Ministerie van Infrastructuur en Milieu

Beveiligingsprofiel Boordcomputer Taxi (PP-BCT)

Versie 1.8

Datum 6 februari 2015
Status Definitief

Beveiligingsprofiel Boordcomputer Taxi (PP-BCT)

Versie 1.8

Datum 6 februari 2015
Status Definitief

Inhoud

Bijlage 1 bij de Regeling boordcomputer taxi

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	CEN Workshop 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.

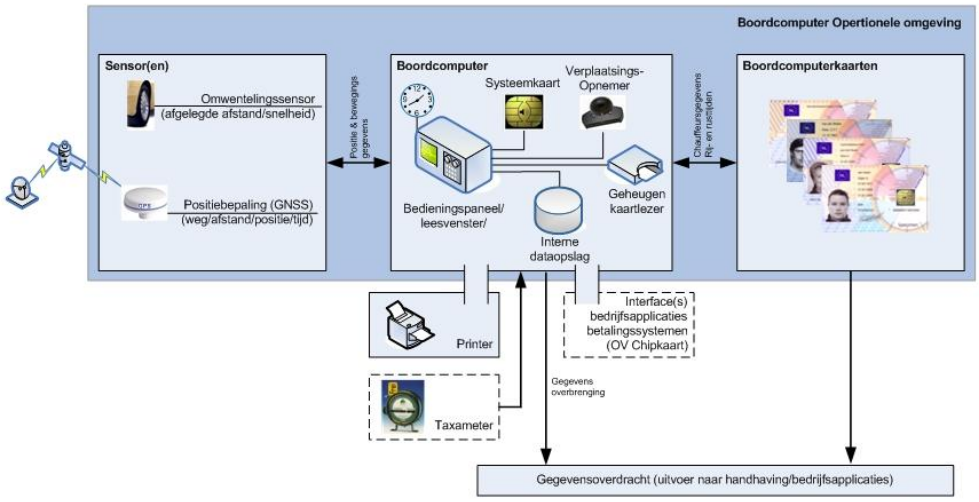
Bij aanvang van de dienst dient een chauffeurskaart in de TOE te zijn geplaatst. De bestuurder meldt zich aan met de chauffeurskaart en een persoonlijk identificatie code (PIN-code). De TOE registreert de persoonlijke arbeids-, rij- en rusttijden van de bestuurder en slaat deze op in het interne geheugen 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.

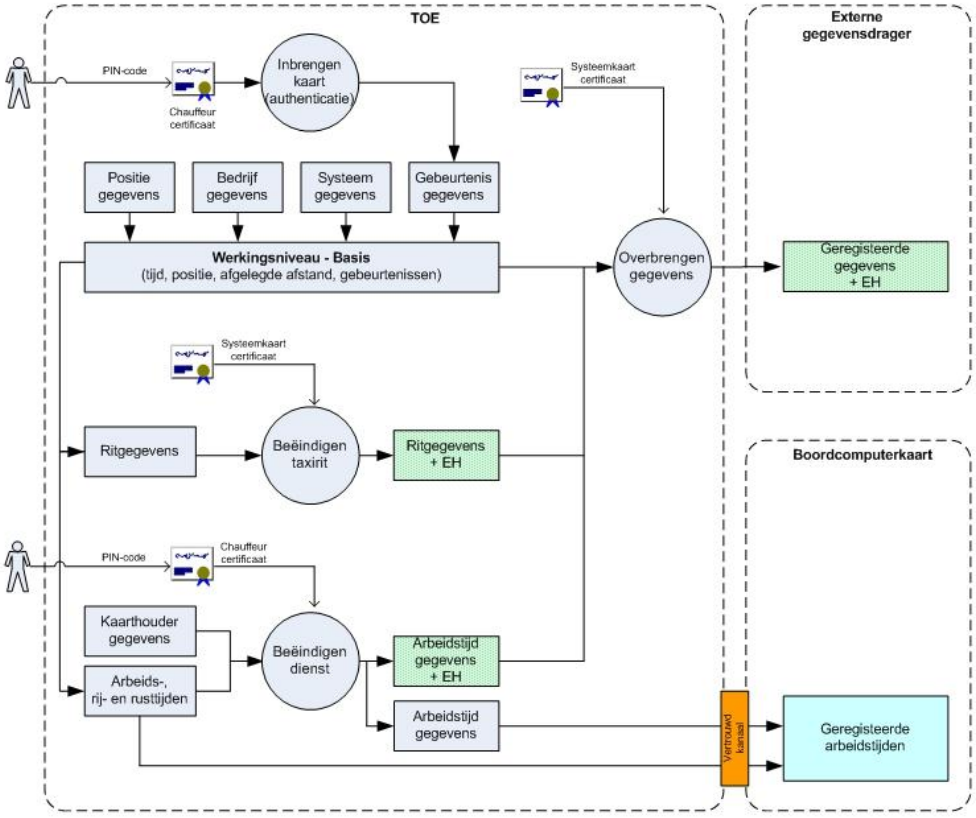
De operationele omgeving van de TOE geïnstalleerd in de auto is weergegeven in onderstaande figuur.



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

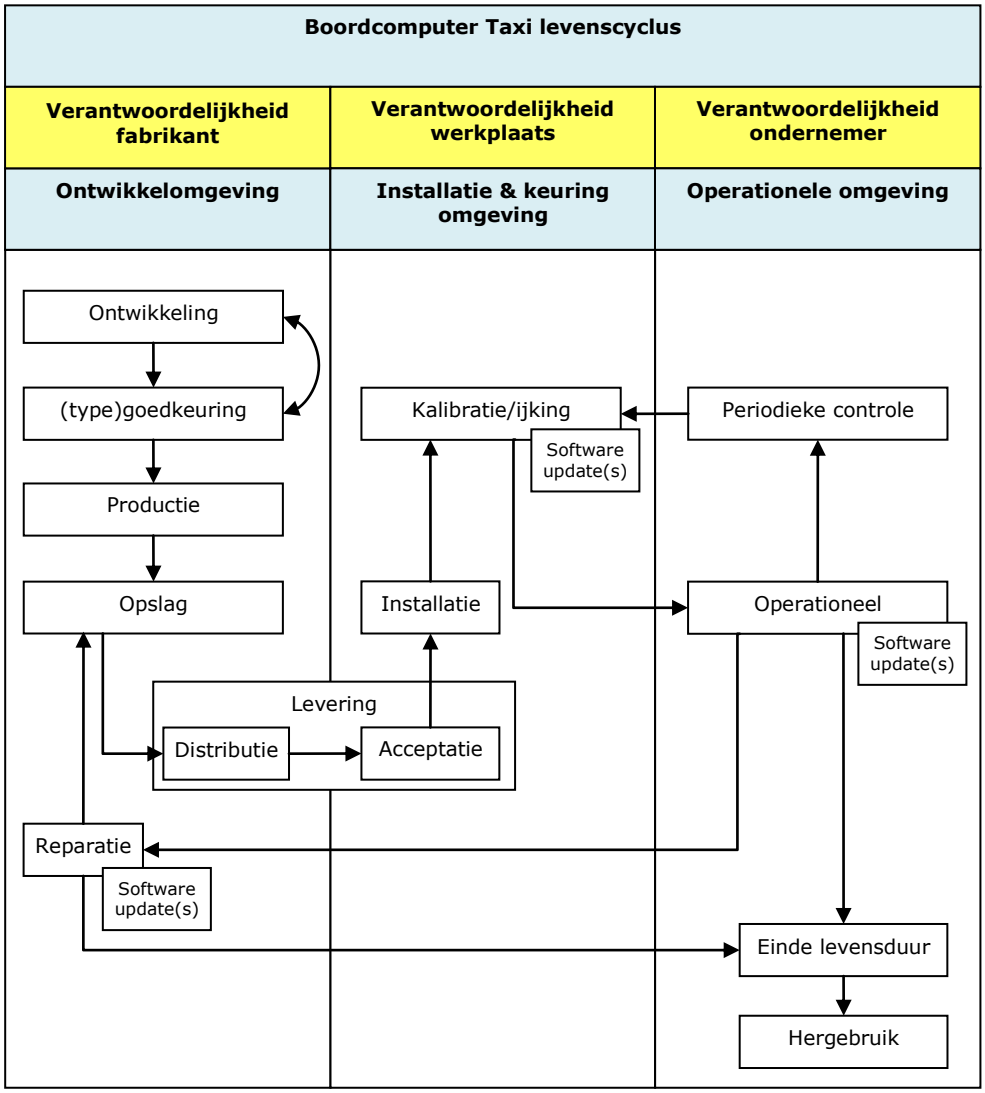
Artikel 3.2 Levenscyclus van de TOE

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

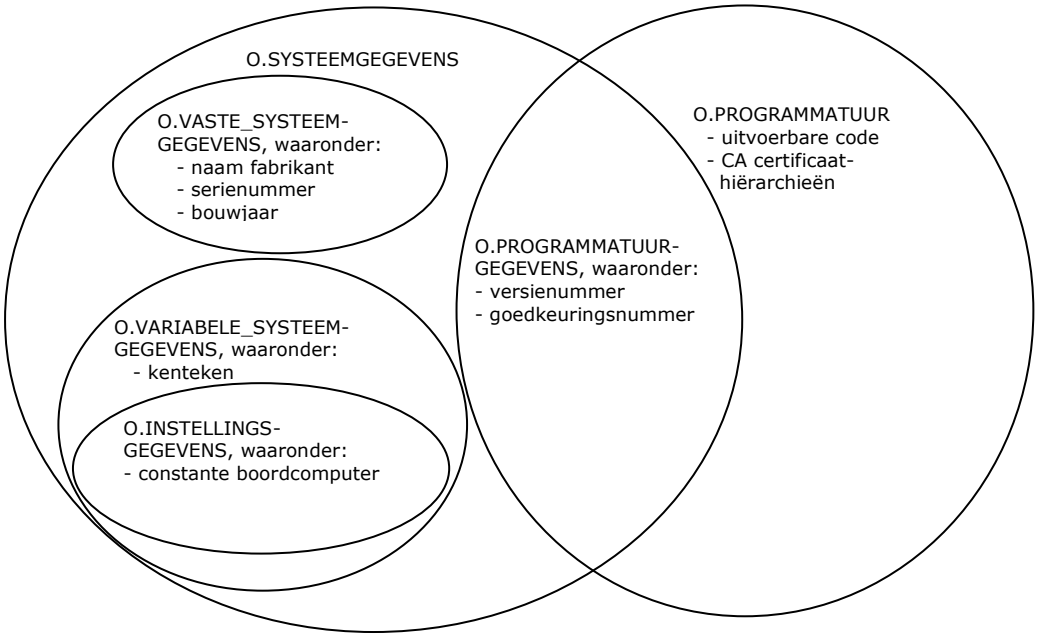
Vaste gegevens van de TOE, zoals de naam van diens fabrikant, het serienummer en het bouwjaar.

O.VARIABELE_SYSTEEMGEGEVENS

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

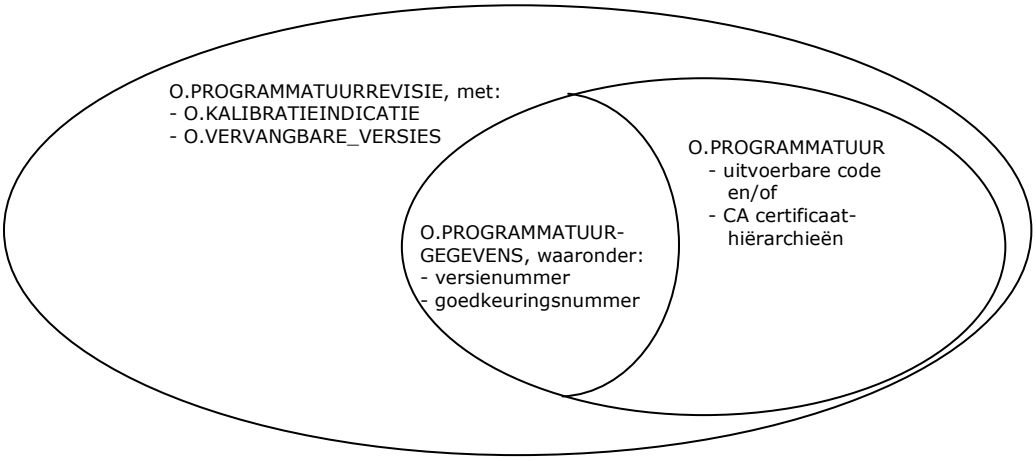
O.INSTELLINGSGEGEVENS
Die subset van O.VARIABELE_SYSTEEMGEGEVENS die aan kalibratie onderhevig is.
O.PROGRAMMATUUR
De combinatie van TOE uitvoerbare code en gegevens zoals de CA certificaat-hiërarchie(ën) nodig voor het verifiëren van de geldigheid en authenticiteit van certificaten van boordcomputer- 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.

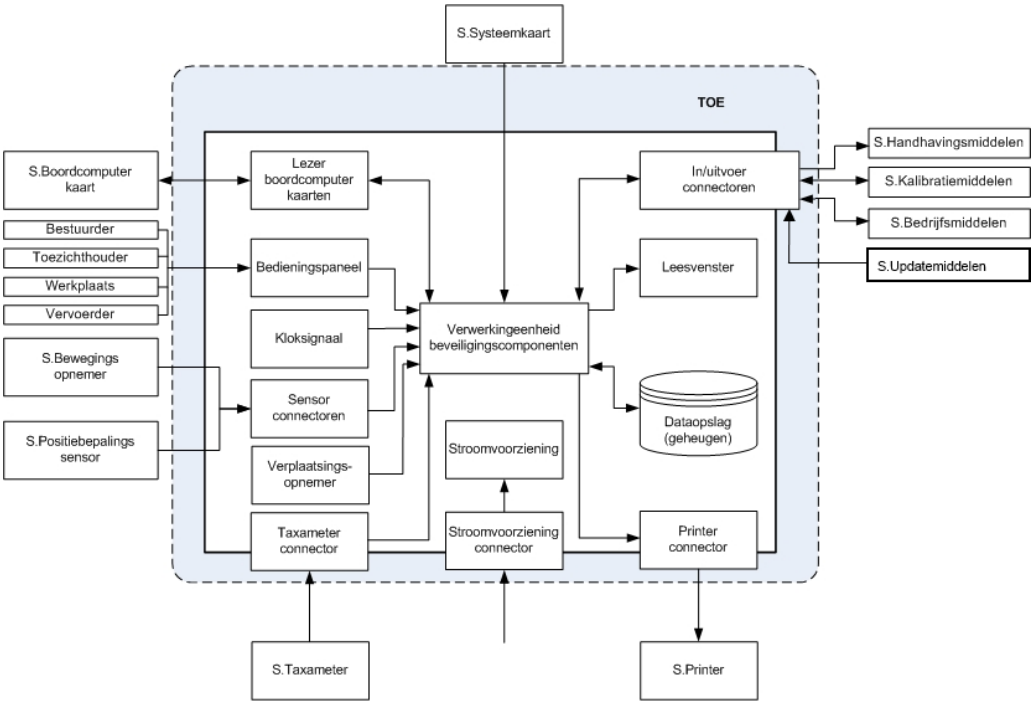


Figuur 5

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;

[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.

- 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.

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

[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.

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
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.BOORDCOMPUTERKAART 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.

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

- 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:
  - 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,

[6] Zie FDP_DAU.2

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;
    - 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

[7] Vervallen.

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.

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;

[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.

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;
- 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 programmatuur-revisie, 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.

[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.

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.

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.