggen in Operationele Modus Arbeidstijd en Operationele Modus Taxivervoer;
  - O.RITGEGEVENS vastleggen in Operationele Modus Taxivervoer.
  - Altijd O.PROGRAMMATUURREVISIEs (kunnen) inlezen van S.UPDATEMIDDELEN en (t.b.v. een eventuele update) vastleggen;
  - Direct na het uitvoeren van een software update met een O.PROGRAMMATUURREVISIE de na de update geldende O.BASISGEGEVENS, O.GEBEURTENISGEGEVENS en O.SYSTEEMGEGEVENS vastleggen in Operationele Modus Basis c.q. Activerings- en Keuringsmodus;
  - O.BEDRIJFSGEGEVENS van een bepaalde vervoerder (kunnen) inlezen van S.BEDRIJFSMIDDELEN, indien:

[4] Er zijn geen relevante beveiligingsattributen.
[5] Zie FPT_STM.1

- de TSF voor de desbetreffende vervoerder is vergrendeld en
- de O.BEDRIJFSGEGEVENS zijn ondertekend door een S.ONDERNEMERSKAART van de desbetreffende vervoerder;
- De volgende gegevens:
  - O.SYSTEEMGEGEVENS en
  - alle O.BASISGEGEVENS, O.ARBEIDSTIJDENGEGEVENS, O.RITGEGEVENS, O.BEDRIJFSGEGEVENS, O.KAARTHOUDERGEGEVENS en O.GEBEURTENISGEGEVENS geregistreerd gedurende de periode dat de TSF voor de desbetreffende vervoerder is vergrendeld of vergrendeld geweest (bedrijfsvergrendeling)

  (kunnen) uitvoeren naar S.BEDRIJFSMIDDELEN, indien:
  - de TSF voor de desbetreffende vervoerder is vergrendeld en
  - de TSF, als onderdeel van O.BEDRIJFSGEGEVENS, beschikt over een unieke autorisatie voor deze uitvoer die
    - een nog niet verstreken geldigheidsperiode voor deze uitvoer vermeldt.
- NB: Als gegevens worden vastgelegd dan is dat inclusief de elektronische handtekening[6].

- ONBEKEND mag de in de TOE operationele O.PROGRAMMATUUR door de O.PROGRAMMATUUR uit een (van S.UPDATEMIDDELEN afkomstige) O.PROGRAMMATUURREVISIE vervangen indien:
  - de O.PROGRAMMATUURREVISIE integer en authentiek is,
  - het versienummer van de in de TOE operationele O.PROGRAMMATUUR correspondeert met het criterium in O.VERVANGBARE_VERSIES uit de O.PROGRAMMATUURREVISIE en
  - de O.KALIBRATIEINDICATIE uit de O.PROGRAMMATUURREVISIE negatief is.
- ONBEKEND mag O.SYSTEEMGEGEVENS tonen op een leesvenster.
- BESTUURDER mag de eigen:
  - O.RITGEGEVENS, O.ARBEIDSTIJDENGEGEVENS en O.KAARTHOUDERGEGEVENS tonen op een leesvenster;
  - O.ARBEIDSTIJDENGEGEVENS opslaan op de S.CHAUFFEURSKAART;
  - O.ARBEIDSTIJDENGEGEVENS van de S.CHAUFFEURSKAART overbrengen naar de TOE;
  - O.RITGEGEVENS en O.KAARTHOUDERGEGEVENS uitvoeren naar S.PRINTER.
- BESTUURDER mag O.SYSTEEMGEGEVENS tonen op een leesvenster.
- TOEZICHTHOUDER mag alle O.BASISGEGEVENS, O.ARBEIDSTIJDENGEGEVENS, O.RITGEGEVENS, O.BEDRIJFSGEGEVENS, O.KAARTHOUDERGEGEVENS, O.GEBEURTENISGEGEVENS en O.SYSTEEMGEGEVENS
  - tonen op een leesvenster;
  - uitvoeren naar S.PRINTER;
  - uitvoeren naar S.HANDHAVINGSMIDDELEN.
- TOEZICHTHOUDER mag, mits de TOE is gedeactiveerd, O.POSITIEGEGEVENS
  - uitvoeren naar S.HANDHAVINGSMIDDELEN.
- WERKPLAATS mag de TOE deactiveren.
- WERKPLAATS mag O.VARIABELE_SYSTEEMGEGEVENS aanpassen
  - vanaf het bedieningspaneel;
  - vanaf S.KALIBRATIEMIDDELEN.
- WERKPLAATS mag de in de TOE operationele O.PROGRAMMATUUR door de O.PROGRAMMATUUR uit een (van S.UPDATEMIDDELEN afkomstige) O.PROGRAMMATUURREVISIE vervangen indien:
  - de O.PROGRAMMATUURREVISIE integer en authentiek is en
  - het versienummer van de in de TOE operationele O.PROGRAMMATUUR correspondeert met het criterium in O.VERVANGBARE_VERSIES uit de O.PROGRAMMATUURREVISIE.
- WERKPLAATS mag alle O.BASISGEGEVENS, O.RITGEGEVENS, O.ARBEIDSTIJDENGEGEVENS, O.BEDRIJFSGEGEVENS, O.KAARTHOUDERGEGEVENS, O.GEBEURTENISGEGEVENS en O.SYSTEEMGEGEVENS
  - tonen op een leesvenster;
  - uitvoeren naar S.PRINTER;
  - uitvoeren naar S.KALIBRATIEMIDDELEN.
- VERVOERDER mag alle O.BASISGEGEVENS, O.ARBEIDSTIJDENGEGEVENS, O.RITGEGEVENS, O.BEDRIJFSGEGEVENS, O.KAARTHOUDERGEGEVENS en O.GEBEURTENISGEGEVENS geregistreerd gedurende de periode dat de TSF voor de desbetreffende vervoerder is vergrendeld of vergrendeld geweest (bedrijfsvergrendeling)
  - tonen op een leesvenster;
  - uitvoeren naar S.PRINTER;
  - uitvoeren naar S.BEDRIJFSMIDDELEN.
- VERVOERDER mag alle O.SYSTEEMGEGEVENS
  - tonen op een leesvenster;
  - uitvoeren naar S.PRINTER;

[6] Zie FDP_DAU.2

- uitvoeren naar S.BEDRIJFSMIDDELEN.
- VERVOERDER mag O.BEDRIJFSGEGEVENS aanpassen
  - vanaf het bedieningspaneel;
  - vanaf S.BEDRIJFSMIDDELEN.

FDP_ACF.1.3 -[7]

FDP_ACF.1.4 De TSF zal expliciet toegang van subjecten naar objecten weigeren gebaseerd op de volgende regel:
- Alle niet in FDP_ACF.1.2 genoemde toegang is niet toegestaan

FDP_ETC.2 Export van gegevens met attributen
FDP_ETC.2.1 De TSF dwingt het gebruik van het BCT-toegangsbeleid af wanneer O.BASISGEGEVENS, O.ARBEIDSTIJDENGEGEVENS, O.RITGEGEVENS, O.POSITIEGEGEVENS, O.BEDRIJFSGEGEVENS, O.GEBEURTENISGEGEVENS en O.SYSTEEMGEGEVENS gegevens worden overgebracht naar externe gegevensdragers of inrichtingen buiten de TSF.
FDP_ETC.2.2 De TSF exporteert gegevens inclusief de bijbehorende elektronische handtekening over deze gegevens, behalve als deze naar S.PRINTER of het leesvenster worden geëxporteerd.
FDP_ETC.2.3 De TSF garandeert dat de elektronische handtekening onlosmakelijk is geassocieerd met de geëxporteerde gegevens.
FDP_ETC.2.4 De TSF dwingt de volgende regels af wanneer gegevens worden geëxporteerd van de TSF:
- De TSF handhaaft de rangschikking van gegevens (berichtvolgorde) bij gegevensoverdracht naar externe gegevensdragers of inrichtingen;

FDP_ITC.1 Import van gegevens zonder attributen
FDP_ITC.1.1 De TSF dwingt het gebruik van het BCT-toegangsbeleid af wanneer gegevens worden ingelezen van S.BOORDCOMPUTERKAARTEN, S.BEWEGINGSOPNEMER, S.POSITIEBEPALINGSSENSOR, S.HANDHAVINGSMIDDELEN, S.KALIBRATIEMIDDELEN, S.BEDRIJFSMIDDELEN, S.UPDATEMIDDELEN of S.TAXAMETER.**FDP_ITC.1.2** De TSF negeert attributen wanneer gegevens worden ingelezen door de TSF.
FDP_ITC.1.3 De TSF dwingt de volgende regels af wanneer gegevens worden ingelezen door de TSF:
- De TSF verwerkt gegevens alleen wanneer deze afkomstig zijn van:
  - de interne tijdklok van de TSF;
  - de interne verplaatsingsopnemer van de TSF;
  - contact signaal (ignition sense);
  - invoer door de gebruiker via het bedieningspaneel;
  - S.BEWEGINGSOPNEMER;
  - S.POSITIEBEPALINGSSENSOR;
  - S.BOORDCOMPUTERKAARTEN;
  - S.SYSTEEMKAART;
  - S.TAXAMETER;
  - S.BEDRIJFSMIDDELEN;
  - S.UPDATEMIDDELEN.

Artikel 6.4 Handtekeningen

FDP_DAU.2 Data authenticatie met identiteit
FDP_DAU.2.1 De TSF kan een bewijs van de validiteit van gegevens genereren als volgt:
- Een hash van O.RITGEGEVENS wordt ondertekend door de S.SYSTEEMKAART over de volledige set van desbetreffende O.RITGEGEVENS direct bij het registreren van deze gegevens per individuele rit;
- Een hash van O.ARBEIDSTIJDGEGEVENS wordt ondertekend door S.CHAUFFEURSKAART direct bij het registreren van deze gegevens bij het beëindigen van de dienst van de bestuurder of het afsluiten van de kaartsessie;
- Een hash van O.ARBEIDSTIJDGEGEVENS wordt ondertekend door S.SYSTEEMKAART direct bij het registreren van deze gegevens indien de S.CHAUFFEURSKAART niet beschikbaar is;
- Een hash van alle gegevens overgebracht naar S.HANDHAVINGSMIDDELEN, S.BEDRIJFSMIDDELEN, S.KALIBRATIEMIDDELEN wordt ondertekend door de S.SYSTEEMKAART op het moment van de overdracht;
- Hashes van alle geregistreerde O.BASISGEGEVENS, O.ARBEIDSTIJDENGEGEVENS, O.RITGEGEVENS, O.POSITIEGEGEVENS, O.BEDRIJFSGEGEVENS en O.GEBEURTENISGEGEVENS worden ondertekend door S.SYSTEEMKAART.

[7] Vervallen.

FDP_DAU.2.2 De TSF levert S.BOORDCOMPUTERKAART een mogelijkheid om het bewijs van de integriteit en authenticiteit van de gegevens en de identiteit van de gebruiker die de gegevens heeft ondertekend te verifiëren.

FTP_ITC.1 Vertrouwd kanaal tussen TSFs
FTP_ITC.1.1 De TSF levert een communicatiekanaal tussen de TSF en de S.SYSTEEMKAART. Dit communicatiekanaal is gescheiden van andere communicatiekanalen, levert zekere identificatie van de eindpunten, en beschermt de data op het kanaal tegen wijzigen of lekken.
FTP_ITC.1.2 De TSF mag alleen zelf communicatie initiëren over het vertrouwde kanaal.
FTP_ITC.1.3 De TSF zal communicatie initiëren over het vertrouwde kanaal voor het door S.SYSTEEMKAART laten zetten van handtekeningen en het ontvangen van deze handtekeningen.

FCS_COP.1 Cryptografische operaties
FCS_COP.1.1 De TSF zal hash-operaties uitvoeren volgens zowel het SHA-1 en het SHA-256 cryptografische algoritme zoals gedefinieerd in de ISO/IEC 10118-3, FIPS PUB 180-2 en ETSI TS 102 176-1 standaarden.

Artikel 6.5 Beveiligingsaudit

FAU_GEN.1 Genereren van gebeurtenisgegevens[8]
FAU_GEN.1.1 De TSF genereert een gebeurtenis record van de volgende gebeurtenissen:
- het aanzetten van de TOE;
- het uitzetten van de TOE;
- het optreden van storingen[9] in de werking van de TSF;
  a. een storing in de werking van de registratiefunctie;
  b. een storing in de werking van de beveiligingsfuncties;
  c. een storing in de werking van de sensoren;
  d. een storing in de overbrenging naar een externe interface
  e. een storing in de werking van de systeemkaart;
  f. een storing in de werking van de boordcomputerkaarten.
- het optreden van fouten[10] in de werking van de TSF;
  a. een integriteitfout in de programmatuur;
  b. een integriteitfout in de systeemgegevens;
  c. een integriteitfout in de opgeslagen gebruikersgegevens;
  d. een integriteitfout bij de gegevensuitvoer naar de chauffeurskaart;
  e. een fout in de registratiefunctie;
  f. een fout die de beveiliging van de boordcomputer in gevaar brengt;
  g. een fout bij de gegevensuitvoer naar externe inrichtingen;
  h. een fout bij het gebruik van de systeemkaart;
  i. een fout bij het gebruik van de boordcomputerkaart;
  j. een fout in de bewegingsensor;
  k. een fout in de positiebepalingsensor;
  l. een fout in de koppeling met de taxameter.
- het inbrengen van S.BOORDCOMPUTERKAART;
- het uitnemen van S.BOORDCOMPUTERKAART;
- het inbrengen van een ongeldige S.BOORDCOMPUTERKAART;
- het inbrengen van een S.CHAUFFEURSKAART waarvan blijkt dat de datum en het tijdstip van de laatste registratie op S.CHAUFFEURSKAART op een later tijdstip valt dan de actuele datum en tijdstip volgens de tijdwaarneming van de TSF;
- het niet juist afsluiten van de kaartsessie;
- het inbrengen van S.CHAUFFEURSKAART waarvan blijkt dat de laatste kaartsessie niet juist is afgesloten;
- het ontstaan van onvoldoende opslagcapaciteit;
- het verdwijnen van onvoldoende opslagcapaciteit;
- het ontstaan van onvoldoende opslagcapaciteit op de S.CHAUFFEURSKAART;
- het verdwijnen van onvoldoende opslagcapaciteit op de S.CHAUFFEURSKAART;
- het ontstaan van een onderbreking van ten minste 5 seconden in de stroomvoorziening van de TOE;
- het verdwijnen van een onderbreking van ten minste 5 seconden in de stroomvoorziening van de TOE;

[8] Er wordt geen door de CC voorgedefinieerd niveau van gebeurtenissen gebruikt.
[9] Een storing treedt op wanneer een onderbreking in de correcte werking van de boordcomputer door een gebeurtenis of fout een permanent karakter heeft.
[10] Een fout treedt op wanneer de correcte werking van de boordcomputer gedurende korte tijd wordt onderbroken.

– het begin van een periode waarin de contactgeschakelde voedingsbron is uitgeschakeld in de toestand rijden;
– het einde van een periode waarin de contactgeschakelde voedingsbron is uitgeschakeld in de toestand rijden;
– het vaststellen van een toestand verplaatsen door de verplaatsingsopnemer van de TOE wanneer er geen O.BEWEGINGSGEGEVENS van de S.BEWEGINGSOPNEMER worden verkregen;
– het begin van het niet kunnen verkrijgen van O.POSITIEGEGEVENS gedurende 5 minuten;
– het einde van het niet kunnen verkrijgen van O.POSITIEGEGEVENS gedurende 5 minuten;
– een afwijking van meer dan twee procent tussen de, met behulp van O.BEWEGINGSGEGEVENS en de constante van de boordcomputer in de O.SYSTEEMGEGEVENS, berekende afstand en de werkelijke afstand;
– een afwijking van meer dan vijf procent tussen de O.BEWEGINGSGEGEVENS en de O.POSITIEGEGEVENS;
– het ontstaan van een onderbreking in de koppeling met S.TAXAMETER;
– het verdwijnen van een onderbreking in de koppeling met S.TAXAMETER;
○ het overbrengen van gegevens inclusief de naam van de gebruikte interface;
– het activeren van de TSF;
– het keuren van de TSF;
– het deactiveren van de TSF;
– het vergrendelen van de TSF;
– het inschakelen van een werkingsmodus inclusief naam werkingsmodus;
– het uitschakelen van een werkingsmodus inclusief naam werkingsmodus;
– het begin van rijden in de operationele modus werkingsniveau taxivervoer zonder S.CHAUFFEURSKAART;
– het einde van rijden in de operationele modus werkingsniveau taxivervoer zonder S.CHAUFFEURSKAART;
– het detecteren van een niet-succesvolle authenticatiepoging;
– het installeren van een programmatuurrevisie;
– starten of stoppen van audit- en beveiligingsfuncties;
– het uitblijven of weigeren van een elektronische handtekening door S.CHAUFFEURSKAART of S.SYSTEEMKAART;
– het detecteren van een niet-geautoriseerde (poging tot) wijziging van de TSF configuratie, waaronder het detecteren van een (of meer) van de volgende aan het installeren van een programmatuurrevisie gerelateerde situaties:
  a. een integriteit- of authenticiteitfout in de aangeboden O.PROGRAMMATUURREVISIE;
  b. het versienummer van de in de TOE operationele O.PROGRAMMATUUR correspondeert niet met het criterium in O.VERVANGBARE_VERSIES uit de aangeboden O.PROGRAMMATUURREVISIE;
  c. het aanbieden van een O.PROGRAMMATUURREVISIE met een positieve O.KALIBRATIEINDICATIE terwijl de TOE zich niet in activerings- en keuringsmodus bevindt;
– toegang tot het gebeurtenissenlogboek.

FAU_GEN.1.2 De TSF legt per gebeurtenis ten minste de volgende informatie vast zoals die geldt op het moment van optreden:
○ een automatisch gegenereerd oplopend volgnummer;
○ type van de gebeurtenis (de gebeurteniscode);
○ de datum en het tijdstip als gecoördineerde wereldtijd;
○ de kilometerstand;
○ de verplaatsingstoestand van de auto (rijden/stilstaan);
○ de werkingsmodus en werkingsniveau van de TOE;
○ waar relevant, de uitkomst van de gebeurtenis;
○ waar relevant, aanvullende relevante informatie, waaronder, bij detectie van een niet geautoriseerde (poging tot) installeren van een programmatuurrevisie, vermelding van de specifieke reden waarom dit niet geautoriseerd is;
als een storing of fout is opgetreden tevens:
○ de gebeurteniscode van de aanleiding voor de storing of fout;
als een S.BOORDCOMPUTERKAART is ingebracht in de TSF tevens:
○ het kaartnummer en kaartsoort;
○ de gebruikeridentificatiecode;
als geen S.BOORDCOMPUTERKAART is ingebracht, maar de gebruiker is geïdentificeerd met een burgerservicenummer:
○ het burgerservicenummer.

FAU_SAA.1 Detectie van potentiële inbreuk op beveiliging
FAU_SAA.1.1 De TSF beschouwt de in FAU_GEN.1.1 met een – gemarkeerde gebeurtenissen als beveiligingsrelevant.

FAU_ARP.1 Automatische respons op gebeurtenissen
FAU_ARP.1.1 De TSF geeft een waarschuwingsignaal op het leesvenster wanneer een beveiligingsrelevante gebeurtenis wordt gedetecteerd.

FAU_STG.1 Bescherming van gebeurtenisgegevens
FAU_STG.1.1 De TSF beschermt de opgeslagen gebeurtenis records in O.GEBEURTENISGEGEVENS tegen ongeautoriseerd verwijderen.
FAU_STG.1.2 De TSF voorkomt ongeautoriseerde aanpassingen in de opgeslagen gebeurtenis records in O.GEBEURTENISGEGEVENS.

FAU_STG.4 Voorkomen van verlies van gebeurtenisgegevens
FAU_STG.4.1 De TSF overschrijft de oudste gebeurtenis records met nieuwere wanneer de opslagcapaciteit voor de O.GEBEURTENISGEGEVENS vol is.

FRU_RSA.2 Maximum en minimum quotas
FRU_RSA.2.1 -[11]
FRU_RSA.2.2 De TSF garandeert een minimum hoeveelheid opslagcapaciteit voldoende voor 365 dagen van normaal gebruik tegelijkertijd te gebruiken voor:
- O.BASISGEGEVENS;
- O.RITGEGEVENS;
- O.POSITIEGEGEVENS;
- O.BEDRIJFSGEGEVENS;
- O.GEBEURTENISGEGEVENS;

FPT_STM.1 Tijd
FPT_STM.1.1 De TSF is in staat om betrouwbare tijdsregistraties uit te voeren in de Universal Time Coordinated met een afwijking van ten hoogste één (1) seconde en een resolutie van één (1) seconde of nauwkeuriger.

Artikel 6.6 Bescherming van de BCT

FPT_PHP.1 Passieve detectie van fysieke aanvallen
FPT_PHP.1.1 De TSF zal een laboratorium in staat stellen om fysieke aanvallen ondubbelzinnig te detecteren[12].
FPT_PHP.1.2 De TSF zal het mogelijk maken om te bepalen dat fysieke aanvallen op de TSF, de S.SYSTEEMKAART of de verbinding tussen TSF en de S.SYSTEEMKAART hebben plaatsgevonden.

FPT_TST.1 Testen van de TSF
FPT_TST.1.1 De TSF zal een verzameling zelf-testen doen bij het opstarten om de correcte werking van de TSF te demonstreren.
FPT_TST.1.2 De TSF zal TOEZICHTHOUDER, WERKPLAATS en VERVOERDER de mogelijkheden bieden om de integriteit van de TSF data te verifiëren.
FPT_TST.1.3 De TSF zal ONBEKEND, TOEZICHTHOUDER, WERKPLAATS en VERVOERDER de mogelijkheden bieden om de integriteit van de op de TOE operationele O.PROGRAMMATUUR, waaronder de TSF uitvoerbare programmatuurcode (executables), te verifiëren.

Artikel 7 Garantieniveau

Voor de typegoedkeuring van de boordcomputer wordt een Common Criteria garantieniveau vereist van ten minste EAL3. Dit niveau analyseert de geclaimde beveiligingsfuncties door middel van een analyse van functionele en interface specificatie, (gebruikers)documentatie en een beschrijving van de architectuur van de boordcomputer. De analyse wordt ondersteund met onafhankelijk testen, verificatie van de testresultaten van de ontwikkelaar een beperkt onderzoek naar zwakheden. Daarnaast worden aspecten van de gebruikte ontwerpmiddelen, configuratiebeheer en leveringsprocedures beschouwd.

In combinatie met een uitgebreid en formeel geëvalueerd beveiligingsprofiel (Protection Profile), een periodiek onderzoek en actieve handhaving, kan aannemelijk worden gemaakt dat goedgekeurde boordcomputers voldoende weerstand zullen bieden tegen de onderkende dreigingen en dat gebrekkig functionerende boordcomputers kunnen worden opgespoord.

[11] Vervallen. Er worden geen maximum quota geëist.
[12] Dat wil zeggen dat de fysieke aanvallen detecteerbaar moeten zijn door een laboratorium (zoals het NFI), maar niet noodzakelijk detecteerbaar hoeven te zijn door bijvoorbeeld een toezichthouder.

Artikel 8 Rationale

Artikel 8.1 Beveiligingsdoelstellingen

Deze sectie bevat een uitleg dat de beveiligingsdoelstellingen het gehele beveiligingsprobleem adresseren. Dit beveiligingsprobleem bestaat uit drie delen:
- Dreigingen: Dit profiel bevat geen dreigingen, dus er is ook geen uitleg
- Beveiligingsbeleid: Zie sectie 8.1.1
- Aannames: Zie sectie 8.1.2

Artikel 8.1.1 Beveiligingsbeleid

Deze sectie bevat een uitleg dat de beveiligingsdoelstellingen alle delen van het beveiligingsbeleid implementeren.

P.VASTLEGGEN
Deze wordt direct ondervangen door OT.VASTLEGGEN. Daarnaast vindt indirecte ondersteuning plaats door OT.FYSIEKE_BEVEILIGING en OT.AUTHENTICATIE_BOORDCOMPUTERKAART.

P.BEWAREN_EN_BORGEN
Het bewaren van de gegevens wordt ondervangen door:
- OT.OPSLAAN, wat de gegevens en alle elektronische handtekeningen opslaat.

Het detecteren van de wijzigingen in de vastgelegde gegevens wordt ondervangen door:
- Het aanbieden van de gegevens aan de systeemkaart (OT.KOPPELEN_AAN_SYSTEEMKAART) en het door deze ondertekenen van de gegevens (OE.SYSTEEMKAART);
- Het aanbieden van gegevens aan de boordcomputerkaart (OT.KOPPELEN_AAN_BOORDCOMPUTERKAART) en het door deze ondertekenen van de gegevens (OE.BOORDCOMPUTERKAART).

Het onweerlegbaar koppelen aan de TOE wordt ondervangen door:
- Het aanbieden van de gegevens aan de systeemkaart (OT.KOPPELEN_AAN_SYSTEEMKAART) en het door deze ondertekenen van de gegevens (OE.SYSTEEMKAART);
- Dat de systeemkaart een certificaat bevat welk onweerlegbaar is gekoppeld aan de TOE (OE.SYSTEEMKAART).

Het onweerlegbaar koppelen aan de boordcomputerkaarthouder wordt ondervangen door:
- Het aanbieden van gegevens aan de boordcomputerkaart (OT.KOPPELEN_AAN_BOORDCOMPUTERKAART) en het door deze ondertekenen van de gegevens (OE.BOORDCOMPUTERKAART);
- Dat de boordcomputerkaart een certificaat bevat welk onweerlegbaar is gekoppeld aan de boordcomputerkaarthouder (OE.BOORDCOMPUTERKAART);
- Dat de boordcomputerkaarthouder zich authenticeert met een PIN bij het insteken van de kaart (OT.AUTHENTICATIE_BOORDCOMPUTERKAART);
- Dat de boordcomputerkaarthouder zijn kaart veilig bewaart en zijn PIN geheim houdt. (OE.BOORDCOMPUTERKAARTHOUDER).

Daarnaast vindt indirecte ondersteuning plaats door OT.FYSIEKE_BEVEILIGING, OT.AUDIT en OT.BEWAKING_INTEGRITEIT.

P.ACTIES
Deze wordt direct ondervangen door OT.AUDIT, OT.UITVOEREN_GEGEVENS, OT.INVOEREN_GEGEVENS, OT_VEILIG_UPDATEN, OT.AUTHENTICATIE_BOORDCOMPUTERKAART en OE.BEDIENING. Daarnaast vindt indirecte ondersteuning plaats door OT.FYSIEKE_BEVEILIGING en OT.BEWAKING_INTEGRITEIT.

P.UITVOEREN_GEGEVENS
Deze wordt direct ondervangen door OT.UITVOEREN_GEGEVENS, OT.AUTHENTICATIE_BOORDCOMPUTERKAART en OE.BEDIENING. Daarnaast vindt indirecte ondersteuning plaats door OE.PRINTER.

P.INVOEREN_GEGEVENS
Deze wordt direct ondervangen door OT.INVOEREN_GEGEVENS, OT.AUTHENTICATIE_BOORDCOMPUTERKAART en OE.BEDIENING.

P.VEILIG_UPDATEN
Deze wordt direct ondervangen door OT.VEILIG_UPDATEN, OE.VEILIG_UPDATEN, OT.AUTHENTICATIE_BOORDCOMPUTERKAART en OE.BEDIENING. Daarnaast vindt indirecte ondersteuning plaats door OT.INVOEREN_GEGEVENS.

P.DEACTIVERING
Deze wordt direct ondervangen door OE.DEACTIVERING (voor deactivering en verwijderen gegevens), OT.UITVOEREN_GEGEVENS (voor wat betreft het uitvoeren van gegevens) en OT.AUTHENTICATIE-_BOORDCOMPUTERKAART.

Artikel 8.1.2 Aannames

Deze sectie bevat een uitleg dat de beveiligingsdoelstellingen alle aannames implementeren.

A.BEDIENING
Deze wordt direct ondervangen door OE.BEDIENING.

A.SENSOREN
Deze wordt direct ondervangen door OE.SENSOREN.

A.SYSTEEMKAART
Deze wordt direct ondervangen door OE.SYSTEEMKAART.

A.BOORDCOMPUTERKAART
Deze wordt direct ondervangen door OE.BOORDCOMPUTERKAART.

A.BOORDCOMPUTERKAARTHOUDER
Deze wordt direct ondervangen door OE.BOORDCOMPUTERKAARTHOUDER.

A.PRINTER
Deze wordt direct ondervangen door OE.PRINTER.

A.VOOR_ACTIVERING
Deze wordt direct ondervangen door OE.VOOR_ACTIVERING.

Artikel 8.2 Beveiligingsdoelstellingen voor de TOE

OT.AUDIT
Deze wordt gerealiseerd door FAU_GEN.1 die specificeert welke gegevens er van welke gebeurtenissen worden vastgelegd.
Dit wordt ondersteund door:
- FPT_STM.1 die aangeeft dat er een klok is die nauwkeurig de tijd aangeeft (zodat de juiste datum en tijd wordt opgeslagen bij de gebeurtenisgegevens)
- FAU_SAA.1 die aangeeft welke van de gebeurtenissen beveiligingsrelevant zijn
- FAU_ARP.1 die aangeeft dat beveiligingsrelevante gegevens ook allemaal worden getoond op het leesvenster
- FAU_STG.1 die aangeeft dat de gegevens niet zo maar kunnen worden verwijderd of veranderd
- FRU_RSA.2 dat vastlegt dat er genoeg opslagruimte moet zijn voor 365 dagen normaal gebruik
- FAU_STG.4 dat vastlegt dat oude gegevens worden overschreven als de opslagruimte vol raakt

OT.AUTHENTICATIE_BOORDCOMPUTERKAART
Deze wordt gerealiseerd door FIA_UID.1 (Boordcomputerkaarten) en FIA_UAU.1 (Boordcomputerkaarten) welke de I&A regels voor boordcomputerkaarten geven
Dit wordt ondersteund door:
- FIA_AFL.1 die aangeeft wat er gebeurt bij falende authenticatie
- FIA_UAU.6 die aangeeft dat er onder sommige omstandigheden nogmaals moet worden geauthenticeerd
- FTA_SSL.2 die tijdelijke blokkade van een sessie toelaat
- FTA_SSL.3 die aangeeft wanneer een sessie wordt afgebroken

OT.VASTLEGGEN
Deze wordt gerealiseerd door FDP_ACC.2 en FDP_ACF.1 die de regels van P.VASTLEGGEN implementeren.
Dit wordt ondersteund door:
- FIA_UID.2 (Overigen) die S.BEWEGINGSSENSOR en S.POSITIEBEPALINGSSENSOR identificeren;
- FDP_ITC.1 die vastlegt dat gegevens mogen worden ingelezen van S.BEWEGINGSSENSOR en S.POSITIEBEPALINGSSENSOR;
- FRU_RSA.2 die vastlegt dat er genoeg opslagruimte moet zijn voor 365 dagen normaal gebruik;
- FIA_UID.1 (Boordcomputerkaarten) die S.BOORDCOMPUTERKAART identificeert;
- FIA_UAU.1 (Boordcomputerkaarten) die S.BOORDCOMPUTERKAART authenticeert.

OT.KOPPELEN_AAN_SYSTEEMKAART
Deze wordt gerealiseerd door FDP_DAU.2 die het zetten van een handtekening implementeert. Dit wordt ondersteund door:
- FIA_UID.2 (Systeemkaart) die S.SYSTEEMKAART identificeert.
- FCS_COP.1 die een hash genereert (de hash wordt getekend in plaats van de gegevens)
- FTP_ITC.1 die ervoor zorgdraagt dat de hash niet wordt veranderd voordat deze wordt getekend
- FDP_ACF.1 die specificeert dat de handtekening ook wordt opgeslagen

OT.KOPPELEN_AAN_BOORDCOMPUTERKAART
Deze wordt gerealiseerd door FDP_DAU.2 die het zetten van een handtekening implementeert. Dit wordt ondersteund door:
- FIA_UID.1 (Boordcomputerkaarten) die S.BOORDCOMPUTERKAART identificeert.
- FIA_UAU.1 (Boordcomputerkaarten) die S.BOORDCOMPUTERKAART authenticeert.
- FCS_COP.1 die een hash genereert (de hash wordt getekend in plaats van de gegevens)
- FDP_ACF.1 die specificeert dat de handtekening ook wordt opgeslagen
- FMT_SMR.2 die de verschillende rollen specificeert die bij de verschillende boordcomputerkaarten horen

OT.OPSLAAN
Zie OT.VASTLEGGEN, OT.KOPPELEN_AAN_SYSTEEMKAART en OT.KOPPELEN_AAN_BOORDCOMPUTERKAART. Daarnaast wordt dit ondersteund door:
- FRU_RSA.2 die vastlegt dat er genoeg opslagruimte moet zijn voor 365 dagen normaal gebruik

OT.UITVOEREN_GEGEVENS
Deze wordt gerealiseerd door FDP_ACC.2 en FDP_ACF.1 die de regels van P.UITVOEREN_GEGEVENS implementeren. Dit wordt ondersteund door:
- FIA_UID.1 (Boordcomputerkaarten) die S.BOORDCOMPUTERKAART identificeert.
- FIA_UAU.1 (Boordcomputerkaarten) die S.BOORDCOMPUTERKAART authenticeert.
- FMT_SMR.2 die de verschillende rollen definieert;
- FIA_UID.2 (Overigen) die de verschillende soorten randapparatuur identificeert waar naar toe kan worden uitgevoerd;
- FDP_ETC.2 die ervoor zorg draagt dat de elektronische handtekening mee wordt uitgevoerd.

OT.INVOEREN_GEGEVENS
Deze wordt gerealiseerd door FDP_ACC.2 en FDP_ACF.1 die de regels van P.INVOEREN_GEGEVENS implementeren. Dit wordt ondersteund door:
- FIA_UID.1 (Boordcomputerkaarten) die S.BOORDCOMPUTERKAART identificeert.
- FIA_UAU.1 (Boordcomputerkaarten) die S.BOORDCOMPUTERKAART authenticeert.
- FMT_SMR.2 die de verschillende rollen definieert;
- FIA_UID.2 (Overigen) die de verschillende soorten randapparatuur identificeert waarvandaan kan worden ingevoerd;
- FDP_ITC.1 die regels voor het invoeren vastlegt.

OT.FYSIEKE_BEVEILIGING
Deze wordt direct gerealiseerd door FPT_PHP.1.

OT.BEWAKING_INTEGRITEIT
Deze wordt direct gerealiseerd door FPT_TST.1.

OT.VEILIG_UPDATEN
Deze wordt direct gerealiseerd door FDP_ACC.2 en FDP_ACF.1 die de regels van P.VEILIG_UPDATEN implementeren. Dit wordt ondersteund door:
- FIA_UID.1 (Boordcomputerkaarten) die S.BOORDCOMPUTERKAART identificeert.
- FIA_UAU.1 (Boordcomputerkaarten) die S.BOORDCOMPUTERKAART authenticeert.
- FMT_SMR.2 die de verschillende rollen definieert;
- FIA_UID.2 (Overigen) die de verschillende soorten randapparatuur identificeert waarvandaan kan worden ingevoerd;
- FDP_ITC.1 die regels voor het invoeren definieert;
- FAU_GEN.1 die gebeurtenissen m.b.t. P.VEILIG_UPDATEN definieert.

Artikel 8.3 Afhankelijkheden

De volgende afhankelijkheden zijn niet vervuld:
- FMT_MSA.3 (van FDP_ACF.1 en FDP_ITC.1): aangezien er geen attributen worden gebruikt, hoeven de attributen ook niet te worden geïnitialiseerd;
- FDP.ITC.1 of FDP_ITC.2 of FCS_CKM.1 (van FCS.COP.1): aangezien hashing geen sleutels gebruikt,

hoeven de sleutels ook niet te worden geïmporteerd of gegenereerd;
- FCS_CKM.4 (van FCS_COP.1): aangezien hashing geen sleutels gebruikt, hoeven de sleutels ook niet te worden vernietigd.

BIJLAGE 2 BIJ DE REGELING SPECIFICATIES EN TYPEGOEDKEURING BOORDCOMPUTER TAXI

Gegevensoverbrengingsinterface Boordcomputer Taxi

Versie 2.2

Datum 8 december 2014
Status DEFINITIEF

Inhoud

Artikel 1 Definities

In deze bijlage wordt verstaan onder:
a. *XML:* eXtensible Markup Language;
b. *USB:* Universal Serial Bus;
c. *ritadministratie.xsd:* XML schema definitie van het resultaatbericht van de gegevenslevering ritadministratie;
d. *arbeidstijden.xsd:* XML schema definitie van het resultaatbericht van de gegevenslevering Arbeids-, rij en rusttijden;
e. *coordinaten.xsd:* XML schema definitie van het resultaatbericht van de gegevenslevering coördinaten;
f. *gebeurtenis.xsd:* XML schema definitie van het resultaatbericht van de gegevenslevering gebeurtenis;
g. *onderzoek.xsd:* XML schema definitie van het resultaatbericht van de gegevenslevering onderzoek;
h. *chauffeurskaartdata.xsd:* XML schema definitie van het resultaatbericht van de gegevenslevering chauffeurskaartdata;
i. *bcttypes.xsd:* XML schema definitie van de gegevenstypen die in de XML schema definities genoemd onder c. t/m h. worden gebruikt.

Artikel 2 Algemeen

Aan dit document wordt gerefereerd als 'Gegevensoverbrengingsinterface Boordcomputer Taxi Versie 2.2'. Deze versie dateert van 8 december 2014'.

Artikel 2.1 Doel

In dit artikel worden de gemeenschappelijke kenmerken beschreven die gelden voor de gegevensleveringen 'Ritadministratie', 'Arbeids-, rij- en rusttijden', 'Coördinaten', 'Gebeurtenis', 'Onderzoek' en 'Chauffeurskaartdata'.

Artikel 2.2 Hardware koppeling

De overbrengingsinterface die gebruikt wordt voor de gegevensoverbrenging naar een externe gegevensdrager is een USB poort. Er geldt:
a. de USB poort moet aantoonbaar compliant zijn met de specificaties zoals opgesteld door het USB Implementers Forum, Inc.;
b. de USB poort is een USB type A connector.

De snelheidseis, als beschreven in artikel 2.3, is leidend bij de keuze van USB 1.1 of hoger. Als de snelheidseis van alle gegevensleveringen (*'Ritadministratie', 'Arbeids-, rij- en rusttijden', 'Coördinaten', 'Gebeurtenis' 'Onderzoek' en 'Chauffeurskaartdata'*) beschreven in deze bijlage gehaald kan worden met USB 1.1 (12 Mbit/s) dan is USB 1.1 toegestaan, zo niet dan moet USB 2.0 (480 Mbit/s) of hoger gebruikt worden.

Artikel 2.3 Snelheidseis gegevenslevering

Na opvragen van een gegevenslevering moet het corresponderende XML bericht binnen de volgende termijnen beschikbaar zijn op het externe gegevensdrager:
a. Bestand tot 3 Mbyte binnen 10 seconden;
b. Voor iedere Mbyte die het bestand groter is kan de termijn met 3 seconden worden vergroot.

Artikel 2.4 Bestandsformaat

Voor externe opslagmedia moet het bestandssysteem FAT32 ondersteund worden.

Artikel 2.5 Overbrengingsprotocol

De boordcomputer fungeert als host en neemt het initiatief voor gegevensoverdracht naar de externe gegevensdrager.

Artikel 2.6 Totstandkoming gegevenslevering

Om een gegevenslevering tot stand te laten komen, stelt de boordcomputer de houder van een boordcomputerkaart in staat om:
a. zich met de boordcomputerkaart te authenticeren;
b. de externe gegevensdrager met de overbrengingsinterface van de boordcomputer te verbinden;
c. op de boordcomputer één of meerdere gegevensleveringen te selecteren. Standaard zijn alle gegevensleveringen waarvoor de gebruiker is geautoriseerd geselecteerd;
d. op de boordcomputer een periode in te voeren waarover gegevens opgevraagd moeten worden voor de betreffende gegevenslevering(en).
e. op de boordcomputer de betreffende gegevenslevering(en) over de ingevoerde periode met één gebruikershandeling starten.

Nadat alle geselecteerde gegevensleveringen succesvol zijn afgerond en de berichten met de gegevens beschikbaar zijn op de externe gegevensdrager, toont de boordcomputer een melding dat de gegevens beschikbaar zijn.

Artikel 2.6.1 Periode gegevenslevering

De periode, als bedoeld in artikel 2.6, onderdeel d, bedraagt per levering maximaal 1 jaar, met uitzondering van de gegevenslevering 'Onderzoek' die geen maximum periode kent, en de gegevenslevering 'Chauffeurskaartdata' die de periode van de arbeids-, rij- en rusttijdendata van de chauffeurskaart overneemt.

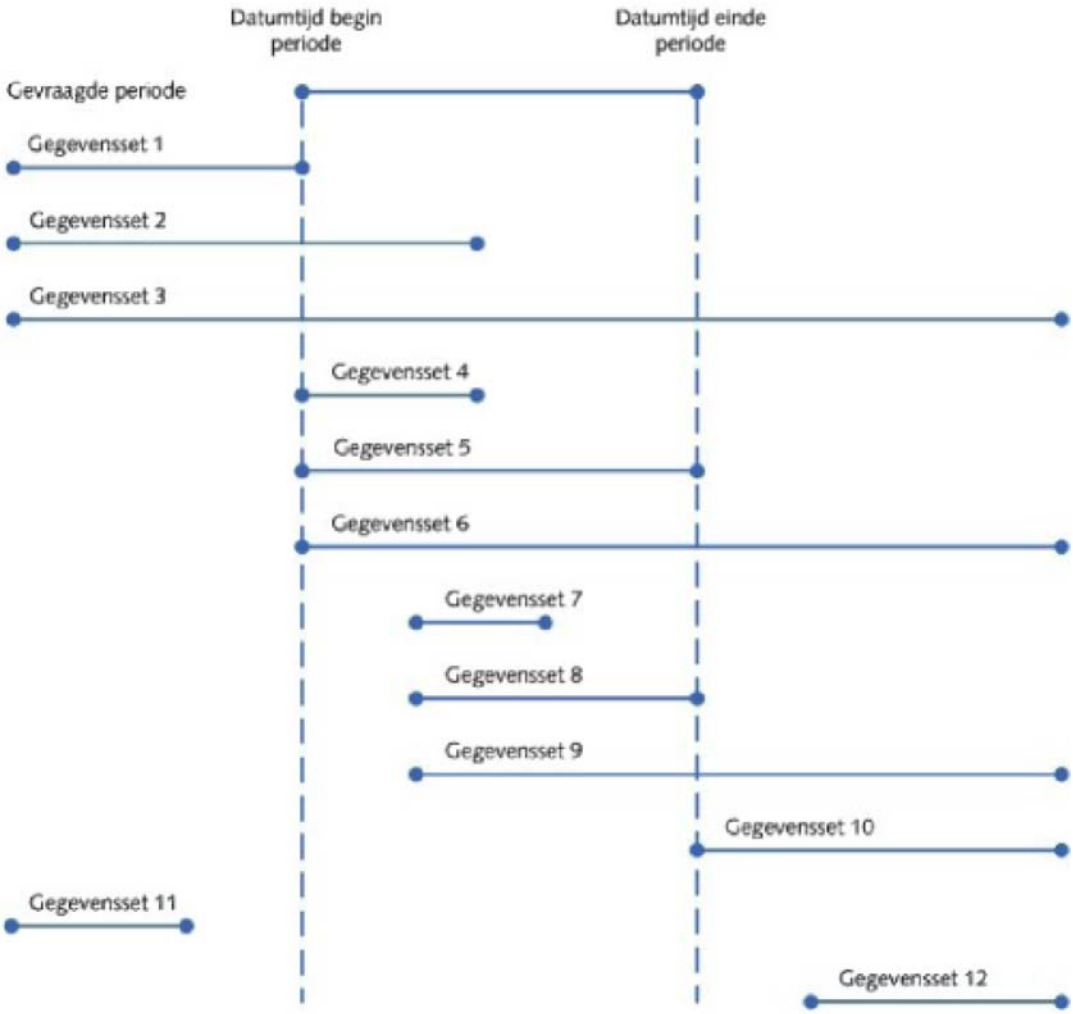
De standaardwaarde voor 'Datumtijd begin periode' is het tijdstip van opvragen minus 29 kalenderdagen, met uitzondering van de gegevenslevering 'Onderzoek', waar 'Datumtijd begin periode' standaard leeg is, en de gegevenslevering 'Chauffeurskaartdata', waar de standaarwaarde voor 'Datumtijd begin periode' overeenkomt met het oudste record op de chauffeurskaart. 'Datumtijd einde periode' is standaard leeg. Als bij opvragen van een gegevenslevering 'Datumtijd begin periode' leeg is, wordt deze gevuld met de datum en het tijdstip van de activering. Is 'Datumtijd einde periode' leeg, dan wordt 'Datumtijd einde periode' gevuld met de datum en het tijdstip waarop het bericht wordt samengesteld;

In de gegevenslevering 'Coördinaten', 'Gebeurtenis' en 'Onderzoek' worden alle gegevens opgenomen die binnen de opgevraagde periode vallen.

In de gegevenslevering 'Ritadministratie', 'Arbeidstijd' en 'Chauffeurskaartdata' worden alle gegevensets opgenomen die de gevraagde periode, inclusief grenzen, overlappen. In de onderstaande tabel is de selectie voor deze gegevensleveringen verder uitgewerkt. Alle gegevensets worden opgenomen die voldoen aan één van de onderstaande condities:

Conditie 1	Datumtijd begin gegevenset ligt vóór Datumtijd begin periode en Datumtijd einde gegevenset is gelijk aan Datumtijd begin periode
Conditie 2	Datumtijd begin gegevenset ligt vóór Datumtijd begin periode en Datumtijd einde gegevenset ligt ná Datumtijd begin periode en Datumtijd einde gegevenset ligt vóór Datumtijd einde periode
Conditie 3	Datumtijd begin gegevenset ligt vóór Datumtijd begin periode en Datumtijd einde gegevenset ligt ná Datumtijd einde periode
Conditie 4	Datumtijd begin gegevenset is gelijk aan Datumtijd begin periode en Datumtijd einde gegevenset ligt ná Datumtijd begin periode en Datumtijd einde gegevenset ligt vóór Datumtijd einde periode
Conditie 5	Datumtijd begin gegevenset is gelijk aan Datumtijd begin periode en Datumtijd einde gegevenset is gelijk aan Datumtijd einde periode
Conditie 6	Datumtijd begin gegevenset is gelijk aan Datumtijd begin periode en Datumtijd einde gegevenset ligt na Datumtijd einde periode
Conditie 7	Datumtijd begin gegevenset ligt na Datumtijd begin periode en Datumtijd begin gegevenset ligt voor Datumtijd einde periode en Datumtijd einde gegevenset ligt na Datumtijd begin periode en Datumtijd einde gegevenset ligt voor Datumtijd einde periode
Conditie 8	Datumtijd begin gegevenset ligt na Datumtijd begin periode en Datumtijd begin gegevenset ligt voor Datumtijd einde periode en Datumtijd einde gegevenset is gelijk aan Datumtijd einde periode
Conditie 9	Datumtijd begin gegevenset ligt na Datumtijd begin periode en Datumtijd begin gegevenset ligt voor Datumtijd einde periode en Datumtijd einde gegevenset ligt na Datumtijd einde periode
Conditie 10	Datumtijd begin gegevenset is gelijk aan Datumtijd einde periode en Datumtijd einde gegevenset ligt na Datumtijd einde periode

De tabel kan als volgt gevisualiseerd worden. Alle gegevenssets behalve gegevensset 11 en 12 worden in het bericht opgenomen.



Figuur 1

Artikel 2.6.2 Verwerking gegevenslevering

Aanvragen van een gegevenslevering is een synchrone aanvraag die direct verwerkt moet worden.

Als de boordcomputer bezig is met de verwerking van een aanvraag voor een gegevenslevering, dan is het niet mogelijk om dezelfde gegevenslevering of een andere gegevenslevering aan te vragen zolang de huidige aanvraag niet is afgerond.

Het is wel eenvoudig mogelijk om een aanvraag te onderbreken. Na onderbreken van de huidige aanvraag is een nieuwe aanvraag van een gegevenslevering direct (< 1 seconde wachten) mogelijk.

De overige functies van de boordcomputer blijven functioneren als de boordcomputer bezig is met het verwerken van een aanvraag voor een gegevenslevering *'Ritadministratie', 'Arbeids-, rij- en rusttijden', 'Coördinaten', 'Gebeurtenis', 'Onderzoek' of 'Chauffeurskaartdata'*.

Overschrijven van een bericht op de externe gegevensdrager met dezelfde naam, is alleen toegestaan na een bevestiging van de gebruiker.

Artikel 2.7 Authenticatie en autorisatie

Aanvragen van de gegevensleveringen *'Ritadministratie', 'Arbeids-, rij- en rusttijden', 'Coördinaten', 'Gebeurtenis', 'Onderzoek' en 'Chauffeurskaartdata'* moet alleen mogelijk zijn voor daartoe geauthenticeerde en geautoriseerde gebruikers.

Artikel 2.8 Integriteit

De door de boordcomputer geregistreerde gegevens worden voorzien van een elektronische handtekening zodat achteraf de authenticiteit en integriteit van deze gegevens kan worden vastgesteld. Voor het aanmaken van de elektronische handtekeningen worden de boordcomputerkaarten gebruikt.

De integriteit van gegevens wordt onderverdeeld in 'integriteit exportbericht' en 'integriteit geregistreerde gegevens'.

Artikel 2.8.1 Integriteit exportbericht

De boordcomputer kent zes gegevensleveringen, te weten *'Ritadministratie', 'Arbeids-, rij- en rusttijden', 'Coördinaten', 'Gebeurtenis', 'Onderzoek' en 'Chauffeurskaartdata'*. Deze gegevensleveringen worden elk in een exportbericht vanuit de boordcomputer overgebracht. Dit exportbericht is een XML bericht dat bestaat uit een gegevenslevering-element zoals gespecificeerd in één van de artikelen 3 t/m 8, gevolgd door een element met een elektronische handtekening berekend over het gegevenslevering-element en de identificatie van de sleutel gebruikt voor het berekenen van de elektronische handtekening.

Voor het genereren en de opmaak van de elektronische handtekening wordt gebruik gemaakt van de W3C Recommendation 'XML Signature Syntax and Processing Version 1.1' (XMLDSIG11) van 11 april 2013. De XMLDSIG11 specificatie (http://www.w3.org/TR/xmldsig-core1/) is een door het World Wide Web Consortium (W3C) ontworpen standaard voor de XML syntax en het genereren van elektronische handtekeningen.

Het XML exportbericht bestaat uit een <Envelope>-element met daarin een van de gegevenslevering-elementen <Ritadministratie>, <Arbeidstijden>, <Coordinaten>, <Gebeurtenis>, <Onderzoek> of <Chauffeurskaartdata>, gevolgd door een <Signature>-element. Het gegevenslevering-element bevat een resultaatbericht van een gegevenslevering zoals gespecificeerd in één van de artikelen 3 t/m 8. Het <Signature>-element is opgebouwd conform de XMLDSIG11 specificatie en bevat achtereenvolgens de elementen

a. <SignedInfo> met daarin o.a. verwijzingen naar en de 'message digests' van het gegevenslevering-element respectievelijk het <KeyInfo> element,
b. <SignatureValue> met daarin de elektronische handtekening over het <SignedInfo> element en
c. <KeyInfo> met daarin een representatie van het certificaat behorende bij de sleutel die voor de handtekening werd gebruikt.

Het XML exportbericht kent, afhankelijk van de omsloten gegevenslevering, een van de volgende structuren:

```
<?xml version="1.0" encoding="UTF-8"?>
<Envelope xmlns="urn:envelope">
  <Ritadministratie xmlns="http://www.ritadministratie.org"
Id="idGegevenslevering">
    <!-- opbouw conform Ritadministratie.xsd -->
  </Ritadministratie>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <!-- opbouw conform specificatie hieronder -->
  </Signature>
</Envelope>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<Envelope xmlns="urn:envelope">
  <Arbeidstijden xmlns="http://www.arbeidstijden.org" Id="idGegevenslevering">
    <!-- opbouw conform Arbeidstijden.xsd -->
  </Arbeidstijden>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <!-- opbouw conform specificatie hieronder -->
  </Signature>
</Envelope>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<Envelope xmlns="urn:envelope">
  <Coordinaten xmlns="http://www.coordinaten.org" Id="idGegevenslevering">
    <!-- opbouw conform Coordinaten.xsd -->
  </Coordinaten>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <!-- opbouw conform specificatie hieronder -->
  </Signature>
</Envelope>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<Envelope xmlns="urn:envelope">
  <Gebeurtenis xmlns="http://www.gebeurtenis.org" Id="idGegevenslevering">
    <!-- opbouw conform Gebeurtenis.xsd -->
  </Gebeurtenis>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <!-- opbouw conform specificatie hieronder -->
  </Signature>
</Envelope>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<Envelope xmlns="urn:envelope">
  <Onderzoek xmlns="http://www.onderzoek.org" Id="idGegevenslevering">
    <!-- opbouw conform Onderzoek.xsd -->
  </Onderzoek>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <!-- opbouw conform specificatie hieronder -->
  </Signature>
</Envelope>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<Envelope xmlns="urn:envelope">
  <Chauffeurskaartdata xmlns="http://www.chauffeurskaartdata.org"
Id="idGegevenslevering">
    <!-- opbouw conform Chauffeurskaartdata.xsd -->
  </Chauffeurskaartdata>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <!-- opbouw conform specificatie hieronder -->
  </Signature>
</Envelope>
```

Het <Signature> element in eender welke van de zes bovenstaande XML exportberichten heeft altijd de volgende, aan de XMLDSIG11 conformerende, opbouw:

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#"/><SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256"/><Reference URI="#idGegevenslevering"><Transforms><Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><Transform
Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116"><xsl:transform
xmlns:xsl="http://www.w3.org/1999/XSL/Transform" version="1.0"><xsl:output
method="xml" version="1.0" encoding="UTF-8" standalone="yes" omit-xml-
declaration="yes" indent="no"/><xsl:template match="@*|*"><xsl:copy><xsl:apply-
templates select="@*|*"/><xsl:apply-templates
select="text()"/></xsl:copy></xsl:template><xsl:template
match="text()"><xsl:choose><xsl:when test="../@codering = 'base64'"><xsl:value-
of select="translate(normalize-space(.), ' ',
'')"/></xsl:when><xsl:otherwise><xsl:value-of select="normalize-
space(.)"/></xsl:otherwise></xsl:choose></xsl:template></xsl:transform></Transfo
rm></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><DigestValue>SmbaHv5W5yFiDf
AClpPHPzWdTL5vpu69LoQxEmNUk80=</DigestValue></Reference><Reference
URI="#idKeyInfo"><Transforms><Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><Transform
Algorithm="http://www.w3.org/TR/1999/REC-xslt-19991116"><xsl:transform
xmlns:xsl="http://www.w3.org/1999/XSL/Transform" version="1.0"><xsl:output
method="xml" version="1.0" encoding="UTF-8" standalone="yes" omit-xml-
declaration="yes" indent="no"/><xsl:template match="@*|*"><xsl:copy><xsl:apply-
templates select="@*|*"/><xsl:apply-templates
select="text()"/></xsl:copy></xsl:template><xsl:template
match="text()"><xsl:choose><xsl:when test="local-name(parent::*) =
'X509Certificate'"><xsl:value-of select="translate(normalize-space(.), ' ',
'')"/></xsl:when><xsl:otherwise><xsl:value-of select="normalize-
space(.)"/></xsl:otherwise></xsl:choose></xsl:template></xsl:transform></Transfo
rm></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><DigestValue>HnVvlJkyj+3WB2
cCqhCY2YBa+nl9Iw9MQAv8hbwrUMc=</DigestValue></Reference></SignedInfo>
  <SignatureValue>
    aBjXyxWpdtay5+HYLDOt3qg7MmgRwmW101m9K5wMkil3FOY0pxqRG9j3Lv15BpEt
    AF7ZnchiAGZIeSeAAfskhm8gokbg0RJE4H55DGBjiaU09nlwv1NbUyTeTlk3UBQx
    2jWY90T0PFED+eXp48eZBHlcbIrEDqXcC4TZVHCBeDdoGNfLFal21rLn4dgsM63e
    qDsyaBHCZbXTWb0rnAySKXcU5jSnGpEb2Pcu/XkGkS0AXtmdyGIAZkh5J4AB+ySG
    byCiRuDREkTgfnkMYGOJpTT2eXC/U1tTJN5OWTdQFDHaNZj3RPQ8UQP55enjx5kE
    eVxsisQOpdwLhNlUcIF4Nw==
  </SignatureValue>
  <KeyInfo Id="idKeyInfo">
    <X509Data>
      <X509Certificate>
        MIIETTCCA7agAwIBAgIJANaOuOCRgiz3MA0GCSqGSIb3DQEBBQUAMIG8MQswCQYD
        VQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTE9MDsGA1UEChM0WE1MIFNlY3Vy
        aXR5IExpYnJhcnkgKGh0dHA6Ly93d3cuYWxla3NleS5jb20veG1sc2VjKTEeMBwG
        ...
        T9kRU3FU01jUiX2+kbdnghZAOJm0ziRNxfNPwIIWPKYXyXEKQQzrnxyFey1hP7cg
        6A==
      </X509Certificate>
    </X509Data>
  </KeyInfo>
</Signature>
```

Toelichting:

a. de waarden op een **gele** achtergrond betreffen voorbeelden; deze waarden moeten door de boordcomputer berekend en/of bepaald worden;
b. het gegevenslevering-element uit de omvattende <Envelop> bevat het resultaat bericht van een gegevenslevering en heeft een Id gelijk aan 'idGegevenslevering';
c. het <KeyInfo> heeft een Id gelijk aan 'idKeyInfo';
d. het <SignedInfo> element verwijst met twee <Reference> elementen naar twee te ondertekenen elementen op basisvan hun Id (zie de tekst op een **blauwe** achtergrond);
e. zowel het gegevenlevering-element als het <KeyInfo>-element worden als volgt getransformeerd: eerst gecanonicaliseerd en daarna van alle overbodige witruimte ontdaan:
    1. de witruimte van alle text() nodes worden genormaliseerd met normalize-space(.);
    2. de (enige) text() node van elk element met Base64 gecodeerde inhoud wordt bovendien van alle (resterende) spaties ontdaan met translate(..., ' ', '') (zie de tekst op een **groene** achtergrond).
f. het <DigestValue> element van het eerste <Reference> element moet worden gevuld met de Base64 codering van de SHA-256 hash van het (volgens e. getransformeerde) gegevenslevering-element;
g. het <DigestValue> element van het tweede <Reference> element moet worden gevuld met de Base64 codering van de SHA-256 hash van het (volgens e. getransformeerde) <KeyInfo>-element;
h. het <SignedInfo> element moet, zoals hierboven weergegeven, ontdaan van alle overbodige

witruimte in de envelop worden opgenomen, omdat de XMLDSIG11 standaard niet voorziet in het toepassen van enige andere transformatie dan canonicaliseren van dit element;

i. het <SignatureValue> element moet worden gevuld met de Base64 codering van de RSA-SHA256 (PKCS#1 v1.5) handtekening die berekend is over het (volgens h. opgemaakte en daarna gecanocaliseerde) <SignedInfo> element. Voor het opbouwen van deze handtekening wordt verwezen naar sectie 6.4.2 van XMLDSIG11;
j. het <X509Certificate> element moet worden gevuld met de Base64 codering van het DER-gecodeerde certificaat behorende bij de RSA-sleutel waarmee de <SignatureValue> is berekend (in dit geval het boordcomputercertificaat);
k. Alle canonicalisatie moet plaatsvinden conform 'Exclusive XML Canonicalization Version 1.0, 18 July 2002' (XML-EXC-C14N) met identifier http://www.w3.org/2001/10/xml-exc-c14n#;
l. Alle XSL transformaties moeten plaatsvinden conform 'XSL Transformations (XSLT) Version 1.0, 16 November 1999' (XSLT) met identifier http://www.w3.org/TR/1999/REC-xslt-19991116 en de daaraan gerelateerde standaard 'XML Path Language (XPath) Version 1.0, 16 November 1999' met identifier http://www.w3.org/TR/1999/REC-xpath-19991116;
m. Alle Base64 codering vindt in eerste instantie plaats op basis van de specificatie in XMLDSIG11;
n. Voorafgaand aan hashing en/of ondertekening van een XML node moet die node worden gecanonicaliseerd volgens XML-EXC-C14N en moet:
    1. elke text-node worden genormaliseerd volgens de XPath normalize-space functie;
    2. elke text-node die Base64 gecodeerd is bovendien worden ontdaan van alle resterende spaties conform de XPath functie translate(string, ' ', '').

De keuze van het algoritme voor de Digest en de Signature is afhankelijk van het certificaat op de kaart waarmee de handtekening wordt gezet. Als dit in de toekomst anders wordt dan SHA-256 respectievelijk RSA-SHA256' zullen de algoritmes voor Digest en Signature meeveranderen.

Artikel 2.8.2 Integriteit geregistreerde gegevens

Bepaalde gegevenssets, die door de boordcomputer taxi worden geregistreerd, dienen vanaf het moment van vastleggen de waarborg van integriteit en authenticiteit te bevatten. In de specificatie van elke soort gegevenslevering in artikel 3 t/m 8 wordt aangegeven welke gegevensset dit betreft, op welke momenten deze gegevensset met een elektronische handtekening worden ondertekend en als zodanig moeten worden vastgelegd en met welke private sleutel die ondertekening moet gebeuren.

Voor een gegevensset die bij vastleggen elektronisch ondertekend wordt, wordt een tekenbericht gegenereerd. Dit tekenbericht is, op enkele uitzonderingen na, gelijk aan het (corresponderende) XML exportbericht:

```
<?xml version="1.0" encoding="UTF-8"?>
<Envelope xmlns="urn:envelope">
  <Data xmlns="namespace van het XML Schema van de betreffende gegevenslevering"
Id="idData">
    <!-- opbouw conform XML Schema van de betreffende gegevenslevering -->
  </Data>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <!-- opbouw conform specificatie hieronder -->
  </Signature>
</Envelope>
```

Voor de namespace en de structuur van het betreffende <Data> element wordt verwezen naar de artikelen 3.4, 4.4, 6.4, 7.4, respectievelijk 8.4.

Ook het <Signature> element van het tekenbericht wijkt op slechts enkele onderdelen af van die van het XML exportbericht:

a. Het eerste <Reference> element heeft een andere URI, namelijk '#idData';
b. De inhoud van het <X509Certificate> element representeert, afhankelijk van het gestelde in de artikelen 3.1, 4.1, 6.1, 7.1, respectievelijk 8.1, ofwel het boordcomputercertificaat ofwel het chauffeurskaartcertificaat.

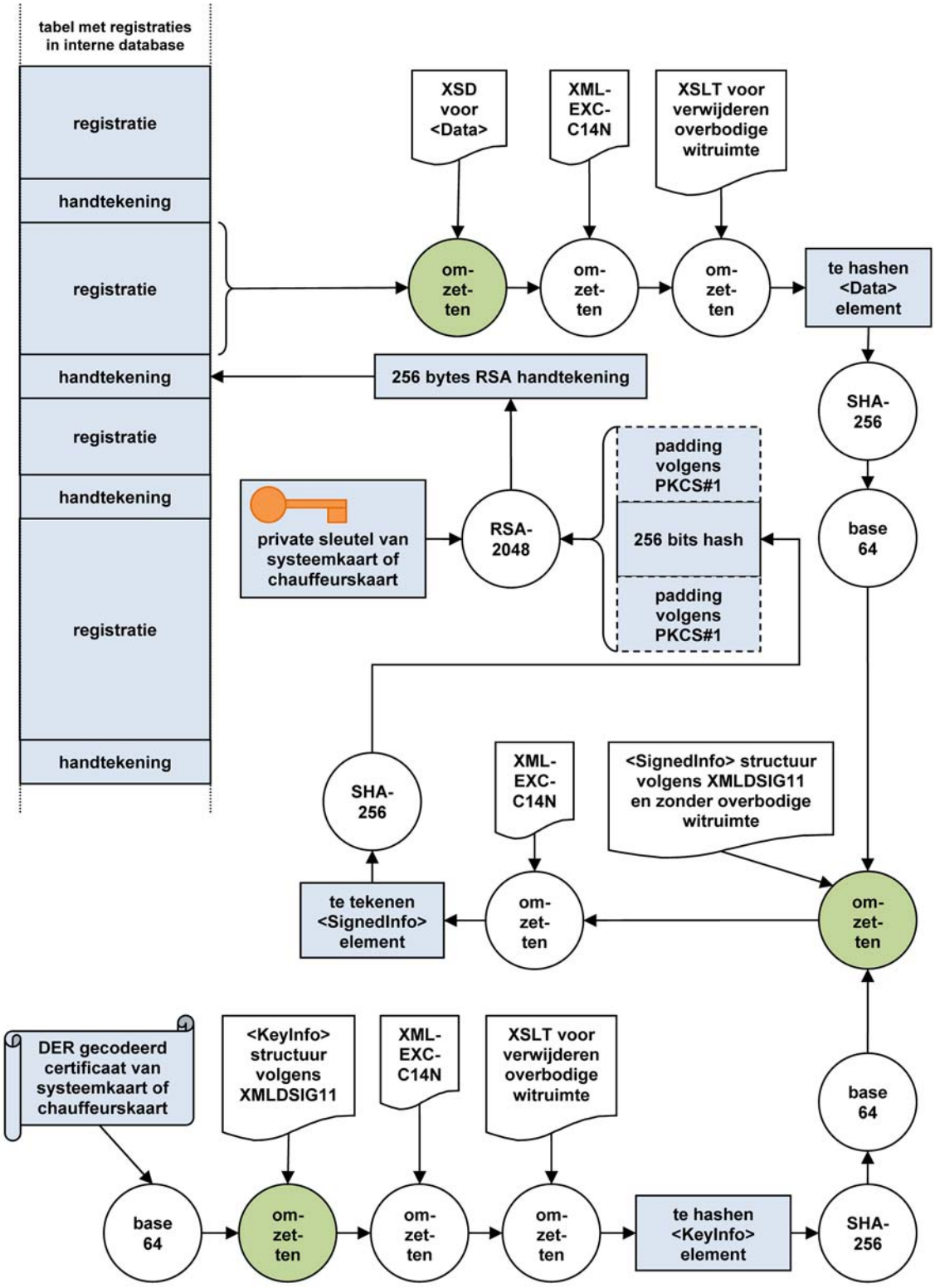
Na generatie van het tekenbericht wordt de waarde van het element <SignatureValue> als <Integriteit> element opgeslagen bij de gegevens waarover de elektronische handtekening is berekend. Het tekenbericht zelf hoeft niet te worden opgeslagen, zolang de getekende gegevens in de vorm waarin zij werden getekend kunnen worden gereproduceerd. Dat betekent dat de boordcomputer, behalve de gegevens die het <Data> element vormen, het certificaat dat voor ondertekening werd gebruikt, moet vastleggen.

Het genereren en vastleggen van de elektronische handtekening over het <Data> element vindt plaats bij het vastleggen van de gegevens die het <Data> element vormen.

Bij het samenstellen van een exportbericht worden de gegevens van het <Data> element onveranderd overgenomen uit de administratie op de boordcomputer. Het <Data> element wordt opnieuw geproduceerd, en moet exact gelijk zijn aan het <Data> element waarvoor een elektronische handtekening is berekend bij vastleggen van het gegeven. De geregistreerde elektronische handtekening moet worden overgenomen in het <Integriteit> element, het is niet toegestaan om de elektronische handtekening opnieuw te berekenen. Ook moet per <Integriteit> element het voor de betreffende handtekening gebruikte certificaat onveranderd worden overgenomen uit de administratie op de boordcomputer.

Artikel 2.8.3 Processchema's

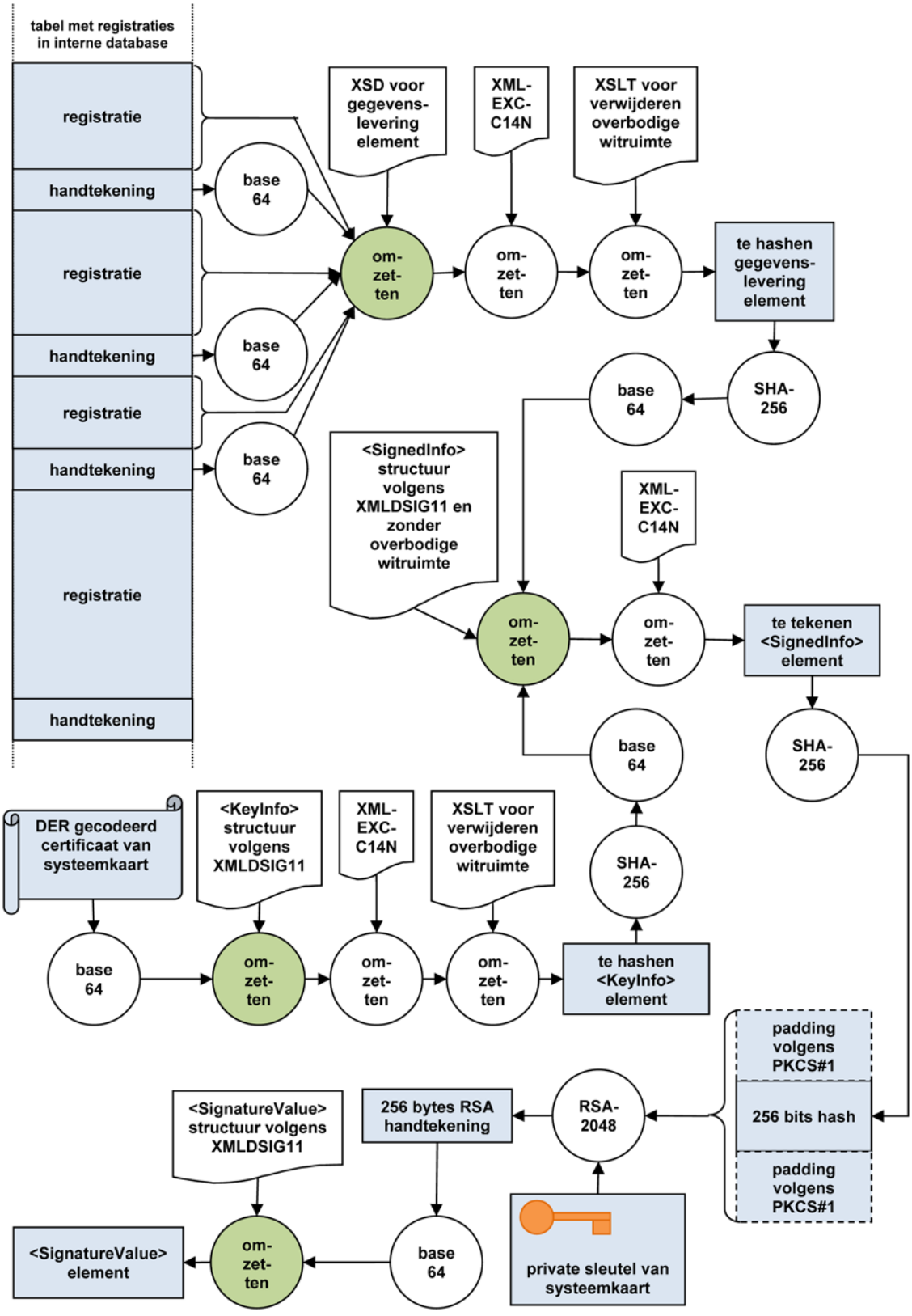
Een mogelijk proces voor samenstellen van de elementen voor een tekenbericht en het genereren van de elektronische handtekening over die elementen is weergegeven in figuur 2.



Figuur 2

Van de output van de groen gekleurde deelprocessen kan het tekenbericht (zonder <SignatureValue>) worden samengesteld. De 256-bytes RSA handtekening zou daarna gebruikt kunnen worden voor het completeren van het tekenbericht, maar moet in ieder geval worden gearchiveerd in de boordcomputer.

Figuur 3 geeft een mogelijk proces voor samenstellen van de elementen van een exportbericht weer. Het exportbericht kan worden geassembleerd met de output van de groen gekleurde deelprocessen.



Figuur 3

Artikel 2.9 Foutafhandeling

Bij het opvragen van de gegevensleveringen kunnen foutsituaties optreden. Hierbij kan onderscheid gemaakt worden tussen functionele fouten, technische fouten en niet volledige gegevens.

Artikel 2.9.1 Functionele fouten

Bij onderstaande foutsituaties moet de boordcomputer de bijbehorende foutmelding tonen:

Foutsituatie	Afhandeling
Boordcomputer is niet vergrendeld sinds laatste activering.	Verwerking gegevenslevering(en) stopt en de boordcomputer toont de melding 'Boordcomputer is niet vergrendeld sinds laatste activering'.
Er is geen externe gegevensdrager verbonden met de overbrengingsinterface van de boordcomputer als de gebruiker een gegevenslevering start.	Verwerking gegevenslevering(en) stopt en de boordcomputer toont de melding 'Geen externe gegevensdrager beschikbaar'.
'*Datumtijd begin periode*' bevat geen geldige waarde als de gebruiker een gegevenslevering start. 'Datumtijd begin periode' is verplicht.	Verwerking gegevenslevering(en) stopt en de boordcomputer toont de melding 'Datumtijd begin periode bevat geen geldige waarde'.
'*Datumtijd einde periode*' bevat geen geldige waarde als de gebruiker een gegevenslevering start. 'Datumtijd einde periode' mag leeg zijn.	Verwerking gegevenslevering(en) stopt en de boordcomputer toont de melding 'Datumtijd einde periode bevat geen geldige waarde'.
'*Datumtijd einde periode*' ligt voor '*Datumtijd begin periode*' als de gebruiker een gegevenslevering start.	Verwerking gegevenslevering(en) stopt en de boordcomputer toont de melding 'Datumtijd einde periode ligt voor Datumtijd begin periode'.
Overige functionele foutsituaties	Verwerking gegevenslevering stopt en de boordcomputer toont een foutmelding.

Artikel 2.9.2 Technische fouten

Foutsituatie	Afhandeling
Exporteren van een bericht naar de externe gegevensdrager gaat fout.	Verwerking gegevenslevering(en) stopt en de boordcomputer toont de melding 'Exporteren van een bericht naar de externe gegevensdrager is niet gelukt'.
Overige technische foutsituaties.	Verwerking gegevenslevering stopt en de boordcomputer toont een foutmelding.

Artikel 2.9.3 Onvolledige gegevens

Het niet volledig zijn van gegevens op de boordcomputer mag geen reden zijn om een resultaat bericht niet te exporteren.

Artikel 2.10 Overige kenmerken

Kenmerk	Invulling
Tekenset bericht	De Unicode tekensets 'Basic Latin', 'Latin-1 Supplement' en 'Latin Extended-A', alsmede de controle karakters tab, linefeed en carriage return karakters. Code points: U+0009, U+000A, U+000D, U+0020 t/m U+007E en U+00A0 t/m U+017F.
Codering bericht	UTF-8

Artikel 3 Ritadministratie

Artikel 3.1 Gegevens en functionele en technische berichtstructuur

Voor het bericht 'Ritadministratie' worden de volgende gegevens en functionele en technische berichtstructuur onderkend:

Entiteit / attribuut	XML element	Inhoud	G	C
BERICHT	Ritadministratie; Id="idGegevenslevering"	SEQ	V	1

Entiteit / attribuut	XML element	Inhoud	G	C
Datumtijd samenstellen bericht	DatTdSmBr	DT	V	1
KORTE IDENTIFICATIE BOORDCOMPUTER	KortIdBCT	SEQ	V	1
Goedkeuringsnummer	GdKrgsNr	S28 *)	V	1
Programmatuur versienummer	ProgVrNr	C50	V	1
PERIODE	Periode	SEQ	V	1
Datumtijd begin periode	DatTdBegPr	DT	V	1
Datumtijd einde periode	DatTdEndPr	DT	V	1
AUTO	Auto	SEQ	V	1
Kenteken	Kntkn	S6	V	1
CERTIFICAAT BOORDCOMPUTER	CertificaatBCT	SEQ	V	1
Publieke sleutel boordcomputer	PubliekeSleutel; codering="base64"	B *)	V	1
VERVOERDER	Vervoerder	SEQ	V	1..*
KvK-nummer	KvKnr	S12 *)	V	1
P-nummer	Pnr	S8 *)	V	1
ONDERNEMERSKAART	Ondernemerskaart	SEQ	V	1..*
Ondernemerskaart volgnummer	OkVgNr	S5 *)	V	1
RIT	Rit	SEQ	C	0..*
DATA	Data; Id="idData"	SEQ	V	1
Rit volgnummer	RtVgNr	I(1..∞)	V	1
Mutatiecode	MtCd	{'I', 'D', 'M'}	V	1
Datumtijd registratie	DatTdReg	DT	V	1
Type rit	Type	{'B', 'O'}	V	1
Coördinaat beginpunt rit	LocBeg	SEQ	V	1
Breedtegraad	Lat	D2.6(-90..+90)	V	1
Lengtegraad	Lon	D3.6(-180..+180)	V	1
Datumtijd begin rit	DatTdBeg	DT	V	1
Km stand begin rit	KmStdBeg	I8(0..MAX)	V	1
Coördinaat eindpunt rit	LocEnd	SEQ	C	0..1
Breedtegraad	Lat	D2.6(-90..+90)	V	1
Lengtegraad	Lon	D3.6(-180..+180)	V	1
Datumtijd einde rit	DatTdEnd	DT	C	0..1
Km stand einde rit	KmStdEnd	I8(0..MAX)	C	0..1
Ritprijs	Prijs	I(0..∞)	C	0..1
BESTUURDER	Bestuurder	SEQ	V	1
Chauffeursidentificatienummer	ChIdNr	S9 *)	V	1
Chauffeurskaart volgnummer	CkVgNr	S5 *)	V	1
INTEGRITEIT	Integriteit	SEQ	C	0..1
Elektronische handtekening boordcomputer	ElHdBc; codering="base64"	B	K	1
Elektronische handtekening fout	ElHdFout	S		
Datumtijd handtekening	DatTdHd	DT	V	1

Voor de legenda van het bovenstaande overzicht wordt verwezen naar artikel 10.

Toelichting:
a. De PERIODE is het tijdvak waarover de gebruiker de ritadministratie heeft opgevraagd.
b. RIT wordt per BESTUURDER uniek geïdentificeerd door een volgnummer.
c. Er zijn 2 mogelijke waarden voor 'Type rit': 'B' voor een beladen rit en 'O' voor een onbeladen rit.
d. De DATA van een RIT moet ondertekend worden met de elektronische handtekening van de boordcomputer om de integriteit van de ritgegevens achteraf te kunnen bepalen. Daartoe bevat INTEGRITEIT het attribuut 'Elektronische handtekening boordcomputer'. Indien bij het genereren van de handtekening een gebeurtenis met foutcode S005 of F008 optreedt, wordt, in plaats van de handtekening, deze foutcode geregistreerd in het attribuut 'Elektronische handtekening fout'.
e. De Ritprijs is in eurocenten.
f. Een kilometerstand wordt opgenomen als een geheel getal, afgerond of afgekapt op een hele kilometer.
g. Voor een RIT wordt de bestuurder opgenomen in het bericht.
h. Alleen als de chauffeurskaart niet beschikbaar is tijdens registratie van een RIT moet 'Chauffeurskaart volgnummer' van de BESTUURDER volledig gevuld worden met nullen.
i. De attributen 'Coördinaat eindpunt rit', 'Datumtijd einde rit', 'Km stand einde rit', 'Ritprijs' en de entiteit INTEGRITEIT zijn verplicht tenzij de RIT nog niet is beëindigd.
j. De mutatiecode van een RIT is 'I' als het volgnummer van de RIT voor de eerste keer wordt geregistreerd. De I staat voor Insert.
k. Annuleren van de laatste handmatig ingevoerde 'Aanvang rit' is mogelijk. Het te annuleren record bevat alleen gegevens van het begin van de rit ('Rit volgnummer', 'Mutatiecode', 'Datumtijd registratie', 'Type rit', 'Coördinaat beginpunt rit', 'Datumtijd begin rit' en 'Km stand begin rit'). Annuleren moet op de volgende manier worden aangegeven:
    1. De gegevens van het te annuleren record worden ongewijzigd ondertekend met de elektronische handtekening van de boordcomputer.
    2. Een nieuwe record wordt geregistreerd met de volgende gegevens: het volgnummer is gelijk aan het volgnummer van het te annuleren record uit k.1, mutatiecode is 'D', 'Datumtijd registratie' is het tijdstip van registreren van dit nieuwe record, en de waarden van de overige attributen zijn gelijk aan de waarden van de overeenkomstige attributen van het te annuleren record. Ook dit record moet ondertekend worden met de elektronische handtekening van de boordcomputer.
l. Annuleren van de laatste handmatig ingevoerde 'Einde rit' is mogelijk. Het te annuleren record bevat zowel gegevens van het begin van de rit ('Volgnummer', 'Mutatiecode', 'Datumtijd registratie', 'Type rit', 'Coördinaat beginpunt rit', 'Datumtijd begin rit' en 'Km stand begin rit') als einde van de rit ('Coördinaat einde rit', 'Datumtijd einde rit', 'Km stand einde rit', 'Ritprijs'). Annuleren moet op de volgende manier worden aangegeven:
    1. De gegevens van het te annuleren record worden ongewijzigd ondertekend met de elektronische handtekening van de boordcomputer als dit nog niet is gebeurd.
    2. Een nieuwe record wordt geregistreerd met de volgende gegevens: het volgnummer is gelijk aan het volgnummer van het te annuleren record uit l.1, mutatiecode is 'D', 'Datumtijd registratie' is het tijdstip van registreren van dit nieuwe record, en de waarden van de overige attributen zijn gelijk aan de waarden van de overeenkomstige attributen van het te annuleren record. Ook dit record moet ondertekend worden met de elektronische handtekening van de boordcomputer.
    3. Een volgend nieuw record wordt geregistreerd met de volgende gegevens: het volgnummer is gelijk aan het volgnummer van het te annuleren record uit l.1, mutatiecode is 'M', 'Datumtijd registratie' is het tijdstip van registreren van dit nieuwe record, de waarden van de attributen 'Type rit', 'Coördinaat begin rit', 'Datumtijd begin rit' en 'Km stand begin rit' zijn gelijk aan de waarden van de overeenkomstige attributen van het te annuleren record, en de attributen 'Coördinaat einde rit', 'Datumtijd einde rit', 'Km stand einde rit' en 'Ritprijs' zijn initieel leeg om gevuld te worden bij het opnieuw uitvoeren van de handmatige actie 'Einde rit'.
m. het attribuut 'Publieke sleutel boordcomputer' dient te worden gevuld met het gehele X509 certificaat van de boordcomputer.

Artikel 3.2 Ritadministratie.xsd

De onderstaande Ritadministratie.xsd wordt gebruikt.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- XML Schema definitie van de gegevenslevering Ritadministratie van
Boordcomputers Taxi -->
<!-- Naam: Ritadministratie.xsd -->
<!-- Eigenaar: Staat der Nederlanden, Ministerie van Infrastructuur en Milieu --
>
<!-- Versie: 2.0.1 -->
<!-- Datum: 1 september 2014 -->
<!-- Ingangdatum: 1 januari 2015 -->
<!-- Chameleon include: bcttypes.xsd -->
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://www.ritadministratie.org"
  targetNamespace="http://www.ritadministratie.org"
  id="bctRitadministratie"
  version="2.0.1"
  xml:lang="NL"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <xs:include schemaLocation="bcttypes.xsd"/>

  <xs:element name="Ritadministratie">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="DatTdSmBr" type="xs:dateTime"/>
        <xs:element name="KortIdBCT" type="KorteIdentiteitBoordcomputer"/>
        <xs:element name="Periode" type="PeriodeBeginEind"/>
        <xs:element name="Auto">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Kntkn" type="Kenteken"/>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="CertificaatBCT" type="X509Certificaat"/>
        <xs:element name="Vervoerder" maxOccurs="unbounded">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="KvKnr" type="KvKnummer"/>
              <xs:element name="Pnr" type="Pnummer"/>
              <xs:element name="Ondernemerskaart" maxOccurs="unbounded">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="OkVgNr"
type="OndernemerskaartVolgnummer"/>
                    <xs:element name="Rit" minOccurs="0" maxOccurs="unbounded">
                      <xs:complexType>
                        <xs:sequence>
                          <xs:element ref="Data"/>
                          <xs:element name="Integriteit"
type="ElektronischeHandtekeningBoordcomputer" minOccurs="0"/>
                        </xs:sequence>
                      </xs:complexType>
                    </xs:element>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
      <xs:attribute name="Id" type="xs:string" fixed="idGegevenslevering"/>
    </xs:complexType>
  </xs:element>

  <xs:element name="Data">
    <xs:complexType>
```

```
      <xs:sequence>
        <xs:element name="RtVgNr" type="xs:positiveInteger"/>
        <xs:element name="MtCd" type="MutatieCode"/>
        <xs:element name="DatTdReg" type="xs:dateTime"/>
        <xs:element name="Type" type="TypeRit"/>
        <xs:element name="LocBeg" type="Coordinaat"/>
        <xs:element name="DatTdBeg" type="xs:dateTime"/>
        <xs:element name="KmStdBeg" type="KmStand"/>
        <xs:element name="LocEnd" type="Coordinaat" minOccurs="0"/>
        <xs:element name="DatTdEnd" type="xs:dateTime" minOccurs="0"/>
        <xs:element name="KmStdEnd" type="KmStand" minOccurs="0"/>
        <xs:element name="Prijs" type="Bedrag" minOccurs="0"/>
        <xs:element name="Bestuurder" type="BestuurderBasisGegevens"/>
      </xs:sequence>
      <xs:attribute name="Id" type="xs:string" fixed="idData"/>
    </xs:complexType>
  </xs:element>

  <!-- Definities bericht specifieke datatypes -->

  <xs:simpleType name="MutatieCode">
    <xs:restriction base="xs:string">
      <xs:enumeration value="I">
        <xs:annotation>
          <xs:documentation>Insert</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="D">
        <xs:annotation>
          <xs:documentation>Delete</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="M">
        <xs:annotation>
          <xs:documentation>Mutatie</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="TypeRit">
    <xs:restriction base="xs:string">
      <xs:enumeration value="B">
        <xs:annotation>
          <xs:documentation>Beladen Rit</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="O">
        <xs:annotation>
          <xs:documentation>Onbeladen Rit</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="Coordinaat">
    <xs:sequence>
      <xs:element name="Lat" type="BreedteGraad"/>
      <xs:element name="Lon" type="LengteGraad"/>
    </xs:sequence>
  </xs:complexType>

  <xs:simpleType name="Bedrag">
    <xs:restriction base="xs:integer">
      <xs:minInclusive value="0"/>
    </xs:restriction>
  </xs:simpleType>

</xs:schema>
```

Voor de definitie van bcttypes.xsd wordt verwezen naar artikel 9.

Artikel 3.3 Volgorde gegevens

De geselecteerde ritten moeten gegroepeerd per vervoerder, en daarbinnen per ondernemerskaart, in oplopende volgorde van volgnummer worden opgenomen in de ritadministratie.

Artikel 3.4 Integriteit gegevens

Alle ritten worden ondertekend worden met een elektronische handtekening op basis van de private sleutel van de systeemkaart.

De ritadministratie bevat een element <Rit> en <Rit> bevat de elementen <Data> en <Integriteit>. Het <Data> element bevat de volgende ritgegevens:
a. RtVgNr
b. MtCd
c. DatTdReg
d. Type
e. LocBeg.Lat en LocBeg.Lon
f. DatTdBeg
g. KmStdBeg
h. LocEnd.Lat en LocEnd.Lon
i. DatTdEnd
j. KmStdEnd
k. Prijs
l. Bestuurder.ChIdNr
m. Bestuurder.CkVgNr

Het <Integriteit> element bevat de elektronische handtekening van het bijbehorende Data element.

Bij het samenstellen van de ritadministratie moeten de gegevens van het <Data> element onveranderd worden overgenomen uit de ritadministratie op de boordcomputer. Het berekenen van de 'Elektronische handtekening boordcomputer' van het <Data> element van een <Rit> wordt gedaan bij het beëindigen van de rit. De vastgelegde 'Elektronische handtekening boordcomputer' wordt per <Rit> onveranderd overgenomen in het onderliggende <Integriteit> element.

Artikel 3.5 Overige kenmerken

Artikel 3.5.1 Naamgeving

De naamgeving van de gegevenslevering 'Ritadministratie' is als volgt:

```
Ritadministratie_Kenteken-DatumtijdSamenstellenBericht_DatumtijdBeginPeriode
_DatumtijdEindePeriode.xml
```

Hierbij worden de cursief gedrukte gegevens gevuld met de corresponderende registratiewaarde. De volgende formaten worden hierbij gebruikt:

Gegeven	Formaat
Kenteken	Zoals opgenomen in de gegevenslevering zelf
DatumtijdSamenstellenBericht	CCYYMMDDHHMMSS
DatumtijdBeginPeriode	CCYYMMDDHHMM
DatumtijdEindePeriode	CCYYMMDDHHMM

Artikel 3.5.2 Berichtgrootte

Bij 100 ritten is het bericht 'ritadministratie' maximaal 100 Kbyte groot.

Artikel 4 Arbeids-, rij- en rusttijden

Artikel 4.1 Gegevens en functionele en technische berichtstructuur

Voor het bericht 'Arbeids-, rij- en rusttijden' worden de volgende gegevens en functionele en technische berichtstructuur onderkend:

Entiteit / attribuut	XML element	Inhoud	G	C
BERICHT	Arbeidstijden; Id="idGegevenslevering"	SEQ	V	1
Datumtijd samenstellen bericht	DatTdSmBr	DT	V	1
KORTE IDENTIFICATIE BOORDCOMPUTER	KortIdBCT	SEQ	V	1
Goedkeuringsnummer	GdKrgsNr	S28 *)	V	1
Programmatuur versienummer	ProgVrNr	C50	V	1
PERIODE	Periode	SEQ	V	1
Datumtijd begin periode	DatTdBegPr	DT	V	1
Datumtijd einde periode	DatTdEndPr	DT	V	1
AUTO	Auto	SEQ	V	1
Kenteken	Kntkn	S6	V	1
VERVOERDER	Vervoerder	SEQ	V	1..*
KvK-nummer	KvKnr	S12 *)	V	1
P-nummer	Pnr	S8 *)	V	1
ONDERNEMERSKAART	Ondernemerskaart	SEQ	C	0..*
Ondernemerskaart volgnummer	OkVgNr	S5 *)	V	1
BESTUURDER	Bestuurder	SEQ	C	0..*
Chauffeursidentificatienummer	ChIdNr	S9 *)	V	1
Chauffeurskaart volgnummer	CkVgNr	S5 *)	V	1
CERTIFICAAT	Certificaat	CHOICE	V	1
CERTIFICAAT CHAUFFEUR	CertificaatChauffeur	SEQ	K	1
Publieke sleutel chauffeur	PubliekeSleutel; codering="base64"	B *)	V	1
CERTIFICAAT BOORDCOMPUTER	CertificaatBCT	SEQ	K	1
Publieke sleutel boordcomputer	PubliekeSleutel; codering="base64"	B *)	V	1
ARBEIDSTIJD	Arbeidstijd	SEQ	C	0..*
DATA	Data; Id="idData"	SEQ	V	1
Arbeidstijd volgnummer	ArVgNr	I(1..∞)	V	
Datumtijd registratie	DatTdReg	DT	V	
Datumtijd begin arbeidstijd	DatTdBeg	DT	V	
Datumtijd einde arbeidstijd	DatTdEnd	DT	V	
onbenoemde keuze uit een van de volgende 3 attributen		CHOICE	C	0..*
RIJTIJD	Rijtijd	SEQ	C	0..1
Rijtijd volgnummer	RtVgNr	I(1..∞)	V	1
Datumtijd registratie	DatTdReg	DT	V	1
Datumtijd begin rijtijd	DatTdBeg	DT	V	1
Datumtijd einde rijtijd	DatTdEnd	DT	V	1

Entiteit / attribuut	XML element	Inhoud	G	C
PAUZE	Pauze	SEQ	C	0..1
Pauze volgnummer	PzVgNr	I(1..∞)	V	1
Mutatiecode	MtCd	{'I', 'D'}	V	1
Datumtijd registratie	DatTdReg	DT	V	1
Datumtijd begin pauze	DatTdBeg	DT	V	1
Datumtijd einde pauze	DatTdEnd	DT	V	1
ANDERE WERKZAAMHEDEN	AdrWrkzmhdn	SEQ	C	0..1
Andere werkzaamheden volgnummer	AwVgNr	I(1..∞)	V	1
Mutatiecode	MtCd	{'I', 'D'}	V	1
Datumtijd registratie	DatTdReg	DT	V	1
Datumtijd begin andere werkzaamhd.	DatTdBeg	DT	V	1
Datumtijd einde andere werkzaamhd.	DatTdEnd	DT	V	1
INTEGRITEIT	Integriteit	SEQ	V	1
Elektronische handtekening chauffeur	ElHdCh; codering="base64"	B	K	1
Elektronische handtekening boordcomputer	ElHdBc; codering="base64"	B		
Elektronische handtekening fout	ElHdFout	S		
Datumtijd handtekening	DatTdHd	DT	V	1

Voor de legenda van het bovenstaande overzicht wordt verwezen naar artikel 10.

Toelichting:

a. De PERIODE is het tijdvak waarover de gebruiker de ritadministratie heeft opgevraagd.
b. ARBEIDSTIJD wordt per BESTUURDER uniek geïdentificeerd door een volgnummer.
c. RIJTIJD wordt per BESTUURDER uniek geïdentificeerd door een volgnummer.
d. PAUZE wordt per BESTUURDER uniek geïdentificeerd door een volgnummer.
e. ANDERE WERKZAAMHEDEN wordt per BESTUURDER uniek geïdentificeerd door een volgnummer.
f. De DATA van ARBEIDSTIJD, inclusief bijbehorende voorkomens van RIJTIJD, PAUZE en ANDERE WERKZAAMHEDEN, moet ondertekend worden met een elektronische handtekening om de integriteit van de gegevens achteraf te kunnen bepalen. Indien de chauffeurskaart aanwezig is wordt getekend met de elektronische handtekening van de chauffeur, indien de chauffeurskaart niet aanwezig is wordt getekend met de elektronische handtekening van de boordcomputer. Indien bij het genereren van de handtekening een gebeurtenis met foutcode S005, S006, F008 of F009 optreedt, wordt, in plaats van de handtekening, deze foutcode geregistreerd in het attribuut 'Elektronische handtekening fout'.
g. De mutatiecode van een PAUZE of ANDERE WERKZAAMHEDEN is 'I' als het volgnummer van de PAUZE of ANDERE WERKZAAMHEDEN voor de eerste keer wordt geregistreerd. De I staat voor Insert.
h. Annuleren van de laatste handmatige actie is mogelijk. Voor PAUZE en ANDERE WERKZAAMHEDEN moet dit op volgende manier worden aangegeven:
    1. De bestaande PAUZE of ANDERE WERKZAAMHEDEN wordt niet gewijzigd.
    2. Een nieuwe PAUZE of ANDERE WERKZAAMHEDEN wordt geregistreerd met het volgnummer van de PAUZE of ANDERE WERKZAAMHEDEN die geannuleerd moet worden.
    3. Datumtijd registratie van de nieuwe PAUZE of ANDERE WERKZAAMHEDEN is het tijdstip van registratie van de nieuwe PAUZE of ANDERE WERKZAAMHEDEN.
    4. Mutatiecode van de nieuwe PAUZE of ANDERE WERKZAAMHEDEN is 'D' om aan te geven dat de PAUZE of ANDERE WERKZAAMHEDEN met dit specifieke volgnummer geannuleerd moet worden.
i. Ook in de taxivervoermodus zonder chauffeurskaart moeten ARBEIDSTIJD, RIJTIJD, PAUZE en ANDERE WERKZAAMHEDEN worden vastgelegd. Alle voorkomens van ARBEIDSTIJD, RIJTIJD, PAUZE en ANDERE WERKZAAMHEDEN die zijn vastgelegd zonder chauffeurskaart worden per VERVOERDER uitgeleverd voor een BESTUURDER met het handmatig ingegeven Chauffeursidentificatienummer en het Chauffeurskaart volgnummer gevuld met nullen.

j. Een bericht bevat per BESTUURDER de optionele attributen ‘Publieke sleutel chauffeur’ en ‘Publieke sleutel boordcomputer’ waarvan precies 1 attribuut verplicht gevuld moet worden. Als de BESTUURDER bekend is moet het attribuut ‘Publieke sleutel chauffeur’ gevuld worden met het gehele X509 handtekeningcertificaat van de chauffeur, als de bestuurder onbekend is moet het attribuut ‘Publieke sleutel boordcomputer’ gevuld worden met het gehele X509 certificaat van de boordcomputer.
k. Een bericht bevat per ARBEIDSTIJD de optionele attributen ‘Elektronische handtekening chauffeur’ en ‘Elektronische handtekening boordcomputer’ waarvan precies 1 attribuut verplicht gevuld moet worden. Als de bijbehorende BESTUURDER bekend is moet het attribuut ‘Elektronische handtekening chauffeur’ gevuld worden, als de bestuurder onbekend is moet het attribuut ‘Elektronische handtekening boordcomputer’ gevuld worden.

Artikel 4.2 Arbeidstijden.xsd

De onderstaande Arbeidstijden.xsd wordt gebruikt.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- XML Schema definitie van de gegevenslevering Arbeidstijden van
Boordcomputers Taxi -->
<!-- Naam: Arbeidstijden.xsd -->
<!-- Eigenaar: Staat der Nederlanden, Ministerie van Infrastructuur en Milieu --
>
<!-- Versie: 2.0.1 -->
<!-- Datum: 1 september 2014 -->
<!-- Ingangdatum: 1 januari 2015 -->
<!-- Chameleon include: bcttypes.xsd -->
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://www.arbeidstijden.org"
  targetNamespace="http://www.arbeidstijden.org"
  id="bctArbeidstijden"
  version="2.0.1"
  xml:lang="NL"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <xs:include schemaLocation="bcttypes.xsd"/>

  <xs:element name="Arbeidstijden">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="DatTdSmBr" type="xs:dateTime"/>
        <xs:element name="KortIdBCT" type="KorteIdentiteitBoordcomputer"/>
        <xs:element name="Periode" type="PeriodeBeginEind"/>
        <xs:element name="Auto">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Kntkn" type="Kenteken"/>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="Vervoerder" maxOccurs="unbounded">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="KvKnr" type="KvKnummer"/>
              <xs:element name="Pnr" type="Pnummer"/>
              <xs:element name="Ondernemerskaart" minOccurs="0"
maxOccurs="unbounded">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="OkVgNr"
type="OndernemerskaartVolgnummer"/>
                    <xs:element name="Bestuurder" minOccurs="0"
maxOccurs="unbounded">
                      <xs:complexType>
                        <xs:complexContent>
                          <xs:extension base="BestuurderBasisGegevens">
                            <xs:sequence>
                              <xs:element name="Certificaat">
                                <xs:complexType>
                                  <xs:choice>
                                    <xs:element name="CertificaatChauffeur"
type="X509Certificaat"/>
                                    <xs:element name="CertificaatBCT"
type="X509Certificaat"/>
                                  </xs:choice>
                                </xs:complexType>
                              </xs:element>
                              <xs:element name="Arbeidstijd" minOccurs="0"
maxOccurs="unbounded">
                                <xs:complexType>
                                  <xs:sequence>
```

```
                                    <xs:element ref="Data"/>
                                    <xs:element name="Integriteit"
type="ElektronischeHandtekeningChauffeurOfBoordcomputer"/>
                                  </xs:sequence>
                                </xs:complexType>
                              </xs:element>
                            </xs:sequence>
                          </xs:extension>
                        </xs:complexContent>
                      </xs:complexType>
                    </xs:element>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
      <xs:attribute name="Id" type="xs:string" fixed="idGegevenslevering"/>
    </xs:complexType>
  </xs:element>

  <xs:element name="Data">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="ArVgNr" type="xs:positiveInteger"/>
        <xs:element name="DatTdReg" type="xs:dateTime"/>
        <xs:element name="DatTdBeg" type="xs:dateTime"/>
        <xs:element name="DatTdEnd" type="xs:dateTime"/>
        <xs:choice minOccurs="0" maxOccurs="unbounded">
          <xs:element name="Rijtijd">
            <xs:complexType>
              <xs:sequence>
                <xs:element name="RtVgNr" type="xs:positiveInteger"/>
                <xs:element name="DatTdReg" type="xs:dateTime"/>
                <xs:element name="DatTdBeg" type="xs:dateTime"/>
                <xs:element name="DatTdEnd" type="xs:dateTime"/>
              </xs:sequence>
            </xs:complexType>
          </xs:element>
          <xs:element name="Pauze">
            <xs:complexType>
              <xs:sequence>
                <xs:element name="PzVgNr" type="xs:positiveInteger"/>
                <xs:element name="MtCd" type="MutatieCode"/>
                <xs:element name="DatTdReg" type="xs:dateTime"/>
                <xs:element name="DatTdBeg" type="xs:dateTime"/>
                <xs:element name="DatTdEnd" type="xs:dateTime"/>
              </xs:sequence>
            </xs:complexType>
          </xs:element>
          <xs:element name="AdrWrkzmhdn">
            <xs:complexType>
              <xs:sequence>
                <xs:element name="AwVgNr" type="xs:positiveInteger"/>
                <xs:element name="MtCd" type="MutatieCode"/>
                <xs:element name="DatTdReg" type="xs:dateTime"/>
                <xs:element name="DatTdBeg" type="xs:dateTime"/>
                <xs:element name="DatTdEnd" type="xs:dateTime"/>
              </xs:sequence>
            </xs:complexType>
          </xs:element>
        </xs:choice>
      </xs:sequence>
      <xs:attribute name="Id" type="xs:string" fixed="idData"/>
    </xs:complexType>
  </xs:element>

  <!-- Definities bericht specifieke datatypes -->
```

```
  <xs:simpleType name="MutatieCode">
    <xs:restriction base="xs:string">
      <xs:enumeration value="I">
        <xs:annotation>
          <xs:documentation>Insert</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="D">
        <xs:annotation>
          <xs:documentation>Delete</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
    </xs:restriction>
  </xs:simpleType>

</xs:schema>
```

Artikel 4.3 Volgorde gegevens

De geselecteerde arbeidstijden moeten gegroepeerd per vervoerder, en daarbinnen per ondernemerskaart, en daarbinnen per bestuurder in oplopende volgorde van volgnummer worden opgenomen. Binnen een arbeidstijd moeten de rijtijd, pauze en andere werkzaamheden elk in oplopende volgorde van volgnummer worden opgenomen.

Artikel 4.4 Integriteit gegevens

Alle arbeidstijden worden ondertekend met een elektronische handtekening. Voor het plaatsen van de elektronische handtekening wordt gebruik gemaakt van de private sleutel van de chauffeurskaart indien deze aanwezig is, en van de private sleutel van de systeemkaart indien de chauffeurskaart niet aanwezig is.

De 'Arbeids-, rij- en rusttijden' bevat een element <Arbeidstijd> en <Arbeidstijd> bevat de elementen <Data> en <Integriteit>. Het <Data> element bevat de volgende arbeidstijd gegevens:

a. ArVgNr
b. DatTdReg
c. DatTdBeg
d. DatTdEnd
e. Rijtijd
f. RtVgNr
g. DatTdReg
h. DatTdBeg
i. DatTdEnd
j. Pauze
k. PzVgNr
l. MtCd
m. DatTdReg
n. DatTdBeg
o. DatTdEnd
p. AdrWrkzmhdn
q. AwVgNr
r. MtCd
s. DatTdReg
t. DatTdBeg
u. DatTdEnd

Het <Integriteit> element bevat de elektronische handtekening chauffeur of elektronische handtekening boordcomputer van het bijbehorende <Data> element.

Bij het samenstellen van bericht 'Arbeids-, rij- en rusttijden' moeten de gegevens van het <Data> element onveranderd worden overgenomen uit de boordcomputer. Het berekenen van de 'Elektronische handtekening chauffeur' of 'Elektronische handtekening boordcomputer' van het <Data> element moet gebeuren bij het beëindigen van een arbeidstijd. De vastgelegde 'Elektronische handtekening chauffeur' of 'Elektronische handtekening boordcomputer' moeten per arbeidstijd onveranderd worden overgenomen in het onderliggende <Integriteit> element.

Artikel 4.5 Overige kenmerken

Artikel 4.5.1 Naamgeving

De naamgeving van de gegevenslevering 'Arbeidstijd' is als volgt:

```
Arbeidstijd_Kenteken-DatumtijdSamenstellenBericht_DatumtijdBeginPeriode
_DatumtijdEindePeriode.xml
```

Hierbij worden de cursief gedrukte gegevens gevuld met de corresponderende registratiewaarde. De volgende formaten worden hierbij gebruikt:

Gegeven	Formaat
Kenteken	Zoals opgenomen in de gegevenslevering zelf
DatumtijdSamenstellenBericht	CCYYMMDDHHMMSS
DatumtijdBeginPeriode	CCYYMMDDHHMM
DatumtijdEindePeriode	CCYYMMDDHHMM

Artikel 4.5.2 Berichtgrootte

Bij 100 arbeidstijden is het bericht 'arbeidstijd' maximaal 120 Kbyte groot.

Artikel 5 Coördinaten

Artikel 5.1 Gegevens en functionele en technische berichtstructuur

Voor het bericht 'Coördinaten' worden de volgende gegevens en functionele en technische berichtstructuur onderkend:

Entiteit / attribuut	XML element	Inhoud	G	C
BERICHT	Arbeidstijden; Id="idGegevenslevering"	SEQ	V	1
Datumtijd samenstellen bericht	DatTdSmBr	DT	V	1
KORTE IDENTIFICATIE BOORDCOMPUTER	KortIdBCT	SEQ	V	1
Goedkeuringsnummer	GdKrgsNr	S28 *)	V	1
Programmatuur versienummer	ProgVrNr	C50	V	1
PERIODE	Periode	SEQ	V	1
Datumtijd begin periode	DatTdBegPr	DT	V	1
Datumtijd einde periode	DatTdEndPr	DT	V	1
AUTO	Auto	SEQ	V	1..2
Kenteken	Kntkn	S6	V	1
VERVOERDER	Vervoerder	SEQ	V	1..*
KvK-nummer	KvKnr	S12 *)	V	1
P-nummer	Pnr	S8 *)	V	1
ONDERNEMERSKAART	Ondernemerskaart	SEQ	V	1..*
Ondernemerskaart volgnummer	OkVgNr	S5 *)	V	1
COORDINAAT	COORD	SEQ	C	0..*
Coördinaat volgnummer	VgNr	I(1..∞)	V	1
Datumtijd registratie	Dt	DT	V	1
Breedtegraad	Lat	D2.6(-90..+90)	V	1
Lengtegraad	Lon	D3.6(-180..+180)	V	1

Entiteit / attribuut						XML element	Inhoud	G	C
					Werkingsmodus	Md	{'O', 'C', 'B', 'K'}	V	1
					Werkingsniveau	Nv	{'T', 'A', 'B'}	C	0..1

Voor de legenda van het bovenstaande overzicht wordt verwezen naar artikel 10.

Toelichting:
a. De PERIODE is het tijdvak waarover de gebruiker de coördinaten heeft opgevraagd.
b. COORDINAAT wordt per VERVOERDER uniek geïdentificeerd door een volgnummer.
c. In werkingsmodus 'Operationele modus' is het attribuut 'Werkingsniveau' verplicht.
d. Alle coördinaten met een datumtijd registratie die ligt voor het tijdstip van de laatste activering van de boordcomputer worden gegroepeerd bij dezelfde AUTO – VERVOERDER – ONDERNEMERS-KAART combinatie waarbij 'Kenteken', 'KvK-nummer', 'P-nummer' en 'Ondernemerskaart volgnummer' worden gevuld met de lege string ('').
e. Alle coördinaten die zijn geregistreerd na het tijdstip van de laatste activering worden geleverd met het kenteken van de auto, het KvK-nummer en P-nummer van de vervoerder en het volgnummer van de ondernemerskaart waarvoor de coördinaten zijn geregistreerd.
f. Alleen de werkingsmodus 'Operationele Modus' kent meerdere werkingsniveaus. Bij de overige modi wordt werkingsniveau 'Basis' aangehouden.

Artikel 5.2 Coordinaten.xsd

De onderstaande Coordinaten.xsd wordt gebruikt.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- XML Schema definitie van de gegevenslevering Coordinaten van Boordcomputers
Taxi -->
<!-- Naam: Coordinaten.xsd -->
<!-- Eigenaar: Staat der Nederlanden, Ministerie van Infrastructuur en Milieu --
>
<!-- Versie: 2.0.0 -->
<!-- Datum: 1 augustus 2014 -->
<!-- Ingangdatum: 1 januari 2015 -->
<!-- Chameleon include: bcttypes.xsd -->
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://www.coordinaten.org"
  targetNamespace="http://www.coordinaten.org"
  id="bctCoordinaten"
  version="2.0.0"
  xml:lang="NL"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <xs:include schemaLocation="bcttypes.xsd"/>

  <xs:element name="Coordinaten">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="DatTdSmBr" type="xs:dateTime"/>
        <xs:element name="KortIdBCT" type="KorteIdentiteitBoordcomputer"/>
        <xs:element name="Periode" type="PeriodeBeginEind"/>
        <xs:element name="Auto" maxOccurs="2">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Kntkn" type="Kenteken"/>
              <xs:element name="Vervoerder" maxOccurs="unbounded">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="KvKnr" type="KvKnummer"/>
                    <xs:element name="Pnr" type="Pnummer"/>
                    <xs:element name="Ondernemerskaart" maxOccurs="unbounded">
                      <xs:complexType>
                        <xs:sequence>
                          <xs:element name="OkVgNr"
type="OndernemerskaartVolgnummer"/>
                          <xs:element name="COORD" minOccurs="0"
maxOccurs="unbounded">
                            <xs:complexType>
                              <xs:sequence>
                                <xs:element name="VgNr"
type="xs:positiveInteger"/>
                                <xs:element name="Dt"
type="DatumTijdRegistratie"/>
                                <xs:element name="Lat" type="BreedteGraad"/>
                                <xs:element name="Lon" type="LengteGraad"/>
                                <xs:element name="Md" type="Werkingsmodus"/>
                                <xs:element name="Nv" type="Werkingsniveau"
minOccurs="0"/>
                              </xs:sequence>
                            </xs:complexType>
                          </xs:element>
                        </xs:sequence>
                      </xs:complexType>
                    </xs:element>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
```

```
      <xs:attribute name="Id" type="xs:string" fixed="idGegevenslevering"/>
    </xs:complexType>
  </xs:element>

  <!-- Definities bericht specifieke datatypes -->

  <xs:simpleType name="DatumTijdRegistratie">
    <xs:restriction base="xs:dateTime"/>
  </xs:simpleType>

</xs:schema>
```

Artikel 5.3 Volgorde gegevens

De geselecteerde coördinaten moeten gegroepeerd per kenteken, en daarbinnen per vervoerder, en daarbinnen per ondernemerskaart, in oplopende volgorde van volgnummer, in het bericht worden opgenomen.

Artikel 5.4 Integriteit gegevens

Het bericht 'Coördinaten' wordt ondertekend met een elektronische handtekening van de boordcomputer. De afzonderlijke coördinaten worden niet ondertekend.

Artikel 5.5 Overige kenmerken

Artikel 5.5.1 Naamgeving

De naamgeving van de gegevenslevering 'Coördinaten' is als volgt:

```
Coordinaten_Kenteken-DatumtijdSamenstellenBericht_DatumtijdBeginPeriode
_DatumtijdEindePeriode.xml
```

Hierbij worden de cursief gedrukte gegevens gevuld met de corresponderende registratiewaarde. De volgende formaten worden hierbij gebruikt:

Gegeven	Formaat
Kenteken	Het kenteken van de auto waarin de boordcomputer als laatste is geactiveerd.
DatumtijdSamenstellenBericht	CCYYMMDDHHMMSS
DatumtijdBeginPeriode	CCYYMMDDHHMM
DatumtijdEindePeriode	CCYYMMDDHHMM

Artikel 5.5.2 Berichtgrootte

Een bericht 'Coördinaten' bevat maximum 1.440 coördinaten per dag, wanneer de auto continu rijdt en 1 coördinaat per minuut wordt vastgelegd. Voor de periode van een dag geeft dat een bericht van maximaal 236 Kbyte. Per jaar is het bericht 'Coördinaten' maximaal 84 Mbyte groot.

Artikel 6 Gebeurtenis

Artikel 6.1 Gegevens en functionele en technische berichtstructuur

Voor het bericht 'Gebeurtenis' worden de volgende gegevens en functionele en technische berichtstructuur onderkend:

Entiteit / attribuut	XML element	Inhoud	G	C
BERICHT	Gebeurtenis; Id="idGegevenslevering"	SEQ	V	1
Datumtijd samenstellen bericht	DatTdSmBr	DT	V	1
KORTE IDENTIFICATIE BOORDCOMPUTER	KortIdBCT	SEQ	V	1
Goedkeuringsnummer	GdKrgsNr	S28 *)	V	1

Entiteit / attribuut	XML element	Inhoud	G	C
Programmatuur versienummer	ProgVrNr	C50	V	1
PERIODE	Periode	SEQ	V	1
Datumtijd begin periode	DatTdBegPr	DT	V	1
Datumtijd einde periode	DatTdEndPr	DT	V	1
AUTO	Auto	SEQ	V	1
Kenteken	Kntkn	S6	V	1
CERTIFICAAT BOORDCOMPUTER	CertificaatBCT	SEQ	K	1
Publieke sleutel boordcomputer	PubliekeSleutel; codering=”base64”	B *)	V	1
VERVOERDER	Vervoerder	SEQ	V	1..*
KvK-nummer	KvKnr	S12 *)	V	1
P-nummer	Pnr	S8 *)	V	1
ONDERNEMERSKAART	Ondernemerskaart	SEQ	V	1..*
Ondernemerskaart volgnummer	OkVgNr	S5 *)	V	1
GEBEURTENIS	Gbrtns	SEQ	C	0..*
DATA	Data	SEQ	V	1
Gebeurtenis volgnummer	GbVgNr	I(1..∞)	V	1
Code	Code	S4	V	1
Datumtijd registratie	DatTdReg	DT	V	1
Km stand	KmStd	I8(0..MAX)	V	1
Status rijden auto	StRdnAt	{‘R’, ‘S’}	V	1
Werkingsmodus	WrkngsMds	{‘O’, ‘C’, ‘B’, ‘K’}	V	1
Werkingsniveau	WrkngsNv	{‘T’, ‘A’, ‘B’}	V	1
Aanvullende relevante informatie	AanvInfo	S100	O	0..1
BESTUURDER	Bestuurder	SEQ	C	0..1
Chauffeursidentificatienummer	ChIdNr	S9 *)	V	1
Chauffeurskaart volgnummer	CkVgNr	S5 *)	V	1
INTEGRITEIT	Integriteit	SEQ	V	1
Elektronische handtekening boordcomputer	ElHdBc; codering=”base64”	B	K	1
Elektronische handtekening fout	ElHdFout	S		
Datumtijd handtekening	DatTdHd	DT	V	1

Voor de legenda van het bovenstaande overzicht wordt verwezen naar artikel 10.

Toelichting:
a. de PERIODE is het tijdvak waarover de gebruiker de gebeurtenissen heeft opgevraagd.
b. GEBEURTENIS wordt per VERVOERDER uniek geïdentificeerd door een volgnummer.
c. BESTUURDER is verplicht als tijdens het optreden van de gebeurtenis de werkingsmodus ‘Operationele Modus’ actief is in het werkingsniveau ‘Arbeidstijd’ of ‘Taxivervoer’.
d. Alleen de werkingsmodus ‘Operationele Modus’ kent meerdere werkingsniveaus. Bij de overige modi wordt werkingsniveau ‘Basis’ aangehouden.
e. De DATA van een GEBEURTENIS moet ondertekend worden met de elektronische handtekening van de boordcomputer om de integriteit van de gegevens achteraf te kunnen bepalen. Daartoe bevat INTEGRITEIT het attribuut ‘Elektronische handtekening boordcomputer’. Indien bij het genereren van de handtekening een gebeurtenis met foutcode S005 of F008 optreedt, wordt, in

plaats van de handtekening, deze foutcode geregistreerd in het attribuut 'Elektronische handtekening fout'.

f. Het attribuut 'Status rijden auto' wordt ingevuld op basis van gegevens van de verplaatsingsopnemer.
g. Een kilometerstand wordt opgenomen als een geheel getal, afgerond of afgekapt op een hele kilometer.
h. Door het vullen van het attribuut 'Aanvullende relevante informatie' kan waar relevant aanvullende informatie worden toegevoegd voor een bepaalde code.
i. Indien er geen bestuurder actief is tijdens registratie van een gebeurtenis moet BESTUURDER niet worden opgenomen in de registratie.
j. Alleen als er een bestuurder actief, maar de chauffeurskaart niet beschikbaar is tijdens registratie van een GEBEURTENIS moet 'Chauffeurskaart volgnummer' van de BESTUURDER gevuld worden met nullen.
k. Het attribuut 'Publieke sleutel boordcomputer' dient te worden gevuld met het gehele X509 certificaat van de boordcomputer.

Artikel 6.2 Gebeurtenis.xsd

De onderstaande Gebeurtenis.xsd wordt gebruikt.

```
        <xs:element name="WrkngsNv" type="Werkingsniveau" />
        <xs:element name="AanvInfo" type="AanvullendeRelevanteInfo"
minOccurs="0"/>
        <xs:element name="Bestuurder" type="BestuurderBasisGegevens"
minOccurs="0"/>
      </xs:sequence>
      <xs:attribute name="Id" type="xs:string" fixed="idData"/>
    </xs:complexType>
  </xs:element>

  <!-- Definities bericht specifieke datatypes -->

  <xs:complexType name="Gebeurtenis">
    <xs:sequence>
      <xs:element ref="Data"/>
      <xs:element name="Integriteit"
type="ElektronischeHandtekeningBoordcomputer"/>
    </xs:sequence>
  </xs:complexType>

  <xs:simpleType name="Code">
    <xs:restriction base="xs:string">
      <xs:length value="4"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="StatusRijdenAuto">
    <xs:restriction base="xs:string">
      <xs:enumeration value="R">
        <xs:annotation>
          <xs:documentation>Rijden</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="S">
        <xs:annotation>
          <xs:documentation>Stilstaan</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="AanvullendeRelevanteInfo">
    <xs:restriction base="xs:string">
      <xs:maxLength value="100"/>
    </xs:restriction>
  </xs:simpleType>

</xs:schema>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- XML Schema definitie van de gegevenslevering Gebeurtenis van Boordcomputers
Taxi -->
<!-- Naam: Gebeurtenis.xsd -->
<!-- Eigenaar: Staat der Nederlanden, Ministerie van Infrastructuur en Milieu --
>
<!-- Versie: 2.0.1 -->
<!-- Datum: 1 september 2014 -->
<!-- Ingangdatum: 1 januari 2015 -->
<!-- Chameleon include: bcttypes.xsd -->
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://www.gebeurtenis.org"
  targetNamespace="http://www.gebeurtenis.org"
  id="bctGebeurtenis"
  version="2.0.1"
  xml:lang="NL"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <xs:include schemaLocation="bcttypes.xsd"/>

  <xs:element name="Gebeurtenis">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="DatTdSmBr" type="xs:dateTime"/>
        <xs:element name="KortIdBCT" type="KorteIdentiteitBoordcomputer"/>
        <xs:element name="Periode" type="PeriodeBeginEind"/>
        <xs:element name="Auto">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Kntkn" type="Kenteken"/>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="CertificaatBCT" type="X509Certificaat"/>
        <xs:element name="Vervoerder" maxOccurs="unbounded">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="KvKnr" type="KvKnummer"/>
              <xs:element name="Pnr" type="Pnummer"/>
              <xs:element name="Ondernemerskaart" maxOccurs="unbounded">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="OkVgNr"
type="OndernemerskaartVolgnummer"/>
                    <xs:element name="Gbrtns" type="Gebeurtenis" minOccurs="0"
maxOccurs="unbounded"/>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
      <xs:attribute name="Id" type="xs:string" fixed="idGegevenslevering"/>
    </xs:complexType>
  </xs:element>

  <xs:element name="Data">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="GbVgNr" type="xs:positiveInteger"/>
        <xs:element name="Code" type="Code"/>
        <xs:element name="DatTdReg" type="xs:dateTime"/>
        <xs:element name="KmStd" type="KmStand"/>
        <xs:element name="StRdnAt" type="StatusRijdenAuto"/>
        <xs:element name="WrkngsMds" type="Werkingsmodus"/>
```

Artikel 6.3 Volgorde gegevens

De geselecteerde gebeurtenissen moeten gegroepeerd per vervoerder, en daarbinnen per ondernemerskaart, in oplopende volgorde van volgnummer, in het bericht worden opgenomen.

Artikel 6.4 Integriteit gegevens

Alle gebeurtenissen worden ondertekend op basis van de private sleutel van de boordcomputer.

Het bericht Gebeurtenis bevat een element <Gebeurtenis> en het element <Gebeurtenis> bevat de elementen <Data> en <Integriteit>. Het <Data> element bevat de volgende gegevens:
a. GbVgNr
b. Code
c. DatTdReg
d. KmStd
e. StRdnAt
f. WrkngsMds
g. WrkngsNv
h. AanvInfo
i. Bestuurder.ChIdNr
j. Bestuurder.CkVgNr

Het <Integriteit> element bevat de elektronische handtekening boordcomputer van het bijbehorende <Data> element.

Bij het samenstellen van het bericht 'Gebeurtenis' moeten de gegevens van het <Data> element onveranderd worden overgenomen uit de administratie op de boordcomputer. Het berekenen van de 'Elektronische handtekening boordcomputer' van het Data element van een Rit moet gebeuren bij het optreden van de gebeurtenis. De vastgelegde 'Elektronische handtekening boordcomputer' moet per gebeurtenis onveranderd worden overgenomen in het onderliggende <Integriteit> element.

Artikel 6.5 Codetabel

In de onderstaande tabel staat de in het bericht op te nemen code per gebeurtenis vermeld.

Code	Omschrijving
S001	een storing in de werking van de registratiefuntie
S002	een storing in de werking van de beveiligingsfuncties
S003	een storing in de werking van de sensoren
S004	een storing in de overbrenging van gegevens naar een externe interface zoals beschreven in deze bijlage
S005	een storing in de werking van de systeemkaart
S006	een storing in de werking van de boordcomputerkaart
S007 t/m S999	gereserveerd voor overheidsdoeleinden
F001	een integriteitsfout in de uitvoercode
F002	een integriteistfout in de systeemgegevens
F003	een integriteitfout in de opgeslagen gebruikersgegevens
F004	een integriteitfout bij de gegevensuitvoer naar de chauffeurskaart
F005	een fout in de registratiefunctie
F006	een fout die de beveiliging van de boordcomputer in gevaar brengen
F007	een fout bij de gegevensuitvoer naar externe inrichtingen
F008	een fout bij het gebruik van de systeemkaart
F009	een fout bij het gebruik van de boordcomputerkaart
F010	een fout in de bewegingsensor
F011	een fout in de positiebepalingsensor
F012	een fout in de koppeling met de taxameter
F013 t/m F999	gereserveerd voor overheidsdoeleinden
M001	het aanzetten van de boordcomputer
M002	het uitzetten van de boordcomputer
M003	het inbrengen van een boordcomputerkaart
M004	het uitnemen van een boordcomputerkaart
M005	het inbrengen van een ongeldige boordcomputerkaart
M006	het inbrengen van een chauffeurskaart waarvan blijkt dat de datum en het tijdstip van de laatste registratie op de chauffeurskaart, op een later tijdstip valt dan de actuele datum en het tijdstip van de boordcomputer
M007	het niet op een juiste wijze afsluiten van een kaartsessie
M008	het inbrengen van een chauffeurskaart waarvan blijkt dat de laatste kaartsessie niet juist is afgesloten
M009	het ontstaan van onvoldoende opslagcapaciteit op het geheugen van de boordcomputer

Code	Omschrijving
M010	het verdwijnen van onvoldoende opslagcapaciteit op het geheugen van de boordcomputer
M011	het ontstaan van onvoldoende opslagcapaciteit op de chauffeurskaart
M012	het verdwijnen van onvoldoende opslagcapaciteit op de chauffeurskaart
M013	het ontstaan van een onderbreking van ten minste 5 seconden in de stroomvoorziening van de boordcomputer
M014	het verdwijnen van een onderbreking van ten minste 5 seconden in de stroomvoorziening van de boordcomputer
M015	het begin van een periode waarin de contactgeschakelde voedingsbron is uitgeschakeld in de toestand rijden
M016	het einde van een periode waarin de contactgeschakelde voedingsbron is uitgeschakeld in de toestand rijden
M017	het optreden van een toestand verplaatsen zonder dat er sprake is van een toestand rijden
M019	het begin van het niet kunnen verkrijgen van positiegegevens gedurende 5 minuten
M020	het einde van het niet kunnen verkrijgen van positiegegevens gedurende 5 minuten
M021	een afwijking van meer dan twee procent tussen de, met behulp van bewegingsgegevens van de bewegingsopnemer en de constante van de boordcomputer, berekende afstand en de werkelijke afstand
M022	een afwijking van meer dan vijf procent tussen de berekende afstand op basis van gegevens van de bewegingsopnemer en positiebepalingsensor
M023	het overbrengen van gegevens inclusief de naam van de externe interface
M024	gebeurtenissen die kunnen duiden op het in gevaar brengen van de beveiliging van de boordcomputer
M025	het activeren van de boordcomputer
M026	het keuren van de boordcomputer
M027	het deactiveren van de boordcomputer
M028	het inschakelen van een bedrijfsvergrendeling van de boordcomputer
M029	inschakelen van een werkingsmodus inclusief naam werkingsmodus
M030	het uitschakelen van een werkingsmodus inclusief naam werkingsmodus
M031	het begin van rijden in de operationele modus werkingsniveau taxivervoer zonder chauffeurskaart
M032	het einde van rijden in de operationele modus werkingsniveau taxivervoer zonder chauffeurskaart
M033	het detecteren van een niet-succesvolle authenticatiepoging
M034	installeren van een programmatuurrevisie
M035	starten van audit- en beveiligingsfuncties
M036	stoppen van audit- en beveiligingsfuncties
M037	het uitblijven of weigeren van een elektronische handtekening
M038	niet-geautoriseerde wijziging in de configuratie van de boordcomputer
M039	toegang tot het gebeurtenissenlogboek
M040 t/m M999	gereserveerd voor overheidsdoeleinden

Een fabrikant is vrij om voor eigen doeleinden codes aan de bovenstaande reeks toe te voegen. Elke code moet bestaan uit een hoofdletter gevolgd door drie cijfers.

Artikel 6.6 Overige kenmerken

Artikel 6.6.1 Naamgeving

De naamgeving van de gegevenslevering 'Gebeurtenis' is als volgt:

```
Gebeurtenis_Kenteken-DatumtijdSamenstellenBericht_DatumtijdBeginPeriode
_DatumtijdEindePeriode.xml
```

Hierbij worden de cursief gedrukte gegevens gevuld met de corresponderende registratiewaarde. De volgende formaten worden hierbij gebruikt:

Gegeven	Formaat
Kenteken	Zoals opgenomen in de gegevenslevering zelf
DatumtijdSamenstellenBericht	CCYYMMDDHHMMSS
DatumtijdBeginPeriode	CCYYMMDDHHMM
DatumtijdEindePeriode	CCYYMMDDHHMM

Artikel 6.6.2 Berichtgrootte

Bij 100 gebeurtenissen is het bericht 'Gebeurtenis' maximaal 100 Kbyte groot.

Artikel 7 Onderzoek

Artikel 7.1 Gegevens en functionele en technische berichtstructuur

Voor het bericht 'Onderzoek' worden de volgende gegevens en functionele en technische berichtstructuur onderkend:

Entiteit / attribuut	XML element	Inhoud	G	C
BERICHT	Onderzoek; Id="idGegevenslevering"	SEQ	V	1
Datumtijd samenstellen bericht	DatTdSmBr	DT	V	1
KORTE IDENTIFICATIE BOORDCOMPUTER	KortIdBCT	SEQ	V	1
Goedkeuringsnummer	GdKrgsNr	S28 *)	V	1
Programmatuur versienummer	ProgVrNr	C50	V	1
PERIODE	Periode	SEQ	V	1
Datumtijd begin periode	DatTdBegPr	DT	V	1
Datumtijd einde periode	DatTdEndPr	DT	V	1
AUTO	Auto	SEQ	V	1
Kenteken	Kntkn	S6	V	1
CERTIFICAAT BOORDCOMPUTER	CertificaatBCT	SEQ	K	1
Publieke sleutel boordcomputer	PubliekeSleutel; codering="base64"	B *)	V	1
IDENTIFICATIE BOORDCOMPUTER	IdentificatieBCT	SEQ	V	1
Naam fabrikant	NmFb	S *)	V	1
Serienummer	SrNr	C50 *)	V	1
Versienummer	VrNr	C50	V	1
Bouwjaar	BwJr	I(1..∞)	V	1
Goedkeuringsnummer	GdKrgsNr	S28 *)	V	1
PROGRAMMATUUR	Programmatuur	SEQ	V	1..*
Versienummer	VrNr	C50	V	1
Datumtijd installatie	DatTdIns	DT	V	1
ACTIVERINGSONDERZOEK	ActiveringsOnderzoek	SEQ	V	1
DATA	Data	SEQ	V	1
Volgnummer	VgNr	I(1..∞)	V	1
Km stand	KmStd	I8(1..MAX)	V	1
Datumtijd onderzoek	DatTdOndrzk	DT	V	1
Constante boordcomputer	CnstBCT	I(0..∞)	V	1
Effectieve omtrek wielband	EffOmtrkWlbd	I(0..∞)	V	1
Bandenmaat	BdMt	S(min 1 karakter, maar geen spaties)	V	1
Koppeling taxameter	KpTxMtr	{'Aanwezig', 'Afwezig'}	V	1
Resultaat	Rslt	{'Positief', 'Negatief'}	V	1
Opmerking	Opm	S100	V	1
WERKPLAATS	Werkplaats	SEQ	V	1

Entiteit / attribuut	XML element	Inhoud	G	C
Erkenningsnummer	ErkNr	S20 *)	V	1
Keuringskaart volgnummer	KkVgNr	S5 *)	V	1
INTEGRITEIT	Integriteit	SEQ	V	1
Elektronische handtekening boordcomputer	ElHdBc; codering=”base64”	B	K	1
Elektronische handtekening fout	ElHdFout	S		
Datumtijd handtekening	DatTdHd	DT	V	1
PERIODIEK ONDERZOEK	PeriodiekOnderzoek	SEQ	C	0..*
DATA	Data	SEQ	V	1
Volgnummer	VgNr	I(1..∞)	V	1
Km stand	KmStd	I8(1..MAX)	V	1
Datumtijd onderzoek	DatTdOndrzk	DT	V	1
Constante boordcomputer	CnstBCT	I(0..∞)	V	1
Effectieve omtrek wielband	EffOmtrkWlbd	I(0..∞)	V	1
Bandenmaat	BdMt	S(min 1 karakter, maar geen spaties)	V	1
Koppeling taxameter	KpTxMtr	{‘Aanwezig’, ‘Afwezig’}	V	1
Resultaat	Rslt	{‘Positief’, ‘Negatief’}	V	1
Opmerking	Opm	S100	V	1
WERKPLAATS	Werkplaats	SEQ	V	1
Erkenningsnummer	ErkNr	S20 *)	V	1
Keuringskaart volgnummer	KkVgNr	S5 *)	V	1
INTEGRITEIT	Integriteit	SEQ	V	1
Elektronische handtekening boordcomputer	ElHdBc; codering=”base64”	B	K	1
Elektronische handtekening fout	ElHdFout	S		
Datumtijd handtekening	DatTdHd	DT	V	1

Voor de legenda van het bovenstaande overzicht wordt verwezen naar artikel 10.

Toelichting:
a. De PERIODE is het tijdvak waarover de gebruiker de gebeurtenissen heeft opgevraagd.
b. ACTIVERINGSONDERZOEK wordt uniek geïdentificeerd door een volgnummer.
c. PERIODIEK ONDERZOEK wordt uniek geïdentificeerd door een volgnummer.
d. Constante boordcomputer is in impulsen per kilometer.
e. Effectieve omtrek wielband is in millimeters.
f. Bandenmaat is in inches.
g. De DATA van een ACTIVERINGSONDERZOEK c.q. een PERIODIEK ONDERZOEK moet ondertekend worden met de elektronische handtekening van de boordcomputer om de integriteit van de gegevens achteraf te kunnen bepalen. Daartoe bevat INTEGRITEIT het attribuut ‘Elektronische handtekening boordcomputer’. Indien bij het genereren van de handtekening een gebeurtenis met foutcode S005 of F008 optreedt, wordt, in plaats van de handtekening, deze foutcode geregistreerd in het attribuut ‘Elektronische handtekening fout’.
h. Een kilometerstand wordt opgenomen als een geheel getal, afgerond of afgekapt op een hele kilometer.
i. Het attribuut ‘Publieke sleutel boordcomputer’ dient te worden gevuld met het gehele X509 certificaat van de boordcomputer.

Artikel 7.2 Onderzoek.xsd

De onderstaande Onderzoek.xsd dient te worden gebruikt.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- XML Schema definitie van de gegevenslevering Onderzoek van Boordcomputers
Taxi -->
<!-- Naam: Onderzoek.xsd -->
<!-- Eigenaar: Staat der Nederlanden, Ministerie van Infrastructuur en Milieu --
>
<!-- Versie: 2.0.0 -->
<!-- Datum: 1 augustus 2014 -->
<!-- Ingangdatum: 1 januari 2015 -->
<!-- Chameleon include: bcttypes.xsd -->
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://www.onderzoek.org"
  targetNamespace="http://www.onderzoek.org"
  id="bctOnderzoek"
  version="2.0.0"
  xml:lang="NL"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <xs:include schemaLocation="bcttypes.xsd"/>

  <xs:element name="Onderzoek">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="DatTdSmBr" type="xs:dateTime"/>
        <xs:element name="KortIdBCT" type="KorteIdentiteitBoordcomputer"/>
        <xs:element name="Periode" type="PeriodeBeginEind"/>
        <xs:element name="Auto">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Kntkn" type="Kenteken"/>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="CertificaatBCT" type="X509Certificaat"/>
        <xs:element name="IdentificatieBCT">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="NmFb" type="xs:string"/>
              <xs:element name="SrNr" type="SerieNummer"/>
              <xs:element name="VrNr" type="VersieNummer"/>
              <xs:element name="BwJr" type="xs:positiveInteger"/>
              <xs:element name="GdKrgsNr" type="GoedkeuringsNummer"/>
              <xs:element name="Programmatuur" maxOccurs="unbounded">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="VrNr" type="VersieNummer"/>
                    <xs:element name="DatTdIns" type="xs:dateTime"/>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="ActiveringsOnderzoek" type="Onderzoek"/>
        <xs:element name="PeriodiekOnderzoek" type="Onderzoek" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
      <xs:attribute name="Id" type="xs:string" fixed="idGegevenslevering"/>
    </xs:complexType>
  </xs:element>

  <xs:element name="Data">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="VgNr" type="xs:positiveInteger"/>
        <xs:element name="KmStd" type="KmStand"/>
```

```
        <xs:element name="DatTdOndrzk" type="xs:dateTime"/>
        <xs:element name="CnstBCT" type="ConstanteBCT"/>
        <xs:element name="EffOmtrkWlbd" type="EffectieveOmtrekWielband"/>
        <xs:element name="BdMt" type="BandMaat"/>
        <xs:element name="KpTxMtr" type="KoppelingTaxameter"/>
        <xs:element name="Rslt" type="Resultaat"/>
        <xs:element name="Opm" type="Opmerking"/>
        <xs:element name="Werkplaats">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="ErkNr" type="Erkenningsnummer"/>
              <xs:element name="KkVgNr" type="KeuringskaartVolgnummer"/>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
      <xs:attribute name="Id" type="xs:string" fixed="idData"/>
    </xs:complexType>
  </xs:element>

  <!-- Definities bericht specifieke datatypes -->

  <xs:simpleType name="SerieNummer">
    <xs:restriction base="xs:string">
      <xs:maxLength value="50"/>
      <xs:pattern value="[0-9A-Za-z]+([-.][0-9A-Za-z]+)*"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="Onderzoek">
    <xs:sequence>
      <xs:element ref="Data"/>
      <xs:element name="Integriteit"
type="ElektronischeHandtekeningBoordcomputer" />
    </xs:sequence>
  </xs:complexType>

  <xs:simpleType name="ConstanteBCT">
    <xs:restriction base="xs:nonNegativeInteger"/>
  </xs:simpleType>

  <xs:simpleType name="EffectieveOmtrekWielband">
    <xs:restriction base="xs:nonNegativeInteger"/>
  </xs:simpleType>

  <xs:simpleType name="BandMaat">
    <xs:restriction base="xs:token">
      <xs:pattern value="[^ ]+"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="KoppelingTaxameter">
    <xs:restriction base="xs:string">
      <xs:enumeration value="Aanwezig"/>
      <xs:enumeration value="Afwezig"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="Resultaat">
    <xs:restriction base="xs:string">
      <xs:enumeration value="Positief"/>
      <xs:enumeration value="Negatief"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="Opmerking">
    <xs:restriction base="xs:string">
      <xs:maxLength value="100"/>
    </xs:restriction>
  </xs:simpleType>
```

```
  <xs:simpleType name="Erkenningsnummer">
    <xs:restriction base="xs:string">
      <xs:maxLength value="20"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="KeuringskaartVolgnummer">
    <xs:restriction base="xs:string">
      <xs:length value="5"/>
    </xs:restriction>
  </xs:simpleType>

</xs:schema>
```

Artikel 7.3 Volgorde gegevens

Als eerste wordt het geselecteerde activeringsonderzoek in het bericht opgenomen. Daarna worden de geselecteerde periodieke onderzoeken in oplopende volgorde van volgnummer in het bericht opgenomen.

Artikel 7.4 Integriteit gegevens

Het activeringsonderzoek en de periodieke onderzoeken worden ondertekend op basis van de private sleutel van de boordcomputer.

Het bericht 'Onderzoek' bevat het element <ActiveringsOnderzoek> en nul of meer <PeriodiekOnderzoek> elementen. Elke instantie van een van beide elementen bevat de elementen <Data> en <Integriteit>. Het <Data> element bevat elk van deze gevallen dezelfde gegevens:

a. VgNr
b. KmStd
c. DatTdOndrzk
d. CnstBCT
e. EffOmtrkWlbd
f. BdMt
g. KpTxMtr
h. Rslt
i. Opm
j. Werkplaats.ErkNr
k. Werkplaats.KkVgNr

Het <Integriteit> element bevat de elektronische handtekening van het bijbehorende <Data> element.

Bij het samenstellen van het bericht 'Onderzoek' moeten de gegevens van het <Data> element onveranderd worden overgenomen uit de registratie op de boordcomputer. Het berekenen van de elektronische handtekening van het <Data> element van een 'Onderzoek' wordt gedaan bij het afronden van een onderzoek. De vastgelegde elektronische handtekening wordt per onderzoek overgenomen in het onderliggende <Integriteit> element.

Artikel 7.5 Overige kenmerken

Artikel 7.5.1 Naamgeving

De naamgeving van de gegevenslevering 'Onderzoek' is als volgt:

```
Onderzoek_Kenteken-DatumtijdSamenstellenBericht_DatumtijdBeginPeriode
_DatumtijdEindePeriode.xml
```

Hierbij worden de cursief gedrukte gegevens gevuld met de corresponderende registratiewaarde. De volgende formaten worden hierbij gebruikt:

Gegeven	Formaat
Kenteken	Zoals opgenomen in de gegevenslevering zelf
DatumtijdSamenstellenBericht	CCYYMMDDHHMMSS

Gegeven	Formaat
DatumtijdBeginPeriode	CCYYMMDDHHMM
DatumtijdEindePeriode	CCYYMMDDHHMM

Artikel 7.5.2 Berichtgrootte

Bij 10 onderzoeken is het bericht 'onderzoek' maximaal 10 Kbyte groot.

Artikel 8 Chauffeurskaartdata

Artikel 8.1 Gegevens en functionele en technische berichtstructuur

Voor het bericht 'Chauffeurskaartdata' worden de volgende gegevens en functionele en technische berichtstructuur onderkend:

Entiteit / attribuut	XML element	Inhoud	G	C
BERICHT	Chauffeurskaartdata; Id="idGegevenslevering"	SEQ	V	1
Datumtijd samenstellen bericht	DatTdSmBr	DT	V	1
KORTE IDENTIFICATIE BOORDCOMPUTER	KortIdBCT	SEQ	V	1
Goedkeuringsnummer	GdKrgsNr	S28 *)	V	1
Programmatuur versienummer	ProgVrNr	C50	V	1
PERIODE	Periode	SEQ	V	1
Datumtijd begin periode	DatTdBegPr	DT	V	1
Datumtijd einde periode	DatTdEndPr	DT	V	1
BESTUURDER	Bestuurder	SEQ	V	1
Chauffeursidentificatienummer	ChIdNr	S9 *)	V	1
Chauffeurskaart volgnummer	CkVgNr	S5 *)	V	1
CERTIFICAAT	Certificaat	SEQ	V	1
CERTIFICAAT CHAUFFEUR	CertificaatChauffeur	SEQ	V	1
Publieke sleutel chauffeur	PubliekeSleutel; codering="base64"	B *)	V	1
CHAUFFEURSKAARTDATA	ChKrtData	SEQ	C	0..1
DATA	Data; Id="idData"	SEQ	V	1
Chauffeursactiviteiten	ChauffeursActiviteiten; codering="base64"	B *)	V	1
Boordcomputercertificaten	BCTCertificaten; codering="base64"	B *)	V	1
INTEGRITEIT	Integriteit	SEQ	V	1
Elektronische handtekening chauffeur	ElHdCh; codering="base64"	B	K	1
Elektronische handtekening fout	ElHdFout	S		
Datumtijd handtekening	DatTdHd	DT	V	1

Voor de legenda van het bovenstaande overzicht wordt verwezen naar artikel 10.

Toelichting:
a. De PERIODE bestrijkt het eerste tot en met het laatste record op de chauffeurskaart. De 'Datumtijd begin periode' en 'Datumtijd einde periode' in de gegevenslevering worden overgenomen uit 'Chauffeursactiviteiten' in de CHAUFFEURSKAARTDATA.
b. 'Chauffeursactiviteiten' bevat de Base64 gecodeerde weergave van de binaire inhoud van het bestand 'EF.Driver_Activity_Data', overgenomen van de chauffeurskaart.
c. 'Boordcomputercertificaten' bevat de Base64 gecodeerde weergave van de binaire inhoud van het bestand 'EF.BCT_Certificates', overgenomen van de chauffeurskaart.

d. De DATA van CHAUFFEURSKAARTDATA moet ondertekend worden met de elektronische handtekening van de chauffeur om de integriteit van de gegevens achteraf te kunnen bepalen. Daartoe bevat INTEGRITEIT het attribuut 'Elektronische handtekening chauffeur'. Indien bij het genereren van de handtekening een gebeurtenis met foutcode S006 of F009 optreedt, wordt, in plaats van de handtekening, deze foutcode geregistreerd in het attribuut 'Elektronische handtekening fout'.
e. Het attribuut 'Publieke sleutel chauffeur' dient te worden gevuld met het gehele X509 handtekeningcertificaat van de chauffeur.

Artikel 8.2 Chauffeurskaartdata.xsd

De onderstaande Chauffeurskaartdata.xsd wordt gebruikt.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- XML Schema definitie van de gegevenslevering Chauffeurskaartdata van
Boordcomputers Taxi -->
<!-- Naam: Chauffeurskaartdata.xsd -->
<!-- Eigenaar: Staat der Nederlanden, Ministerie van Infrastructuur en Milieu --
>
<!-- Versie: 2.0.1 -->
<!-- Datum: 1 september 2014 -->
<!-- Ingangdatum: 1 januari 2015 -->
<!-- Chameleon include: bcttypes.xsd -->
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://www.chauffeurskaartdata.org"
  targetNamespace="http://www.chauffeurskaartdata.org"
  id="bctChauffeurskaartdata"
  version="2.0.1"
  xml:lang="NL"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <xs:include schemaLocation="bcttypes.xsd"/>

  <xs:element name="Chauffeurskaartdata">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="DatTdSmBr" type="xs:dateTime"/>
        <xs:element name="KortIdBCT" type="KorteIdentiteitBoordcomputer"/>
        <xs:element name="Periode" type="PeriodeBeginEind"/>
        <xs:element name="Bestuurder">
          <xs:complexType>
            <xs:complexContent>
              <xs:extension base="BestuurderBasisGegevens">
                <xs:sequence>
                  <xs:element name="Certificaat">
                    <xs:complexType>
                      <xs:sequence>
                        <xs:element name="CertificaatChauffeur"
type="X509Certificaat"/>
                      </xs:sequence>
                    </xs:complexType>
                  </xs:element>
                </xs:sequence>
              </xs:extension>
            </xs:complexContent>
          </xs:complexType>
        </xs:element>
        <xs:element name="ChKrtData" minOccurs="0" maxOccurs="1">
          <xs:complexType>
            <xs:sequence>
              <xs:element ref="Data"/>
              <xs:element name="Integriteit"
type="ElektronischeHandtekeningChauffeur"/>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
      <xs:attribute name="Id" type="xs:string" fixed="idGegevenslevering"/>
    </xs:complexType>
  </xs:element>

  <xs:element name="Data">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="ChauffeursActiviteiten" type="BCTBinaireData"/>
        <xs:element name="BCTCertificaten" type="BCTBinaireData"/>
      </xs:sequence>
      <xs:attribute name="Id" type="xs:string" fixed="idData"/>
    </xs:complexType>
  </xs:element>

  <!-- Geen bericht specifieke datatypes -->

</xs:schema>
```

Artikel 8.3 Volgorde gegevens

De chauffeurskaartdata wordt overgenomen zoals deze wordt aangetroffen op de chauffeurskaart.

Artikel 8.4 Integriteit gegevens

Chauffeurskaartdata wordt ondertekend met een elektronische handtekening. Voor het plaatsen van de elektronische handtekening wordt gebruik gemaakt van de private sleutel behorende bij het handtekeningcertificaat van de chauffeurskaart.

Het bericht 'Chauffeurskaartdata' bevat een element <ChKrtData> en <ChKrtData> bevat de elementen <Data> en <Integriteit>. Het <Data> element bevat de base64 representaties van de binaire inhoud van de chip-bestanden 'EF.Driver_Activity_Data' en 'EF.BCT_Certificates', zoals overgenomen uit de chauffeurskaart, in de volgende respectievelijke elementen:
a. ChauffeursActiviteiten
b. BCTCertificaten

Het <Integriteit> element bevat de elektronische handtekening chauffeur van het bijbehorende <Data> element.

Bij het samenstellen van bericht 'Chauffeurskaartdata' moeten de gegevens van het <Data> element zoals hierboven gespecificeerd worden overgenomen uit de chauffeurskaart. Het berekenen van de 'Elektronische handtekening chauffeur' moet gebeuren zodra deze data van de chauffeurskaart is overgenomen. De vastgelegde 'Elektronische handtekening chauffeur' moet onveranderd worden overgenomen in het onderliggende <Integriteit> element.

Artikel 8.5 Overige kenmerken

Artikel 8.5.1 Naamgeving

De naamgeving van de gegevenslevering 'Chauffeurskaartdata' is als volgt:

`Chauffeurskaartdata_`*`Chauffeursidentificatienummer`*`_`*`Chauffeurskaartvolgnummer`*`-`
`DatumtijdSamenstellenBericht``_`*`DatumtijdBeginPeriode`*`_`*`DatumtijdEindePeriode`*`.xml`

Hierbij worden de cursief gedrukte gegevens gevuld met de corresponderende registratiewaarde. De volgende formaten worden hierbij gebruikt:

Gegeven	Formaat
Chauffeursidentificatienummer	Zoals opgenomen in de gegevenslevering zelf
Chauffeurskaartvolgnummer	Zoals opgenomen in de gegevenslevering zelf
DatumtijdSamenstellenBericht	CCYYMMDDHHMMSS
DatumtijdBeginPeriode	CCYYMMDDHHMM
DatumtijdEindePeriode	CCYYMMDDHHMM

Artikel 8.5.2 Berichtgrootte

Het bericht 'Chauffeurskaartdata' is maximaal 200 Kbyte groot.

Artikel 9 Toelichting specificaties gegevensleveringen en algemene XSD

Artikel 9.1 Toelichting bij specificaties van gegevensleveringen

De toelichting bij elk van de functioneel/technische specificaties van een gegevenslevering uit artikelen 3 t/m 8 bestaat uit de navolgende legenda:

Kolomkop / waarde	Betekenis
Entiteit / attribuut:	Functionele beschrijving van het gegeven. De visuele groepering van entiteiten en attributen representeert de hiërarchische structuur van het bericht.
XML element:	De technische berichtstructuur is XML. In deze kolom wordt de naam van het XML element waarin het betreffende gegeven wordt opgeslagen vermeld. Indien het betreffende element een XML attribuut kent, dan is diens naam en waarde bij de elementnaam opgenomen (bijv. codering="base64").
Inhoud:	Datatype, lengte en vorm van de inhoud van het XML element:

Kolomkop / waarde		Betekenis
	*)	Waarde zoals overgenomen uit de betreffende boordcomputerkaart.
	{lijst}	Eén van de waarden in de lijst.
	B	Binaire data gecodeerd als Base64.
	C#	Een reeks van maximaal # karakters beginnend en eindigend met een letter of cijfer met daartussenin optioneel een of meer letters, cijfers, punten (‘.’) en/of liggende streepjes (‘-’).
	CHOICE	Wordt gebruikt wanneer de inhoud van een entiteit naar keuze of conditie één van twee of meer onderliggende entiteiten/attributen moet bevatten. Gebruik wordt nader toegelicht.
	D#.#	Een reëel getal met de vermelde precisie (de # links van de punt representeert het maximale aantal cijfers van het gehele deel en de # rechts van de punt representeert het maximale aantal decimalen).
	D#.#(bereik)	Een reëel getal met de vermelde precisie (zie D#.#) en binnen het vermelde bereik inclusief de vermelde eindwaarden.
	DT	Tijdstip gecodeerd als een datum en een tijd in UTC.
	I	Een geheel getal in het bereik -oneindig tot +oneindig.
	I#	Een geheel getal van maximaal # cijfers.
	I#(bereik)	Een geheel getal van maximaal # cijfers binnen het vermelde bereik inclusief de vermelde eindwaarden. Het symbool MAX staat hierbij voor het getal bestaande uit even zo veel 9’s als # aangeeft.
	I(bereik)	Een geheel getal binnen het vermelde bereik inclusief de vermelde eindwaarden. Het symbool ‘∞’ staat hierbij voor oneindig.
	S	Een onbepaald lange reeks van willekeurige karakters.
	S#	Een reeks van maximaal # willekeurige karakters.
	SEQ	Een geordende groep van onderliggende elementen.
G:		Gebruik van het gegeven:
	C	Conditioneel. Gebruik wordt nader toegelicht.
	K	Keuze. Wordt gebruikt wanneer er naar keuze of conditie één van twee of meer elementen moet worden gebruikt. Gebruik wordt nader toegelicht.
	O	Optioneel. Gebruik naar keuze.
	V	Verplicht.
C:		Cardinaliteit: specificeert hoe veel keer het element wordt herhaald. Hierbij staat ∞ voor een onbeperkt aantal keren.

Artikel 9.2 Algemene XML schema definities in bcttypes.xsd

De berichtstructuren uit artikelen 3 t/m 8 maken allen gebruik van een algemene XSD: bcttypes.xsd. Dit is een XML schema definitie zonder default namespace en zonder targetNamespace. Daardoor neemt het de default namespace en targetNamespace van elke XML schema definitie die bcttypes.xsd 'include' aan. Dit effect heet: 'chameleon include'.

De inhoud van bcttypes.xsd is als volgt:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- XML Schema definities van basistypen voor de Boordcomputer Taxi -->
<!-- Naam: bcttypes.xsd -->
<!-- Eigenaar: Staat der Nederlanden, Ministerie van Infrastructuur en Milieu --
>
<!-- Versie: 2.0.1 -->
<!-- Datum: 1 september 2014 -->
<!-- Ingangdatum: 1 januari 2015 -->
<!-- Opmerking: Dit schema heeft zelf geen targetNamespace en kan daarom met een
     zogenaamde chameleon include worden opgenomen in de targetNamespace van een
     willekeurig ander XML Schema.
     Om dit schema zelf te valideren moet het xs:schema element een dummy xmlns
     krijgen en targetNamespace met dezelfde naam. -->
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  id="bctTypes"
  version="2.0.1"
  xml:lang="NL"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <!-- Definities complexe datatypes -->

  <xs:complexType name="BestuurderBasisGegevens">
    <xs:sequence>
      <xs:element name="ChIdNr" type="ChauffeursIdentificatieNummer"/>
      <xs:element name="CkVgNr" type="ChauffeurskaartVolgnummer"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="ElektronischeHandtekeningBoordcomputer">
    <xs:sequence>
      <xs:choice>
        <xs:element name="ElHdBc" type="BCTBinaireData"/>
        <xs:element name="ElHdFout" type="xs:string"/>
      </xs:choice>
      <xs:element name="DatTdHd" type="xs:dateTime"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="ElektronischeHandtekeningChauffeur">
    <xs:sequence>
      <xs:choice>
        <xs:element name="ElHdCh" type="BCTBinaireData"/>
        <xs:element name="ElHdFout" type="xs:string"/>
      </xs:choice>
      <xs:element name="DatTdHd" type="xs:dateTime"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="ElektronischeHandtekeningChauffeurOfBoordcomputer">
    <xs:sequence>
      <xs:choice>
        <xs:element name="ElHdCh" type="BCTBinaireData"/>
        <xs:element name="ElHdBc" type="BCTBinaireData"/>
        <xs:element name="ElHdFout" type="xs:string"/>
      </xs:choice>
      <xs:element name="DatTdHd" type="xs:dateTime"/>
    </xs:sequence>
  </xs:complexType>
```

```
<xs:complexType name="KorteIdentiteitBoordcomputer">
  <xs:sequence>
    <xs:element name="GdKrgsNr" type="GoedkeuringsNummer"/>
    <xs:element name="ProgVrNr" type="VersieNummer"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="PeriodeBeginEind">
  <xs:sequence>
    <xs:element name="DatTdBegPr" type="xs:dateTime"/>
    <xs:element name="DatTdEndPr" type="xs:dateTime"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="X509Certificaat">
  <xs:sequence>
    <xs:element name="PubliekeSleutel" type="BCTBinaireData"/>
  </xs:sequence>
</xs:complexType>

<!-- Definities simpele datatypes met attributen -->

<xs:complexType name="BCTBinaireData">
  <xs:simpleContent>
    <xs:extension base="xs:base64Binary">
      <xs:attribute name="codering" type="xs:string" fixed="base64"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<!-- Definities simpele datatypes -->

<xs:simpleType name="BreedteGraad">
  <xs:restriction base="xs:decimal">
    <xs:minInclusive value="-90"/>
    <xs:maxInclusive value="90"/>
    <xs:fractionDigits value="6"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ChauffeursIdentificatieNummer">
  <xs:restriction base="xs:string">
    <xs:maxLength value="9"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ChauffeurskaartVolgnummer">
  <xs:restriction base="xs:string">
    <xs:length value="5"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="GoedkeuringsNummer">
  <xs:restriction base="xs:string">
    <xs:maxLength value="28"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Kenteken">
  <xs:restriction base="xs:string">
    <xs:length value="6"/>
  </xs:restriction>
</xs:simpleType>
```

```
<xs:simpleType name="KmStand">
  <xs:restriction base="xs:nonNegativeInteger">
    <xs:maxExclusive value="99999999"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="KvKnummer">
  <xs:restriction base="xs:string">
    <xs:maxLength value="12"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="LengteGraad">
  <xs:restriction base="xs:decimal">
    <xs:minInclusive value="-180"/>
    <xs:maxInclusive value="180"/>
    <xs:fractionDigits value="6"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="OndernemerskaartVolgnummer">
  <xs:restriction base="xs:string">
    <xs:length value="5"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Pnummer">
  <xs:restriction base="xs:string">
    <xs:maxLength value="8"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="VersieNummer">
  <xs:restriction base="xs:string">
    <xs:maxLength value="50"/>
    <xs:pattern value="[0-9A-Za-z]+([-.][0-9A-Za-z]+)*"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Werkingsmodus">
  <xs:restriction base="xs:string">
    <xs:enumeration value="O">
      <xs:annotation>
        <xs:documentation>Operationele modus</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="C">
      <xs:annotation>
        <xs:documentation>Controlemodus</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="B">
      <xs:annotation>
        <xs:documentation>Bedrijfsmodus</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="K">
      <xs:annotation>
        <xs:documentation>Activerings- en keuringsmodus</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
  </xs:restriction>
</xs:simpleType>
```

```
  <xs:simpleType name="Werkingsniveau">
    <xs:restriction base="xs:string">
      <xs:enumeration value="T">
        <xs:annotation>
          <xs:documentation>Taxivervoer</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="A">
        <xs:annotation>
          <xs:documentation>Arbeidstijd</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="B">
        <xs:annotation>
          <xs:documentation>Basis</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
    </xs:restriction>
  </xs:simpleType>

</xs:schema>
```

BIJLAGE 4

OPENBAAR

Technische specificaties gebruik boordcomputer- en systeemkaarten Boordcomputer Taxi

Versie 1.7

Datum 25 april 2012
Status DEFINITIEF

Colofon

Projectnaam	Boordcomputer Taxi
Documenttitel	Technische specificaties gebruik boordcomputer- en systeemkaarten
Classificatie	**OPENBAAR**
Versienummer	1.7
Status	DEFINITIEF
Datum	25 april 2012
Contactpersoon	Inspectie Leefomgeving en Transport Project Boordcomputer Taxi Nieuwe Uitleg 1 I 2514 BP Den Haag Postbus 90653 I 2509 LR Den Haag
Bijlage(n)	Geen
Auteur(s)	Peter G.J. Breur Piet E. Pieters

Wijzigingshistorie

Versie	Datum	Omschrijving
1.2	***4 mei 2010***	Eerste versie voor publicatie
1.3c2	***14 okt 2010***	Wijzigingen naar aanleiding van door Morpho en Collis uitgevoerde tests met gepersonaliseerde exemplaren van de geselecteerde contactchip:
		1) Kaart blijkt geen ondersteuning te bieden voor het selecteren van de DF.CIA op basis van een File Identifier (voorheen 5015h). Selectie van de DF.CIA kan uitsluitend op basis van de Application Identifier plaatsvinden. De APDU's van de desbetreffende SELECT FILE commando's zijn aangepast in § 8.9 t/m § 8.21.
		2) De APDU's voor het lezen en schrijven van EF's waren door offsets in P1P2 te plaatsen, impliciet gebaseerd op de EVEN variant van READ BINARY, respectievelijk UPDATE BINARY. Deze variant biedt echter geen ondersteuning voor offsets groter dan 32767. Vooral voor het lezen en schrijven van EF.Driver_Activity_Data is dit relevant. In § 8.9 t/m § 8.21 zijn de desbetreffende "P1P2" vermeldingen dan ook veranderd in het meer generieke woord "offset". Met aanvullende teksten in hoofdstuk 9 wordt de lezer op het bestaan van een ODD variant, die hogere offsets ondersteunt, gewezen.
		3) De opslagcapaciteit van de kaart blijkt kleiner dan verwacht. Daarom is er gekozen voor het kunnen opslaan van maximaal 3 (in plaats van 4) Systeemkaartcertificaten in EF.BCT_Certificates. Wijzigingen in § 6.1 en § 8.18 t/m § 8.21
		4) De kaart blijkt onvoldoende capaciteit te hebben voor het opslaan van een EF.Driver_Activity_Data van 64KB (65536 bytes). Tijdens personalisatie zal echter per kaart een zo groot mogelijke ruimte voor deze EF worden gereserveerd. Per kaart is die grootte dus verschillend. Hoe hiermee om te gaan, is nu vermeld in § 7.1 en § 9.5. Daarnaast is de vermelding van 64K in hoofdstuk 5, alinea 1 aangepast.
		5) In hoofdstuk 10 Referenties [8] t/m [12] bijgewerkt.
1.3c3	***15 okt 2010***	Een boordcomputer dient een bestuurder (tijdig) te waarschuwen dat de momenteel op de chauffeurskaart opgeslagen arbeids-, rij- en rusttijden moeten worden geëxporteerd. Voorheen bood de chauffeurskaart de boordcomputer hiertoe geen informatie. Dergelijke informatie is nu toegevoegd:
		1) Aan hoofdstuk 6 is bovenstaande rationale toegevoegd.
		2) Aan EF.BCT_Certificates in § 6.1 is een gegevensstructuur toegevoegd die vermeldt wanneer en naar welke boordcomputer welke dailyrecords zijn geëxporteerd.
		3) Aan § 7.3 "Afsluiten van een kaartsessie" zijn extra processtappen toegevoegd.
		4) Aan hoofdstuk 8 zijn nieuwe paragrafen (§ 8.22 t/m § 8.23) met de extra benodigde functies toegevoegd
1.3c4	***28 okt 2010***	Meer wijzigingen naar aanleiding van door Morpho en Collis uitgevoerde tests:
		1) De Kaartstructuur documenten bevatten kleine fouten en zijn bijgewerkt van versie 1.5 naar 1.6. In hoofdstuk 10 zijn de betreffende Referenties ([8] t/m [12]) geactualiseerd.
		2) In § 8.5, 8.6 en 8.7 werd gesproken over een "PSO Hash commando met '6C'h in Lc om SHA256 aan te duiden". Omdat dat niet correct is, zijn er tekstverbeteringen in deze paragrafen aangebracht. Ook § 8.8 is met deze aanvullingen in lijn gebracht.
1.3c5	***5 nov 2010***	Wijzigingen naar aanleiding van interne review IVW:
		1) Eerste alinea van de Inleiding geactualiseerd.
		2) In § 2.5 een grammaticale verbetering aangebracht.
		3) In § 5.1 de noodzaak van een correct gevuld DriverCardNumber verklaard.

Versie	Datum	Omschrijving
		4) In § 5.1.2 expliciet vermeld dat het tijdformaat van een 24-uurs klok uitgaat.
		5) In § 5.2 de referentie naar hoofdstuk 7 hersteld.
		6) In § 5.2.7 een grammaticale verbetering aangebracht.
		7) In § 6.1 de zin onder Figuur 10 verbeterd.
		8) In § 7.1, puntje 1 een referentie opgenomen.
		9) In § 7.1, punt 4, 2e aandachtsstreepje grammaticale verbeteringen aangebracht.
		10) In § 7.3 de eerste twee alinea's duidelijker verwoord.
		11) In hoofdstuk 10 de omschrijving van referentie [14] gecorrigeerd.
		12) In scenario A.6 ontbrekende teksten toegevoegd.
1.3c6	***11 nov 2010***	Wijzigingen naar aanleiding van document review door Collis:
		1) In § 8.7, puntje 4 de tekst "van minimaal 1 en maximaal 64 bytes" ingevoegd.
		2) In § 9.4 het voorbeeld aangepast aan hetgeen in tabel 29 in referentie [7] staat: Bij een Read Binary Odd kan voor P1P2 alleen een SFI meegegeven worden en geen file id
1.4	***6 dec 2010***	Doorvoeren naamswijziging ministerie
1.5	***29 jun 2011***	Wijzigingen met betrekking tot het refereren aan private sleutelobjecten:
		1) In § 8.5 twee keer de tekst "06" veranderd in "86" en voetnoot aangepast
		2) In § 8.6 twee keer de tekst "05" veranderd in "85" en voetnoot aangepast
		3) In § 8.7 twee keer de tekst "05" veranderd in "85" en voetnoot aangepast
		4) In § 8.8 twee keer de tekst "05" veranderd in "85" en voetnoot aangepast
1.6	***12 dec 2011***	Aanpassing §4.6 Authenticatiescenario Systeemkaart-Boordcomputer
1.7	***25 apr 2012***	Wijzigingen naar aanleiding van uitgevoerde tests:
		1) In § 8.5 stap toegevoegd voor selectie hash template en algoritme
		2) In § 8.6 stap toegevoegd voor selectie hash template en algoritme
		3) In § 8.7 stap toegevoegd voor selectie hash template en algoritme
		4) Bijlage B toegevoegd met uitgewerkte voorbeelden van een aantal functies

Inhoud

1 Inleiding

Met de inwerkingtreding van de 'Ministeriele Regeling specificaties en typegoedkeuring boordcomputer taxi' zijn de specificaties van de 'Boordcomputer Taxi' (BCT) van kracht geworden. Met deze regelgeving wordt elke taxi in Nederland voorzien van een boordcomputer, die zowel de arbeids-, rij- en rusttijden van de taxichauffeur als de rittenstaat behorend bij de taxi vastlegt.

Om de authenticiteit en integriteit van de vastgelegde data te waarborgen, voorziet de boordcomputer deze data van elektronische handtekeningen. Daartoe wordt een zogeheten 'Public Key Infrastructure' worden opgezet. De boordcomputer wordt voorzien van een certificaat en een sleutelpaar (publieke- en private sleutels), zodat hij in staat is data elektronisch te ondertekenen en de authenticiteit van aangeboden gebruikerskaarten vast te stellen. Het certificaat en het sleutelpaar van de boordcomputer worden hiertoe opgeslagen op een chipkaart, de zogeheten systeemkaart, die in een speciaal kaartslot van de boordcomputer wordt geplaatst.

Alle gebruikers van de boordcomputer worden voorzien van gebruikerskaarten, de zogeheten boordcomputerkaarten. Deze kaarten bevatten evenals de systeemkaart certificaten en sleutelparen.

Toegang tot de boordcomputer is alleen mogelijk na authenticatie van een boordcomputerkaart door (de logica van) de boordcomputer.

Binnen de groep gebruikers van de boordcomputer zijn vier rollen te onderscheiden, namelijk die van bestuurder, vervoerder, werkplaats en toezichthouder. Elk van deze rollen is gebonden aan een apart type boordcomputerkaart. Elke rol heeft zijn eigen autorisatieniveau, bijvoorbeeld waar het gaat om toegang tot de op de boordcomputer vastgelegde data.

Binnen BCT zijn dus vijf verschillende chipkaarten te onderscheiden:
- Een apparaatgebonden systeemkaart behorend bij een boordcomputer;
- Een persoonsgebonden chauffeurskaart behorend bij een bestuurder;
- Een organisatiegebonden ondernemerskaart behorend bij een vervoerder;
- Een organisatiegebonden keuringskaart behorend bij een werkplaats;
- Een persoonsgebonden inspectiekaart behorend bij een toezichthouder.

1.1 Bereik van dit document

Dit document bevat technische specificaties en richtlijnen voor het gebruik van de hierboven genoemde chipkaarten. Dit document is primair bedoeld voor fabrikanten van boordcomputers. De hoofdstukken 2 en 5 t/m 8, alsmede bijlage A, zijn echter ook interessant voor ontwikkelaars van toepassingen bedoeld om chauffeurskaarten uit te lezen.

2 Opbouw boordcomputer- en systeemkaarten

2.1 ISO/IEC 7816-15 structuur

De boordcomputer- en systeemkaarten zijn uitgevoerd als ISO/IEC 7816-15 kaarten. De algemene opbouw van ISO/IEC 7816-15 kaarten staat beschreven in Referentie [3]. De opbouw per kaart wordt in de specificatie documenten van de afzonderlijke kaarten beschreven (Referenties [8] t/m [12]).

2.2 Certificaten

De op de boordcomputer- en systeemkaarten gebruikte certificaten zijn X.509 certificaten uitgegeven conform PKIoverheid. Er worden verschillende X.509 certificaten gebruikt, zoals voor authenticatie, handtekening en vertrouwelijkheid. Zie verder Referentie [13] in hoofdstuk 10.

2.3 Asymmetrische sleutels

Asymmetrische sleutels worden gebruikt voor authenticatie, vertrouwelijkheid en handtekening. De publieke sleutels zijn opgeslagen in de X.509 certificaten (zie § 2.2) en de private sleutels intern in de kaarten.
De asymmetrische sleutels die in de kaarten gebruikt worden zijn RSA sleutels met een lengte van 2048 bits.

2.4 PIN/PUK

De eigenschappen van de PIN en PUK (PIN Unblock Key) per kaart worden in de specificatie documenten van de afzonderlijke kaarten beschreven (Referenties [8] t/m [12] in hoofdstuk 10).

De PIN wordt algemeen gebruikt voor de authenticatie van de kaarthouder en bij persoonsgebonden boordcomputerkaarten voor het zetten van elektronische handtekeningen. De PUK kan gebruikt worden om de PIN te deblokkeren.

2.5 Gegevens

Op alle kaarten zijn gegevens zoals voorgeschreven in ISO/IEC 7816-15 opgeslagen. Er zijn echter twee typen kaarten waarop ook andere gegevens toegevoegd kunnen worden: de systeemkaart en de chauffeurskaart.

2.5.1 Systeemkaart

Op de systeemkaart kan eenmalig het serienummer van de boordcomputer opgeslagen worden. Dit staat beschreven in hoofdstuk 3. Verder worden er (tijdens de gebruiksfase) op de systeemkaart geen gegevens opgeslagen.

2.5.2 Chauffeurskaart

Op de chauffeurskaart worden de arbeids-, rij- en rusttijden van de chauffeur, alsmede de systeemkaartcertificaten van de laatst gebruikte boordcomputers opgeslagen. Dit wordt beschreven in hoofdstuk 5.

2.5.3 Relatie gegevens boordcomputer – chauffeurskaart

Voor de boordcomputer is het niet vastgelegd hoe de gegevens opgeslagen moeten worden. Wel is vastgelegd welke gegevens er opgeslagen moeten worden en hoe en in welk formaat ze beschikbaar moeten zijn voor gegevenslevering.
Vanwege beperkingen voor wat betreft het formaat en de mogelijkheden voor controle en uitlezen van de gegevens, is voor de chauffeurskaart wel exact vastgelegd hoe de gegevens opgeslagen moeten worden. Dit staat beschreven in hoofdstuk 5.

2.6 Toegangscondities

Specifieke toegangscondities worden gegeven in de specificatiedocumenten van de afzonderlijke boordcomputerkaarten.

Algemeen geldt voor de toegangscondities:
- Lezen PIN, PUK en RSA sleutels: niet toegestaan.
- Lezen gegevens: geen beperking.
- Schrijven van de RSA sleutels: niet toegestaan.
- Gebruik van de RSA sleutels voor authenticiteit en elektronische handtekeningen: alleen mogelijk na een succesvolle verificatie van de PIN. Bij systeemkaarten wordt Secure Messaging in plaats van een PIN gebruikt.
- Gebruik van de PIN (alleen op boordcomputerkaarten): geen beperkingen.
- Deblokkeren van de PIN (alleen op boordcomputerkaarten): alleen mogelijk na een succesvolle verificatie van de PUK.
- Wijzigen van de PIN (alleen op boordcomputerkaarten): alleen mogelijk na een succesvolle verificatie van de (huidige) PIN of, als aanvulling op deblokkeren, na succesvolle verificatie van de PUK.
- Gebruik van de PUK (alleen op boordcomputerkaarten): geen beperkingen.
- Schrijven: bij systeemkaarten alleen mogelijk in Secure Messaging en bij chauffeurskaarten alleen mogelijk na een succesvolle verificatie van de PIN.

3 Koppelen Systeemkaart

De systeemkaart moet initieel aan de boordcomputer gekoppeld worden om de boordcomputer te laten functioneren. Onderstaande paragrafen geven een nadere specificatie van boordcomputerproductie, respectievelijk systeemkaartvervanging.

3.1 Communicatiebeveiliging tussen boordcomputerunits en systeemkaarten

Een boordcomputer wordt gevormd door de combinatie van een boordcomputerunit en een systeemkaart. De boordcomputerunit wordt hierbij beschouwd als de gebruiker/houder van de systeemkaart. Net zoals een boordcomputerkaart uitsluitend door zijn rechtmatige houder mag worden gebruikt (voor het plaatsen van elektronische handtekeningen), mag ook een systeemkaart uitsluitend door zijn rechtmatige “houder” worden gebruikt. Om dit rechtmatige gebruik te waarborgen wordt elke systeemkaart voorzien van een geheime sleutel die in de boordcomputerunit dient te worden voorgeprogrammeerd.

Het communicatiekanaal (voor het plaatsen van elektronische handtekeningen) tussen een boordcomputerunit en zijn gekoppelde systeemkaart moet beveiligd zijn om de integriteit, authenticiteit en vertrouwelijkheid van de uitgewisselde gegevens te beschermen. Omdat de koppeling tussen een boordcomputerunit en “zijn” systeemkaart een-op-een is, is er voor het opzetten van een veilig communicatiekanaal geen noodzaak voor asymmetrische cryptografie, maar kan met symmetrische cryptografie worden volstaan. De symmetrische sleutel(set) die voor deze communicatiebeveiliging wordt gebruikt is per boordcomputer uniek; elke systeemkaart wordt voorzien van een symmetrische communicatiesleutel(set) die in de bijbehorende boordcomputerunit dient te worden voorgeprogrammeerd.

Er bestaan vijf soorten combinaties van boordcomputerunits en systeemkaarten:
1. Niet-gekoppelde boordcomputerunit – niet-gekoppelde eerste systeemkaart;
2. Boordcomputerunit gekoppeld aan eerste systeemkaart (= boordcomputer);

3. Boordcomputerunit – ontkoppelde/onklaar gemaakte systeemkaart;
4. Boordcomputer – niet-gekoppelde vervangende systeemkaart;
5. Boordcomputerunit gekoppeld aan vervangende systeemkaart (= boordcomputer);

Combinatie 1 is van toepassing in de fabriek waar de boordcomputerunit wordt geproduceerd. Combinatie 2 wordt gemaakt bij de boordcomputerfabrikant voorafgaand aan de distributie van de resulterende boordcomputer. Combinaties 1 en 2 vallen daarmee onder de noemer "boordcomputerproductie".

Combinaties 3, 4 en 5 betreffen het "in het veld" (buiten de fabriek) op een boordcomputer vervangen van de huidige gekoppelde systeemkaart door een andere systeemkaart. Deze combinaties vallen onder de noemer "systeemkaartvervanging".

Onderstaande subparagrafen geven een nadere specificatie van boordcomputerproductie, respectievelijk systeemkaartvervanging.

3.1.1 Boordcomputerproductie

Elke boordcomputerfabrikant die een typegoedkeuring heeft verkregen kan, per typegoedkeuringsnummer, bij de Kaartuitgever een verzoek voor een transportkey indienen. De Kaartuitgever zal, na verificatie van het typegoedkeuringsnummer, via de Personalisator een transportkey voor het typegoedkeuringsnummer genereren. Deze transportkey zal op een pinmailer aan de fabrikant worden verzonden.

Wanneer de fabrikant boordcomputers van het desbetreffende type wil gaan produceren, zal de fabrikant op basis van het typegoedkeuringsnummer een of meer batches van systeemkaarten bestellen bij de Kaartuitgever. De Kaartuitgever / Personalisator gebruikt de eerder vastgelegde transportkey (zie voorgaande alinea) om de te produceren systeemkaarten mee te beschermen. De door de fabrikant geproduceerde boordcomputerunits dienen door de fabrikant te worden voorgeprogrammeerd met diezelfde transportkey.

Met het bovenstaande scenario kan elke nieuw geproduceerde boordcomputerunit (van een specifiek type) communiceren met elke gepersonaliseerde eerste systeemkaart (voor datzelfde boordcomputertype).

Nadat de operator bij de fabrikant een boordcomputerunit van een nieuwe systeemkaart (uit de bij de fabrikant aanwezige voorraad) heeft voorzien, dient die operator de "koppelfunctie" van de boordcomputerunit te gebruiken. Die koppelfunctie dient de typespecifieke transportkey te vervangen met een door de boordcomputerunit gegenereerde "true random" waarde. Deze sleutelvervanging dient uiteraard zowel in de boordcomputerunit als in de systeemkaart te gebeuren. Hierna kan de betreffende boordcomputerunit uitsluitend nog met de betreffende systeemkaart werken.

De onderstaande tabel geeft een overzicht van de toegangscondities en de inhoud van de verschillende security objecten van systeemkaart en boordcomputerunit zowel voor als na het koppelproces.

Tabel 1. Toegangscondities/inhoud van objecten bij eerste systeemkaarten

Security / Data Object	Access Condition				Geproduceerd	Gekoppeld
	Read	Write	Use	Reset		
STK1.RSA.Private	never	never	SM	n.a.	rsakey1	rsakey1
STK1.DO.NextKey	SM	SM	n.a.	n.a.	transportkey2	transportkey2
STK1.DO.BC.Serial	Always	SM	n.a.	n.a.	Leeg	Serienr. BCT
STK1.SMkeyset	never	SM	always	n.a.	transportkey1	uniquekey1
BCT.Secret	**BCT custom access conditions**				**transportkey1**	**uniquekey1**

NB. *De constructie en/of logica van de boordcomputer dient het object BCT.SECRET op adequate wijze te beschermen tegen ontvreemding (dit geheim mag uitsluitend toegankelijk zijn voor de boordcomputerlogica en uitsluitend voor de in dit document beschreven doelen worden toegepast.*

De Personalisator levert een systeemkaart op met de volgende waarden:
- Een per kaart unieke en nergens onthouden waarde in het RSA private key object;
- Een per typegoedkeuringsnummer unieke en bij de Personalisator en fabrikant bekende, bewaarde en geheimgehouden waarde "transportkey1" in het object SMkeyset;

- Een per kaart unieke en bij de Personalisator bewaarde waarde “transportkey2” in het ***data***object NextKey;
- Een lege string in het dataobject BC.Serial.

Omdat de waarde “transportkey1” geheimgehouden is, is een gepersonaliseerde niet-gekoppelde kaart tijdens distributie *onbruikbaar* voor:
- Het gebruik van de RSA private key
  (nodig voor het zetten van elektronische handtekeningen);
- Het uitlezen van het object NextKey
  (nodig voor het koppelen aan een vervangende systeemkaart);
- Het beschrijven van het object BC.Serial
  (nodig als onderdeel van het koppelproces).

Omdat de waarde “transportkey1” wel bij de fabrikant bekend is, is die waarde voorgeprogrammeerd in het “Secret” object van elke nieuw geproduceerde boordcomputerunit. Hiermee kan een boordcomputerunit het koppelproces doorlopen:
1. Lees de waarde “transportkey1” uit de variabele Secret;
2. Genereer een nieuwe unieke (random) waarde “uniquekey1”;
3. Gebruik “transportkey1” als een 3DES sleutelset om via een MUTUAL AUTHENTICATE een veilig kanaal (MAC_ENC Secure Messaging kanaal) op te zetten met de systeemkaart (zie § 4.6);
4. Gebruik een PUT DATA om de SMkeyset te wijzigen in “uniquekey1”, gebruikmakend van het SM kanaal;
5. Gebruik het SM kanaal om het dataobject BC.SERIAL te beschrijven met het serienummer van de boordcomputer.
   Het dataobject BC.SERIAL is 64 bytes groot. In de eerste byte dient de lengte van het serienummer in bytes te worden opgeslagen als een (unsigned) byte. Het serienummer, weergegeven als een (8-bits) ASCII string, wordt vanaf de tweede byte opgeslagen. De maximale lengte van een serienummer is hiermee 63 karakters (bytes);
6. Overschrijf de variabele Secret met “uniquekey1” en vernietig daarbij de kennis van “transportkey1”;
7. Sluit de kaartsessie.

NB. *Het initiëren van het koppelproces kan, naar keuze van de fabrikant, een (beschermde) menugestuurde optie zijn of automatisch gebeuren als gevolg van het herkennen van een nog niet gekoppelde systeemkaart in het systeemkaartslot*.

De systeemkaart is nu een-op-een gekoppeld aan de boordcomputerunit die met zijn kennis van “uniquekey1” een MAC_ENC SM kanaal kan opzetten en daarmee het volgende kan doen:
- Zetten van elektronische handtekeningen;
- Uitlezen van NextKey voor het koppelen van een vervangende systeemkaart;
- Opnieuw doorlopen van het koppelproces om de waarde “uniquekey1” te wijzigen in een nieuwe waarde.

Ondersteuning van de laatstgenoemde mogelijkheid is niet voorgeschreven, maar kan als extra veiligheidsmaatregel periodiek worden gedaan.

3.1.2 Systeemkaartvervanging

Dit beveiligingsconcept voorziet, teneinde reguliere certificaatvervanging te ondersteunen, in de mogelijkheid om de systeemkaart van een boordcomputer te vervangen door een andere.

Om dit “in het veld” door een werkplaats te kunnen laten doen is het concept voor vervanging dusdanig dat er geen kennis van enig geheim vereist is bij degene die de vervanging uitvoert. Hiertoe is met de Personalisator afgesproken:
1. dat elke eerste systeemkaart een dataobject NextKey bevat met daarin een unieke waarde “transportkey2”,
2. dat de Personalisator die waarde voor elke systeemkaart in escrow houdt en
3. dat de Personalisator het SMkeyset object van de desbetreffende vervangende systeemkaart vult met die onthouden waarde.

Uiteraard zal het NextKey dataobject van de vervangende systeemkaart ook weer worden gevuld met een nieuwe unieke waarde (“transportkey3”), zodat een volgende vervanging ook weer kan worden uitgevoerd.

Zoals in de vorige paragraaf is uitgelegd, worden nieuw geproduceerde boordcomputerunits in de fabriek voorgeprogrammeerd met de (typespecifieke) “transportkey1”. In die veilige omgeving kan

elke willekeurige nieuwe boordcomputerunit (van een bepaald type) dan ook gekoppeld worden aan elke willekeurige gepersonaliseerde "eerste systeemkaart" (voor datzelfde boordcomputertype).

Bij het vervangen van een systeemkaart wordt de oude systeemkaart gebruikt om de boordcomputerunit te voorzien van de transportkey die nodig is voor de koppeling aan de vervangende systeemkaart. Hierbij blijft die transportkey onzichtbaar voor degene die de vervanging uitvoert. Omdat bovendien geldt dat de transportkey van elke vervangende systeemkaart uniek is voor die kaart, is bovendien gewaarborgd dat een vervangende systeemkaart uitsluitend in één (1) specifieke boordcomputer zal kunnen werken.

NB. Bij het bestellen van een vervangende systeemkaart wordt aan de Personalisator aangeduid om welke "voorloper" het gaat. Hiervoor wordt het systeemkaartnummer gebruikt dat als volgt is opgebouwd: "S" + boordcomputernummer (hetzelfde als dat van de voorloper) + kaartvolgnummer (1 hoger dan dat van de voorloper).

De onderstaande tabel geeft een overzicht van de toegangscondities en de inhoud van de verschillende security objecten van systeemkaart 1 en 2 en van de boordcomputerunit zowel voor als na het koppelproces.

Tabel 2. Toegangscondities/inhoud van objecten bij systeemkaartvervanging

Security / Data Object	Access Condition				Gekoppeld 1	Ontkoppeld 1 / Geprod. 2	Gekoppeld 2
	Read	Write	Use	Reset			
STK1.RSA.Private	never	never	SM	n.a.	rsakey1	rsakey1	n.a.
STK1.DO.NextKey	SM	SM	n.a.	n.a.	transportkey2	***random***	n.a.
STK1.DO.BC.Serial	Always	SM	n.a.	n.a.	Serienr. BCT	Leeg	
STK1.SMkeyset	never	SM	always	n.a.	uniquekey1	random/blocked	n.a.
BCT.Secret	**BCT custom access conditions**				**uniquekey1**	**transportkey2**	**uniquekey2**
STK2.RSA.Private	never	never	SM	n.a.	n.a.	rsakey2	rsakey2
STK2.DO.NextKey	SM	SM	n.a.	n.a.	n.a.	transportkey3	transportkey3
STK2.DO.BC.Serial	Always	SM	n.a.	n.a.	n.a.	Leeg	Serienr. BCT
STK2.SMkeyset	never	SM	always	n.a.	n.a.	transportkey2	uniquekey2

Het koppelen van de boordcomputerunit aan de vervangende systeemkaart volgt dezelfde stappen als bij het koppelen aan de eerste (of voorgaande) systeemkaart zoals beschreven in § 3.1.1. Het verschil zit hem in de volgende voorbereidende stappen:

1. Initieer de vervanging door het aanroepen van de desbetreffende functie op de boordcomputer;
2. Lees de waarde "uniquekey1" uit de variabele Secret;
3. Gebruik (indien er nog geen MAC_ENC Secure Messaging kanaal bestaat) "uniquekey1" als een 3DES sleutelset om via een MUTUAL AUTHENTICATE een veilig kanaal (MAC_ENC Secure Messaging kanaal) op te zetten met de huidige systeemkaart;
4. Lees, gebruikmakend van het SM kanaal, de waarde "transportkey2" uit het dataobject NextKey;
5. Maak, gebruikmakend van het SM kanaal, de huidige systeemkaart onklaar:
6. Overschrijf het NextKey data object met een random waarde;
7. Overschrijf het SMkeyset object met een random waarde;
8. Overschrijf het BC.Serial object met een random of een lege waarde;
9. Overschrijf de variabele Secret met "transportkey2" en vernietig daarbij de kennis die de boordcomputerunit van de huidige systeemkaart had;
10. Sluit de kaartsessie;
11. Vervang systeemkaart 1 fysiek voor systeemkaart 2.
12. Hierna dezelfde 7 stappen als bij 1e koppelproces.

13.

NB. *Stap 1 kan, naar keuze van de fabrikant, geïnitieerd worden door een (beschermde) menugestuurde optie of automatisch starten wanneer het systeemkaartslot geopend wordt (maar voorafgaand aan het verbreken van de elektrische verbinding tussen boordcomputereenheid en systeemkaart). Hierbij geniet de laatste methode de voorkeur omdat dit een effectieve bescherming tegen misbruik van de systeemkaart biedt.*

4 Beveiligde gegevensoverdracht

Overeenkomstig het gestelde in Referentie [14] hoeft de gegevensoverdracht tussen boordcomputer en boordcomputerkaart niet te worden beveiligd. Volgens diezelfde referenties dient de gegevensoverdracht tussen boordcomputerlogica en systeemkaart wel beveiligd te zijn.

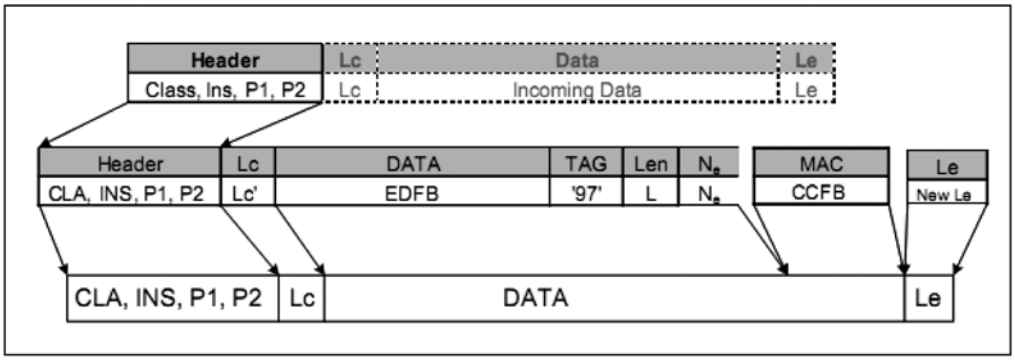
Deze beveiligde gegevensoverdracht wordt bereikt door het versleutelen van de gegevens en het toevoegen van een cryptografische controlesom (MAC) aan de binnen het commando of het antwoord gezonden gegevensobjecten (MAC-ENC mode).

De MAC van binnen een commando gezonden gegevens moet de commando-kop en alle gezonden gegevensobjecten integreren (=> CLA = '0C', en alle gegevensobjecten moeten worden ingekapseld met tags waarin b1 = 1).
De MAC moet door de ontvanger geverifieerd worden.

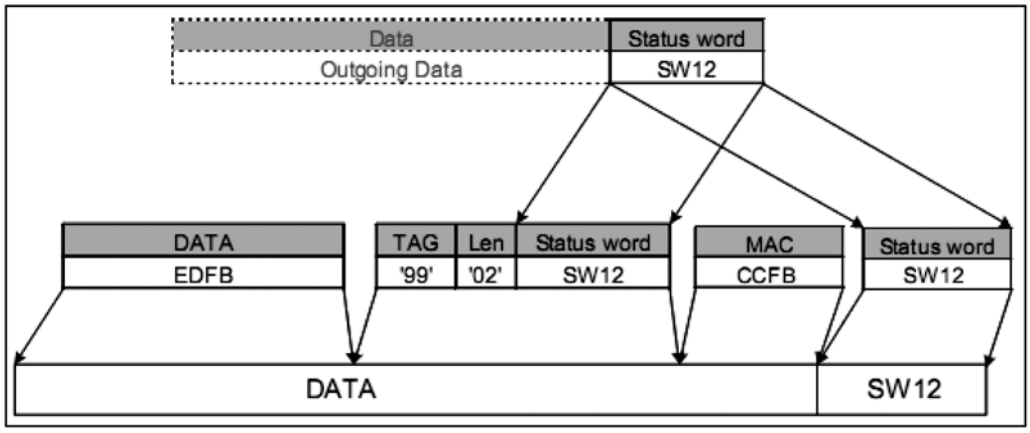
De bytes van de statusinformatie van het antwoord moeten altijd door een MAC worden beveiligd, met uitzondering van de gevallen beschreven in paragraaf 4.2.

4.1 Structuur van commando's en antwoorden bij beveiligde gegevensoverdracht

In de onderstaande figuren zijn schematisch een beveiligd commando en een beveiligd antwoord weergegeven. Voor een verdere beschrijving hiervan wordt verwezen naar Referentie [7], section 7.1.9 en section 7.1.10.



Figuur 1: Beveiligd commando



Figuur 2: Beveiligd antwoord

4.2 Fouten bij de beveiligde gegevensoverdracht

Wanneer de systeemkaart tijdens het verwerken van een commando een Secure Messaging-fout ontdekt, dan moeten de statuswoorden zonder Secure Messaging teruggezonden worden. Overeenkomstig ISO/IEC 7816-4 moeten de onderstaande statuswoorden gebruikt worden om Secure Messaging-fouten aan te geven:

'69 82' Veiligheids toestand voldoet niet,
'69 85' Sessiesleutels zijn niet beschikbaar,
'69 87' Verwachte Secure Messaging-gegevensobjecten ontbreken,
'69 88' Secure Messaging-gegevensobjecten onjuist.

Wanneer de systeemkaart statuswoorden zonder Secure Messaging gegevensobjecten of met een foutieve Secure Messaging gegevensobjecten terugzendt, moet de sessie door de boordcomputerlogica afgebroken worden.

In het geval van een Secure Messaging-fout vervallen de sessiesleutels en SSC.

4.3 Sessiesleutels

Voor beveiligde gegevensoverdracht tussen de boordcomputerlogica en de systeemkaart worden twee 16 bytes lange sessiesleutels gebruikt. De methode om deze sessiesleutels SK_{ENC} en SK_{MAC} te genereren wordt beschreven in Referentie [7], section 7.1.4.

4.4 Zendsequentieteller (SSC)

Tijdens de authenticatie procedure wordt er door zowel de systeemkaart als door de boordcomputer-logica een 8 bytes random gegenereerd, RND.BCT resp. RND.ICC.

De vier minst significante bytes (LSB) van beiden worden gebruikt om de initiële waarde voor de SSC te bepalen: SSC = RND.ICC (4 LSB) || RND.BCT (4 LSB).

De SSC wordt iedere keer voordat een MAC berekend wordt met 1 verhoogd, dus voor de eerste MAC-berekening wordt de waarde SSC + 1 gebruikt.

4.5 Algoritmes

Het algoritme dat gebruikt wordt voor het berekenen van cryptogrammen wordt beschreven in Referentie [7], section 7.1.9 en section 7.1.10.
Het algoritme dat gebruikt wordt voor het berekenen van cryptografische controlesommen (MACs) wordt beschreven in Referentie [7], section 7.1.12.

De MAC is 8 bytes lang.

Iedere keer voordat er een MAC berekend wordt, wordt de zendsequentieteller (SSC) met 1 verhoogd.

4.6 Authenticatiescenario Systeemkaart-Boordcomputer

Het authenticatiescenario tussen systeemkaart en boordcomputer wordt uitgevoerd zoals beschreven is in Referentie [7], section 5.2.2.

Hierbij moet gelet worden op de volgende punten:
1. Er wordt gebruik gemaakt van symmetrische sleutels (zie hoofdstuk 3). De initiële sleutels worden afgeleid van “transportkey1”:
   - KS.KMAC bestaat uit de eerste 16 bytes van “transportkey1”,
   - KS.KENC bestaat uit de laatste 16 bytes van “transportkey1”.
2. Na het uitlezen van EF.SN.ICC worden de laatste 8 bytes hiervan gebruikt voor SN.ICC.
3. Bij het berekenen van de MAC moet gebruik gemaakt worden van padding, zoals beschreven is in Referentie [7], section 10.1.

Na een succesvolle uitvoering van de Mutual Authenticate kunnen de sessiesleutels en de SSC berekend worden, zoals beschreven is in Referentie [7], section 7.1.4 en 7.1.5.
Er is dan een secure messaging kanaal tussen de systeemkaart en de boordcomputer (MAC-ENC mode) en alle volgende commando’s en antwoorden moeten beveiligde gegevensoverdracht gebruiken.

5 Gegevens op chauffeurskaart (EF.Driver_Activity_Data)

Op de chauffeurskaart worden de arbeids- rij- en rusttijden van een chauffeur opgeslagen in de bestandsstructuur EF.Driver_Activity_Data. De grootte van die bestandsstructuur wordt door de Personalisator op elke chauffeurskaart gemaximeerd (zie ook § 7.1, § 9.5 en Referentie [9] in hoofdstuk 10).

5.1 Opbouw van EF.Driver_Activity_Data

Figuur 3: EF.Driver_Activity_Data

Naam	Grootte (bytes)
PointerOldestDayRecord	2
PointerLastDayRecord	2
DriverCardNumber	16

Naam	Grootte (bytes)
DailyRecords	variabel

EF.Driver_Activity_Data is opgebouwd uit de volgende elementen:

- **PointerOldestDayRecord:** specificeert het begin van de geheugenplaats (aantal bytes vanaf het begin van EF.Driver_Activity_Data) van de oudste volledige dagregistratie in DailyRecords.
  De initiële waarde (na personalisatie) is '00 00'H (0) wat betekent dat er nog geen DailyRecords bestaan.
  Na toevoeging van het eerste DailyRecord moet de waarde '00 14'H (20) zijn.
  De maximale waarde wordt door de lengte van EF.Driver_Activity_Data bepaald.
  Gegevenssoort: INTEGER (unsigned)
- **PointerLastDayRecord:** specificeert het begin van de geheugenplaats (aantal bytes vanaf het begin van EF.Driver_Activity_Data) van de meest recente dagregistratie in DailyRecords.
  De initiële waarde (na personalisatie) is '00 00'H (0) wat betekent dat er nog geen DailyRecords bestaan.
  Na toevoeging van het eerste DailyRecord moet de waarde '00 14'H (20) zijn.
  De maximale waarde wordt door de lengte van EF.Driver_Activity_Data bepaald.
  Gegevenssoort: INTEGER (unsigned)
- **DriverCardNumber:** betreft een kopie van het chauffeurskaartnummer zoals dat ook aanwezig is in het subjectSerialNumber-veld van het ("read-only") authenticiteitcertificaat van de chauffeurskaart. Na personalisatie zal dit element gevuld zijn met het chauffeurskaartnummer. Handhavingsapplicaties downloaden in principe uitsluitend EF_Driver_Activity_Data van een chauffeurskaart. Om die applicaties te informeren over het chauffeurskaartnummer, dient een boord computer de correcte invulling van dit veld telkens na een succesvolle login te verifiëren en zo nodig te herstellen (zie ook § 7.1).
  Gegevenssoort: PrintableString (16 bytes)
- **DailyRecords:** de records waarin de gegevens van de activiteiten van de chauffeur opgeslagen worden (zie Figuur 4). Voor iedere dag dat de kaart gebruikt wordt, wordt een DailyRecord aangemaakt. De gegevens van minimaal de laatste 31 kalenderdagen worden op de kaart bewaard.

5.1.1 DailyRecord

Een DailyRecord bevat alle gegevens van de activiteiten van de chauffeur op een bepaalde dag. Na personaliseren bestaat er nog geen enkel DailyRecord.

Figuur 4: DailyRecord

Naam	Grootte (bytes)
DayRecordLength	2
PointerLastSessionRecord	2
PreviousDayRecordLength	2
DayRecordDate	4
SessionRecords	variabel

Een DailyRecord bestaat uit de volgende elementen:

- **DayRecordLength:** de lengte van het huidige DailyRecord.
  De initiële waarde bij een nieuw DailyRecord (dat nog geen enkel SessionRecord omvat) is '00 0A'H (10); de lengte van de kop van dit DailyRecord (zonder de SessionRecords).
  Gegevenssoort: INTEGER (unsigned)
- **PointerLastSessionRecord:** specificeert het begin van de geheugenplaats (aantal bytes vanaf het begin van EF.Driver_Activity_Data) van de meest recente sessie in dit DailyRecord.
  De initiële waarde bij een nieuw DailyRecord (dat nog geen enkel SessionRecord bevat) is '00 00'H (0).
  Nadat aan dit DailyRecord het eerste SessionRecord is toegevoegd, moet de waarde 10 hoger zijn dan het startadres van dit DailyRecord; bij het eerste SessionRecord van het eerstgeboekte DailyRecord zal dit 20 + 10 = 30 ('00 1E'H) zijn.
  Uitgezonderd de waarde 0, zal de waarde van PointerLastSessionRecord nooit kleiner zijn dan 30 ('00 1E'H).
  Gegevenssoort: INTEGER (unsigned)
- **DayPreviousRecordLength:** de lengte van het vorige DailyRecord. Is er geen vorige DailyRecord omdat deze de oudste is, dan is de waarde '00 00'H (0).
  Uitgezonderd de waarde 0, zal de waarde van DayPreviousRecordLength nooit kleiner zijn dan 10 ('00 0A'H).
  Gegevenssoort: INTEGER (unsigned)

- **DayRecordDate:** de datum waarvoor dit DailyRecord is. Dit is in het formaat JJJJMMDD. Gegevenssoort: BCD
- **SessionRecords:** een of meerdere SessionRecords (zie Figuur 5) voor deze dag.

5.1.2 SessionRecord

Een SessionRecord bevat de gegevens van de activiteiten van de chauffeur voor een kaartsessie. Indien er meerdere kaartsessies op een dag zijn, zijn er voor die dag ook meerdere SessionRecords. Na personaliseren bestaat er nog geen enkel SessionRecord.

Figuur 5: SessionRecord

Naam	Grootte (bytes)	
PointerLastActivityRecord	2	
PointerLastPWActivityRecord	2	
SignatureDateTime		
SignatureDate	8 nibbles	
SignatureTime	6 nibbles	
SessionSignature	256	
SessionCreationDateTime		
SessionCreationDate	8 nibbles	
SessionCreationTime	6 nibbles	299
SystemCardNumber		
Boordcomputernr	9 nibbles	
Kaartvolgnummer	5 nibbles	
Kenteken	6	
CompanyCardNumber		
KvKnummer	12 nibbles	
Kaartvolgnummer	5 nibbles	
Pnummer	7 nibbles	
ActivityRecords	variabel	variabel

De lengte van een SessionRecord kop (zonder de ActivityRecords) is 299 bytes.

Een SessionRecord bestaat uit de volgende elementen:
- **PointerLastActivityRecord:** specificeert het begin van de geheugenplaats (aantal bytes vanaf het begin van EF.Driver_Activity_Data) van de het laatste ActivityRecord in deze SessionRecords.
  De initiële waarde bij een nieuw SessionRecord (nog zonder ActivityRecords) is '00 00'H (0).
  Uitgezonderd de waarde 0, zal de waarde van PointerLastActivityRecord nooit kleiner zijn dan 20+10+299 = 329 ('01 49'H).
  Gegevenssoort: INTEGER (unsigned)
- **PointerLastPWActivityRecord:** specificeert het begin van de geheugenplaats (aantal bytes vanaf het begin van EF.Driver_Activity_Data) van het laatste ActivityRecord met een activiteit "Start pauze" of "Start werk".
  De initiële waarde bij een nieuw SessionRecord (nog zonder ActivityRecords) is '00 00'H (0).
  Zo lang er nog geen "Start pauze" of "Start werk" ActivityRecord in dit SessionRecord aanwezig is, blijft de waarde gelijk aan 0.
  Uitgezonderd de waarde 0, zal de waarde van PointerLastPWActivityRecord nooit kleiner zijn dan 20+10+299 = 329 ('01 49'H).
  Gegevenssoort: INTEGER (unsigned)
- **SignatureDateTime:** het tijdstip direct voorafgaand aan het berekenen van de SessionSignature. Voor verdere informatie over de handtekening zetten, zie 5.4.
  Dit veld bestaat uit twee delen:
  - **SignatureDate:**
    formaat JJJJMMDD,
    initiële waarde bij een nieuw SessionRecord: '00000000'H,
    gegevenssoort BCD.
  - **SignatureTime:**
    formaat hhmmss (24-uurs klok)
    initiële waarde bij een nieuw SessionRecord: '000000'H,
    gegevenssoort BCD.
- **SessionSignature:** de door de boordcomputer gezette handtekening over de gegevens zoals gespecificeerd in § 5.4.
  De initiële waarde bij een nieuw SessionRecord is "ongedefinieerd".
  Gegevenssoort: OCTET_STRING(SIZE(256))
- **SessionCreationDateTime:** het tijdstip waarop dit SessionRecord werd gecreëerd.
  Dit veld bestaat uit twee delen:
  - **SignatureDate:**
    formaat JJJJMMDD,

initiële waarde bij een nieuw SessionRecord: de datum waarop dit SessionRecord werd gecreëerd,
gegevenssoort BCD.
  - **SignatureTime:**
    formaat hhmmss
    initiële waarde bij een nieuw SessionRecord: het tijdstip waarop dit SessionRecord werd gecreëerd,
    gegevenssoort BCD.
- **SystemCardNumber:** bestaat uit 2 delen:
  - **Boordcomputernr**: het nummer van de systeemkaart zoals op het moment van creëren van dit SessionRecord bekend in de boordcomputer (9 digits BCD)
  - **Kaartvolgnummer**: het volgnummer van de systeemkaart zoals op het moment van creëren van dit SessionRecord bekend in de boordcomputer (5 digits BCD)
- **Kenteken:** het kenteken van het voertuig zoals op het moment van creëren van dit SessionRecord bekend in de boordcomputer (6 bytes ASCII)
- **CompanyCardNumber:** bestaat uit 2 delen:
  - **KvKnummer**: Kamer van Koophandel nummer van de ondernemer zoals op het moment van creëren van dit SessionRecord bekend in de boordcomputer (12 digits BCD)
  - **Kaartvolgnummer**: volgnummer van de ondernemerskaart zoals op het moment van creëren van dit SessionRecord bekend in de boordcomputer (5 digits BCD)
- **Pnummer:** personenvervoernummer van de ondernemer zoals op het moment van creëren van dit SessionRecord bekend in de boordcomputer (7 digits BCD)
- **ActivityRecords:** een of meerdere ActivityRecords (zie Figuur 6).

5.1.3 ActivityRecord

Er wordt een aantal types ActivityRecords onderscheiden aan de hand van de activiteit.

Figuur 6: ActivityRecord

Activiteit Type	Kop				Gegevens		Opmerking
	activiteit	handm.	rijden	tijdstip	Veld 1	Veld 2	
Login	'00001'B	'0'B	'0'/'1'B	hh:mm:ss	geen	geen	Het tijdstip waarop de BCT het inloggen constateerde.
		'1'B					Een login kan geen handmatig ingesteld tijdstip hebben. Deze combinatie komt dus niet voor.
(Start) pauze	'00010'B	'0'B	'0'/'1'B	hh:mm:ss	geen	geen	Het tijdstip waarop de BCT de start van de pauze constateerde. Recordvorm indien dit record niet het laatste ActivityRecord van de sessie is.
					aantal secondes pauze		Het tijdstip waarop de BCT de start van de pauze constateerde. Recordvorm indien dit record het laatste ActivityRecord van de sessie is.
		'1'B			geen		Het handmatig opgegeven tijdstip dat de pauze aanving. Recordvorm indien dit record niet het laatste ActivityRecord van de sessie is.
					aantal secondes pauze		Het handmatig opgegeven tijdstip dat de pauze aanving. Recordvorm indien dit record het laatste ActivityRecord van de sessie is.
(Start) werk	'00011'B	'0'B	'0'/'1'B	hh:mm:ss	aantal secondes rijden	geen	Het tijdstip waarop de BCT de start van werk constateerde. Recordvorm indien dit record niet het laatste ActivityRecord van de sessie is.
						aantal secondes werk	Het tijdstip waarop de BCT de start van werk constateerde. Recordvorm indien dit record het laatste ActivityRecord van de sessie is.
		'1'B				geen	Het handmatig opgegeven tijdstip dat werk aanving. Recordvorm indien dit record niet het laatste ActivityRecord van de sessie is.
						aantal secondes werk	Het handmatig opgegeven tijdstip dat werk aanving. Recordvorm indien dit record het laatste ActivityRecord van de sessie is.

Activiteit Type	Kop				Gegevens		Opmerking
	activiteit	handm.	rijden	tijdstip	Veld 1	Veld 2	
Afsluiting	'00100'B	'0'B	'0'/'1'B	hh:mm:ss	geen	geen	reguliere Afsluiting: Het tijdstip waarop de BCT het afsluiten en aftekenen van de sessie constateerde.
Nieuwe eindtijd		'1'B					handmatige Afsluting / Nieuwe eindtijd: Het handmatig opgegeven tijdstip dat een sessie ("werkdag") stopte.
Dagovergang	'00101'B	'0'B	'0'/'1'B	23:59:59	geen	geen	Middernacht automatisch: Een dagovergang geconstateerd tijdens normale modus.
		'1'B					Middernacht handmatig: Een dagovergang geconstateerd tijdens handmatige invoer.

Een ActivityRecord heeft een kop van 24 bits (3 bytes) groot die de volgende elementen bevat:
- **activiteit**: geeft het type activiteit aan (5 bits).
- **handmatig**: geeft aan of het tijdstip van de activiteit handmatig of automatisch is geboekt (1 bit).
- **rijden**: geeft aan of de activiteit tijdens het rijden of stilstaan is geboekt (1 bit).
- **tijdstip**: geeft het starttijdstip van de activiteit aan in het formaat hhmmss. Dit formaat is als volgt opgebouwd:
  - **hh**: 5 bits
  - **mm**: 6 bits
  - **ss**: 6 bits

Noot 1: Bij de activiteit "Start werk" wordt een Rijtijdveld aan de kop toegevoegd. Dit werkt als volgt:
- gedurende het werk wordt volautomatisch bijgehouden hoeveel secondes er gereden worden (3 bytes INTEGER (unsigned)). Wanneer (na een periode van rijden gedurende werktijd) het aantal secondes gewijzigd is, wordt hetzelfde record opnieuw geschreven, waarbij de kop gelijk blijft en het aantal secondes aangepast. Dit bijwerken van rijtijd moet ook plaatsvinden indien de laatste keer bijwerken (meer dan) vijf minuten geleden was. Er wordt dus geen nieuw record aangemaakt.

Noot 2: Bij zowel de activiteit "Start werk" als "Start pauze" wordt een Tijdsduurveld aan de kop toegevoegd. Dit werkt als volgt:
- gedurende het werk / de pauze wordt volautomatisch bijgehouden hoeveel secondes er verstreken zijn sinds de activiteit startte (3 bytes INTEGER (unsigned)). Telkens wanneer de auto stopt en telkens vijf minuten na de vorige vastlegging van de tijdsduur worden de laatste 3 bytes van hetzelfde record opnieuw geschreven, waarbij de voorgaande bytes gelijk blijven en het aantal secondes aangepast. Er wordt dus geen nieuw record aangemaakt.
- Het eerstvolgende toe te voegen ActivityRecord overschrijft deze laatste 3 bytes (de daadwerkelijke tijdsduur van de dan voorafgaande "Start werk" / "Start pauze" activiteit wordt met de starttijd van de nieuwe activiteit definitief vastgelegd).

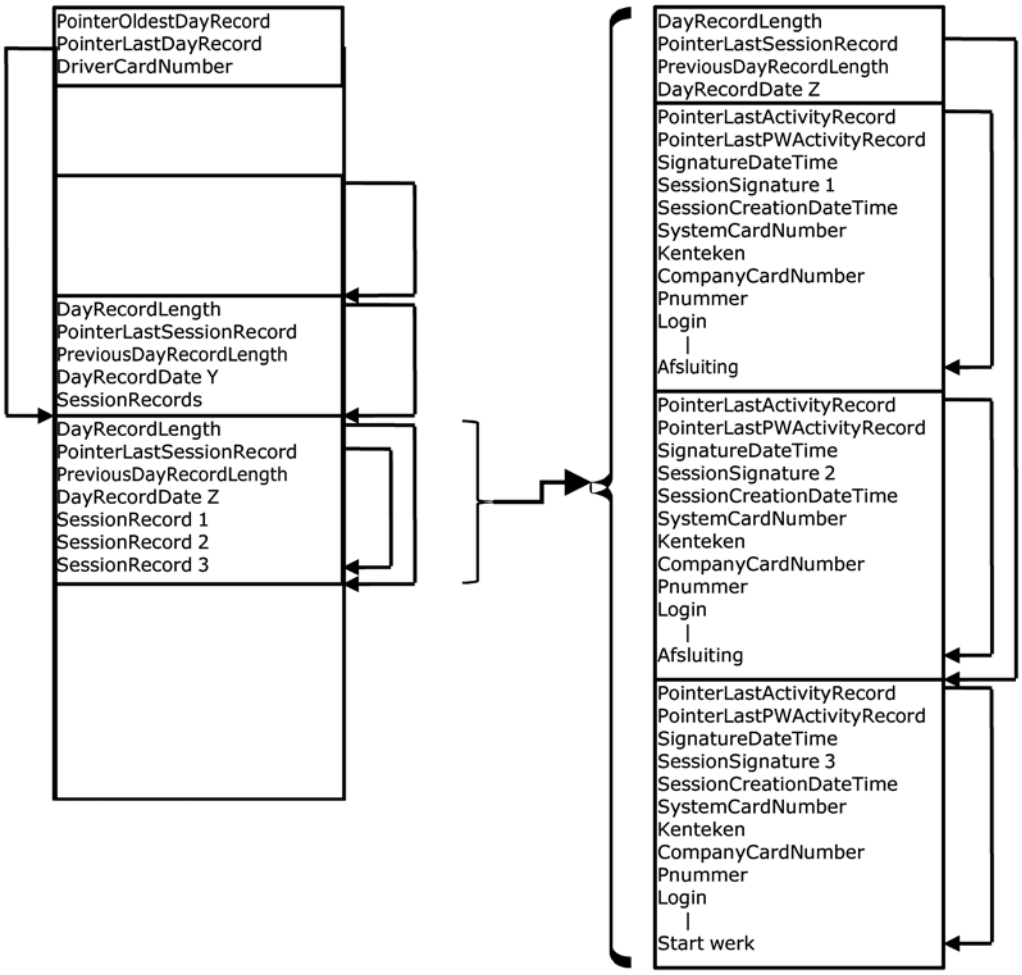
Noot 3: Bij iedere toevoeging van een ActivityRecord bestaat de mogelijkheid dat er een nieuw DailyRecord en/of nieuw SessionRecord aangemaakt moet worden. Zie hiervoor ook § 7.5 en § 0.

5.1.4 Overzicht

De gegevens worden per dag vastgelegd en moeten minimaal 31 kalenderdagen beschikbaar blijven op de kaart. Voor iedere dag dat er gegevens op de chauffeurskaart vastgelegd moeten worden, wordt er een DailyRecord aangemaakt.

Naast de arbeids- rij- en rusttijden zelf moet ook vastgelegd worden voor welke ondernemer en in welk voertuig deze tijden gemaakt zijn en welke boordcomputer er gebruikt is. Dit wordt per sessie vastgelegd in het SessionRecord.

In Figuur 7 staat een overzicht van EF.Driver_Activity_Data en hoe de verschillende records hier onder vallen.



Figuur 7: Overzicht EF.Driver_Activity_Data

5.2 Schrijven naar EF.Driver_Activity_Data

Activiteiten van de chauffeur worden opgeslagen in ActivityRecords. In Figuur 6 worden de verschillende typen van ActivityRecords genoemd. Het verloop van een sessie staat in hoofdstuk 7 beschreven. Het exacte verloop van het toevoegen van een ActivityRecord staat in § 0.

5.2.1 Toevoegen van de eerste activiteit binnen een SessionRecord

Elk van de navolgende subparagrafen (5.2.2 t/m 5.2.7) gaat er van uit dat de toe te voegen activiteit niet de ***eerste*** activiteit binnen het betreffende SessionRecord is. Indien dat echter wél het geval is, moeten de instructies voor het overschrijven van de PointerLastActivityRecord en de DayRecordLength velden telkens worden vervangen door de volgende:

1. In het SessionRecord dient PointerLastActivityRecord gezet te worden op PointerLastSessionRecord + 299;
2. In het huidige DailyRecord dient de DayRecordLength verhoogd te worden met de (ongecorrigeerde) lengte van het toe te voegen ActivityRecord:
   - Voor een “Start werk”, verhogen met 9;
   - Voor een “Start pauze”, verhogen met 6;
   - Voor elke andere activiteit, verhogen met 3.

5.2.2 Toevoegen “Login” activiteit

De “Login” activiteit geeft de werkelijke tijd aan dat de chauffeurskaart in de boordcomputer ingebracht is en de authenticatie plaatsgevonden heeft. Dit is het login-tijdstip. Dit staat beschreven in 7.1. Bij een “Login” wordt er een nieuw ActivityRecord aangemaakt.

PointerLastSessionRecord geeft het begin van het huidige SessionRecord aan.
In dit SessionRecord wordt

1. PointerLastActivityRecord verhoogd met de lengte van de laatste ActivityRecord (verminderd met 3 indien het huidige ActivityRecord een “Start werk” of “Start pauze” betreft).
2. het ActivityRecord “Login” toegevoegd op de plaats die aangegeven wordt door de verhoogde PointerLastActivityRecord. Dit record bestaat uit 3 bytes (alleen een kop). De handmatig bit staat altijd op ‘0’B.
3. SessionSignature = de tussentijdse handtekening (zie 5.4).

In het huidige DailyRecord wordt
1. DayRecordLength = oude waarde DayRecordLength + 3 (verminderd met 3 indien het (inmiddels) vorige ActivityRecord een “Start werk” of “Start pauze” betreft).
2. Direct na het toevoegen van de “Login” activiteit wordt een (automatisch) geklokte “Start werk” activiteit toegevoegd.

5.2.3 Toevoegen “Start pauze” activiteit

Bij een “Start pauze” wordt er een nieuw ActivityRecord aangemaakt.

PointerLastSessionRecord geeft het begin van het huidige SessionRecord aan.
In dit SessionRecord wordt
1. PointerLastActivityRecord verhoogd met de lengte van de laatste ActivityRecord (verminderd met 3 indien het huidige ActivityRecord een “Start werk” of “Start pauze” betreft).
2. PointerLastPWActivityRecord wordt gelijkgesteld aan de zojuist verhoogde PointerLastActivityRecord.
3. het ActivityRecord “Start pauze” toegevoegd op de plaats die aangegeven wordt door de verhoogde PointerLastActivityRecord. Dit record bestaat uit 6 bytes (een kop + een tijdsduurteller), waarbij de tijdsduurteller initieel wordt gevuld met ‘00 00 00’H en daarna periodiek wordt bijgewerkt volgens Noot 2 in § 5.1.3.
4. SessionSignature = de tussentijdse handtekening (zie 5.4).

In het huidige DailyRecord wordt
1. DayRecordLength = oude waarde DayRecordLength + 6 (verminderd met 3 indien het (inmiddels) vorige ActivityRecord een “Start werk” of “Start pauze” betreft).

5.2.4 Toevoegen “Start werk” activiteit

Bij een “Start werk” wordt er een nieuw ActivityRecord aangemaakt.

“Start werk” wijkt af van de andere activiteiten. Hierin wordt bijgehouden hoeveel secondes het voertuig gereden heeft gedurende deze activiteit. Zolang de chauffeur nog aan het werk is en het voertuig afwisselend rijdt en stilstaat, wordt iedere keer zodra het voertuig stopt het aantal secondes dat er gereden is bijgewerkt. Er wordt dus niet iedere keer een nieuw ActivityRecord aangemaakt.

PointerLastSessionRecord geeft het begin van het huidige SessionRecord aan.
In dit SessionRecord wordt
1. PointerLastActivityRecord verhoogd met de lengte van de laatste ActivityRecord (verminderd met 3 indien het huidige ActivityRecord een “Start werk” of “Start pauze” betreft).
2. PointerLastPWActivityRecord wordt gelijkgesteld aan de zojuist verhoogde PointerLastActivityRecord.
3. het ActivityRecord “Start werk” toegevoegd op de plaats die aangegeven wordt door de verhoogde PointerLastActivityRecord.
   Dit record bestaat uit een kop van 3 bytes gevolgd door 2 x 3 bytes data.
   De data geeft het aantal secondes aan dat er met het voertuig gereden is en het aantal secondes dat deze activiteit in totaal duurde. Bij het begin van “Start werk” zijn beiden ‘00 00 00’H. Deze waardes worden conform Noten 1 en 2 in § 5.1.3 tussentijds bijgewerkt tot er een andere activiteit plaats vindt.
4. SessionSignature = de tussentijdse handtekening (zie 5.4).

In het huidige DailyRecord wordt
1. DayRecordLength = oude waarde DayRecordLength + 9 (verminderd met 3 indien het (inmiddels) vorige ActivityRecord een “Start werk” of “Start pauze” betreft).

5.2.5 Toevoegen “Afsluiting” activiteit

Bij een normale afsluiting door de chauffeur, “Afsluiting”, wordt er een nieuw ActivityRecord aangemaakt.

PointerLastSessionRecord geeft het begin van het huidige SessionRecord aan.
In dit SessionRecord wordt
1. PointerLastActivityRecord verhoogd met de lengte van de laatste ActivityRecord (verminderd met 3 indien het huidige ActivityRecord een “Start werk” of “Start pauze” betreft).
2. het ActivityRecord “Afsluiting” toegevoegd op de plaats die aangegeven wordt door de verhoogde PointerLastActivityRecord. Dit record bestaat uit 3 bytes (alleen een kop).
3. SessionSignature = de definitieve handtekening (zie 5.4).

In het huidige DailyRecord wordt
1. DayRecordLength = oude waarde DayRecordLength + 3 (verminderd met 3 indien het (inmiddels) vorige ActivityRecord een “Start werk” of “Start pauze” betreft).

5.2.6 Toevoegen “Nieuwe eindtijd” (=handmatige Afsluiting) activiteit

Wanneer er bij een sessie nog activiteiten toegevoegd worden, kan het voorkomen dat de eindtijd aangepast moet worden. Dit wordt gedaan met een “Nieuwe eindtijd” activiteit. Hierbij wordt er een nieuwe ActivityRecord aangemaakt.

PointerLastSessionRecord geeft het begin van het huidige SessionRecord aan.
In dit SessionRecord wordt
1. PointerLastActivityRecord verhoogd met de lengte van de laatste ActivityRecord (verminderd met 3 indien het huidige ActivityRecord een “Start werk” of “Start pauze” betreft).
2. het ActivityRecord “Nieuwe eindtijd” toegevoegd op de plaats die aangegeven wordt door de verhoogde PointerLastActivityRecord. De handmatig-bit staat hier altijd op ‘1’B. Dit record bestaat uit 3 bytes (alleen een kop).
3. SessionSignature = de definitieve handtekening (zie 5.4).

In het huidige DailyRecord wordt
1. DayRecordLength = oude waarde DayRecordLength + 3 (verminderd met 3 indien het (inmiddels) vorige ActivityRecord een “Start werk” of “Start pauze” betreft).

5.2.7 Toevoegen “Dagovergang (handmatig/automatisch)” activiteit

Wanneer er een sessie actief is, de laatstgeboekte activiteit een “Start werk” of “Start pauze” is en:
- (situatie 1) het betreft een automatische activiteit en de BCT-klok geeft 0:00:00u aan OF;
- (situatie 2) er wordt een handmatige activiteit toegevoegd met een tijdstip op of na 0:00:00u van de dag volgend op het huidige DailyRecord,

dan moet:
- de rijtijdteller worden bijgewerkt indien de laatstgeboekte activiteit een “Start werk” betreft,
- de huidige sessie gestopt worden door toevoeging van een “Dagovergang” activiteit met:
  - het tijdstip 23:59:59u
  - het handmatig bit op ‘0’B indien het situatie 1 betreft OF
  - het handmatig bit op ‘1’B indien het situatie 2 betreft,
- de huidige sessie worden “afgetekend” door de boordcomputer
- EN een nieuw DailyRecord voor de volgende kalenderdag worden aangemaakt met een nieuw SessionRecord en een eerste ActivityRecord met
  - hetzelfde ActivityType als de laatstgeboekte activiteit EN
  - het tijdstip op 00:00:00u
  - het handmatig bit op ‘0’B indien het situatie 1 betreft OF
  - het handmatig bit op ‘1’B indien het situatie 2 betreft

Het toevoegen van het nieuwe DailyRecord met een nieuw SessionRecord en een eerste “Start pauze” of “Start werk” activiteit wordt beschreven in respectievelijk § 8.11, § 8.10, § 5.2.1 en § 5.2.3 / 5.2.4. Hier wordt uitsluitend toevoeging van de “Dagovergang” aan het huidige SessionRecord beschreven.

PointerLastSessionRecord geeft het begin van het huidige SessionRecord aan.
In dit SessionRecord wordt
1. PointerLastActivityRecord verhoogd met de lengte van het laatste ActivityRecord verminderd met 3 omdat het huidige ActivityRecord een “Start werk” of “Start pauze” betreft.
2. het ActivityRecord “Dagovergang” toegevoegd op de plaats die aangegeven wordt door de verhoogde PointerLastActivityRecord. De handmatig-bit en het tijdstip worden gevuld zoals hierboven beschreven. Dit record bestaat uit 3 bytes (alleen een kop).
3. SessionSignature = de definitieve handtekening (zie 5.4).

In het huidige DailyRecord blijft DayRecordLength gelijk, omdat het (inmiddels) vorige ActivityRecord een “Start werk” of “Start pauze” betreft.

NB. Indien de invoeging van de dagovergang en de nieuwe kalenderdag het gevolg is van het toevoegen van een handmatige activiteit, dan kán het zo zijn dat er meer dan één kalenderdag tussen de huidige activiteit en de toe te voegen activiteit bestaat. Indien dat zo blijkt te zijn dan dienen de instructies in deze paragraaf te worden herhaald voor iedere betreffende (kalender)dagovergang.

5.3 Algemene opmerkingen bij lezen en schrijven naar EF.Driver_Activity_Data

Bij lees- en schrijfacties (Read Binary en Update Binary) dient met de volgende punten rekening te worden gehouden:

1. EF.Driver_Activity_Data kan records bevatten vanaf positie '00 14'H tot aan het eind (Length_EF.Driver_Activity_Data). De eerste 20 bytes van EF.Driver_Activity_Data worden in beslag genomen worden door twee 16-bits pointers en een 16-bytes veld voor het chauffeurskaartnummer.
2. Wanneer er voor een toevoeging niet meer voldoende ruimte aan het eind van EF.Driver_Activity_Data is, wordt eerst de resterende ruimte benut en daarna gaat het toevoegen verder vanaf het begin van de EF.Driver_Activity_Data. Dit is dan vanaf positie '00 14'H.
3. De lengte van een te lezen of te schrijven record kan nooit langer zijn dan Length_EF.Driver_Activity_Data – 20 ('14'H).
4. De offset bij een Read Binary of Update Binary (Pointer_1) moet kleiner zijn dan Length_EF.Driver_Activity_Data. Indien dit niet het geval is, moet de offset vervangen worden door de Pointer_1 – Length_EF.Driver_Activity_Data + 20 ('14'H).
5. Indien bij een Read Binary de offset (Pointer_1) + het verwachte aantal bytes in de response (Length_1) groter is dan Length_EF.Driver_Activity_Data, dan moet de Read Binary in tweeën gesplitst worden: 1 Read Binary tot aan het eind van EF.Driver_Activity_Data en 1 Read Binary vanaf positie '00 14'H tot aan Pointer_1 + Length_1 – Length_EF.Driver_Activity_Data + 20 ('14'H).
6. Indien bij een Update Binary de offset (Pointer_1) + het aantal weg te schrijven bytes (Length_1) groter is dan Length_EF.Driver_Activity_Data, dan moet de Update Binary in tweeën gesplitst worden: 1 Update Binary tot aan het eind van EF.Driver_Activity_Data en 1 Update Binary vanaf positie '00 14'H tot aan Pointer_1 + Length_1 – Length_EF.Driver_Activity_Data + 20 ('14'H).
7. Bij een Update Binary bestaat de mogelijkheid dat de oudste dagregistratie overschreven wordt. Dit is het geval wanneer data voorbij PointerOldestDayRecord geschreven zou worden. Hier moet dus bij iedere schrijfactie op getest worden.
   Om te voorkomen dat voorbij PointerOldestDayRecord geschreven wordt, moet het oudste DailyRecord weggehaald worden.
   Dit wordt op de volgende manier gedaan:
   1. PointerOldestDayRecord wijst naar het oudste DailyRecord. In dit DailyRecord staat de lengte van dit record (DayRecordLength). Uit deze pointer en lengte kan de positie van het volgende DailyRecord bepaald worden.
   2. In dit volgende DailyRecord wordt de PreviousDayRecordLength op '00 00'H gezet.
   3. PointerOldestDayRecord wordt op de positie van dit volgende DailyRecord gezet.
   4. Wanneer er nog niet genoeg ruimte is voor de toevoeging, moeten de bovenstaande punten herhaald worden.

5.4 Digitale handtekening

Om de integriteit van gegevens te waarborgen, worden digitale handtekeningen gebruikt. Er worden twee soorten digitale handtekeningen onderscheiden:

1. De handtekening die door de chauffeurskaart over de gegevens van de kaartsessie gezet wordt in de boordcomputer.
2. De handtekening die door de boordcomputer gezet wordt over de kaartsessie gegevens op de chauffeurskaart.

In dit document gaat het om de tweede soort, waarbij de handtekeningen op de chauffeurskaart worden opgeslagen. De handtekeningen die op de boordcomputer opgeslagen worden, worden hier verder buiten beschouwing gelaten.

De digitale handtekening wordt berekend over het DriverCardNumber, de DayRecordDate en een deel van het SessionRecord (zie 5.1.2) en wordt opgeslagen in het veld SessionSignature in het betreffende SessionRecord. Daarbij worden de mogelijke vorige SignatureDateTime en handtekening in dit SessionRecord overschreven. Het te ondertekenen DriverCardNumber is een 16-karakter PrintableString zoals die aansluitend op het inloggen van de chauffeur door de boordcomputer uit de eerste 16 bytes van het subject.serialNumber van het authenticiteitcertificaat van de chauffeurskaart is gelezen. De *kopie* van het DriverCardNumber die is opgeslagen in bytes '00 04'H t/m '00 13'H van EF.Driver_Activity_Data mag NIET worden gebruikt bij de berekening van de handtekening.

Om het verlies van gegevens zoveel mogelijk te voorkomen wanneer de chauffeurskaart voortijdig

uitgenomen wordt, wordt er na iedere ***toevoeging*** van een ActivityRecord (zie 5.1.3) een digitale handtekening berekend en opgeslagen.
Bij de berekening van de handtekening wordt van het laatst toegevoegde ActivityRecord alleen de kop van 3 bytes meegenomen. De reden hiervoor is gelegen in de activiteiten "Start werk" en "Start pauze". De 6 respectievelijk 3 gegevensbytes die bij deze activiteitsoorten horen worden te vaak bijgewerkt (voor het telkens herberekenen van handtekeningen) en de laatste 3 gegevensbytes worden sowieso overschreven door de vervolgactiviteit. De rijtijdteller van een "Start werk" activiteit wordt hiermee pas meegenomen in de handtekening nadat een vervolgactiviteit wordt gestart.

Om een handtekening te kunnen berekenen, moet eerst de SignatureDateTime worden bijgewerkt met de huidige datum en tijd volgens BCT-klok, dan moet een hashcode berekend worden. Deze hashcode wordt dan gebruikt als input voor het berekenen van de handtekening. De gegevens voor het berekenen van de hashcode moeten in de hieronder genoemde volgorde staan:

1. DriverCardNumber	16 bytes ASCII
2. DayRecordDate	4 bytes BCD
3. SessionCreationDateTime	4 + 3 bytes BCD
4. SystemCardNumber	4½ + 2½ bytes BCD
5. Kenteken	6 bytes ASCII
6. CompanyCardNumber	6 + 2½ bytes BCD
7. Pnummer	3½ bytes BCD
8. ActivityRecords*)	variable
9. PointerLastActivityRecord	2 bytes INTEGER
10. PointerLastPWActivityRecord	2 bytes INTEGER
11. SignatureDateTime	4 + 3 bytes BCD

*) Van het laatste ActivityRecord wordt alleen de kop (3 bytes) meegenomen.

De berekening van de handtekening wordt volledig door de boordcomputer uitgevoerd en gebeurt als volgt:
- Over de gegevens, als hierboven vermeld, wordt met behulp van de private sleutel voor authenticiteit van de boordcomputer een handtekening gegenereerd volgens PKCS#1 v1.5 met SHA-256.
- De handtekening wordt opgeslagen in het SessionSignature veld van het huidige SessionRecord.

NB. Telkens bij het berekenen van de SHA-256 hash dient de boordcomputerlogica het eerste en grootste deel van de berekening (de hash over de data vanaf het DriverCardNumber t/m de ActivityRecords) uit te voeren, waarna het laatste deel van de hashberekening (over de PointerLastActivitityRecord t/m de SignatureDateTime) door de systeemkaart dient te worden berekend. Ook de PKCS#1 v1.5 handtekening dient door de systeemkaart te worden berekend.

NB2. Met behulp van het certificaat behorende bij de private sleutel voor authenticiteit van de boordcomputer (het boordcomputercertificaat) kan gecontroleerd worden of de gegevens in een SessionRecord authentiek zijn. Behalve het boordcomputercertificaat en het SessionRecord zelf, zijn voor zo'n validatie het DriverCardNumber en de DayRecordDate benodigd. Die twee gegevens staan elders in EF.Driver_Activity_Data opgeslagen. Welk boordcomputercertificaat voor een bepaalde SessionRecord-validatie moet worden gebruikt, kan worden achterhaald door het SystemCardNumber in de SessionRecord-kop uit te lezen.

NB3. Indien bij het valideren van de SessionRecord-data de betreffende EF.BCT_Certificates aanwezig is en het betreffende boordcomputercertificaat is daarin ook (nog) aanwezig, kan de validatie direct worden uitgevoerd. Indien het betreffende boordcomputercertificaat niet (meer) in EF.BCT_Certificates is opgeslagen of indien EF.BCT_Certificates niet voorhanden is, dan kan het betreffende boordcomputercertificaat via de Kaartuitgever worden verkregen.

6 Gegevens op chauffeurskaart (EF.BCT_Certificates)

De certificaten van de boordcomputer die gebruikt zijn bij het berekenen van de handtekeningen op de chauffeurskaart worden opgeslagen in EF.BCT_Certificates. Hierin is plaats voor de systeemkaartcertificaten van de 3 verschillende boordcomputers waarin de chauffeurskaart het laatst is gebruikt.

Een boordcomputer dient een bestuurder (tijdig) te waarschuwen dat de momenteel op de chauffeurskaart opgeslagen arbeids-, rij- en rusttijden moeten worden geëxporteerd (ook wel "gedownload"). Aan EF.BCT_Certificates is daarom een extra gegevensstructuur toegevoegd die vermeldt wanneer en naar welke boordcomputer welke dailyrecords zijn geëxporteerd.

6.1 Opbouw van EF.BCT_Certificates

Figuur 8: EF.BCT_Certificates

Naam	Grootte (bytes)
Rank Index Certificates	3 3 x 7 3 x 2100
IndexOldestDL DownloadLogs FILLER	1 8 x 33 11
Totaal	6600

EF.BCT_Certificates is opgebouwd uit de volgende elementen:

- **Rank:** Hierin wordt aangegeven in welke volgorde (van meest naar minst recent) de navolgende certificaten zijn gebruikt. Iedere byte correspondeert met een van de certificaten in Certificates (byte 1 <-> certificaat 1 en dergelijke). De (initiële) waarde 0 geeft aan dat er geen certificaat op die plaats staat en de waarde 1 – 3 hoe recent het bijbehorende certificaat is (waarbij de waarde 1 het meest recent is).
  Gegevenssoort: INTEGER (unsigned)
- **Index:** Een index bestaat uit een systeemkaartnummer (het boordcomputernummer (BCD-9) gevolgd door het kaartvolgnummer (BCD-5)), voor ieder opgeslagen certificaat (3x). Iedere index correspondeert met een van de certificaten in Certificates (index 1 <-> certificaat 1 en verder).
  De initiële waarde voor iedere index is '00 00 00 00 00 00 00'.
  Gegevenssoort: BCD
- **Certificates:** Hierin worden de 3 meest recente certificaten van boordcomputers opgeslagen. In Rank is te vinden hoe recent een bepaald certificaat is en in Index staat het bijbehorende boordcomputernummer en kaartvolgnummer. Initieel zijn de certificaten gevuld met nullen ('00').
  Indien een certificaat korter is dan 2100 bytes, wordt de resterende ruimte opgevuld met '00'-bytes.
  Gegevenssoort: OCTET STRING
  NB. Een certificaat is een ASN.1 DER gecodeerde TLV-gegevensstructuur die voor BCT certificaten begint met een 8-bits Tag (30h), een byte dat aangeeft dat er 2 lengte bytes volgen (82h) en een 16-bits Length en gevolgd wordt door een Value van zoveel bytes als aangegeven door Length.
- **IndexOldestDL:** Hierin wordt aangegeven welke van de navolgende (8) DownloadLog items het oudste is en dus als eerste overschreven zal worden. Initieel zal dit veld gevuld worden met de waarde 0 ('00'H) en de maximale waarde zal 7 ('07'H) zijn (0 wijst naar DownloadLog_1 en 7 wijst naar DownloadLog_8). Na het overschrijven van DownloadLog_8 zal IndexOldestDL gereset moeten worden naar 0.
  De initiele vulling zal volledig uit nullen ('00'H) bestaan.
  Gegevenssoort: OCTET STRING
- **DownloadLogs:** Hierin wordt informatie bijgehouden van de 8 meest recente keren dat de bestuurder de inhoud van EF.Driver_Activity_Data naar een boord computer heeft gedownload. Elk van deze log items (DownloadLog_1 t/m DownloadLog_8) bestaat uit 33 bytes.
  Gegevenssoort: INTEGER (unsigned)

In Figuur 9 wordt een overzicht van EF.BCT_Certificates gegeven met de initiële waardes.

Figuur 9: Initiële waardes EF.BCT_Certificates

Positie	Gegevens	Bytes	Benaming	
00 00	00	1	Rank_1	**Rank**
00 01	00	1	Rank_2	
00 02	00	1	Rank_3	
00 03	00 – 00	7	Index_1	**Index**
00 0A	00 – 00	7	Index_2	
00 11	00 – 00	7	Index_3	

Positie	Gegevens	Bytes	Benaming	
00 18	00 – 00	2100	Certificate_1	**Certificates**
08 4C	00 – 00	2100	Certificate_2	
10 80	00 – 00	2100	Certificate_3	
18 B4	00	1	IndexOldestDL	**IndexOldestDL**
18 B5	00 – 00	33	DownloadLog_1	**DownloadLogs**
18 D6	00 – 00	33	DownloadLog_2	
18 F7	00 – 00	33	DownloadLog_3	
19 18	00 – 00	33	DownloadLog_4	
19 39	00 – 00	33	DownloadLog_5	
19 5A	00 – 00	33	DownloadLog_6	
19 7B	00 – 00	33	DownloadLog_7	
19 9C	00 – 00	33	DownloadLog_8	
19 BD	00 – 00	11	FILLER	**FILLER**
19 C8	end of file (6600 bytes totaal)			

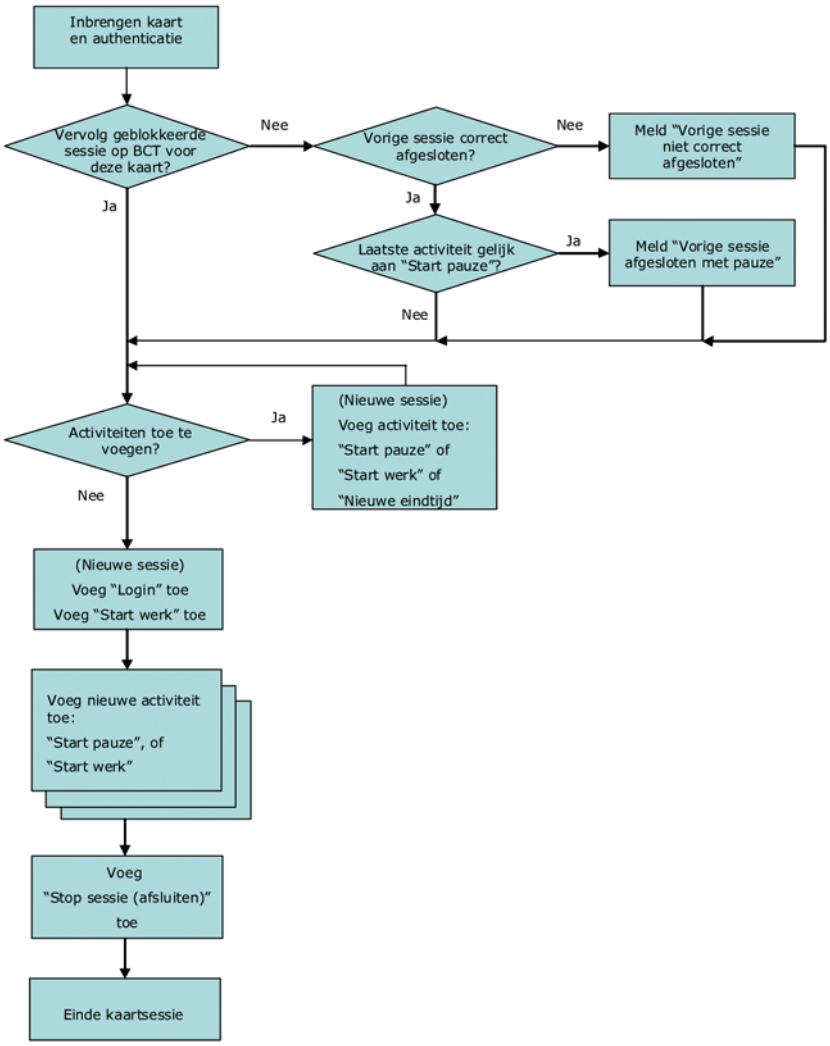
Noot: Positie en gegevens zijn in hexadecimale notatie weergegeven
Noot: CertLength = 2100 (‘08 34’H)

De opbouw van een DownloadLog_X gegevensstructuur is opgenomen in de onderstaande figuur.

Naam	Grootte			
DownloadLog_X				33 bytes
CarAndCompany			25 bytes	
SystemCardNumber		7 bytes		
Boordcomputernr	9 nibbles			
Kaartvolgnummer	5 nibbles			
Kenteken		6 bytes		
CompanyCardNumber		17 nibbles		
KvKnummer	12 nibbles			
Kaartvolgnummer	5 nibbles			
Pnummer		7 nibbles		
DownloadPeriod			8 bytes	
OldestDate		8 nibbles		
DownloadDate		8 nibbles		

7 Kaartsessie

Een kaartsessie is de periode tussen het ingeven van de chauffeurskaart en het wegschrijven van de afsluitende gegevens op de chauffeurskaart door de boordcomputer. In Figuur 10 is het overzicht van een kaartsessie weergegeven.
De wijzigingen in de arbeids- rij- en rusttijden worden tijdens een kaartsessie op de chauffeurskaart opgeslagen in ActivityRecords (zie Figuur 6 en paragrafen 5.2 en 0). Hieronder wordt aangegeven welke informatie op welk ogenblik opgeslagen wordt. Voor voorbeelden van kaartsessies wordt verwezen naar Bijlage A.



Figuur 10: Overzicht kaartsessie

7.1 Begin van een kaartsessie

Het begin van een kaartsessie gaat als volgt:

1. De chauffeurskaart wordt in de boordcomputer ingebracht en er vindt een authenticatie van de chauffeurskaart plaats. Zie hiervoor § 0. Dit ogenblik bepaalt het login-tijdstip wat in stap 5 als activiteitrecord wordt toegevoegd.
2. Direct na het inloggen moet worden geverifieerd of in posities '00 04'H t/m '00 13'H van de EF.Driver_Activity_Data het chauffeurskaartnummer nog steeds overeenstemt met het chauffeurskaartnummer zoals dat in (de eerste 16 bytes van) het subject.serialNumber van het authenticiteitcertificaat is opgeslagen. Indien het niet meer overeenstemt, dienen de genoemde byteposities in EF.Driver_Activity_Data te worden bijgewerkt en dient de gebruiker te worden gewaarschuwd. Ook dient in deze stap de daadwerkelijke grootte van EF.Driver_Activity_Data te worden vastgesteld. Zie hiervoor § 9.5.
3. Er wordt dan gecontroleerd of het certificaat van deze boordcomputer al op deze chauffeurskaart staat en zo niet, dan wordt dit toegevoegd (zie 6 Gegevens op chauffeurskaart (EF.BCT_Certificates)). In beide gevallen wordt dit certificaat als meest recente gemarkeerd. Eventueel andere, reeds bestaande certificaatentries worden gemarkeerd als minder recente. Indien er geen ruimte meer is vervalt de oudste entry.
4. Er wordt gecontroleerd of er op de boordcomputer nog een geblokkeerde sessie voor deze kaart is (zie 7.4):
   – Is er geen geblokkeerde sessie voor deze kaart op de boordcomputer of is de kaart inmiddels in een andere boordcomputer gebruikt, dan wordt gecontroleerd of op de kaart de vorige sessie correct afgesloten was.
   Hiervoor moet de laatste activiteit in het huidige SessionRecord "Afsluiting", "Nieuwe

eindtijd" of "Dagovergang" zijn. Is dit niet het geval, dan wordt de gebruiker er op geattendeerd dat deze vorige sessie niet correct was afgesloten.
- Is de laatste activiteit in het laatste SessionRecord een "Afsluiting", "Dagovergang" of "Nieuwe eindtijd" en wijst de PointerLastPWActivityRecord van dat SessionRecord naar een "Start pauze" activiteit, dan is er iets bijzonders aan de hand. Een arbeidsperiode lijkt dan te eindigen met een pauze. In dit geval dient de boordcomputer de bestuurder er extra op te attenderen dat er mogelijk een handmatige aanvulling / correctie benodigd is die met stap 5 kan worden gedaan.
- Is er nog een geblokkeerde sessie voor deze kaart op de boordcomputer en is de kaart tussentijds niet in een andere boordcomputer gebruikt, dan vervalt de blokkering en wordt de sessie vervolgd.

5. Zijn er, tussen de laatst op de kaart geboekte "Start werk" of "Start pauze" activiteit en het onthouden login-tijdstip, nog activiteiten toe te voegen, dan kan dat nu gebeuren (zie vooral ook het tweede aandachtsstreepje van de vorige stap).
   Bepaal hiertoe de start-datumtijd en de eventuele eind-datumtijd van die laatstgeboekte "Start pauze" of "Start werk" activiteit, waarbij de eindtijd hetzij kan worden gelezen uit de afsluitingsactiviteit die volgt op de "Start werk" / "Start pauze", hetzij kan worden berekend m.b.v. de tijdsduurteller van de "Start werk" / "Start pauze" zelf.
   In dat geval,
   - Presenteer de laatstgeboekte "Start werk" / "Start pauze" inclusief diens uitgelezen start- en eind-datumtijd.
   - Dan kan er een "Start werk" of een "Start pauze" activiteit toegevoegd worden.
     De standaard (start)datumtijd hiervoor is de eind-datumtijd van de laatste "Start werk" of "Start pauze" activiteit; dit kan de gebruiker veranderen in een waarde tussen minimaal de start-datumtijd van die laatste "Start werk" of "Start pauze" activiteit en maximaal het login-tijdstip. De "handmatig"-bit wordt op '1'B gezet.
     Een start die eerder is dan het einde van de vorige "Start werk" of "Start pauze" activiteit, zal die eerdere activiteit geheel of gedeeltelijk veranderen.
     Een start die gelijk is dan het einde van de vorige "Start werk" of "Start pauze" activiteit, zal direct op die eerdere activiteit aansluiten.
     Een start die later is dan het einde van de vorige "Start werk" of "Start pauze" activiteit, zal een rustperiode inlassen.
     Gebruik voor het toevoegen van deze handmatige activiteit de logica beschreven in § 0 en geef daarbij door of een kaartsessie al dan niet gecontinueerd mocht worden.
   - Ook kan er voor gekozen worden om handmatig een "Nieuwe eindtijd" op te geven.
     Ook daarvan kan de datumtijd ingesteld worden tussen minimaal de start-datumtijd van de laatste activiteit en maximaal het login-tijdstip.
     De "handmatig"-bit wordt op '1'B gezet.
     Een nieuw einde dat gelijk is aan de start van de vorige "Start werk" of "Start pauze" activiteit, zal die eerdere activiteit effectief verwijderen.
     Een nieuw einde tussen de start en het (momenteel geldende) einde van de vorige "Start werk" of "Start pauze" activiteit, zal die eerdere activiteit effectief inkorten.
     Een nieuw einde later dan het (momenteel geldende) einde van de vorige activiteit, zal die eerdere activiteit effectief verlengen.
     Gebruik voor het toevoegen van deze handmatige activiteit de logica beschreven in § 0 en geef daarbij door of een kaartsessie al dan niet gecontinueerd mocht worden.
   - Toevoegen kan meerdere keren uitgevoerd worden. De laatst (handmatig) toegevoegde activiteit geldt dan telkens als de "vorige".
   - De mogelijkheid bestaat dat dit toevoegen over meerdere dagen gaat. In dat geval zal de logica beschreven in § 0 de eventuele aanmaak van nieuwe DailyRecords en/of SessionRecords verzorgen.
   - Hoeft er niets meer toegevoegd te worden, dan kan met de volgende stap worden verder gegaan.
6. Vervolgens wordt het login-tijdstip middels een "Login" activiteit toegevoegd (zie 5.2.1), waarna direct een "Start werk" (zie 5.2.4) zal worden toegevoegd. Beide ActivityRecords zullen de handmatig bit op '0'B hebben staan.
   ook nu zullen de toevoegingen gedaan worden conform de logica beschreven in § 0
   Vanaf dit punt begint de reguliere vastlegging van activiteiten.

7.2 Tijdens een kaartsessie

Tijdens een kaartsessie zijn er twee activiteiten mogelijk: "Start pauze" en "Start werk". Voor het toevoegen van deze activiteiten, zie 5.2.1 respectievelijk 5.2.4.
"Start werk" moet regelmatig bijgewerkt worden met het aantal secondes dat er met het voertuig gereden is (zie Noot 1 in § 5.1.3). "Start werk" en "Start pauze" moeten regelmatig bijgewerkt worden met het aantal secondes dat de betreffende activiteit duurt (zie Noot 2 in § 5.1.3).

7.3 Afsluiten van een kaartsessie

Bij het beeindigen van een kaartsessie dient de chauffeur de kaartsessie af te sluiten, voordat hij de chauffeur zijn kaart uit de boordcomputer neemt. Zou hij de sessie niet afsluiten wordt deze geblokkeerd.

Bij het afsluiten van een kaartsessie wordt een "Afsluiting" activiteit toegevoegd, zie 5.2.5.

Direct nadat de "Afsluiting" activiteit is toegevoegd en nog voordat de chauffeur zijn kaart uitneemt, dient de boordcomputer:

1. in EF.BCT_Certificates het DownloadLog controleren en vast te stellen of de laatste download van EF.Driver_Activity_Data naar een boordcomputer al dan niet te lang geleden is of lijkt. Indien dat zo blijkt te zijn, dan dient de boordcomputer de bestuurder hierop te attenderen;
2. de chauffeur de gelegenheid te bieden om de volledige inhoud van EF.Driver_Activity_Data naar het geheugen van de boordcomputer te downloaden. Indien de chauffeur hierop ingaat, dan dient de boordcomputer:
   a. Aan de chauffeur een waarschuwing te tonen dat de kaart (nog) niet mag worden uitgenomen;
   b. De volledige inhoud van EF.Driver_Activity_Data te downloaden naar het geheugen van de boordcomputer;
   c. In EF.BCT_Certificates het DownloadLog bij te werken;
   d. Aan de chauffeur te melden dat de kaart nu mag worden uitgenomen.

7.4 Niet afgesloten kaartsessie

Het is mogelijk dat de chauffeur zijn kaart uit de boordcomputer haalt zonder dat hij de kaartsessie afgesloten heeft. In dat geval is er dus geen ActivityRecord aangemaakt voor het afsluiten van de kaartsessie. De boordcomputer constateert dat de kaart is uitgenomen zonder dat de sessie is afgesloten en blokkeert deze kaartsessie.

De op de boordcomputer geblokkeerde kaartsessie wordt beëindigd door:

- binnen 60 minuten dezelfde chauffeurskaart weer in te brengen in de boordcomputer. Zijn er in de tussentijd activiteiten op de boordcomputer geregistreerd geweest, dan worden die allereerst op de chauffeurskaart bijgewerkt.
- binnen 60 minuten dezelfde chauffeurskaart weer in te brengen en er blijkt dat de kaart in de tussentijd in een andere boordcomputer heeft gezeten. Eventuele tussentijdse activiteiten die op deze boordcomputer waren geregistreerd worden niet meer op de kaart geplaatst.
- een andere boordcomputerkaart in te brengen, uitgezonderd een inspectiekaart.
- een time-out van 60 minuten.

De eerstvolgende keer dat een chauffeurskaart met een niet afgesloten kaartsessie weer in een boordcomputer wordt ingebracht, krijgt de chauffeur een melding dat de kaartsessie niet goed afgesloten was. De uitzondering hierop is het eerste punt hierboven, waarbij de kaartsessie voortgezet wordt.

In alle gevallen wordt na het inloggen de chauffeur de mogelijkheid geboden voor het handmatig toevoegen van activiteiten die hebben plaatsgevonden tussen de laatstgeboekte "Start werk" of "Start pauze" activiteit en het login-tijdstip. Pas nadat dergelijke handmatige boekingen op de kaart zijn bijgeschreven, wordt het Login-tijdstip vastgelegd door het toevoegen van een "Login" ActivityRecord die aangeeft wanneer de kaart weer in de boordcomputer ingebracht is (zie 5.2.1). Direct aansluitend wordt (met hetzelfde tijdstempel) een "Start werk" activiteit toegevoegd.

7.5 Dagoverschrijdende kaartsessie

Het is mogelijk dat een kaartsessie actief is om 12 uur 's nachts. Ook kan dat het geval blijken te zijn tijdens het handmatig invoegen van activiteiten (de laatst geboekte activiteit blijkt "Start werk" of "Start pauze" te zijn en de toe te voegen activiteit blijkt te moeten starten in de kalenderdag na die van zijn voorganger). Omdat de activiteiten per dag opgeslagen worden, moet de kaartsessie hier gesplitst worden.

Hiervoor wordt

1. Indien de huidige activiteit een (automatische) "Start werk" is, het aantal secondes rijden bijgewerkt.
2. Een interne kopie gemaakt van de huidige activiteit ("Start werk" of "Start pauze"). In die kopie wordt het tijdstipveld op 00:00:00 gezet en de handmatig bit dient te reflecteren of deze dagovergang tijdens het handmatig bijwerken van de administratie dan wel tijdens de normale operatie van de boordcomputer werd geconstateerd.

3. Een “Dagovergang” activiteit toegevoegd aan het huidige SessionRecord om 23:59:59 (zie 5.2.7). Het handmatig bit dient ook hierbij te reflecteren of deze dagovergang tijdens het handmatig bijwerken van de administratie dan wel tijdens de normale operatie van de boordcomputer werd geconstateerd.
4. De interne kopie van de voort te zetten activiteit toegevoegd op de eerstvolgende kalenderdag. Omdat dit de eerste activiteit in die volgende kalenderdag betreft, worden er eerst een nieuw DailyRecord en SessionRecord aangemaakt.
5. Indien de splitsing het gevolg van een handmatige toevoeging was:
   a. wordt eerst gecontroleerd of die toevoeging wellicht nóg een of meer kalenderdagen vooruit betreft en indien dat zo is, worden de bovenstaande stappen herhaald,
   b. wordt pas daarna de opgegeven activiteit toegevoegd.

8 Functies

De commando-antwoord paren (zie hoofdstuk 9) vormen het laagste niveau van communicatie met de boordcomputerkaarten.
Met behulp van één of meerdere commando’s kunnen functies benoemd worden die een logische actie vertegenwoordigen, zoals het wijzigen of deblokkeren van een pincode.
Bij deze functies moeten ook de punten uit 5.3 (Algemene opmerkingen bij lezen en schrijven) in acht worden genomen.

8.1 PIN wijzigen

Naam	ChangePIN
Gebruik	Boordcomputerkaarten
Input gegevens	Oude PIN || Nieuwe PIN
Resultaat	‘90 00’H OK
	‘xx xx’H Foutcode van Change Reference Data, afhankelijk van de implementatie

Voor het wijzigen van een PIN moet de oude PIN bekend zijn, anders is dit niet mogelijk.

Voor de oude en nieuwe PIN wordt het PIN formaat 2 gebruikt. Dit is 8 bytes lang en is als volgt opgebouwd:

C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

Waarin:

Naam		Waarde
C	Controle veld	4 bits binair getal ‘0010’B
N	PIN lengte	4 bits binair getal tussen ‘0100’B en ‘1100’B
P	PIN cijfer	4 bits binair getal tussen ‘0000’B en ‘1001’B
P/F	PIN cijfer / Vulteken	Afhankelijk van PIN lengte
F	Vulteken	4 bits binair getal ‘1111’B

De PIN is dus maximaal 12 cijfers lang.

Het gebruikte commando is Change Reference Data, waarbij de PIN reference de waarde ‘01’H heeft en oude PIN || nieuwe PIN als data meegegeven wordt.

8.2 SM keyset wijzigen

Naam	ChangeSMKeySet
Gebruik	Systeemkaart
Input gegevens	Nieuwe Key Set
Resultaat	‘90 00’H OK
	‘xx xx’H Foutcode van Put Data (SDO), afhankelijk van de implementatie

Op de systeemkaart mag deze functie alleen uitgevoerd worden onder beveiligde gegevensoverdracht (zie Hoofdstuk 4).

Voor het wijzigen van een SM key set moet er een Secure Messaging kanaal bestaan en daarmee moet de oude SM key set bekend zijn, anders is dit niet mogelijk.

Het gebruikte commando is Put Data, waarbij de nieuwe (symmetrische) key set als data meegegeven wordt. Het volledige data veld heeft de vorm
‘70 2A BF 8A 03 26 A2 24 90 10’ || Kmac || ‘91 10’ || Kenc

waarbij Kmac en Kenc de 16 bytes sleutels zijn voor de MAC resp. de ENC.

8.3 PIN deblokkeren

Naam	DeblockPIN
Gebruik	Boordcomputerkaarten
Input gegevens	Geen
Resultaat	'90 00'H OK
	'xx xx'H Foutcode van Reset Retry Counter, afhankelijk van de implementatie

Hierbij wordt de bestaande PIN gedeblokkeerd.

Het gebruikte commando is Reset Retry Counter, waarbij P1 de waarde '03'H heeft en P2 (de PIN reference) de waarde '01'H heeft.

Voorafgaand aan dit commando moet een succesvol Verify commando uitgevoerd worden met P1 = '00'H en P2 = '02'H (de PUK reference). Voor de PUK wordt PIN formaat 2 gebruikt (zie onder 8.1).

8.4 PIN deblokkeren en wijzigen

Naam	DeblockAndChangePIN
Gebruik	Boordcomputerkaarten
Input gegevens	Nieuwe PIN
Resultaat	'90 00'H OK
	'xx xx'H Foutcode van Reset Retry Counter, afhankelijk van de implementatie

Hierbij wordt de bestaande PIN gedeblokkeerd en gewijzigd in de Nieuwe PIN.

Het gebruikte commando is Reset Retry Counter, waarbij P1 de waarde '02'H heeft en P2 (de PIN reference) de waarde '01'H heeft.

Voorafgaand aan dit commando moet een succesvol Verify commando uitgevoerd worden met P1 = '00'H en P2 = '02'H (de PUK reference). Voor de PUK wordt PIN formaat 2 gebruikt (zie onder 8.1).

8.5 Elektronische handtekening zetten met een chauffeurs- of inspectiekaart

Naam	SignDataLegally
Gebruik	Chauffeurskaart, Inspectiekaart
Input gegevens	Gegevens waarover handtekening berekend moet worden
Resultaat	Handtekening ‖ '90 00'H OK
	'xx xx'H Foutcode van een van de gebruikte commando's, afhankelijk van de implementatie

Deze functie wordt gebruikt voor het door een natuurlijke persoon zetten van een rechtsgeldige elektronische handtekening met de sleutel-certificaatcombinatie PKI.CH.DS die uitsluitend op chauffeurs- en inspectiekaarten bestaat.

Voor deze functie moet een aantal stappen doorlopen worden:

1. Selectie hash template en algoritme: alvorens de digitale handtekening berekend kan worden, moet het hash template geselecteerd worden en het te gebruiken algoritme.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'H en P2 de waarde 'AA'H. De data bij dit commando is '80 01 40'H ('40'H om de algoritme identifier voor SHA-256 aan te geven).
2. Selectie private key en algoritme: de private key van de BCT Handtekening moet geselecteerd worden met het te gebruiken algoritme.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'H en P2 de waarde 'B6'H. De data bij dit commando is '80 01 42 84 01 86'H ('42'H om "PKCS#1 v1.5 – SHA-256" aan te duiden en '86'H om het Security Data Object (SDO) van PKI.CH.DS aan te duiden).
3. PIN valideren: de private key van de BCT Handtekening mag pas gebruikt worden nadat de PIN gevalideerd is. Dit is nodig voor iedere keer dat deze key gebruikt wordt.
   Dit wordt gedaan met het commando Verify, waarbij P2 (de PIN reference) de waarde '01'H heeft. Voor de PIN wordt PIN formaat 2 gebruikt (zie onder 8.1).
4. Berekenen van de intermediate hash (SHA256) over de input gegevens door de boordcomputerlogica. Hierbij wordt het laatste gegevensblok niet gehashed, maar wordt de intermediate hash en het aantal gehashte bits onthouden voor de volgende stap.
   NB. Wanneer het totaal aan input gegevens uit maximaal 64 bytes bestaat, wordt er geen intermediate hash berekend en worden alle inputgegevens in de volgende stap gebruikt.
5. Berekenen van de uiteindelijke hash (SHA256) door de boordcomputerkaart. Hiervoor wordt het commando PSO Hash gebruikt. Hierbij worden de "intermediate hash value", het aantal gehashte bits en het laatste (of enige) blok inputdata van minimaal 1 en maximaal 64 bytes opgenomen in

het Dataveld van het commando. Bij een succesvol uitgevoerde PSO HASH zal de uiteindelijke hash waarde in het geheugen van de boordcomputerkaart (chip) achterblijven ten behoeve van de volgende en laatste stap.
6. Handtekening berekenen: hierbij wordt met de gekozen private key de handtekening berekend over de in het chipgeheugen aanwezige hashwaarde en geeft de kaart die handtekening terug aan de boordcomputerlogica.
   Dit wordt gedaan met het commando PSO Compute Digital Signature. Le, het verwachte aantal bytes in de response, moet daarbij op '00'H staan.

Zie ook PSO Hash en PSO Compute Digital Signature in Referentie [7].
Voor de vermelde SDO ID wordt verwezen naar de kaartstructuur documenten in Referenties [9] en [12]. Omdat dit SDO een lokaal object is, moet de in de kaartstructuur documenten gespecificeerde keyReference niet letterlijk worden overgenomen, maar met bit8 hoog (dus '86'H in plaats van '06'H).

8.6 Elektronische handtekening zetten met een systeemkaart

Naam	SignDataSystem
Gebruik	Systeemkaart
Input gegevens	Gegevens waarover handtekening berekend moet worden
Resultaat	Handtekening || '90 00'H OK 'xx xx'H Foutcode van een van de gebruikte commando's, afhankelijk van de implementatie

Deze functie wordt gebruikt voor het door een boordcomputer zetten van een elektronische handtekening met de sleutel-certificaatcombinatie PKI.CH.AUT van de systeemkaart.

Op de systeemkaart mag deze functie alleen uitgevoerd worden onder beveiligde gegevensoverdracht (zie Hoofdstuk 4), gebruikmakend van de sleutelset SM.ICC.

Voor deze functie moet een aantal stappen doorlopen worden:
1. Selectie hash template en algoritme: alvorens de digitale handtekening berekend kan worden, moet het hash template geselecteerd worden en het te gebruiken algoritme.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'H en P2 de waarde 'AA'H. De data bij dit commando is '80 01 40'H ('40'H om de algoritme identifier voor SHA-256 aan te geven).
2. Selectie private key en algoritme: de private key van de BCT Authenticiteit moet geselecteerd worden met het te gebruiken algoritme.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'H en P2 de waarde 'B6'H. De data bij dit commando is '80 01 42 84 01 85'H ('42'H om "PKCS#1 v1.5 – SHA-256" aan te duiden en '85'H om het Security Data Object (SDO) van PKI.CH.AUT aan te duiden).
3. Berekenen van de intermediate hash (SHA256) over de input gegevens door de boordcomputerlogica. Hierbij wordt het laatste gegevensblok niet gehashed, maar wordt de intermediate hash en het aantal gehashte bits onthouden voor de volgende stap.
   NB. Wanneer het totaal aan input gegevens uit maximaal 64 bytes bestaat, wordt er geen intermediate hash berekend en worden alle inputgegevens in de volgende stap gebruikt.
4. Berekenen van de uiteindelijke hash (SHA256) door de systeemkaart. Hiervoor wordt het commando PSO Hash gebruikt. Hierbij worden de "intermediate hash value", het aantal gehashte bits en het laatste (of enige) blok inputdata van minimaal 1 en maximaal 64 bytes opgenomen in het Dataveld van het commando. Bij een succesvol uitgevoerde PSO HASH zal de uiteindelijke hash waarde in het geheugen van de systeemkaart (chip) achterblijven ten behoeve van de volgende en laatste stap.
5. Handtekening berekenen: hierbij wordt met de gekozen private key de handtekening berekend over de in het chipgeheugen aanwezige hashwaarde en geeft de kaart die handtekening terug aan de boordcomputerlogica.
   Dit wordt gedaan met het commando PSO Compute Digital Signature. Le, het verwachte aantal bytes in de response, moet daarbij op '00'H staan.

Zie ook PSO Hash en PSO Compute Digital Signature in Referentie [7]).
Voor de vermelde SDO ID wordt verwezen naar het kaartstructuur documenten in Referentie [8].
Omdat dit SDO een lokaal object is, moet de in het kaartstructuur document gespecificeerde keyReference niet letterlijk worden overgenomen, maar met bit8 hoog (dus '85'H in plaats van '05'H).

Noot: Zie ook 5.4 (Digitale handtekening).

8.7 Authenticiteit handtekening zetten met een boordcomputerkaart

Naam	SignDataForAuthenticity

Gebruik	Chauffeurskaart, Ondernemerskaart, Keuringskaart, Inspectiekaart
Input gegevens	Gegevens waarover handtekening berekend moet worden
Resultaat	Handtekening ǁ ‘90 00’H OK ‘xx xx’H Foutcode van een van de gebruikte commando’s, afhankelijk van de implementatie

Deze functie wordt gebruikt voor het door een boordcomputerkaarthouder zetten van een elektronische handtekening met de sleutel-certificaatcombinatie PKI.CH.AUT die op elke boordcomputerkaart bestaat.

NB. Gebruik van deze functie is niet voorzien binnen de regelgeving van Boordcomputer Taxi, maar voor de volledigheid is deze paragraaf toch opgenomen.

Voor deze functie moet een aantal stappen doorlopen worden:
1. Selectie hash template en algoritme: alvorens de digitale handtekening berekend kan worden, moet het hash template geselecteerd worden en het te gebruiken algoritme.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde ‘41’H en P2 de waarde ‘AA’H. De data bij dit commando is ‘80 01 40’H (‘40’H om de algoritme identifier voor SHA-256 aan te geven).
2. Selectie private key en algoritme: de private key van de BCT Authenticiteit moet geselecteerd worden met het te gebruiken algoritme.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde ‘41’H en P2 de waarde ‘B6’H. De data bij dit commando is ‘80 01 42 84 01 85’H (‘42’H om “PKCS#1 v1.5 – SHA-256” aan te duiden en ‘85’H om het Security Data Object (SDO) van PKI.CH.AUT aan te duiden).
3. PIN valideren: de private key van de BCT Authenticiteit mag pas gebruikt worden nadat de PIN gevalideerd is. Een eenmaal uitgevoerde PIN validatie mag – zo lang de kaart in de boordcomputer aanwezig blijft – worden “herbruikt” bij elke volgende keer dat deze key gebruikt wordt.
   Dit wordt gedaan met het commando Verify, waarbij P2 (de PIN reference) de waarde ‘01’H heeft. Voor de PIN wordt PIN formaat 2 gebruikt (zie onder 8.1).
4. Berekenen van de intermediate hash (SHA256) over de input gegevens door de boordcomputerlogica. Hierbij wordt het laatste gegevensblok niet gehashed, maar wordt de intermediate hash en het aantal gehashte bits onthouden voor de volgende stap.
   NB. Wanneer het totaal aan input gegevens uit maximaal 64 bytes bestaat, wordt er geen intermediate hash berekend en worden alle inputgegevens in de volgende stap gebruikt.
5. Berekenen van de uiteindelijke hash (SHA256) door de boordcomputerkaart. Hiervoor wordt het commando PSO Hash gebruikt. Hierbij worden de “intermediate hash value”, het aantal gehashte bits en het laatste (of enige) blok inputdata van minimaal 1 en maximaal 64 bytes opgenomen in het Dataveld van het commando. Bij een succesvol uitgevoerde PSO HASH zal de uiteindelijke hash waarde in het geheugen van de boordcomputerkaart (chip) achterblijven ten behoeve van de volgende en laatste stap.
6. Handtekening berekenen: hierbij wordt met de gekozen private key de handtekening berekend over de in het chipgeheugen aanwezige hashwaarde en geeft de kaart die handtekening terug aan de boordcomputerlogica.
   Dit wordt gedaan met het commando PSO Compute Digital Signature. Le, het verwachte aantal bytes in de response, moet daarbij op ‘00’H staan.

Zie ook PSO Hash en PSO Compute Digital Signature in Referentie [7].
Voor de vermelde SDO ID wordt verwezen naar de kaartstructuur documenten in Referenties [9] t/m [12]. Omdat dit SDO een lokaal object is, moet de in de kaartstructuur documenten gespecificeerde keyReference niet letterlijk worden overgenomen, maar met bit8 hoog (dus ‘85’H in plaats van ‘05’H).

8.8 Authenticeren boordcomputerkaart aan boordcomputer

Naam	AuthenticateCardToBCT
Gebruik	Boordcomputerkaarten
Input gegevens	Random waarde (16 bytes)
Resultaat	Handtekening ǁ ‘90 00’H OK ‘xx xx’H Foutcode van een van de gebruikte commando’s, afhankelijk van de implementatie

Om te controleren of een boordcomputerkaart authentiek is, wordt er een Client/Server authenticatie uitgevoerd (zie Referentie [7]). Hierbij wordt een boordcomputer challenge ondertekend met behulp van de sleutel-certificaatcombinatie PKI.CH.AUT van de een boordcomputerkaart. Deze functie is analoog aan SignDataForAuthenticity, maar wordt hier uitsluitend voor authenticatiedoeleinden gebruikt.

Voor deze functie moeten een aantal stappen doorlopen worden:
1. Selectie private key en algoritme: alvorens de digitale handtekening berekend kan worden, moet

de private key van de BCT Authenticiteit geselecteerd worden en het te gebruiken algoritme. Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'H en P2 de waarde 'A4'H. De data bij dit commando is '80 01 02 84 01 85'H ('02'H om "C/S RSA with DSI according to PKCS#1, parameter Digestinfo" aan te duiden en '85'H om het Security Data Object (SDO) van PKI.CH.AUT aan te duiden).
2. PIN valideren: de private key van de BCT Authenticiteit mag pas gebruikt worden nadat de PIN gevalideerd is. Dit is nodig voor de eerste keer dat deze key gebruikt wordt, maar een eenmaal uitgevoerde PIN validatie mag – zo lang de kaart in de boordcomputer aanwezig blijft – worden "herbruikt" bij elke volgende keer dat deze key gebruikt wordt.
   Dit wordt gedaan met het commando Verify waarbij P2 (de PIN reference) de waarde '01'H heeft. Voor de PIN wordt PIN formaat 2 gebruikt (zie onder 8.1).
3. De boordcomputer stuurt een Internal Authenticate commando naar de boordcomputerkaart. P1 P2 = '00 00' en de data = 16 bytes random.
4. Het antwoord hiervan wordt teruggestuurd naar de boordcomputer en deze controleert met behulp van de publieke key en een padvalidatie van het authenticiteitcertificaat of de boordcomputerkaart authentiek is.
5. Ook de geldigheid van het authenticiteitcertificaat dient te worden gecontroleerd middels minimaal een padvalidatie en een controle van de attributen validity.notBefore en validity.notAfter.
6. Met behulp van het eerste karakter van het kaartnummer, zoals dat in het subject.serialNumber of in de subject.title van het authenticiteitcertificaat is opgeslagen, kan de boordcomputer het kaarttype en daarmee de gebruikerssoort (bestuurder, vervoerder, werkplaats, dan wel toezichthouder) herkennen.

NB. De boordcomputerkaarten ondersteunen Windows/Kerberos smartcard logon. Ook deze wijze van authenticeren is toegestaan, mits ook hier de geldigheid van het authenticiteitcertificaat middels een padvalidatie wordt gevalideerd.

Voor de vermelde SDO ID wordt verwezen naar de kaartstructuur documenten in Referenties [9] t/m [12]. Omdat dit SDO een lokaal object is, moet de in de kaartstructuur documenten gespecificeerde keyReference niet letterlijk worden overgenomen, maar met bit8 hoog (dus '85'H in plaats van '05'H).

8.9 Schrijf nieuw ActivityRecord

Naam	WriteNewActivityRecord
Gebruik	Chauffeurskaart
Input gegevens	ActivityRecord, ActivityDate
Resultaat	90h 00h OK xxh xxh Foutcode van een van de gebruikte commando's, afhankelijk van smartcard implementatie

Deze functie wordt gebruikt om een ActivityRecord toe te voegen in EF.Driver_Activity_Data.

De functie moet gevoed worden met de volgende argumenten met betrekking tot het toe te voegen ActivityRecord:
1. *ActivityDate* de datum (JJJJMMDD) waarop de activiteit startte c.q. gebeurtenis plaatsvond;
2. *ActivityTime* het tijdstip (hhmmss) waarop de activiteit startte c.q. gebeurtenis plaatsvond;
3. *ActivityType*: het type activiteit / gebeurtenis;
4. *ManualBit*: de handmatig-bit die weergeeft of het tijdstempel (datum en tijd) handmatig dan wel automatisch werd bepaald.

Deze functie moet, voorafgaand aan het daadwerkelijk toevoegen van het ActivityRecord, aan de hand van meegestuurde argumenten, het laatst in EF.Driver_Activity_Data geboekte ActivityRecord en de status van de boordcomputer bepalen of voor het ActivityRecord al dan niet een nieuw DailyRecord en/of SessionRecord moet worden aangemaakt en op welke geheugenpositie het nieuwe ActivityRecord moet worden toegevoegd. Stapsgewijs is de daarvoor te volgen logica als volgt:
1. Selecteer EF.Driver_Activity_Data met het commando Select met P1P2 = '04 0C'H en data = 'E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E'H, gevolgd door het commando Select met P1P2 = '02 0C'H en data = '44 01'H.
2. Lees de *PointerLastDayRecord* met het commando Read Binary, waarbij de offset 2 is en het verwachte aantal bytes in de response 2.
   Indien *PointerLastDayRecord* gelijk aan '00 00'H is, dan bestaat er (nog) geen enkel DailyRecord:
   a. Roep de functie voor het toevoegen van een nieuw DailyRecord aan met *ActivityDate* als argument.
   b. Herhaal de stappen vanaf stap 2.
   Indien *PointerLastDayRecord* niet gelijk aan '00 00'H is:
   a. Lees de *DayRecordLength* met het commando Read Binary, waarbij de offset *PointerLastDayRecord* is en het verwachte aantal bytes in de response 2.
   b. Lees de *DayRecordDate* met het commando Read Binary, waarbij de offset *PointerLastDayRe-*

cord + 6 is en het verwachte aantal bytes in de response 4.
Indien *DayRecordDate* groter is dan *ActivityDate*,
dan betreft dit een foutsituatie en stopt verdere verwerking.
Indien *DayRecordDate* kleiner is dan *ActivityDate*,
dan ontbreekt de gewenste DailyRecord
(hou hier ook rekening met Dagovergangen zoals beschreven in § 5.2.7 en § 7.5):

a. Roep de functie voor het toevoegen van een nieuw DailyRecord aan met *ActivityDate* als argument.
b. Herhaal de stappen vanaf stap 2.

Indien *DayRecordDate* gelijk is aan *ActivityDate*:

a. Lees de *PointerLastSessionRecord* met het commando Read Binary, waarbij de offset *PointerLastDayRecord* + 2 is en het verwachte aantal bytes in de response 2.
   Indien de *PointerLastSessionRecord* gelijk aan '00 00'H is,
   dan bevat het DailyRecord (nog) geen enkel SessionRecord:
   i. Roep de functie voor het toevoegen van een nieuw SessionRecord aan.
   ii. Herhaal de stappen vanaf het lezen van *PointerLastSessionRecord*.
   Indien de *PointerLastSessionRecord* niet gelijk aan '00 00'H is:
   i. Lees de *PointerLastActivityRecord* met het commando Read_Binary, waarbij de offset *PointerLastSessionRecord* is en het verwachte aantal bytes in de response 2.
      Indien de *PointerLastActivityRecord* gelijk aan '00 00'H is,
      dan wordt nu het eerste ActivityRecord aan het SessionRecord toegevoegd: zet de *NewActivityPointer* dus op *PointerLastSessionRecord* + Length(*SessionRecordHeader*).
      Indien de *PointerLastActivityRecord* niet gelijk aan '00 00'H is,
      dan bestaat er een eerder ActivityRecord:
      a. Lees de *LastActivityRecordHeader* met het commando Read_Binary, waarbij de offset *PointerLastActivityRecord* is en het verwachte aantal bytes in de response 3.
      b. Bepaal uit de eerste 5 bits van de *LastActivityRecordHeader* de *LastActivityType*.
         Indien de *LastActivityType* gelijk is aan "Afsluiting" of "Nieuwe eindtijd",
         dan moet er een nieuwe sessie worden geboekt:
         i. Roep de functie voor het toevoegen van een nieuw SessionRecord aan.
         ii. Herhaal de stappen vanaf het lezen van *PointerLastSessionRecord*.
         Indien de *LastActivityType* gelijk is aan "Login", "Start werk" of "Start pauze", maar de boordcomputer heeft geen kaartsessie meer actief of geblokkeerd,
         dan moet er ook een nieuwe sessie worden geboekt:
         i. Roep de functie voor het toevoegen van een nieuw SessionRecord aan.
         ii. Herhaal de stappen vanaf het lezen van *PointerLastSessionRecord*.
         Indien de *LastActivityType* gelijk is aan "Start werk",
         Werk dan diens Rijtijdteller voor de laatste maal bij: voer een Update Binary commando uit, waarbij de offset *PointerLastActivityRecord* + 3 is en de data de door de boordcomputer bijgehouden rijtijdteller; reset die laatste ook direct naar nul (0).
         Zet *NewActivityPointer* = *PointerLastActivityRecord* + 6
         Indien de *LastActivityType* NIET gelijk is aan "Start werk",
         Zet *NewActivityPointer* = *PointerLastActivityRecord* + 3

NB1. NewActivityPointer, LastActivityRecordHeader en NewActivityLength maken géén onderdeel van de structuur uit, maar zijn tijdelijke waardes in het geheugen van de boordcomputer.

NB2. Indien het LastActivityRecord een "(Start) werk" of "(Start) pauze" betreft worden met het bovenstaande algoritme de laatste 3 bytes (waarin de tijdsduur van de activiteit tijdelijk werd bijgehouden) overschreven door het nieuw toe te voegen ActivityRecord.

Voeg nu het nieuwe ActivityRecord toe in het in het huidige SessionRecord:

1. Bepaal eerst aan de hand van de *ActivityType* de lengte van het nieuwe ActivityRecord:
   a. Indien "(Start) werk", dan *NewActivityLength* = 9;
   b. Indien "(Start) pauze", dan *NewActivityLength* = 6;
   c. Indien anders, dan *NewActivityLength* = 3;
2. Bepaal dan aan de hand van *NewActivityPointer* + *NewActivityLength* of er nog voldoende vrije ruimte resteert in EF.Driver_Activity_Data en ruim zo nodig een of meer van de oudste DailyRecords op (zie ook 5.3).
3. Voer een Update Binary commando uit, waarbij de offset *PointerLastSessionRecord* is en de data *NewActivityPointer* (hiermee wordt *PointerLastActivityRecord* bijgewerkt).
4. Voer een Update Binary commando uit, waarbij de offset *NewActivityPointer* is en de data bestaat uit 3 bytes:
   a. 5 bits *ActivityType*: het als argument gegeven type activiteit / gebeurtenis;
   b. 1 bit *ManualBit*: de als argument gegeven handmatig-bit;
   c. 1 bit *RijdenBit*: de bit die aangeeft of de auto NU rijdt ('1'B) of stilstaat ('0'B);

d. 17 bits *ActivityTime*: het als argument gegeven (start)tijdstip.

5. Indien de nieuwe activiteit een "(Start) werk" of "(Start) pauze" betreft:
   a. Voer een Update Binary commando uit, waarbij de offset *PointerLastSessionRecord* + 2 is en de data *NewActivityPointer* (hiermee wordt *PointerLast**PW**ActivityRecord* bijgewerkt);
   b. Voer een Update Binary commando uit, waarbij de offset *NewActivityPointer* + 3 is en de data bestaat uit 3 bytes gelijk aan '00 00 00'H;
   c. Reset op de boordcomputer de tijdsduurteller naar nul (0) seconden;
   d. Indien de nieuwe activiteit een "(Start) werk" betreft:
      i. Voer een Update Binary commando uit, waarbij de offset *NewActivityPointer* + 6 is en de data bestaat uit 3 bytes gelijk aan '00 00 00'H;
      ii. Reset op de boordcomputer de rijtijdteller naar nul (0) seconden.
6. Voer een Update Binary commando uit met offset is *PointerLastDayRecord* en als data *DayRecord-Length* + *NewActivityLength* (hiermee wordt *DayRecordLength* bijgewerkt).

Voer tot slot nog de procedure uit voor het door de boordcomputer ondertekenen van het aangepaste SessionRecord, zoals beschreven in § 5.4.

8.10 Schrijf nieuw SessionRecord

Naam	WriteNewSessionRecord
Gebruik	Chauffeurskaart
Input gegevens	StartSessionData
Resultaat	'90 00'H OK 'xx xx'H Foutcode van een van de gebruikte commando's, afhankelijk van de implementatie

Deze functie wordt gebruikt om een nieuw leeg SessionRecord aan het huidige DailyRecord toe te voegen. Deze functie wordt altijd aangeroepen vanuit de functie voor het toevoegen van een ActivityRecord (zie 0)

Hiervoor moeten de volgende stappen doorlopen worden:

1. Selecteer EF.Driver_Activity_Data met het commando Select met P1P2 = '04 0C'H en data = 'E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E'H, gevolgd door het commando Select met P1P2 = '02 0C'H en data = '44 01'H.
2. Lees de PointerLastDayRecord met het commando Read Binary, waarbij de offset 2 is en het verwachte aantal bytes in de response 2. Dit levert de pointer voor het meest recente DailyRecord (Pointer_1).
3. Lees in deze DailyRecord de DayRecordLength met Read Binary, de offset is Pointer_1 en het verwachte aantal bytes in de response is 2. Dit levert de lengte van dit DailyRecord (Length_1). Daarmee wordt de pointer waar het SessionRecord weggeschreven kan worden: Pointer_2 = Pointer_1 + Length_1.
4. Maak een nieuw SessionRecord (alleen de kop) aan met
   – PointerLastActivityRecord = '00 00'H (0).
   – PointerLastPWActivityRecord = '00 00'H (0).
   – SignatureDateTime = '00000000 000000'H
   – SessionSignature = 256 willekeurige bytes.
   – SessionCreationDateTime = de huidige datum en tijd volgens de BCT klok in BCD en geformatteerd als 'JJJJMMDDhhmmss'H
   – SystemCardNumber, Kenteken, CompanyCardNumber en Pnummer zoals die in de boordcomputer bekend zijn.

   Voer een Update Binary commando uit, waarbij de offset Pointer_2 is en de data de weg te schrijven SessionRecord kop.
5. Verhoog DayRecordLength door een Update Binary commando met offset is Pointer_1 en als data Length_1 + 299.
6. Wijzig de PointerLastSessionRecord door een Update Binary commando, waarbij de offset Pointer_1 + 2 is en de data Pointer_2.

Noot: Zie 5.3, aangezien de mogelijkheid bestaat dat de te schrijven data niet aan het eind van EF.Driver_Activity_Data past.

8.11 Schrijf nieuw DailyRecord

Naam	WriteNewDailyRecord
Gebruik	Chauffeurskaart
Input gegevens	Datum (BCD)

Resultaat	'90 00'H OK 'xx xx'H Foutcode van een van de gebruikte commando's, afhankelijk van de implementatie

Deze functie wordt gebruikt om een nieuw leeg DailyRecord toe te voegen. Dit wordt gedaan voor de eerste registratie van een dag. Dit nieuwe DailyRecord bevat nog geen SessionRecords.

Hiervoor moeten de volgende stappen doorlopen worden:
1. Selecteer EF.Driver_Activity_Data met het commando Select met P1P2 = '04 0C'H en data = 'E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E'H, gevolgd door het commando Select met P1P2 = '02 0C'H en data = '44 01'H.
2. Lees de PointerLastDayRecord met het commando Read Binary, waarbij de offset 2 is en het verwachte aantal bytes in de response 2. Dit levert de pointer voor de meest recente DailyRecord (Pointer_1).
3. Lees in deze DailyRecord de DayRecordLength met Read Binary, offset is Pointer_1 en het verwachte aantal bytes in de response is 2. Dit levert de lengte van het DailyRecord (Length_1). Daarmee is de pointer bekend waar de nieuwe DailyRecord weggeschreven kan worden: Pointer_2 = Pointer_1 + Length_1.
4. Maak een nieuwe DailyRecord kop aan met
   – DayRecordLength = '00 0A'H (10)
   – PointerLastSessionRecord = '00 00'H (0)
   – PreviousDayRecordLength = Length_1
   – DayRecordDate = datum in BCD formaat.

   en voer een Update Binary commando uit, waarbij de offset Pointer_2 is en de data de weg te schrijven DailyRecord kop.
5. Verzet de PointerLastDayRecord naar het nieuwe DailyRecord met een Update Binary, waarbij de offset 2 is en de data Pointer_2 is.

Noot: Zie 5.3, aangezien de mogelijkheid bestaat dat de te schrijven data niet aan het eind van EF.Driver_Activity_Data past.

8.12 Selecteer laatste (nieuwste) DailyRecord

Naam	SelectLastDailyRecord
Gebruik	Chauffeurskaart
Input gegevens	Geen
Resultaat	DailyRecordPointer ll '90 00'H OK 'xx xx'H Foutcode van een van de gebruikte commando's, afhankelijk van de implementatie

Hiervoor moeten de volgende stappen doorlopen worden:
1. Indien EF.Driver_Activity_Data nog niet geselecteerd is, selecteer EF.Driver_Activity_Data met het commando Select met P1P2 = '04 0C'H en data = 'E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E'H, gevolgd door het commando Select met P1P2 = '02 0C'H en data = '44 01'H.
2. Lees de PointerLastDayRecord met het commando Read Binary, waarbij de offset 2 is en het verwachte aantal bytes in de response 2. Dit levert de pointer voor de meest recente DailyRecord (DailyRecordPointer).

8.13 Selecteer oudste (eerste) DailyRecord

Naam	SelectOldestDailyRecord
Gebruik	Chauffeurskaart
Input gegevens	Geen
Resultaat	DailyRecordPointer ll '90 00'H OK 'xx xx'H Foutcode van een van de gebruikte commando's, afhankelijk van de implementatie

Hiervoor moeten de volgende stappen doorlopen worden:
1. Indien EF.Driver_Activity_Data nog niet geselecteerd is, selecteer EF.Driver_Activity_Data met het commando Select met P1P2 = '04 0C'H en data = 'E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E'H, gevolgd door het commando Select met P1P2 = '02 0C'H en data = '44 01'H.
2. Lees de PointerOldestDayRecord met het commando Read Binary, waarbij de offset 0 is en het verwachte aantal bytes in de response 2. Dit levert de pointer voor de oudst bekende DailyRecord (DailyRecordPointer).

8.14 Selecteer vorige DailyRecord

Naam	SelectPreviousDailyRecord
Gebruik	Chauffeurskaart

Input gegevens	CurrentDailyRecordPointer (bereik ‘00 14’H t/m (Length_EF.Driver_Activitiy_Data – 1)) PointerOldestDayRecord
Resultaat	DailyRecordPointer || ‘90 00’H OK ‘xx xx’H Foutcode van een van de gebruikte commando’s, afhankelijk van de implementatie

Hiervoor moeten de volgende stappen doorlopen worden:

1. Indien EF.Driver_Activity_Data nog niet geselecteerd is, selecteer EF.Driver_Activity_Data met het commando Select met P1P2 = ‘04 0C’H en data = ‘E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E’H, gevolgd door het commando Select met P1P2 = ‘02 0C’H en data = ‘44 01’H.
2. Indien PointerOldestDayRecord niet was meegegeven als inputgegeven, lees dan PointerOldest-DayRecord met het commando Read Binary met offset = 0 en het verwachte aantal bytes in de respons 2.
3. Als CurrentDailyRecordPointer gelijk is aan PointerOldestDayRecord, dan is de geselecteerde DailyRecord de eerste (oudste) en is er geen vorige DailyRecord aanwezig. Breek dan deze functie af.
4. Zet Pointer_1 = CurrentDailyRecordPointer + 4 om de pointer naar PreviousDayRecordLength te verkrijgen.
5. Als Pointer_1 >= Length_EF.Driver_Activity_Data herbereken dan de positie met de formule: Pointer_1 = (Pointer_1 modulo Length_EF.Driver_Activity_Data) + ‘00 14’H (20)
6. Als nu Pointer_1 precies gelijk is aan (Length_EF.Driver_Activity_Data – 1), dan staat de MSB van PreviousDayRecordLength in de laatste byte van EF.Driver_Activity_Data en de LSB op positie ‘00 14’H (20). Voer dan twee keer het commando Read Binary uit met het verwachte aantal bytes in de response gelijk aan 1; één keer met offset = (Length_EF.Driver_Activity_Data – 1) voor Length_1_MSB en één keer met offset = 20 (‘00 14’H) voor Length_1_LSB. Bereken dan Previous-DayRecordLength = 256 x Length_1_MSB + Length_1_LSB.
7. Als ‘00 14’H <= Pointer_1 < (Length_EF.Driver_Activity_Data – 1) is, dan kan PreviousDayRecord-Length in één keer worden uitgelezen met het commando Read Binary met offset = Pointer_1 en het verwachte aantal bytes in de response 2.
8. Als PreviousDayRecordLength gelijk is aan ‘00 00’H, dan is er geen vorig DailyRecord en dan moet de functie hier worden afgebroken.
9. Bereken nu voorlopig Pointer_2 = CurrentDailyRecordPointer – PreviousDayRecordLength.
10. Indien Pointer_2 kleiner is dan ‘00 14’H (20), voer dan nog de volgende correctie uit: Pointer_2 = Length_EF.Driver_Activity_Data – (20 – Pointer_2).
11. Geef nu de gevraagde DailyRecordPointer = Pointer_2 terug.

8.15 Selecteer volgende DailyRecord

Naam	SelectNextDailyRecord
Gebruik	Chauffeurskaart
Input gegevens	CurrentDailyRecordPointer (bereik ‘00 14’H t/m (Length_EF.Driver_Activitiy_Data – 1)) PointerLastDayRecord
Resultaat	DailyRecordPointer || ‘90 00’H OK ‘xx xx’H Foutcode van een van de gebruikte commando’s, afhankelijk van de implementatie

Hiervoor moeten de volgende stappen doorlopen worden:

1. Indien EF.Driver_Activity_Data nog niet geselecteerd is, selecteer EF.Driver_Activity_Data met het commando Select met P1P2 = ‘04 0C’H en data = ‘E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E’H, gevolgd door het commando Select met P1P2 = ‘02 0C’H en data = ‘44 01’H.
2. Indien PointerLastDayRecord niet was meegegeven als inputgegeven, lees dan PointerLastDayRe-cord met het commando Read Binary met offset = 2 en het verwachte aantal bytes in de respons 2.
3. Als CurrentDailyRecordPointer gelijk is aan PointerLastDayRecord, dan is de geselecteerde DailyRecord de laatste (meest recente) en is er geen volgende DailyRecord aanwezig. Breek dan deze functie af.
4. Zet Pointer_1 = CurrentDailyRecordPointer om de pointer naar DayRecordLength te verkrijgen.
5. Als Pointer_1 precies gelijk is aan (Length_EF.Driver_Activity_Data – 1), dan staat de MSB van DayRecordLength in de laatste byte van EF.Driver_Activity_Data en de LSB op positie ‘00 14’H (20). Voer dan twee keer het commando Read Binary uit met het verwachte aantal bytes in de response gelijk aan 1; één keer met offset = (Length_EF.Driver_Activity_Data – 1) voor Length_1_MSB en één keer met offset = 20 (‘00 14’H) voor Length_1_LSB. Bereken dan DayRecordLength = 256 x Length_1_MSB + Length_1_LSB.
6. Als ‘00 14’H <= Pointer_1 < (Length_EF.Driver_Activity_Data – 1) is, dan kan DayRecordLength in één keer worden uitgelezen met het commando Read Binary met offset = Pointer_1 en het verwachte aantal bytes in de response 2.
7. Bereken nu voorlopig Pointer_2 = CurrentDailyRecordPointer + DayRecordLength.
8. Als Pointer_2 >= Length_EF.Driver_Activity_Data herbereken dan de positie met de formule: Pointer_2 = (Pointer_2 modulo Length_EF.Driver_Activity_Data) + ‘00 14’H (20)
9. Geef nu de gevraagde DailyRecordPointer = Pointer_2 terug.

8.16 Lees huidige / geselecteerde DailyRecord

Naam	ReadSelectedDailyRecord
Gebruik	Chauffeurskaart
Input gegevens	CurrentDailyRecordPointer (bereik '00 14'H t/m (Length_EF.Driver_Activitiy_Data – 1))
Resultaat	Data || '90 00'H OK 'xx xx'H Foutcode van een van de gebruikte commando's, afhankelijk van de implementatie

Hiervoor moeten de volgende stappen doorlopen worden:

1. Indien EF.Driver_Activity_Data nog niet geselecteerd is, selecteer EF.Driver_Activity_Data met het commando Select met P1P2 = '04 0C'H en data = 'E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E'H, gevolgd door het commando Select met P1P2 = '02 0C'H en data = '44 01'H.
2. Zet Pointer_1 = CurrentDailyRecordPointer om de pointer naar DayRecordLength te verkrijgen.
3. Als Pointer_1 precies gelijk is aan (Length_EF.Driver_Activity_Data – 1), dan staat de MSB van DayRecordLength in de laatste byte van EF.Driver_Activity_Data en de LSB op positie '00 14'H (20). Voer dan twee keer het commando Read Binary uit met het verwachte aantal bytes in de response gelijk aan 1; één keer met offset = (Length_EF.Driver_Activity_Data – 1) voor Length_1_MSB en één keer met offset = 20 ('00 14'H) voor Length_1_LSB. Bereken dan DayRecordLength = 256 x Length_1_MSB + Length_1_LSB.
4. Als '00 14'H <= Pointer_1 < (Length_EF.Driver_Activity_Data – 1) is, dan kan DayRecordLength in één keer worden uitgelezen met het commando Read Binary met offset = Pointer_1 en het verwachte aantal bytes in de response 2.
5. Onthou de DayRecordLength nu voorlopig als Length_1.
6. Voer Read Binary commando's uit tot Length_1 bytes gelezen zijn. Per Read Binary kan een maximaal aantal bytes gelezen worden. Dit maximum is van een aantal factoren afhankelijk (zie referentie [7]) en wordt hier max_read genoemd. De eerste Read Binary heeft als offset Pointer_1 en het verwachte aantal bytes '00'H (in het geval dat Length_1 < max_read, dan wordt het verwachte aantal bytes Length_1). Voor iedere volgende Read Binary wordt de offset met max_read verhoogd. Het verwachte aantal bytes in de response is '00'H, behalve bij de laatste Read Binary, daar is het Length_1 modulo max_read.
   NB. Voorafgaand aan elke Read Binary moet worden gecontroleerd of de te lezen bytes verder zouden doorlopen dan EF.Driver_Activity_Data groot is. In zo'n geval dient de betreffende Read Binary in twee slagen te worden uitgevoerd:
   a. De eerste keer met een ongewijzigde offset en een aangepast verwacht aantal_bytes (aantal-_bytes_a), zijnde (Length_EF.DriverActivity_Data – offset_a);
   b. De tweede keer met een gecorrigeerde offset gelijk aan 20 ('00 14'H) en het restant van het verwachte aantal_bytes, zijnde aantal_bytes_b = aantal_bytes – aantal_bytes_a.
   c. Hierna kan vanaf offset ('00 14'H + aantal_bytes_b) worden vervolgd met de eerstvolgende reguliere Read Binary.

8.17 Controleer EF.Driver_Activity_Data structuur

Naam	CheckEFDriverActivityStructure
Gebruik	Chauffeurskaart
Input gegevens	Geen
Resultaat	00 OK 01 Invalid Pointer Value 02 Wrong Length 03 Length Not Matching 04 Record Not Closed 05 Invalid PW Pointer 06 DayRecordLength Wrong 07 DriverCardNumber was overwritten

Hiervoor moeten de volgende stappen doorlopen worden:

1. Selecteer EF.Driver_Activity_Data met het commando Select met P1P2 = '04 0C'H en data = 'E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E'H, gevolgd door het commando Select met P1P2 = '02 0C'H en data = '44 01'H.
2. Lees PointerOldestDayRecord en PointerLastDayRecord.
3. Controleer:
   20 ('00 14'H) <= PointerOldestDayRecord < Length_EF.Driver_Activity_Data of
   PointerOldestDayRecord == 0.
   Wanneer dit niet het geval is, geef dan "Invalid Pointer Value" terug.
4. Controleer:
   20 ('00 14'H) <= PointerLastDayRecord < Length_EF.Driver_Activity_Data of
   PointerLastDayRecord == 0.
   Wanneer dit niet het geval is, geef dan "Invalid Pointer Value" terug.
5. Controleer of DriverCardNumber gelijk is aan de eerste 20 bytes (karakters) van het subject.Serial-Number van het authenticiteitcertificaat.

Wanneer dit niet het geval is, geef dan “DriverCardNumber was overwritten” terug (en herstel de fout).

6. Controleer de DailyRecord structuur (voorwaarts):
   a. Ga met de PointerOldestDayRecord naar de oudste DailyRecord.
   b. Controleer of PreviousDayRecordLength = ‘00 00’H.
      Wanneer dit niet het geval is, geef dan “Wrong Length” terug.
   c. Bepaal mbv de DayRecordLength de positie van het volgende DailyRecord.
   d. Controleer of de PreviousDayRecordLength in dit record gelijk is aan de DayRecordLength van het vorige record.
      Wanneer dit niet het geval is, geef dan “Length Not Matching” terug.
   e. Herhaal de vorige 2 punten totdat
      – het beginpunt van een record gelijk is aan PointerLastDayRecord, of
      – de referenties DayRecordLength/PreviousDayRecordLength niet meer kloppen. Beschouw dan het DailyRecord waar dit nog wel correct was als laatste record. Pas in dit geval ook de PointerLastDayRecord aan.
7. Controleer de DailyRecord structuur (terugwaarts):
   a. Ga met de PointerLastDayRecord naar de laatste DailyRecord.
   b. Bepaal mbv de PreviousDayRecordLength de positie van het vorige DailyRecord.
   c. Controleer of de DayRecordLength in dit record gelijk is aan de PreviousDayRecordLength van het volgende record.
      Wanneer dit niet het geval is, geef dan “Length Not Matching” terug.
   d. Herhaal de vorige 2 punten totdat
      – het beginpunt van een record gelijk is aan PointerOldestDayRecord, of
      – de referenties DayRecordLength/PreviousDayRecordLength niet meer kloppen.
      In het eerste geval moet de PreviousDayRecordLength = ‘00 00’H. Wanneer dit niet het geval is, geef dan “Wrong Length” terug.
      Beschouw in het tweede geval het DailyRecord waar dit nog wel correct was als oudste record. Pas in dat geval ook PointerOldestDayRecord en PreviousDayRecordLength aan.
8. Controleer de laatste DailyRecord:
   a. Ga met de PointerLastDayRecord naar de laatste DailyRecord.
   b. Ga naar het eerste SessionRecord in het DailyRecord (PointerLastDayRecord + 10).
   c. Controleer of dit SessionRecord het laatste is door de beginpositie hiervan te vergelijken met de PointerLastSessionRecord.
   d. Is dit niet het laatste SessionRecord, controleer dan met PointerLastActivityRecord of de laatste activiteit een “Afsluiting” of een “Dagovergang” is. Is dit niet het geval, geef dan ”Record Not Closed” terug.
      Ga met behulp van PointerLastActivityRecord + de lengte van de laatste activiteit naar het volgende SessionRecord en herhaal het vorige punt.
   e. Controleer in het laatste SessionRecord of de PointerLastPWActivityRecord verwijst naar een “Start pauze” of “Start werk” activiteit.
      Is dit niet het geval, geef dan een “Invalid PW Pointer” terug.
   f. Controleer of de lengte van alle SessionRecords in dit DailyRecord samen gelijk is aan de DayRecordLength – 10.
      Is dit niet het geval, geef dan “DayRecordLength Wrong” terug.
9. Bij alle controles en leesacties moet rekening gehouden worden met de lengte van EF.Driver_Activity_Data.

8.18 Controleren op opgeslagen boordcomputercertificaat

Naam	IsCertificatePresent
Gebruik	Chauffeurskaart
Input gegevens	Systeemkaartnummer
Resultaat	Recentll‘90 00’H Certificaat aanwezig met ranking Recent (‘01’H-‘03’H) ‘6A 82’H Certificaat niet aanwezig op chauffeurskaart

In deze functie wordt gecontroleerd of het certificaat behorende bij het systeemkaartnummer al opgeslagen is in EF.BCT_Certificates.

Voor deze functie moeten de volgende stappen doorlopen worden:

1. Selecteer EF.BCT_Certificates met het commando Select met P1P2 = ‘04 0C’H en data = ‘E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E’H, gevolgd door het commando Select met P1P2 = ‘02 0C’H en data = ‘44 02’H.
2. Lees Index_1 t/m Index_3 met het commando Read Binary met offset = 3 (‘00 03’H) en het aantal verwachte bytes in de response 21 (‘15’H), en controleer of Index_x overeenkomt met het systeemkaartnummer.
   Zo ja, lees dan de bijbehorende Rank_x met het commando Read Binary met offset = de offset voor Rank_x en het aantal verwachte bytes in de response 1 en geef het resultaat ll ‘90 00’H terug.

Komt het systeemkaartnummer niet voor, geef dan de foutcode dat het certificaat niet gevonden is.

8.19 Volgorde bijwerken van opgeslagen boordcomputercertificaten

Naam	UpdateRanking
Gebruik	Chauffeurskaart
Input gegevens	Systeemkaartnummer
Resultaat	'90 00'H OK
	'6A 82'H Certificaat niet aanwezig op chauffeurskaart

Indien het certificaat behorende bij het systeemkaartnummer aanwezig is in EF.BCT_Certificates, wordt deze als meest recente in de Rank gezet.

Voor deze functie moeten de volgende stappen doorlopen worden:
1. Selecteer EF.BCT_Certificates met het commando Select met P1P2 = '04 0C'H en data = 'E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E'H, gevolgd door het commando Select met P1P2 = '02 0C'H en data = '44 02'H.
2. Lees Index_1 t/m Index_3 met het commando Read Binary met offset = 3 ('00 03'H) en het aantal verwachte bytes in de response 21 ('15'H) en controleer of één hiervan overeenkomt met het systeemkaartnummer.
   Zo niet, geef dan de foutcode terug dat het bijbehorende certificaat niet aanwezig is.
   Zo ja, lees dan de bijbehorende Rank_Highest
   – Voor Rank_1 t/m Rank_3, met uitzondering van Rank_Highest: als de inhoud van Rank_x < inhoud Rank_Highest en > 0, verhoog dan de inhoud van Rank_x dan met 1. Maak Rank_Highest = '01'.
   – Geef '90 00'H terug.

8.20 Geef opgeslagen boordcomputercertificaat

Naam	GetCertificate
Gebruik	Chauffeurskaart
Input gegevens	Systeemkaartnummer
Resultaat	Certificate||'90 00'H OK
	'6A 82'H Certificaat niet aanwezig op chauffeurskaart

Indien het certificaat behorende bij het systeemkaartnummer aanwezig is in EF.BCT_Certificates, wordt dit als resultaat terug gegeven.
Voor deze functie moeten de volgende stappen doorlopen worden:
1. Selecteer EF.BCT_Certificates met het commando Select met P1P2 = '04 0C'H en data = 'E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E'H, gevolgd door het commando Select met P1P2 = '02 0C'H en data = '44 02'H.
2. Lees Index_1 t/m Index_3 met het commando Read Binary met offset = 3 ('00 03'H) en het aantal verwachte bytes in de response 21 ('15'H) en controleer of één hiervan overeenkomt met het systeemkaartnummer.
   Zo niet, geef dan de foutcode terug dat het bijbehorende certificaat niet aanwezig is.
   Zo ja, ga dan door met stap 3.
3. Voer Read Binary commando's uit tot Length_1 (de certificaatlengte) bytes gelezen zijn. Per Read Binary kan een maximaal aantal bytes gelezen worden. Dit maximum is van een aantal factoren afhankelijk (zie referentie [7]) en wordt hier max_read genoemd. De eerste Read Binary heeft als offset de offset voor Certificate_x en het verwachte aantal bytes '00'H (in het geval dat Length_1 < max_read, dan wordt het verwachte aantal bytes Length_1). Voor iedere volgende Read Binary wordt de offset met max_read verhoogd. Het verwachte aantal bytes in de response is '00'H, behalve bij de laatste Read Binary, daar is het Length_1 modulo max_read.
4. geef het resultaat || '90 00'H terug.

8.21 Sla boordcomputercertificaat op

Naam	StoreCertificate
Gebruik	Chauffeurskaart
Input gegevens	Systeemkaartnummer, certificaat
Resultaat	'90 00'H OK
	'xx xx'H Foutcode van een van de gebruikte commando's, afhankelijk van smartcard implementatie

Het systeemkaartnummer wordt met het bijbehorende certificaat als meest recente opgeslagen in EF.BCT_Certificates. Hierbij wordt de plaats van het minst recente certificaat overschreven.

Voor deze functie moeten de volgende stappen doorlopen worden:
1. Selecteer EF.BCT_Certificates met het commando Select met P1P2 = '04 0C'H en data = 'E8 28 BD

08 0F A0 00 00 01 67 45 53 49 47 4E'H, gevolgd door het commando Select met P1P2 = '02 0C'H en data = '44 02'H.
2. Lees Rank_1 t/m Rank_3 met het commando Read Binary met offset = 0 en het aantal verwachte bytes in de response 3, en zoek de eerste waarde '00' of '03'. Dit is Rank_target.
3. Sla het systeemkaartnummer op in Index_target met het commando Update Binary met offset = de offset voor Index_target en het systeemkaartnummer als data.
4. Sla het certificaat op in Certificate_target met een reeks Update Binary commando's met de offset van het eerste commando gelijkgezet aan de offset voor Certificate_target en telkens de volgende max_write bytes van het certificaat als data. Indien het certificaat korter is dan de gereserveerde lengte voor het certificaat, vul bij het laatste Update Binary commando de rest dan aan met nullen ('00').
   NB. de hoogte van max_write is van een aantal factoren afhankelijk (zie referentie [7]).
5. Voor Rank_1 t/m Rank_3, met uitzondering van Rank_target: als de inhoud van Rank_x > 0, verhoog de inhoud dan met 1. Maak Rank_target = '01'.
6. Geef '90 00'H terug.

8.22 Geef meest recente DownloadLog

Naam	GetLastDownloadLog
Gebruik	Chauffeurskaart
Input gegevens	geen
Resultaat	DownloadLog || '90 00'H OK '6A 82'H DownloadLog niet aanwezig op chauffeurskaart 'xx xx'H Foutcode van een van de gebruikte commando's, afhankelijk van smartcard implementatie

Voor deze functie moeten de volgende stappen doorlopen worden:
1. Selecteer EF.BCT_Certificates met het commando Select met P1P2 = '04 0C'H en data = 'E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E'H, gevolgd door het commando Select met P1P2 = '02 0C'H en data = '44 02'H.
2. Lees IndexOldestDL met het commando Read Binary met offset = '18 B4'H en het aantal verwachte bytes in de response 1
3. Indien de gelezen waarde '00'H is, zet dan de IndexNewestDL (variabele in het geheugen) op 7, anders wordt de IndexNewestDL gelijkgesteld aan IndexOldestDL – 1.
4. Bereken nu de offset van de (meest recente) DownloadLog_X behorende bij IndexNewestDL als volgt: offset_x = '18 B5'H + 33 x IndexNewestDL.
5. Lees de aangeduide DownloadLog_X met het commando Read Binary met offset = offset_x en het verwachte aantal bytes in de respons 33.
6. Indien de respons uit 33 nullen ('00'H) bestaat, geef dan de foutcode terug dat er geen Download-Log records aanwezig zijn, retourneer anders de gelezen respons || '90 00'H.

8.23 Sla DownloadLog op

Naam	StoreDownloadLog
Gebruik	Chauffeurskaart
Input gegevens	DownloadLog
Resultaat	'90 00'H OK 'xx xx'H Foutcode van een van de gebruikte commando's, afhankelijk van smartcard implementatie

Het in de Input opgegeven DownloadLog wordt als het meest recente opgeslagen in DownloadLogs van EF.BCT_Certificates. Hierbij wordt de plaats van het minst recente DownloadLog overschreven.
Voor deze functie moeten de volgende stappen doorlopen worden:
1. Selecteer EF.BCT_Certificates met het commando Select met P1P2 = '04 0C'H en data = 'E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E'H, gevolgd door het commando Select met P1P2 = '02 0C'H en data = '44 02'H.
2. Lees IndexOldestDL met het commando Read Binary met offset = '18 B4'H en het aantal verwachte bytes in de response 1
3. Sla het gegeven DownloadLog op in DownloadLogs met het commando Update Binary met offset = '18 B5'H + 33 x IndexOldestDL. en het DownloadLog als data.
4. Indien de gelezen IndexOldestDL '07'H is, zet dan index_new = '00'H, zet anders index_new op IndexOldestDL + 1.
5. Sla de bijgewerkte index op met het commando Update Binary met offset = '18 B4'H en index_new (1 byte) als data.
6. Geef '90 00'H terug.

9 Commando's

De communicatie met de boordcomputerkaarten gebeurt door middel van commando-antwoord

paren. Het commando wordt naar de boordcomputerkaart toegestuurd en daarop komt een antwoord terug.

Een commando bestaat uit:
- een Class byte (CLA),
- een Instruction byte (INS),
- een Parameter 1 byte (P1),
- een Parameter 2 byte (P2),
- een Lengte gegevens byte (Lc) in het geval er gegevens zijn,
- gegevens (Data), optioneel
- een verwachte lengte antwoord byte (Le), optioneel.

Een antwoord bestaat uit:
- gegevens (Data), optioneel
- statuswoorden (SW1-SW2)

Dit hoofdstuk geeft enkele tips voor het gebruik van de commando's voor het selecteren, uitlezen en beschrijven van transparante elementaire files (transparent EF's). Voor de exacte opbouw van de commando-antwoord paren wordt echter verwezen naar Referentie [7].

De paragrafen hieronder vermelden bepaalde file identifiers en short EF identifiers. Voor een volledig overzicht van de beschikbare short EF identifiers (SFIDs) wordt verwezen naar Referenties [8] t/m [12].

9.1 Selecteren van EF's

Voordat een EF kan worden uitgelezen of beschreven, dient deze geselecteerd te worden. Voordat een EF geselecteerd kan worden, dient eerst de Dedicated File (DF) waar deze EF onderdeel van uitmaakt te worden geselecteerd. Conform Referenties [8] t/m [12] bevat elke BCT kaart de volgende twee DF's:
1. De Master File (MF)
   te selecteren met INS P1 P2 Lc Data = 'A0 00 0C 02 3F00'H
2. De Application DF (DF.CIA)
   te selecteren met INS P1 P2 Lc Data = 'A4 04 0C 0F E828BD080FA000000167455349474E'H

De verwachte respons op elk van de bovenstaande commando's is SW1-SW2 = '90 00'H.

Nadat de betreffende DF is geselecteerd, kan elke daarin opgenomen EF op een van de volgende wijzen worden geselecteerd:
1. Met een expliciete SELECT op basis van de 2-bytes file identifier (FID):
   INS P1 P2 Lc Data = 'A4 02 0C 02 (FID)
2. Met een expliciete SELECT inclusief opvragen van de file control parameters:
   INS P1 P2 Lc Data Le = 'A4 02 04 02 (FID) 00
3. Met een **impliciete** SELECT als onderdeel van het data handling commando:
   a. Voor offsets < 256:
      INS = INS met bit1 = 0 (EVEN instruction)
      P1 = bit8 t/m bit6 = 100b || bit5 t/m bit1 = short EF id
      P2 = offset [0...255]
      Lc Data Le = afhankelijk van de instructie
   b. Voor 0 <= offsets < ∞:
      INS = INS met bit1 = 1 (ODD instruction)
      P1P2 = bit16 t/m bit6 = 0...0b || bit5 t/m bit1 = short EF id
      of
      P1P2 = file identifier
      Lc = de lengte van Data
      Data = minimaal een "offset data object" met tag = 54h
      Le = afhankelijk van de instructie

9.2 Uitlezen van een nog niet geselecteerde EF vanaf een offset < 256

Als voorbeeld van efficiënt coderen volgt hier de kleinste commandoreeks waarmee de 4e t/m 7e byte (willekeurig voorbeeld) van EF.BCT_Certificates kunnen worden uitgelezen:

INS	P1	P2	Lc	Data	Le	Betekenis
A4	04	0C	0F	E828BD080F A000000167 455349474E		Selecteer de DF.CIA obv de AID

INS	P1	P2	Lc	Data	Le	Betekenis
B0	94	03			04	Impliciete SELECT van SFID = 14h, gevolgd door uitlezen van 4 bytes vanaf offset 3

9.3 Uitlezen van de huidige EF vanaf een offset kleiner 32768

Als voorbeeld van efficiënt coderen volgt hier het kleinste commando waarmee de 4000e t/m 4050e byte (willekeurig voorbeeld) van de momenteel geselecteerde EF kunnen worden uitgelezen:

INS	P1	P2	Lc	Data	Le	Betekenis
B0	1F	3F			33	Lees 51 (33h) bytes vanaf offset 7999 (1F3Fh) uit de momenteel geselecteerde EF.

9.4 In de huidige DF Uitlezen van een EF vanaf een offset groter dan 32767

Als voorbeeld van efficiënt coderen volgt hier de kleinste commandoreeks waarmee de 40000e t/m 40001e byte en dan de 40002e t/m 40003e byte (willekeurig voorbeeld) van de nog niet eerder geselecteerde EF.Driver_Activity_Data kunnen worden uitgelezen (uitgangspunt is dat de DF.CIA wel al geselecteerd is):

INS	P1	P2	Lc	Data	Le	Betekenis
B1	00	13	04	54 02 9C3F	02	Selecteer de EF met short file identifier (SFI) 13h en lees 2 (02h) bytes vanaf offset 39999 (9C3Fh) uit die EF.
B1	00	00	04	54 02 9C41	02	Lees de volgende 2 bytes uit diezelfde EF.

9.5 Opvragen van de FCP's o.a. voor de grootte van EF.Driver_Activity_Data

Omdat EF.Driver_Activity_Data per chauffeurskaart een eigen grootte heeft, is het noodzakelijk om minimaal één keer per kaartsessie te achterhalen wat die grootte exact is. Hiervoor biedt de chip (conform referentie [7]) en diens personalisatie de mogelijkheid om van EF's de file control parameters (FCP) op te vragen. Er van uitgaande dat de DF.CAI reeds is geselecteerd, is het betreffende commando voor de EF.Driver_Activity_Data als volgt:

INS	P1	P2	Lc	Data	Le	Betekenis
A4	02	04	02	4401	00	A4 = SELECT 02 = selecteer een EF 04 = vraag ook om FCP 02 = lengte van Data 4401 = EF file identifier 00 = retourneer alle beschikbare bytes

De chips zijn zodanig geprogrammeerd dat dit resulteert in de volgende respons (voorbeeld):

62 1B 80 02 xx xx 82 01 01 83 02 44 01 88 01 98 A1 08 8C 02 01 00 9C 02 01 00 8A 01 05 90 00

De betekenis van deze respons is hieronder uitgewerkt:

Bytes	Betekenis
62 1B	Hier volgen 27 (1Bh) bytes met FCP informatie
80 02 xx xx	De lengte van de file is gecodeerd in 2 bytes en bedraagt xxxx
82 01 01	Het file descriptor byte is 01h; het betreft een transparante EF
83 02 44 01	De file identifier van deze file is 4401h
88 01 98	De short file identifier van deze file is 13h (deze is gecodeerd in b8 t/m b4 van het derde byte, omdat b3 t/m b1 0 zijn): **10011**000
A1 08	Hier volgen 8 bytes met proprietary security attributen (dit zijn voorbeelden. Voor daadwerkelijke invulling zie Referentie [7])
8C 02 01 00	2 bytes met proprietary security attributen voor contactchip
9C 02 01 00	2 bytes met proprietary security attributen voor contactloze chip
8A 01 05	Het life cycle status byte van deze EF is 05h (operational state – activated)

Bytes	Betekenis
90 00	SW1-SW2 geeft “Normal processing” aan

Voor een compleet overzicht van FCP wordt verwezen naar § 3.3.4.1 van Referentie [7].

10 Referenties

De onderstaande referenties worden in dit document gebruikt:

[1] [1] ISO/IEC 7816-4 Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange. Edition: 2005.
[2] ISO/IEC 7816-8 Identification cards – Integrated circuit cards – Part 8: Commands for security operations. Edition: 2004.
[3] ISO/IEC 7816-15 Identification cards – Integrated circuit cards with contacts – Part 15: Cryptographic information application (2004-01-15).
[4] ISO/IEC 9797-1 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher.
[5] [9] ISO/IEC 9797-2 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function.
[6] [11] CWA 14890-1 Application Interface for smart cards used as Secure Signature Creation Devices – Part 1: Basic requirements. March 2004.
[7] [13] European card for e-services and national e-ID applications (IAS ECC) – Technical Specifications – Revision 1.0.1 – February 2009.
[8] BCT Kaartstructuur Systeemkaart v1.6. Inspectie Verkeer en Waterstaat.
[9] BCT Kaartstructuur Chauffeurskaart v1.6. Inspectie Verkeer en Waterstaat.
[10]BCT Kaartstructuur Ondernemerskaart v1.6. Inspectie Verkeer en Waterstaat.
[11]BCT Kaartstructuur Keuringskaart v1.6. Inspectie Verkeer en Waterstaat.
[12]BCT Kaartstructuur Inspectiekaart v1.6. Inspectie Verkeer en Waterstaat.
[13]BCT Certificaatprofielen en CRL model BCT kaarten v1.2. Inspectie Verkeer en Waterstaat.
[14]Regeling specificaties en typegoedkeuring boordcomputer taxi. Inspectie Verkeer en Waterstaat.
[15]Certificaatprofielen BCT Kaart CA’s v1.0. Inspectie Verkeer en Waterstaat.
[16]Generieke certificaatprofielen MinVenW PKIoverheid CSP v1.1, Ministerie van Verkeer en Waterstaat

11 Begrippen en afkortingen

De onderstaande begrippen en afkortingen worden in dit document gebruikt:

ATR	Antwoord op terugstellen
BCT	BoordComputer Taxi
CBC	Cipher Block Chaining
CC	Cryptografische controlesom
CG	Cryptogram
CH	Commando-kop
CLA	Klasse byte in CH
D()	Decodering met DES
DES	Data encryptie standaard
DO	Gegevensobject
E()	Codering met DES
Hash	Hashing
INS	Instructie byte in CH
IVW	Inspectie Verkeer en Waterstaat
Lc	Lengte van de data in een commando
Le	Lengte van het verwachte antwoord in een commando
MAC	Message Authentication Code
PB	Padding bytes
PI	Padding indicatorbyte (voor gebruik bij cryptogram voor vertrouwelijkheid DO)
PIN	Persoonlijk identificatie nummer
PKCS	Public Key Cryptography Standards
PUK	PIN unblock key
PV	Ongecodeerde waarde
P1	Parameter 1 byte in CH
P2	Parameter 2 byte in CH
RSA	Asymmetrisch encryptiealgoritme
SSC	Zendsequentieteller
SM	Beveiligde overbrenging
SW	Status woord (2 bytes) in een antwoord
TLV	Label – lengte – waarde
XOR	Exclusieve disjunctie
‘xx’B	Bit waarde
‘xx’H	Hexadecimale waarde

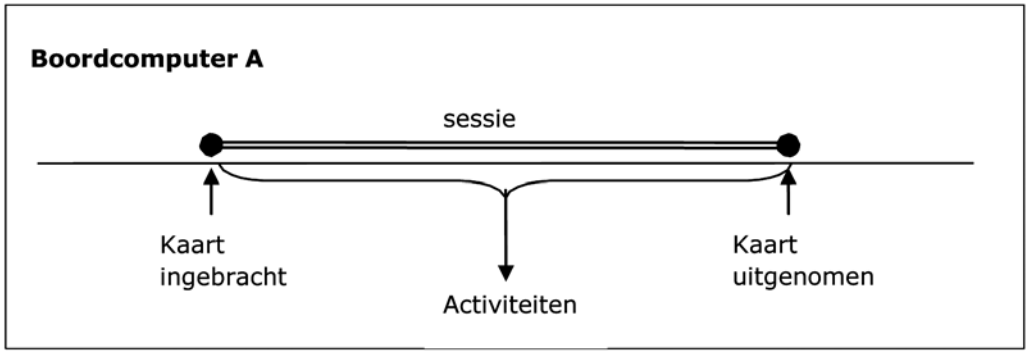
3DES	Drievoudig DES algoritme
||	Verbindingsoperator

Bijlage A Scenario's kaartsessies

Hieronder volgt een aantal scenario's die het wegschrijven van gegevens op de chauffeurskaart tijdens een kaartsessie toelichten.

A.1 Scenario 1: Normale kaartsessie

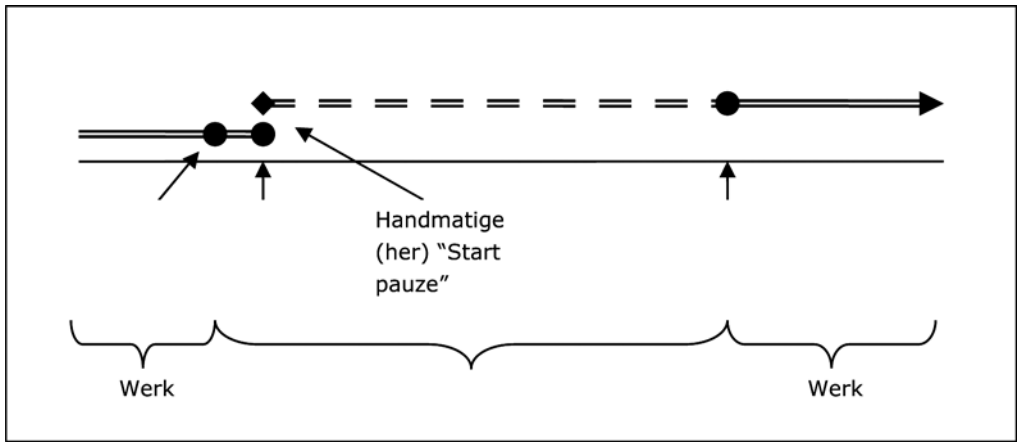
- De kaartsessie wordt begonnen met het inbrengen van de chauffeurskaart in de boordcomputer.
- Er zijn geen wijzigingen of aanvullingen sinds de vorige kaartsessie.
- Diverse activiteiten vinden plaats en worden op de chauffeurskaart opgeslagen.
- De kaartsessie wordt normaal afgesloten waarna de chauffeurskaart uit de boordcomputer genomen kan worden.



Activiteit	Tijdstip	Handm.
Login	8:00:00	'0'B
Start werk	8:00:00	'0'B
Start pauze	10:30:00	'0'B
Start werk	11:00:00	'0'B
Afsluiting	13:15:00	'0'B

A.2 Scenario 2: Sessie afgesloten met pauze, nieuwe sessie met einde pauze

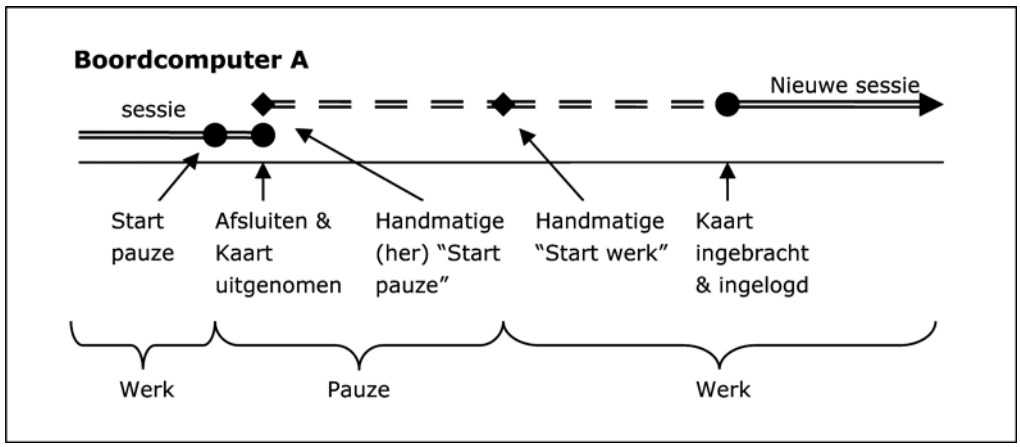
- Bij een bestaande kaartsessie wordt op de boordcomputer ingegeven dat de pauze begint. Hierna wordt de kaartsessie afgesloten en de chauffeurskaart uit de boordcomputer genomen.
- Na het opnieuw inbrengen van de chauffeurskaart constateert de boordcomputer dat de vorige sessie na een "Start pauze" werd afgesloten. Omdat een arbeidsperiode hiermee lijkt te eindigen met een pauze, wordt de chauffeur hier extra op geattendeerd. Sowieso vraagt de boordcomputer of er nog activiteiten moeten worden toegevoegd sinds de laatste activiteit. De chauffeur besluit zijn bezigheden (pauze genieten) tussen die laatste afsluiting en het huidige inlogmoment handmatig te boeken, om te voorkomen dat hij de periode tussen afsluiten en inloggen niet kan verantwoorden.
- Omdat bij het inbrengen van de chauffeurskaart standaard een "Start werk" toegevoegd wordt, hoeft de chauffeur, na de handmatige toevoeging, het hervatten van werk niet expliciet aan te geven.



Activiteit	Tijdstip	Handm.	SessionRecord
...			n
Start pauze	13:14:30	'0'B	n
Afsluiting	13:15:00	'0'B	n
Start pauze	13:15:00	'1'B	n+1
Login	13:45:00	'0'B	n+1
Start werk	13:45:00	'0'B	n+1
...			n+1

A.3 Scenario 3: Sessie afgesloten met pauze, nieuwe sessie met einde pauze en andere werkzaamheden

- Bij een bestaande kaartsessie wordt op de boordcomputer ingegeven dat de pauze begint. Hierna wordt de kaartsessie afgesloten en de chauffeurskaart uit de boordcomputer genomen.
- Na het opnieuw inbrengen van de chauffeurskaart constateert de boordcomputer dat de vorige sessie na een "Start pauze" werd afgesloten. Omdat een arbeidsperiode hiermee lijkt te eindigen met een pauze, wordt de chauffeur hier extra op geattendeerd. Sowieso vraagt de boordcomputer of er nog activiteiten moeten worden toegevoegd sinds de laatste activiteit. De chauffeur besluit zijn bezigheden (pauze genieten) na die laatste afsluiting handmatig te boeken.
- De werkzaamheden waren in werkelijkheid echter eerder gestart dan het moment van inloggen, daarom wordt voorafgaand aan het inlogmoment ook nog handmatig een "Start werk" toegevoegd. De pauze stopt hiermee dus eerder dan het inlogmoment.
- De boordcomputer boekt zelf ook nog een "Start werk" na de inlogboeking.

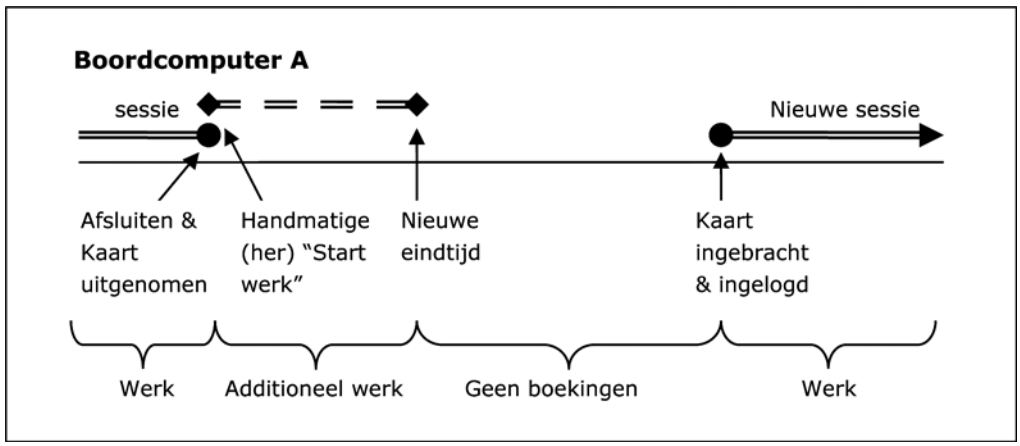


Activiteit	Tijdstip	Handm.	SessionRecord
...			n
Start pauze	13:14:30	'0'B	n
Afsluiting	13:15:00	'0'B	n

Activiteit	Tijdstip	Handm.	SessionRecord
Start pauze	13:15:00	'1'B	n+1
Start werk	13:30:00	'1'B	n+1
Login	13:45:00	'0'B	n+1
Start werk	13:45:00	'0'B	n+1
...			n+1

A.4 Scenario 4: Sessie afgesloten, volgende dag toevoegen van andere werkzaamheden aan de vorige dag

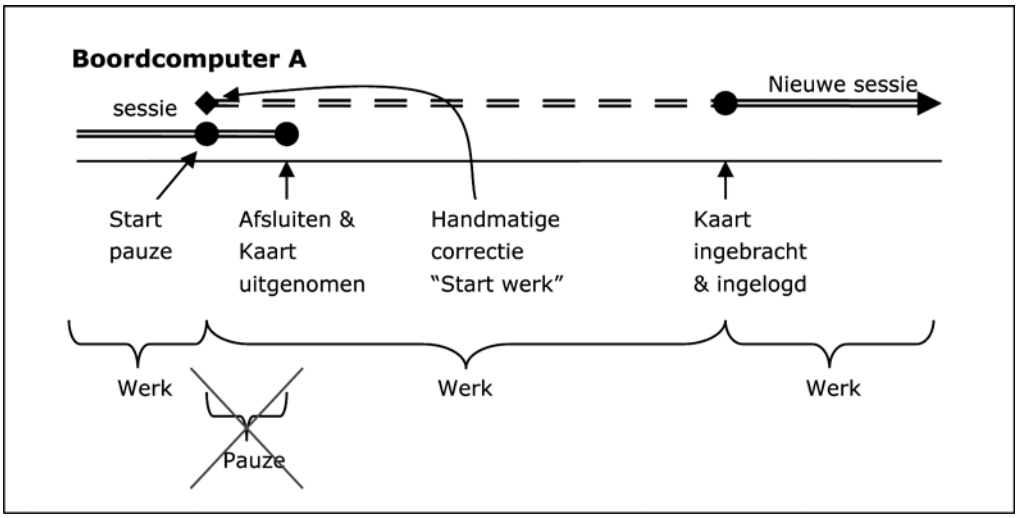
- Na de laatste activiteit wordt de kaartsessie afgesloten en de chauffeurskaart uit de boordcomputer genomen.
- Bij het inbrengen van de chauffeurskaart in de boordcomputer de volgende dag, wordt gevraagd of er nog activiteiten sinds het einde van de vorige kaartsessie zijn geweest. Dat is het geval, want er zijn de vorige dag, na het verlaten van de auto, nog andere werkzaamheden verricht. Dit wordt eerst toegevoegd.
- Daarna kunnen de activiteiten voor de nieuwe dag beginnen.



Activiteit	Tijdstip	Handm.	SessionRecord
...			n
Start werk	13:00:00	'0'B	n
Afsluiting	15:15:00	'0'B	n
Start werk	15:15:00	'1'B	n+1
Nieuwe eindtijd	16:15:00	'1'B	n+1
Hier wordt ook een nieuw DailyRecord met een eerste SessionRecord ingevoegd			
Login	9:00:00	'0'B	n+2
Start werk	9:01:00	'0'B	n+2
...			n+2

A.5 Scenario 5: Sessie afgesloten, pauze vervangen door andere werkzaamheden

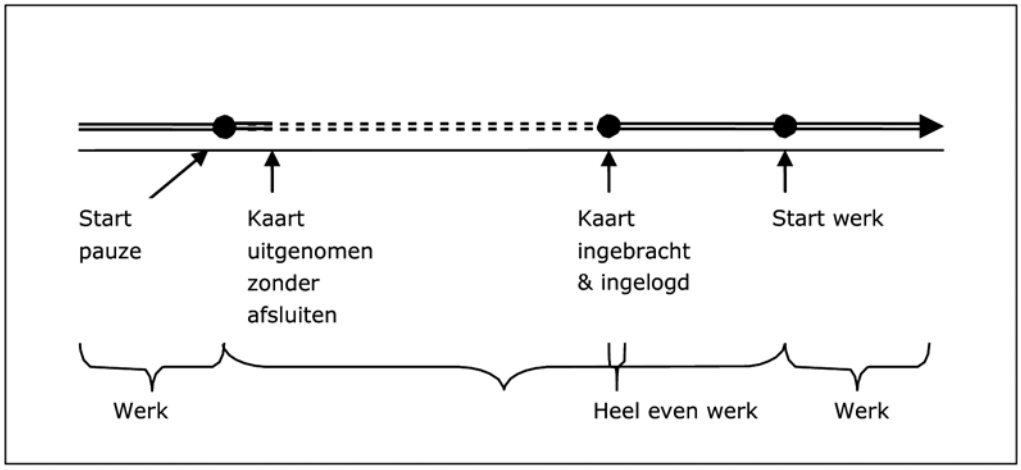
- Bij een bestaande kaartsessie wordt op de boordcomputer ingegeven dat de pauze begint. Hierna wordt de kaartsessie afgesloten en de chauffeurskaart uit de boordcomputer genomen.
- Later blijkt dat de pauze niet doorgegaan is en dat in plaats daarvan andere werkzaamheden verricht zijn tot het huidige tijdstip.
- Bij het inbrengen van de chauffeurskaart in de boordcomputer moet dit gecorrigeerd worden. De boordcomputer zal de bestuurder attenderen op het feit dat de laatstgeboekte en afgesloten activiteit een pauze was. Na het bevestigen van de vraag of er nog handmatig activiteiten moeten worden toegevoegd, kan de chauffeur een "Start werk" laten ingaan op hetzelfde moment dat de "Start pauze" begon. De pauze wordt hiermee in feite overschreven door andere werkzaamheden.



Activiteit	Tijdstip	Handm.	SessionRecord
...			n
Start pauze	16:40:00	'0'B	n
Afsluiting	16:41:00	'0'B	n
Start werk	16:40:00	'1'B	n+1
Login	17:10:00	'0'B	n+1
Start werk	17:11:00	'0'B	n+1
...			n+1

A.6 Scenario 6: Sessie niet afgesloten, vervolg zelfde werkzaamheden

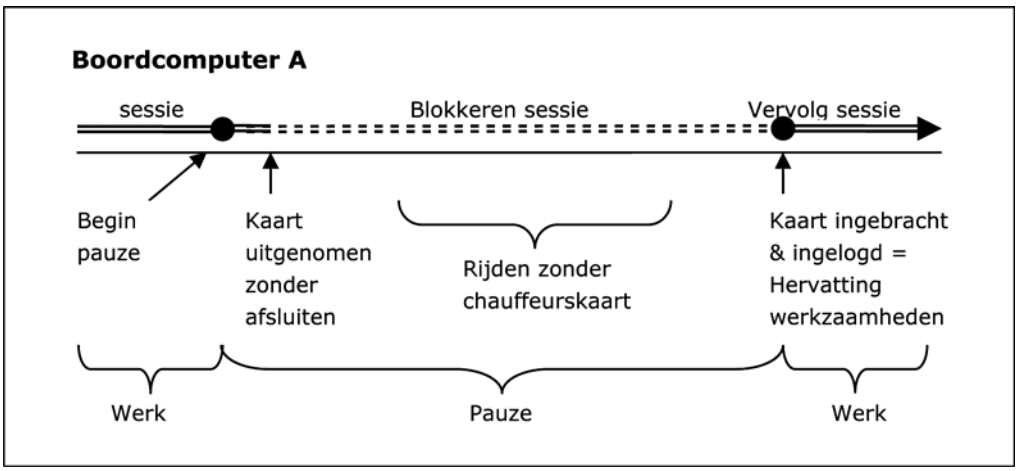
- Bij een bestaande kaartsessie wordt op de boordcomputer ingegeven dat de pauze begint. De chauffeur neemt de kaart uit zonder dat de kaartsessie is afgesloten. Hierop blokkeert de boordcomputer deze kaartsessie.
- Enige tijd later (binnen de 60 minuten) wordt de chauffeurskaart weer in de boordcomputer ingebracht. Omdat het dezelfde kaart is als waarvan de kaartsessie geblokkeerd is, zal de boordcomputer deze blokkering opheffen.
- Omdat de kaart wel even verwijderd is geweest, zal de boordcomputer de chauffeur vragen of er sinds de "Start pauze" nog (andere) activiteiten zijn geweest. Aangezien dit niet het geval was, maakt de chauffeur geen gebruik van de mogelijkheid tot het handmatig toevoegen van activiteiten.
- De boordcomputer boekt nu de login automatisch gevolgd door een "Start werk" (na inloggen moet een boordcomputer namelijk altijd in werkniveau terechtkomen). Gezien het echter nog pauze is, zal de chauffeur direct ingeven dat het (nog steeds/weer) pauze is. Vanaf nu is het echter pauze met de kaart in de boordcomputer.
- De chauffeur beëindigt de pauze op het ogenblik dat hij weer gaat werken.



Activiteit	Tijdstip	Handm.	SessionRecord	Opmerking
...			n	
Start pauze	15:00:00	'0'B	n	
(kaart uitnemen)			n	Sessie geblokkeerd op BCT
			n	Sessie geblokkeerd op BCT
(kaart inbrengen)			n	Geen handm. toevoegingen
Login	15:30:00	'0'B	n	Ingevoegd door BCT
Start werk	15:30:00	'0'B	n	Ingevoegd door BCT
Start pauze	15:30:30	'0'B	n	(terug)gezet door bestuurder
Start werk	15:40:00	'0'B	n	Aangegeven door bestuurder
...			n	

A.7 Scenario 7: Sessie niet afgesloten, andere activiteiten ertussendoor

- Bij een bestaande kaartsessie wordt op de boordcomputer ingegeven dat de pauze begint. De chauffeur neemt zijn kaart uit de boordcomputer zonder af te sluiten. Hierop blokkeert de boordcomputer de kaartsessie.
- Daarna wordt er met het voertuig gereden, zonder een chauffeurskaart (in zijn pauze is dit toegestaan).
- Binnen 60 minuten na het uitnemen wordt de chauffeurskaart weer in de boordcomputer gebracht, dus de kaartsessie is nog geblokkeerd. Het is dezelfde kaart die ingebracht wordt als die waarvan de kaartsessie geblokkeerd is en dus wordt de blokkering opgeheven.
- De chauffeur begint weer met werken.

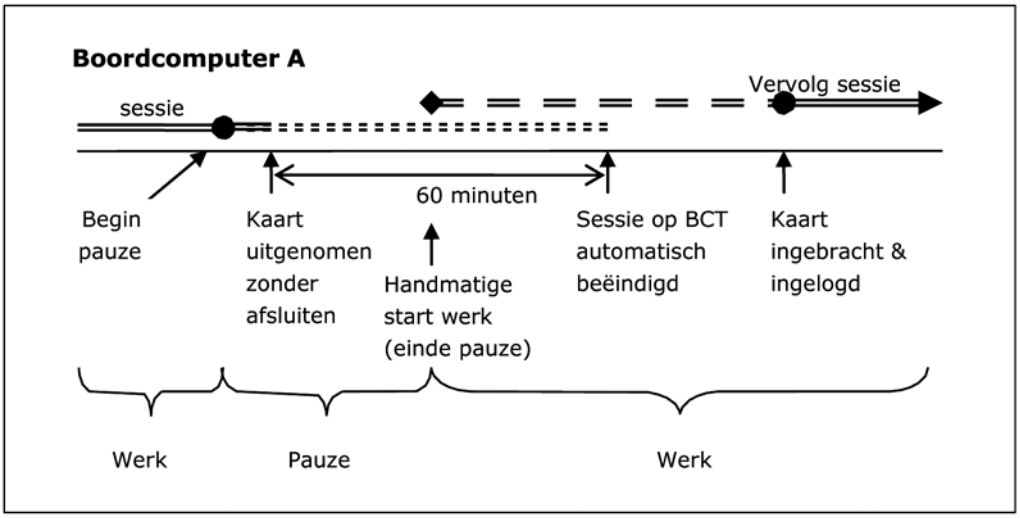


Activiteit	Tijdstip	Handm.	SessionRecord
...			n
Start pauze	16:00:00	'0'B	n

Activiteit	Tijdstip	Handm.	SessionRecord
(kaart uitnemen)			n
			n
(rijden zonder chauffeurskaart)			n
			n
(kaart inbrengen)			n
Login	16:25:00	‘0’B	n
Start werk	16:25:00	‘0’B	n
...			n

A.8 Scenario 8: Sessie niet afgesloten, later automatisch beëindigd

- Bij een bestaande kaartsessie wordt op de boordcomputer ingegeven dat de pauze begint. De chauffeur neemt zijn kaart uit de boordcomputer zonder af te sluiten. Hierop blokkeert de boordcomputer de kaartsessie.
- Aangezien er na 60 minuten nog niets gebeurd is, wordt op de boordcomputer de geblokkeerde kaartsessie automatisch afgesloten.
- Als de chauffeur daarna zijn kaart weer in de boordcomputer brengt, wordt gesignaleerd dat de sessie op de kaart niet goed afgesloten was.
- Verder wordt gevraagd of er nog activiteiten sinds het einde van de vorige kaartsessie zijn geweest. Dat is zo, want de pauze was eigenlijk binnen de 60 minuten afgelopen waarna andere werkzaamheden zijn begonnen.
- Omdat op de boordcomputer de sessie al beëindigd was, wordt een nieuwe kaartsessie begonnen.



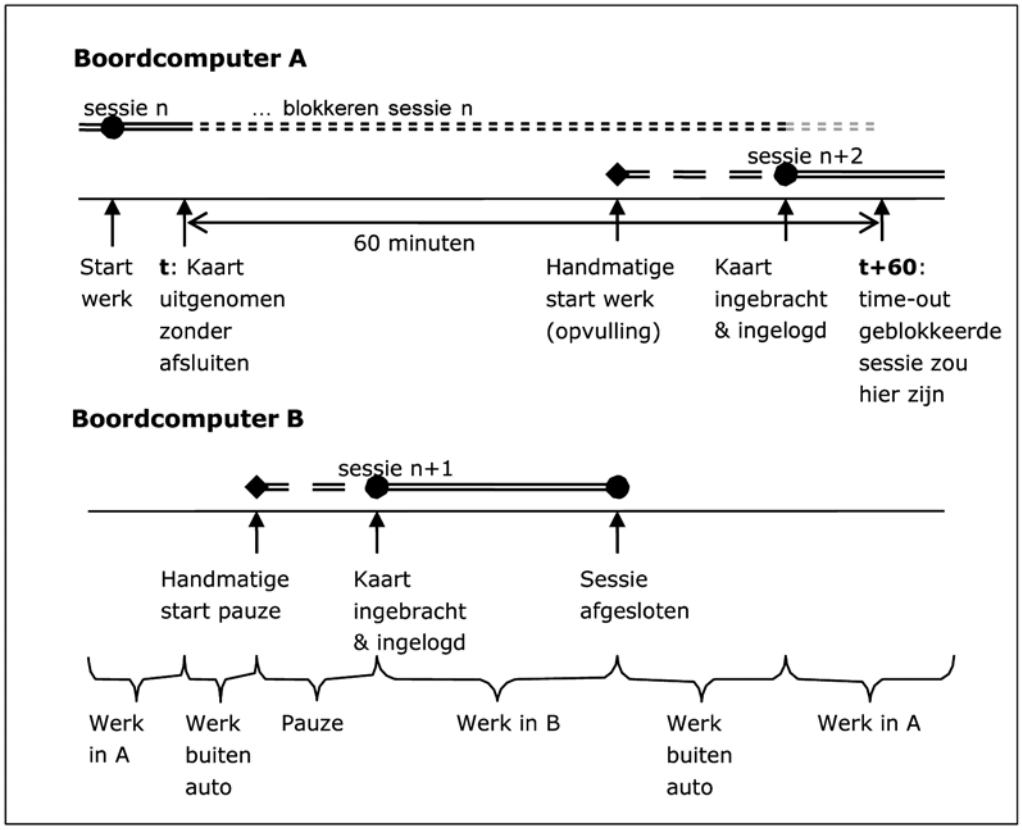
Activiteit	Tijdstip	Handm.	SessionRecord
...			n
Start pauze	16:00:00	‘0’B	n
(kaart uitnemen om 16:00:02)			
(sessie time-out om 17:00:02)			
(kaart inbrengen om 17:25:00)			
(nieuw sessierecord)			
Start werk	16:30:00	‘1’B	n+1
Login	17:25:00	‘0’B	n+1
Start werk	17:26:00	‘0’B	n+1
...			

A.9 Scenario 9: Sessie niet afgesloten, kaart tussendoor in ander voertuig

- Boordcomputer A: de laatstgeboekte activiteit is “Start werk” en de chauffeur neemt zijn kaart uit de boordcomputer zonder af te sluiten. Hierop blokkeert de boordcomputer de kaartsessie (n). Er vinden voorlopig geen andere activiteiten plaats.
- Boordcomputer B: de chauffeurskaart wordt binnen de 60 minuten na het uitnemen uit boordcomputer A ingebracht in B:

- Er wordt geconstateerd dat de vorige sessie (op A) niet goed afgesloten is.
- Er wordt een nieuwe kaartsessie (n+1) gestart.
- Er wordt gevraagd of er nog andere werkzaamheden of pauze moeten worden toegevoegd of aangepast. Hierbij geeft de chauffeur aan dat hij 10 minuten voor het inloggen met pauze ging, waarmee de periode tussen uitnemen van de kaart en de start van die pauze kan worden beschouwd als een voortzetting van het werk (buiten de auto). Hierna worden geen andere handmatige activiteiten opgevoerd, waardoor de boordcomputer het inloggen zal boeken en in werkniveau zal gaan staan.
- Nieuwe activiteiten worden opgeslagen op de kaart.
- De kaartsessie wordt afgesloten binnen de 60 minuten na het uitnemen uit boordcomputer A.
- Hierna werkt de chauffeur een kwartiertje buiten de auto.

- Boordcomputer A: de chauffeurskaart wordt ingebracht na het kwartiertje werk, maar nog steeds binnen 60 minuten na het uitnemen uit boordcomputer A. Op boordcomputer A is de kaartsessie dus nog steeds geblokkeerd:
  - Het is dezelfde kaart die ingebracht wordt als die waarvan de kaartsessie geblokkeerd is en dus wordt de blokkering opgeheven.
  - Aangezien bij het uitlezen van de kaart gezien wordt dat er in de tussentijd een kaartsessie op een andere boordcomputer is geweest, kan de gedeblokkeerde sessie niet worden voortgezet, maar zal op boordcomputer A een nieuwe sessie (n+2) starten.
  - De boordcomputer biedt de chauffeur de mogelijkheid om de laatste activiteit van de vorige sessie (n+1) te vervangen, te wijzigen of aan te vullen. Hiervan maakt de chauffeur gebruik door een handmatige “Start werk” op te voeren die start op het tijdstip dat die vorige sessie (n+1) werd afgesloten. Het “kwartiertje werk” is hiermee verantwoord.
  - Dan boekt boordcomputer A het nieuwste login tijdstip en gaat over tot niveau werken.
- De nieuwe kaartsessie (n+2) verloopt verder normaal.



Activiteit	Tijdstip	Handm.	SessionRecord
...			n
Start werk	16:00:00	‘0’B	n
(kaart uitnemen uit A om 17:00)			n
(kaart inbrengen in B om 17:25)			
(nieuw sessierecord)			

Activiteit	Tijdstip	Handm.	SessionRecord
Start pauze (10 min pauze gehad)	17:15:00	‘1’B	n+1
Login	17:25:00	‘0’B	n+1
Start werk	17:25:00	‘0’B	n+1
Afsluiting	17:40:00	‘0’B	n+1
(kaart inbrengen in A om 17:55)			
(nieuw sessierecord)			
Start werk (opvullen van 15 min)	17:40:00	‘1’B	n+2
Login	17:55:00	‘0’B	n+2
Start werk	17:55:00	‘0’B	n+2
...			n+2

Bijlage B Referentie data

Hieronder volgt een aantal voorbeelden van functies met de uitgewerkte hexadecimale codes. Dit geeft een beter inzicht in het toepassen van deze functies in de Boordcomputer Taxi.

B.1 Het opzetten van Secure Messaging

Voor het opzetten van Secure Messaging, zoals beschreven staat in 4.6, worden de volgende stappen uitgevoerd:

1. Lees de inhoud van EF.SN.ICC door middel van een read binary met SFI ’1C’h en een offset ’00’h.

```
Read_Binary
  Sent:                00 B0 9C 00 00
    Cla                  '00'h
    Ins                  'B0'h
    P1                   '9C'h
    P2                   '00'h
    Le                   '00'h
Read_Binary_Response
  Received:            5A 0A 99 98 05 14 30 00 00 04 80 7F 90 00
    DATA                 '5A 0A 99 98 05 14 30 00 00 04 80 7F'h
    STATUS               '90 00'h
```

   De laatste 8 bytes van de response data wordt gebruikt als SN.ICC.

2. Selecteer het te gebruiken algoritme voor de mutual authenticate en de symmetrische sleutel referentie.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde ’C1’h en P2 de waarde ’A4’h. De data bij dit commando is ’80 01 8C 83 01 03’h (’8C’h om “symmetric mutual authentication algorithm with SHA-256” aan te duiden en ’03’h om het Security Data Object (SDO) van PKI.KS.SM.ICC aan te duiden).

```
MSE
  Sent:                00 22 C1 A4 06 80 01 8C 83 01 03
    Cla                  '00'h
    Ins                  '22'h
    P1                   'C1'h
    P2                   'A4'h
    Lc                   '06'h
    Data                 80 01 8C 83 01 03
MSE_Response
  Received:            90 00
```

3. Vraag om een random waarde door middel van Get Challenge.

```
Get_Challenge
  Sent:                00 84 00 00 08
    Cla                  '00'h
    Ins                  '84'h
    P1                   '00'h
    P2                   '00'h
    Le                   '08'h
Get_Challenge_Response
  Received:            6D A5 42 C6 A1 B9 A9 13 90 00
    DATA                 '6D A5 42 C6 A1 B9 A9 13'h
    STATUS               '90 00'h
```

De response data is de RND.ICC.

4. Genereer een random waarde van 8 bytes voor RND.IFD, een random waarde van 32 bytes voor K.IFD en bepaal een serienummer SN.IFD van 8 bytes.
5. Stel het bericht S samen:
   S = RND.IFD || SN.IFD || RND.ICC || SN.ICC || K.IFD.
6. Bereken de encrypted waarde van S met CBC Triple DES encryptie, ICV '00'h en de encryptie sleutel ENC.KEY (laatste 16 bytes van transportkey1):
   ENC = CBCTDes('00', S, ENC.KEY).
7. Bereken de Retail MAC over de encrypted waarde van S met ICV '00'h en de MAC sleutel MAC.KEY (eerste 16 bytes van transportkey1):
   MAC = RMac('00', ENC || '80', MAC.KEY).
   NB. Gebruik altijd padding met '80 ...' achter de data.
8. Voer een Mutual Authenticate commando uit met als data ENC || MAC.

```
Mutual_Authenticate
  Sent:                00 82 00 00 48 FD C4 21 31 71 ...
     Cla                  '00'h
     Ins                  '82'h
     P1                   '00'h
     P2                   '00'h
     Lc                   '48'h
     AUT_TOK              FD C4 21 31 71 ...
     Le                   '48'h
Mutual_Authenticate_Response
  Received:            0E 70 90 22 0E E2 75 F5 E7 A4 ...
     ENC_TEXT             '0E 70 90 22 0E E2 75 F5 E7 A4 ...'h
     MAC                  '5E DE FB 7C 75 F2 48 5A'h
     STATUS               '90 00'h
```

9. Wanneer de status van de response '90 00'h is, is er ook response data beschikbaar.
   a. Haal de encrypted data ENC_R en de MAC uit deze data.
   b. Bereken de Retail MAC over ENC_R met ICV '00'h en de MAC sleutel MAC.KEY:
      MAC_R = RMac('00', ENC_R || '80', MAC.KEY).
      Ook hier moet weer de padding met '80 ...' gebruikt worden.
   c. Bereken de decrypted waarde van ENC_R met Inverse CBC Triple DES encryptie, ICV '00'h en de encryptie sleutel ENC.KEY:
      DEC_S = InvCBCTDes('00', ENC_R, ENC.KEY).
10. Wanneer de berekende MAC_R gelijk is aan de MAC uit de response data van de Mutual Authenticate, dan is DEC_S gelijk aan
    RND.ICC || SN.ICC || RND.IFD || SN.IFD || K.ICC.
11. Hieruit kunnen de volgende waardes berekend worden:
    - K_ICC_IFD = K.IFD xor K.ICC

- SK_ENC = 1e 16 bytes van SHA256(K_ICC_IFD || '00 00 00 01')
- SK_MAC = 1e 16 bytes van SHA256(K_ICC_IFD || '00 00 00 02')
- SSC = laatste 4 bytes RND.ICC || laatste 4 bytes RND.IFD

B.2 Het sturen van commando's met Secure Messaging

Na het opzetten van de secure messaging verbinding, moeten alle volgende commando's met secure messaging uitgevoerd worden. Dit staat beschreven in 4.1 t/m 4.5.
Hierbij worden de SK_ENC, SK_MAC en SSC gebruikt die na het opzetten van de secure messaging verbinding te berekenen zijn (zie hierboven).

Om te komen van een normaal commando tot een commando onder secure messaging, moeten de volgende stappen doorlopen worden:

1. Verhoog de SSC met 1.
2. De Cla byte 'xx' wordt 'xC' (Cla').
3. Als het commando data bevat (Lc > 0), dan moet deze data encrypt worden. Bereken de encrypted waarde van de data met CBC Triple DES encryptie, ICV '00'h en de encryptie sleutel SK_ENC:
   ENC = CBCTDes('00', data || '80', SK_ENC).
   Ook hier moet weer de padding met '80 ...' gebruikt worden.
4. De SecuredData waarover een Retail MAC berekend moet worden is afhankelijk van Lc en Le:
   - **Lc > 0, Le > 0**
     SSC || Cla || Ins || P1 || P2 || '80' || '87' || Length(ENC)+1 || '01' || ENC || '97' || Length(Le) || Le || '80'
   - **Lc > 0, Le = 0**
     SSC || Cla || Ins || P1 || P2 || '80' || '87' || Length(ENC)+1 || '01' || ENC || '80'
   - **Lc = 0, Le > 0**
     SSC || Cla || Ins || P1 || P2 || '80' || '97' || Length(Le) || Le || '80'
   - **Lc = 0, Le = 0**
     SSC || Cla || Ins || P1 || P2 || '80'

   Let op dat er padding met '80 ...' gebruikt moet worden na P2 en, indien Lc > 0 of Le > 0, aan het eind van de data.
   De te gebruiken ICV is '00'h en de te gebruiken sleutel is SK_MAC.
5. Het te versturen commando ziet er dan als volgt uit:
   Cla' || Ins || P1 || P2 || Length(SecuredData) + 10 || SecuredData || '8E 08'|| MAC || '00'
6. Het formaat van de response onder secure messaging is afhankelijk van het terug krijgen van data:
   - **data terug (even Ins)**
     '87' || Length(EncryptedData) + 1 || '01'|| EncryptedData || '99 02' || SW || '8E 08' || MAC || SW
   - **data terug (oneven Ins)**
     '85' || Length(EncryptedData) || EncryptedData || '99 02' || SW || '8E 08' || MAC || SW
   - **geen data terug**
     '99 02' || SW || '8E 08' || MAC || SW
7. Verhoog de SSC met 1.
8. Bereken een Retail MAC over de volgende data, afhankelijk van het formaat van de response:
   - **data terug (even Ins)**
     SSC || '87' || Length(EncryptedData) + 1 || '01'|| EncryptedData || '99 02' || SW || '80'
   - **data terug (oneven Ins)**
     SSC || '85' || Length(EncryptedData) || EncryptedData || '99 02' || SW || '80'
   - **geen data terug**
     SSC || '99 02' || SW || '80'

   In alle gevallen wordt er op het eind padding met '80' gebruikt.
   De te gebruiken ICV is '00'h en de te gebruiken sleutel is SK_MAC.
9. Vergelijk de berekende Retail MAC met de MAC uit de response. Deze moeten gelijk aan elkaar zijn.
10. Zijn de ontvangen en berekende MAC gelijk aan elkaar, dan kan de EncryptedData, indien aanwezig, decrypted worden.
    Bereken de decrypted waarde van EncryptedData met Inverse CBC Triple DES encryptie, ICV '00'h en de encryptie sleutel SK_ENC:
    DecryptedData = InvCBCTDes('00', EncryptedData, SK_ENC).

Zie de tabel hieronder voor een voorbeeld van een commando, het commando met secure messaging en het antwoord met secure messaging.

```
Command: 00 A4 04 0C 0F E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E
  CLASS                '00'h
  INS                  'A4'h
  P1                   '04'h
  P2                   '0C'h
  Lc                   '0F'h
  DATA                 'E8 28 BD 08 0F A0 00 00 01 67 45 53 49 47 4E'h
  Le                   ''h

Secured_Command: 0C A4 04 0C 1D 87 11 01 2A 53 6D EB 1D 3D B0 12 F9 4D
5D 06 E2 1D 66 07 8E 08 70 4C 67 9B 68 B2 FD 98 00
  CLA                  '0C'h
  INS                  'A4'h
  P1                   '04'h
  P2                   '0C'h
  Lc                   '1D'h
  DATA
    Tdd                  '87'h
    Ldd                  '11'h
    Vdd                  '01'h
    SecData              '2A 53 6D EB 1D 3D B0 12 F9 4D 5D 06 E2 1D 66
    07'h
    Tle                  ''h
    Lle                  ''h
    Vle                  ''h
    Tcc                  '8E'h
    Lcc                  '08'h
    CCKS                 '70 4C 67 9B 68 B2 FD 98'h
  Le2                  '00'h

Secured_Response: 99 02 90 00 8E 08 F7 D4 20 0F 77 D5 DB CD 90 00
  DATA
    SignedData           ''h
    SignedSW
      Tsw                  '99'h
      Lsw                  '02'h
      SW                   '90 00'h
    Cryptogram
      Tcc                  '8E'h
      Lcc                  '08'h
      CryptoCC             'F7 D4 20 0F 77 D5 DB CD'h
  STATUS               '90 00'h
```

B.3 Het zetten van een handtekening met een boordcomputerkaart

B.3.1 SignDataLegally

Voor het zetten van een elektronische handtekening met een boordcomputerkaart, zoals beschreven staat in 8.5, worden de volgende stappen uitgevoerd:

1. Allereerst moet het hash template met het te gebruiken algoritme geselecteerd worden.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'h en P2 de waarde 'AA'h. De data bij dit commando is '80 01 40'h ('40'h om de algoritme identifier voor SHA-256 aan te geven).

```
MSE
  Sent:                00 22 41 AA 03 80 01 40
    Cla                  '00'h
    Ins                  '22'h
    P1                   '41'h
    P2                   'AA'h
    Lc                   '03'h
    Data                 '80 01 40'h
MSE_Response
  Received:            90 00
```

2. Selecteer het te gebruiken algoritme en de private sleutel van de BCT Handtekening.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'h en P2 de waarde 'B6'h. De data bij dit commando is '80 01 42 84 01 86'h ('42'h om "PKCS#1 v1.5 – SHA-256" aan te duiden en '86'h om het Security Data Object (SDO) van PKI.CH.DS aan te duiden).

```
MSE
  Sent:                00 22 41 B6 06 80 01 42 84 01 86
    Cla                  '00'h
    Ins                  '22'h
    P1                   '41'h
    P2                   'B6'h
    Lc                   '06'h
    Data                 '80 01 42 84 01 86'h
MSE_Response
  Received:            90 00
```

3. De private sleutel van de BCT Handtekening mag pas gebruikt worden nadat de PIN gevalideerd is. Dit is nodig voor iedere keer dat deze sleutel gebruikt wordt. Dit wordt gedaan met het commando Verify, waarbij P2 (de PIN reference) de waarde '01'h heeft. Voor de PIN wordt PIN formaat 2 gebruikt.

```
Verify
  Sent:                00 20 00 01 08 24 95 99 FF FF FF FF FF
    Cla                  '00'h
    Ins                  '20'h
    P1                   '00'h
    P2                   '01'h
    Lc                   '08'h
    CHV                  '24 12 34 FF FF FF FF FF'h
Verify_Response
  Received:            90 00
```

4. Wanneer de input gegevens uit meer dan 64 bytes bestaan, moet er een intermediate hash met SHA-256 berekend worden door de boordcomputerlogica. Hierbij wordt het laatste gegevensblok niet gehashed, maar wordt de intermediate hash en het aantal gehashte bits onthouden voor de volgende stap.
   Wanneer het totaal aan input gegevens uit maximaal 64 bytes bestaat, wordt er geen intermediate hash berekend en worden alle inputgegevens in de volgende stap gebruikt.
5. Het berekenen van de uiteindelijke hash met SHA-256 wordt door de boordcomputerkaart gedaan. Hiervoor wordt het commando PSO Hash gebruikt. Hierbij worden de "intermediate hash value", het aantal gehashte bits en het laatste (of enige) blok inputdata van minimaal 1 en maximaal 64 bytes opgenomen in het Dataveld van het commando. Bij een succesvol uitgevoerde PSO HASH

zal de uiteindelijke hash waarde in het chipgeheugen van de boordcomputerkaart achterblijven ten behoeve van de volgende en laatste stap.

```
Total data = '90 00 80 32 BB BB ... BB'h

PSOHash
  Sent:                00 2A 90 A0 36 90 00 80 32 BB BB ... BB
    Cla                  '00'h
    Ins                  '2A'h
    P1                   '90'h
    P2                   'A0'h
    Lc                   '36'h
    HCD                  '90 00 80 32 BB BB ... BB'h
PSOHash_Response
  Received:            90 00
```

6. Met de gekozen private sleutel wordt de handtekening berekend over de in het chipgeheugen aanwezige hashwaarde.
   Dit wordt gedaan met het commando PSO Compute Digital Signature. Le, het verwachte aantal bytes in de response, moet daarbij op '00'h staan.

```
Compute_Dig_Sign
  Sent:                00 2A 9E 9A 00
    Cla                  '00'h
    Ins                  '2A'h
    P1                   '9E'h
    P2                   '9A'h
    Le                   '00'h
Compute_Dig_Sign_Response
  Received:            09 2E CC 87 65 75 87 ...
    DATA                 '09 2E CC 87 65 75 87 ... '
    STATUS               '90 00'h
```

7. Een elektronische handtekening kan gecontroleerd worden op de volgende manier:
   a. Selecteer het certificaat EF.C.PKI.CH.DS op de boordcomputerkaart.
   b. Lees het certificaat met behulp van (meerdere) Read Binary.
   c. Haal de Public Exponent en de Modulus uit het certificaat.
   d. Voer een RSA decryptie uit van de response data van Compute Digital Signature met de Public Exponent en de Modulus.
   e. De decrypted data moet overeenkomen met:
      '00 01 FF .. FF 00' || SHA_256_Digest || SHA256(input data),
      waarbij SHA_256_Digest = '30 31 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20'h.

B.3.2 SignDataForAuthenticity

Voor het zetten van een elektronische handtekening met de sleutel-certificaatcombinatie PKI.CH.AUT van een boordcomputerkaart, zoals beschreven staat in 8.7, worden de volgende stappen uitgevoerd:

1. Allereerst moet het hash template met het te gebruiken algoritme geselecteerd worden.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'h en P2 de waarde 'AA'h. De data bij dit commando is '80 01 40'h ('40'h om de algoritme identifier voor SHA-256 aan te geven).

```
MSE
  Sent:                00 22 41 AA 03 80 01 40
    Cla                  '00'h
    Ins                  '22'h
    P1                   '41'h
    P2                   'AA'h
    Lc                   '03'h
    Data                 '80 01 40'h
MSE_Response
  Received:            90 00
```

2. Selecteer het te gebruiken algoritme en de private sleutel van de BCT Authenticiteit.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'h en P2 de waarde 'B6'h. De data bij dit commando is '80 01 42 84 01 85'h ('42'h om "PKCS#1 v1.5 – SHA-256" aan te duiden en '85'h om het Security Data Object (SDO) van PKI.CH.AUT aan te duiden).

```
MSE
  Sent:                00 22 41 B6 06 80 01 42 84 01 85
    Cla                  '00'h
    Ins                  '22'h
    P1                   '41'h
    P2                   'B6'h
    Lc                   '06'h
    Data                 '80 01 42 84 01 85'h
MSE_Response
  Received:            90 00
```

3. De private sleutel van de BCT Authenticiteit mag pas gebruikt worden nadat de PIN gevalideerd is. Een eenmaal uitgevoerde PIN validatie mag – zo lang de kaart in de boordcomputer aanwezig blijft – worden "herbruikt" bij elke volgende keer dat deze sleutel gebruikt word. Dit wordt gedaan met het commando Verify, waarbij P2 (de PIN reference) de waarde '01'h heeft. Voor de PIN wordt PIN formaat 2 gebruikt.

```
Verify
  Sent:                00 20 00 01 08 24 95 99 FF FF FF FF FF
    Cla                  '00'h
    Ins                  '20'h
    P1                   '00'h
    P2                   '01'h
    Lc                   '08'h
    CHV                  '24 12 34 FF FF FF FF FF'h
Verify_Response
  Received:            90 00
```

4. Wanneer de input gegevens uit meer dan 64 bytes bestaan, moet er een intermediate hash met SHA-256 berekend worden door de boordcomputerlogica. Hierbij wordt het laatste gegevensblok niet gehashed, maar wordt de intermediate hash en het aantal gehashte bits onthouden voor de volgende stap.
   Wanneer het totaal aan input gegevens uit maximaal 64 bytes bestaat, wordt er geen intermediate hash berekend en worden alle inputgegevens in de volgende stap gebruikt.
5. Het berekenen van de uiteindelijke hash met SHA-256 wordt door de boordcomputerkaart gedaan. Hiervoor wordt het commando PSO Hash gebruikt. Hierbij worden de "intermediate hash value",

het aantal gehashte bits en het laatste (of enige) blok inputdata van minimaal 1 en maximaal 64 bytes opgenomen in het Dataveld van het commando. Bij een succesvol uitgevoerde PSO HASH zal de uiteindelijke hash waarde in het chipgeheugen van de boordcomputerkaart achterblijven ten behoeve van de volgende en laatste stap.

```
Total data = '90 00 80 32 BB BB ... BB'h

PSOHash
  Sent:                00 2A 90 A0 36 90 00 80 32 BB BB ... BB
    Cla                  '00'h
    Ins                  '2A'h
    P1                   '90'h
    P2                   'A0'h
    Lc                   '36'h
    HCD                  '90 00 80 32 BB BB ... BB'h
PSOHash_Response
  Received:            90 00
```

6. Met de gekozen private sleutel wordt de handtekening berekend over de in het chipgeheugen aanwezige hashwaarde.
   Dit wordt gedaan met het commando PSO Compute Digital Signature. Le, het verwachte aantal bytes in de response, moet daarbij op '00'h staan.

```
Compute_Dig_Sign
  Sent:                00 2A 9E 9A 00
    Cla                  '00'h
    Ins                  '2A'h
    P1                   '9E'h
    P2                   '9A'h
    Le                   '00'h
Compute_Dig_Sign_Response
  Received:            09 2E CC 87 65 75 87 ...
    DATA                 '09 2E CC 87 65 75 87 ... '
    STATUS               '90 00'h
```

7. Een elektronische handtekening kan gecontroleerd worden op de volgende manier:
   a. Selecteer het certificaat EF.C.PKI.CH.AUT op de boordcomputerkaart.
   b. Lees het certificaat met behulp van (meerdere) Read Binary.
   c. Haal de Public Exponent en de Modulus uit het certificaat.
   d. Voer een RSA decryptie uit van de response data van Compute Digital Signature met de Public Exponent en de Modulus.
   e. De decrypted data moet overeenkomen met:
      '00 01 FF .. FF 00' || SHA_256_Digest || SHA256(input data),
      waarbij SHA_256_Digest = '30 31 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20'h.

B.4 Het zetten van een handtekening met een systeemkaart

NB. Deze functie moet uitgevoerd worden onder secure messaging, zoals beschreven is in B.2. Voor het overzicht worden onderstaande commando's en responses echter zonder deze secure messaging weergegeven.

Voor het zetten van een elektronische handtekening met een systeemkaart, zoals beschreven staat in 8.6, worden de volgende stappen uitgevoerd:

1. Allereerst moet het hash template met het te gebruiken algoritme geselecteerd worden.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'h en P2 de waarde 'AA'h. De data bij dit commando is '80 01 40'h ('40'h om de algoritme identifier voor SHA-256 aan te geven).

```
MSE
  Sent:                 00 22 41 AA 03 80 01 40
    Cla                   '00'h
    Ins                   '22'h
    P1                    '41'h
    P2                    'AA'h
    Lc                    '03'h
    Data                  '80 01 40'h
MSE_Response
  Received:             90 00
```

2. Selecteer het te gebruiken algoritme en de private sleutel van de BCT Authenticiteit.
   Dit wordt gedaan met het commando Manage Security Environment, met P1 de waarde '41'h en P2 de waarde 'B6'h. De data bij dit commando is '80 01 42 84 01 85'h ('42'h om "PKCS#1 v1.5 – SHA-256" aan te duiden en '85'h om het Security Data Object (SDO) van PKI.CH.AUT aan te duiden).

```
MSE
  Sent:                 00 22 41 B6 06 80 01 42 84 01 85
    Cla                   '00'h
    Ins                   '22'h
    P1                    '41'h
    P2                    'B6'h
    Lc                    '06'h
    Data                  '80 01 42 84 01 85'h
MSE_Response
  Received:             90 00
```

3. Wanneer de input gegevens uit meer dan 64 bytes bestaan, moet er een intermediate hash met SHA-256 berekend worden door de boordcomputerlogica. Hierbij wordt het laatste gegevensblok niet gehashed, maar wordt de intermediate hash en het aantal gehashte bits onthouden voor de volgende stap.
   Wanneer het totaal aan input gegevens uit maximaal 64 bytes bestaat, wordt er geen intermediate hash berekend en worden alle inputgegevens in de volgende stap gebruikt.
4. Het berekenen van de uiteindelijke hash met SHA-256 wordt door de systeemkaart gedaan. Hiervoor wordt het commando PSO Hash gebruikt. Hierbij worden de "intermediate hash value", het aantal gehashte bits en het laatste (of enige) blok inputdata van minimaal 1 en maximaal 64 bytes opgenomen in het Dataveld van het commando. Bij een succesvol uitgevoerde PSO HASH zal de uiteindelijke hash waarde in het chipgeheugen van de systeemkaart achterblijven ten behoeve van de volgende en laatste stap.

```
Total data = '90 00 80 32 AA AA ... AA'h

PSOHash
  Sent:                 00 2A 90 A0 36 90 00 80 32 AA AA ... AA
    Cla                   '00'h
    Ins                   '2A'h
    P1                    '90'h
    P2                    'A0'h
    Lc                    '36'h
    HCD                   '90 00 80 32 AA AA ... AA'h
PSOHash_Response
  Received:             90 00
```

5. Met de gekozen private sleutel wordt de handtekening berekend over de in het chipgeheugen aanwezige hashwaarde.
   Dit wordt gedaan met het commando PSO Compute Digital Signature. Le, het verwachte aantal bytes in de response, moet daarbij op '00'h staan.

```
Compute_Dig_Sign
  Sent:                00 2A 9E 9A 00
    Cla                  '00'h
    Ins                  '2A'h
    P1                   '9E'h
    P2                   '9A'h
    Le                   '00'h
Compute_Dig_Sign_Response
  Received:            09 2E CC 87 65 75 87 ...
    DATA                 '09 2E CC 87 65 75 87 ... '
    STATUS               '90 00'h
```

6. Een elektronische handtekening kan gecontroleerd worden op de volgende manier:
   a. Selecteer het certificaat EF.C.PKI.CH.AUT op de systeemkaart.
   b. Lees het certificaat met behulp van (meerdere) Read Binary.
   c. Haal de Public Exponent en de Modulus uit het certificaat.
   d. Voer een RSA decryptie uit van de response data van Compute Digital Signature met de Public Exponent en de Modulus.
   e. De decrypted data moet overeenkomen met:
      '00 01 FF .. FF 00' || SHA_256_Digest || SHA256(input data),
      waarbij SHA_256_Digest = '30 31 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20'h.

TOELICHTING

Algemeen

Deze regeling strekt tot wijziging van de Regeling specificaties en typegoedkeuring boordcomputer taxi en de Regeling erkenning werkplaatsen boordcomputer taxi.

De eerstgenoemde regeling bood potentiële fabrikanten het regelgevend kader voor de tijdige ontwikkeling van een boordcomputer taxi (BCT), voordat vanaf 1 oktober 2011 de BCT geleidelijk zou worden ingevoerd.

De onderhavige regeling behelst wijziging van die regeling naar aanleiding van drie ontwikkelingen die zich sindsdien hebben voorgedaan.

De voornaamste daarvan is dat de taxibranche heeft verzocht om updates van BCT-software ook buiten de erkende werkplaats toe te staan. Dit voorkomt dat taxivoertuigen voor elke update naar een werkplaats moeten gaan, hetgeen de taxi ondernemerstijd en geld kost en logistiek lastig is.
Het voorschrift BCT-softwareupdates uitsluitend in een erkende werkplaats te laten uitvoeren was bedoeld als waarborg voor het behoud van het vereiste beveiligingsniveau van een BCT. Aanvankelijk was voorzien dat slechts incidenteel updates nodig zouden zijn, omdat de in de regeling gespecificeerde functionaliteit van een BCT niet dynamisch van aard is. Hiermee zou een update slechts benodigd zijn ingeval een BCT niet of niet meer aan de vereisten zou voldoen. Fabrikanten hebben er evenwel voor gekozen om BCT's ook te voorzien van niet verplichte functionaliteit die in sommige gevallen zeer dynamisch van aard is. Bovendien vertoonden de BCT's aanvankelijk nog veel kinderziektes. Dit heeft geresulteerd in een hogere updatefrequentie dan voorzien.
Om hieraan tegemoet te komen is met de Inspectie Leefomgeving en Transport (ILT), de Dienst wegverkeer (RDW), de fabrikanten en hun testhuizen een gewijzigd proces voor certificeren, typegoedkeuren, updaten, registreren en inspecteren van BCT software ontwikkeld. Dit proces heeft een aanzienlijke vermindering van administratieve lasten tot gevolg zonder dat afbreuk wordt gedaan aan het vereiste en controleerbare beveiligingsniveau van de BCT.

De wijzigingen die hierop betrekking hebben voorzien er in dat updates die een kalibratie van de BCT tot gevolg hebben in de erkende werkplaats moeten blijven plaatsvinden, maar dat alle andere updates ook buiten de werkplaats, volautomatisch op afstand, veilig kunnen plaatsvinden. Deze wijzigingen hebben vooral gevolgen voor de bijlagen 1 en 2 bij de Regeling specificaties en typegoedkeuring boordcomputer taxi. Deze gevolgen zijn zodanig ingrijpend dat er voor gekozen is deze bijlagen opnieuw vast te stellen.

Voorts hebben fabrikanten in de ontwikkelfase vragen gesteld naar aanleiding van geconstateerde onduidelijkheden en vermeende fouten. Deze vragen zijn met de antwoorden opgenomen in een lijst van veelgestelde vragen, die periodiek is aangevuld en gepubliceerd op de website van ILT.
Naar aanleiding van de antwoorden is de Regeling specificaties en typegoedkeuring boordcomputer taxi op een tweetal punten verduidelijkt.

Tot slot heeft het ministerie in de afgelopen periode de diverse betrokken partijen geconsulteerd om eventuele additionele wensen kenbaar te maken en daaraan gerelateerde wijzigingsverzoeken in te dienen. Deze consultatie heeft geleid tot het identificeren van een aantal omissies, in de praktijk ervaren pijnpunten en mogelijke optimalisaties. Dit heeft geleid tot aanpassingen op de volgende gebieden:
- zodanige verruiming van de specificaties dat er, ook bij niet eerder voorziene praktijksituaties, aan de registratie-eisen kan worden voldaan. Het gaat hier bijvoorbeeld om het leeglopen van accu's doordat vergeten is om de BCT uit te schakelen terwijl de taxi niet gebruikt wordt;
- op een meer voor de hand liggende wijze ordenen van door de BCT weer te geven informatie;
- vereenvoudigen van de wijze waarop de authenticiteit van de gegevenslevering vanuit de chauffeurskaart gedurende een inspectie kan worden gecontroleerd, en
- wegnemen van onduidelijkheid en/of ruimte voor eigen interpretatie bij:
  - de opbouw van uit boordcomputer- en systeemkaarten overgenomen gegevens,
  - de opbouw van gegevensleveringen uit de boordcomputer,
  - de opbouw van de elektronisch te ondertekenen delen van die gegevensleveringen en geregistreerde gegevens,
  - het voldoen aan het Besluit elektronische handtekeningen en het Programma van Eisen voor certificaten (PKI) voor de overheid en
  - de door de boordcomputer te ondersteunen functies.

Van de gelegenheid is gebruik gemaakt om ook de Regeling erkenning werkplaatsen op enkele punten

aan te passen naar aanleiding van geconstateerde omissies en onduidelijkheden.

Handhaafbaarheid en uitvoerbaarheid

De regeling is door ILT en RDW getoetst op handhaafbaarheid en uitvoerbaarheid.

ILT acht de regeling uitvoerbaar en handhaafbaar, mits de RDW toezicht houdt op naleving van de plicht tot melding van software-updates en uniformiteit van exportbestanden.

De RDW heeft in het kader van de toets enkele tekstuele wijzigingen voorgesteld, welke zijn overgenomen.

De RDW acht de Extensible Markup Language schema definitie van resultaatberichten van levering van BCT-gegevens, zoals opgenomen in bijlage 2 bij de regeling, te weinig flexibel. Deze is echter gehandhaafd, omdat meer flexibel maken teveel ruimte zou geven voor interpretatie, terwijl een van de doelstellingen van de onderhavige regeling, zoals hierboven reeds opgemerkt, juist is om onduidelijkheden weg te nemen.

Bedrijfseffecten en administratieve lasten

Deze zijn te onderscheiden in effecten/lasten voor enerzijds de taxiondernemers, anderzijds voor fabrikanten van BCT's.
- Om de bestaande BCT-systemen te laten voldoen aan deze regeling dient de software te worden aangepast. De door de fabrikanten hiertoe te ontwikkelen software dient geïnstalleerd te worden op alle BCT's. De kosten hiervoor per BCT ca. € 20 arbeidsloon voor de installatie.
- De kosten komen daarmee uitgaande van 30.000 taxi's in totaal op € 600.000. Deze kosten zijn eenmalig. Nog niet duidelijk is in hoeverre deze kosten op de taxiondernemers worden verhaald. Bij één van de fabrikanten valt dit onder het servicecontract.

De kosten van softwareontwikkeling verschillen per fabrikant; dit is afhankelijk van het type BCT. De wijzigingen voor het ene type BCT zijn eenvoudiger te programmeren dan voor het andere type. Daarnaast kan de ene fabrikant de software in eigen huis laten ontwikkelen en moet de andere fabrikant dat buiten de deur laten doen. De fabrikanten rekenen hiervoor met bedragen tussen € 30.000,- en € 320.000,-. Er zijn drie fabrikanten actief. Deze kosten komen ten laste van de fabrikant voor zover deze aan zijn afnemers een serviceabonnement heeft aangeboden.

De kosten voor certificering van de software-update worden door de fabrikanten geraamd op € 5000 tot € 25.000 per fabrikant. Deze ruime marge wordt veroorzaakt doordat de kosten voor het grootste deel worden bepaald door de beoordeling van de update door testhuizen, de wijzigingen die na afwijzing nog moeten worden aangebracht en het aantal keren dat de software nog opnieuw moet worden voorgelegd aan een testhuis.

Afhankelijk van de vraag of een software update de meetapparatuur voor de taxiritten beïnvloedt, moet een software-update uitgevoerd worden in een erkende werkplaats. Dat zal alleen in uitzonderlijke gevallen zo zijn. De kosten voor 'reguliere' software-updates blijven beperkt tot de kosten van de software update zelf.

Per taxi betekent dit een besparing van € 50 – € 75 per update, dus over het totaal aan BCT's een besparing van € 1.500.000 tot € 2.250.000.

Fabrikanten verwachten twee tot drie updates per jaar beschikbaar te hebben. De totale besparing komt dan uit op minimaal € 4.500.000 op jaarbasis.

Notificatie

De regeling is op 17 december 2014, onder nummer 2014/0631/NL, ingevolge richtlijn 98/34/EG ter notificatie voorgelegd. Hierop zijn geen reacties ontvangen.

Artikelsgewijs

Artikel I (Regeling specificaties en typegoedkeuring boordcomputer taxi)

Onderdeel A

In artikel 1 is een aantal begrippen gedefinieerd die betrekking hebben op eisen waaraan de BCT moet

voldoen om veilig updaten op afstand mogelijk te maken. De begrippen worden vooral in de bijlagen 1 en 2 gehanteerd.

Onderdeel B

De wijziging van artikel 2, vierde lid, is noodzakelijk omdat de regeling thans vier bijlagen kent.

Onderdeel C

In artikel 7 is sprake van twee metingen van posities. Een afwijking van 3 procent tussen deze twee metingen resulteert in de praktijk in te veel foutmeldingen, terwijl een afwijking van 5 procent acceptabel is.

Onderdeel D

Artikel 9, zevende lid is gewijzigd om beter aan te sluiten op het Programma van Eisen van PKI voor de overheid, waaraan certificatiedienstverleners gehouden zijn voor het uitgeven van certificaten voor het zetten van elektronische handtekeningen conform het Besluit elektronische handtekeningen.

Onderdeel E (artikel 13)

Verandering van de bedrijfsvergrendeling vindt plaats indien de BCT in handen van een andere vervoerder overgaat. Met de bedrijfsvergrendeling zijn de in de BCT opgeslagen gegevens herleidbaar naar de vervoerder waarvoor deze opgeslagen zijn.

Onderdeel F

De aan artikel 14 toegevoegde bepaling strekt ertoe te voorkomen dat de boordcomputer in werking blijft indien na beëindiging van de werkzaamheden abusievelijk is verzuimd deze uit te schakelen.

Onderdelen G en H

Met de artikelen 17 en 18 is een aantal eisen aan de BCT toegevoegd of nader gespecificeerd om interpretatieruimte te verminderen. Dit heeft een andere rangschikking tot gevolg, hetgeen herredigeren van deze artikelen noodzakelijk maakt.

Onderdeel I (artikel 20)

De aanpassing van de BCT aan de in deze regeling neergelegde eisen vergt een zodanige geheugencapaciteit van de hardware, dat naar verwachting van sommige fabrikanten het risico bestaat dat deze zou moeten worden vervangen. Het tijdsbeslag en de kosten, die hieraan verbonden zouden zijn, kunnen worden voorkomen door op de thans gebruikte hardware de geheugencapaciteit voor het opslaan van gegevens te beperken tot een half jaar.

De correcte registratie van bct-gegevens ondervindt hier geen schade van. Immers, op grond van artikel 19, eerste lid, onderscheidenlijk 18, vijfde lid, van de Regeling gebruik boordcomputer en boordcomputerkaarten dient de vervoerder de bct-gegevens elke drie maanden en ingeval van een waarschuwing van het ontstaan van onvoldoende geheugencapaciteit naar zijn vestiging over te brengen.

Onderdelen J tot en met L

De wijzigingen in de artikelen 21 tot en met 23 zijn niet inhoudelijk van aard. Zij strekken slechts tot verduidelijking.

Onderdelen M en N

De artikelen 27 en 28 corrigeren een erratum.

Onderdeel O

Handmatige bevestiging door de chauffeur dat hij foutmeldingen heeft opgemerkt, leidt in geval van telkens herhaalde meldingen tot teveel ongemak voor de deelname aan het verkeer. De wijziging van artikel 29 beoogt de zichtbaarheid van foutmeldingen daarom enigszins in te perken.

Onderdeel P

In artikel 30 zijn enige verduidelijkingen aangebracht. De wijziging van dit artikel is niet inhoudelijk.

Onderdelen Q en S

In de artikelen 31 en 35 wordt thans bepaald in welke gevallen wijzigingen in de programmatuur van de boordcomputer op afstand geüpload mogen worden, en welke wijzigingen uitsluitend in een erkende werkplaats mogen plaatsvinden. De verwijzing naar artikel 13, onder b, van de Regeling erkenning werkplaatsen boordcomputer taxi heeft betrekking op kalibratie.

Onderdeel R

In het toegevoegde artikel 31a is een bepaling opgenomen waarin tot nu toe nog niet werd voorzien. Deblokkering en/of wijziging van de pincode dient door de fabrikant mogelijk gemaakt te worden. Het staat de fabrikant vrij om die mogelijkheid aan de houder van de boordcomputerkaart als service aan te bieden, dan wel erin te voorzien dat de houder van de boordcomputerkaart zelfstandig de pincode kan deblokkeren en/of wijzigen.

Artikel II (Regeling erkenning werkplaatsen boordcomputer taxi)

In artikel 6 is nu tot uiting gebracht dat de eisen voor een erkenning ook gelden voor een mobiele activeringseenheid.

Artikel III

Van het systeem van vaste verandermomenten wordt afgeweken voor zover het de datum van publicatie betreft.

Met betrokken brancheorganisaties is de afspraak gemaakt de onderhavige regeling zo spoedig mogelijk na afloop van de zgn. standstil periode, die op grond van richtlijn 98/34/EG is voorgeschreven, in werking te laten treden. Deze loopt op 17 maart 2015 af indien door lidstaten geen opmerkingen zijn gemaakt.

De afspraken met brancheorganisaties betreffen het mogelijk maken van updates van BCT-software buiten de erkende werkplaats. Zoals hierboven aangegeven voorziet de onderhavige regeling echter ook in optimalisatie van technische eisen. Het spreekt voor zich dat er een overgangsperiode nodig is om te waarborgen dat alle bestaande BCT's, circa 30.000 in aantal, aan deze (aanvullende) technische eisen kunnen voldoen.

Fabrikanten schatten in dat zij zes tot negen maanden nodig hebben voor de ontwikkeling van de software, die nodig is om te voldoen aan de technische eisen zoals in de onderhavige regeling vastgelegd. Voor de procedure die moet leiden tot certificering wordt een periode van drie maanden ingeschat; dezelfde termijn geldt voor het 'uitrollen' van de software over alle bestaande BCT's. De optelsom van deze termijnen leidt tot het opnemen van de datum van 1 juli 2016 als datum waarop iedereen moet voldoen aan de gewijzigde eisen.

De Staatssecretaris van Infrastructuur en Milieu,
W.J. Mansveld