Inspectie Leefomgeving en Transport
Ministerie van Infrastructuur en Waterstaat

Uitgiftebeleid Boordcomputerkaarten en Systeemkaart, Certificate Practice Statement (CPS)

Boordcomputer Taxi

Datum	26 januari 2018
Status	Definitief
Versie	4.5.1

Inhoud

1 Introductie

Een Certificate Practice Statement (CPS) is een schriftelijk vastgelegde verzameling regels die de door een certificaatdienstverlener (TSP) gevolgde procedures en getroffen maatregelen ten aanzien van alle aspecten van de Public Key Infrastructuur (PKI) dienstverlening beschrijft. Het CPS beschrijft daarmee op welke wijze de TSP voldoet aan de eisen zoals gesteld in de van toepassing zijnde Certificate Policy (CP).

Dit document bevat het CPS dat wordt gehanteerd voor het uitgeven van kaarten en Certificaten voor gebruik in de Boordcomputer Taxi (BCT). Het CPS BCT is geschreven door en in beheer bij de Dossierhouder BCT (DH BCT), dat onderdeel uitmaakt van de TSP van het ministerie van Infrastructuur en Waterstaat.

1.1 Achtergrond

1.1.1 Boordcomputer taxi

Het kabinet heeft met haar standpunt 'Taxi naar de Toekomst' beleid ingezet voor een beter taxiproduct voor een reële prijs. Hiervoor heeft het kabinet verschillende trajecten in gang gezet. Zo is er sprake van aanscherping van kwaliteitseisen aan vergunningen voor taxiondernemers en chauffeurs, intensivering van het toezicht, de invoering van een transparante tariefstructuur en de invoering van een boordcomputer taxi. Deze boordcomputer verzorgt een elektronische registratie van de wettelijke verplichting om de uitgevoerde taxiritten en de arbeids-, rij- en rusttijden van de chauffeurs vast te leggen.

De BCT beschikt over de volgende vereiste hoofdfunctionaliteiten, die zijn vastgelegd in de ministeriele regeling 'Specificaties en typegoedkeuring boordcomputer taxi':

- digitale registratie van de ritadministratie;
- digitale registratie van de arbeids- en rusttijden;
- mogelijkheid tot het aansluiten van bedrijfsapparatuur;
- beschikbaar stellen van gegevens ten behoeve van een bon;
- automatische positiebepaling van begin- en eindlocaties van de ritten.

De BCT maakt gebruik van elektronische handtekeningen om de integriteit van de gegevens te waarborgen.

1.1.2 Typen kaarten en certificaten

In totaal zijn er zes verschillende typen kaarten gekoppeld aan het gebruik van de BCT. Deze kaarten bevatten allen een chip waarop één of meerdere certificaten en bijbehorende sleutelparen staan opgeslagen.

Vijf van de kaarttypen worden gebruikt om de gebruikers van de BCT te identificeren. Deze kaarten worden boordcomputerkaarten (BCT kaarten) genoemd. De laatste soort kaart geeft het boordcomputer systeem zijn identiteit. Dit is de systeemkaart.

De volgende kaarttypen worden onderkend:

- **Chauffeurskaart**
  Identificeert de bestuurder en registreert zijn activiteiten. Deze kaart bevat één persoonsgebonden handtekeningcertificaat en één persoonsgebonden authenticiteitcertificaat. Het vertrouwelijkheidcertificaat wordt binnen de BCT niet gebruikt voor chauffeurskaarten.

- **LWT kaart**
  Geeft de bestuurder de mogelijkheid gebruik te maken van het Leer Werk Traject (LWT) voor taxichauffeurs. Hierbij mag hij/zij (voor een periode van maximaal 4 maanden) bepaalde vormen van taxivervoer verrichten, zonder in het bezit te zijn van het vakdiploma taxichauffeur. De werking is exact gelijk aan die van de chauffeurskaart, met dien verstande dat deze een geldigheidsduur heeft van 4 maanden. In dit CPS wordt deze kaart dan ook niet nader gespecificeerd.

- **Ondernemerskaart**
  Identificeert de taxiondernemer en ontgrendelt de toegang tot de voor deze ondernemer opgeslagen gegevens in de BCT. Deze kaart bevat één niet-persoonsgebonden servicecertificaat voor authenticiteit.

- **Keuringskaart**
  Identificeert de erkende werkplaats en ontgrendelt de toegang tot de boordcomputer voor beproevingen en kalibratie. Deze kaart bevat één niet-persoonsgebonden servicecertificaat voor authenticiteit.

- **Inspectiekaart**
  Identificeert de toezichthouder en ontgrendelt de toegang tot de in het geheugen van de boordcomputer opgeslagen gegevens om deze te lezen en/of over te brengen. Deze kaart bevat één persoonsgebonden authenticiteitcertificaat, één persoonsgebonden vertrouwelijkheidcertificaat en één persoonsgebonden handtekeningcertificaat.

- **Systeemkaart**
  Identificeert de boordcomputer en stelt deze in staat gegevens te ondertekenen. Deze kaart bevat één niet-persoonsgebonden servicecertificaat voor authenticiteit.

Alle certificaten op de kaarten zijn van het type X509v3.

De geldigheidsduur van de certificaten op de kaarten is, tot aan het overgaan op een nieuwe ROOT CA, gelijk aan de verloopdatum van de G2-root (23 maart 2020). De normale geldigheidsduur van BCT kaarten is vijf jaar. Voor BCT services kaarten geldt een geldigheidstermijn van drie jaar geldig, terwijl de systeemkaart een geldigheid heeft van tien jaar. Uitzondering hierop is de LWT kaart, welke vier maanden geldig is.

De BCT kaarten hebben onderscheidende kenmerken en verschillende aanvraag- en afgifteprocedures.

1.1.3 CA hiërarchie

Het ministerie van Infrastructuur en Waterstaat realiseert haar Public Key Infrastructuur (PKI) onder de vertrouwensstructuur van de PKI van de Staat der

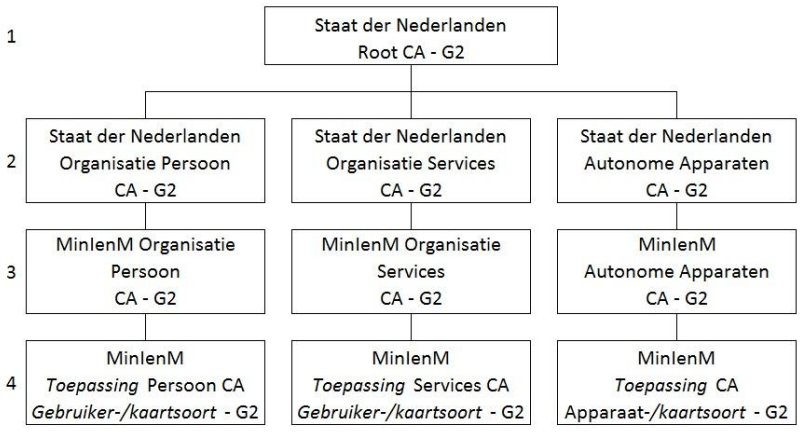
Nederlanden (PKIoverheid) en kiest hiermee het stamcertificaat van de 'Staat der Nederlanden' als hoogste vertrouwenspunt. Het ministerie heeft hiertoe een Trust Service Provider (TSP) ingericht die onderdeel uitmaakt van PKIoverheid.

De TSP van het ministerie van Infrastructuur en Waterstaat (TSP IenW) bestaat uit één dossierhouder die verantwoordelijk is voor de uitgifte van certificaten binnen het eigen domein. De BCT kaarten en systeemkaarten worden onder verantwoordelijkheid van de Dossierhouder BCT uitgegeven door Kiwa Register BV (KIWA). KIWA geeft onder mandaat van de minister van Infrastructuur en Waterstaat vergunningen uit ten behoeve van meerdere modaliteiten, zo ook de BCT kaarten.

1.1.4 PKIoverheid

PKIoverheid faciliteert de Public Key Infrastructuur voor Nederlandse Overheid. Hiertoe beheert PKIoverheid het stamcertificaat van de Staat der Nederlanden. Deze zogenaamde Root Certificate Authority (CA) is de hoogste (self-signed) CA, en eigendom van de Staat der Nederlanden.

Onder deze Root CA staan drie domein CA's gepositioneerd voor respectievelijk Organisatie, Autonome Apparaten en Burger. Deze domein CA's zijn getekend door de Root CA en tekenen op hun beurt weer de CA's van de in het betreffende domein opererende TSP. De CA's van de TSP van het ministerie van Infrastructuur en Waterstaat vallen onder de PKIoverheid domeinen Organisatie en Autonome Apparaten.



Figuur 1 – PKIoverheid hiërarchie

De hiërarchie van PKIoverheid staat beschreven in het Programma van Eisen (PvE) van PKIoverheid (deel 1, Introductie PvE). Zowel de Root CA als de domein CA's worden beheerd door PKIoverheid.

Een beschrijving van het beheer van deze CA's kan teruggevonden worden in het CPS Policy Authority PKIoverheid voor certificaten uit te geven door de Policy Authority van de PKIoverheid. Deze documenten zijn te vinden op http://www.logius.nl/producten/toegang/pkioverheid/.

1.2 Doel en verwijzingen CPS

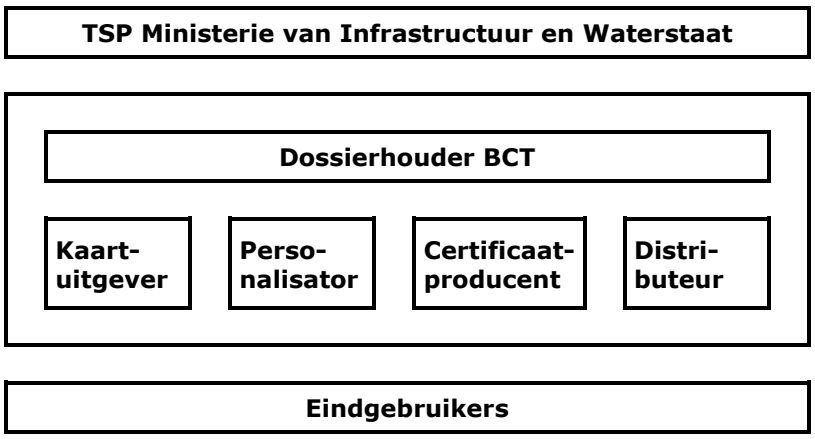
Het CPS van de DH BCT beschrijft op welke wijze invulling wordt gegeven aan de PKI dienstverlening voor de BCT. Het CPS beschrijft de processen, procedures en beheersmaatregelen voor het aanvragen, produceren, verstrekken, beheren en intrekken van de BCT- en systeemkaart certificaten. Met behulp van dit CPS kunnen betrokkenen hun vertrouwen in de door de DH BCT geleverde diensten bepalen. De algemene indeling van dit CPS volgt het model zoals gepresenteerd in het *Request for Comments (RFC) 3647*.

Formeel wordt het voorliggende document aangeduid als 'Uitgiftebeleid Boordcomputerkaarten en Systeemkaart, Certificate Practice Statement', kortweg CPS.

1.3 Betrokken partijen

De volgende partijen zijn betrokken bij de uitgifte van kaarten:

- TSP (belegd bij ministerie van Infrastructuur en Waterstaat, DCI)
- DH BCT (belegd bij ILT, domein Rail en Wegvervoer), inclusief leveranciers van diensten en producten:
  - Kaartuitgever (KIWA)
  - Personalisator (Idemia)
  - Certificaatproducent (KPN)
  - Distributeur (AMP)
- Eindgebruikers:
  - Abonnees
  - Certificaathouders
  - Certificaatbeheerders
  - Vertrouwende partijen



Figuur 2 – Betrokken partijen

1.3.1 Trust Service Provider ministerie van Infrastructuur en Waterstaat (TSP)

Het TSP certificaat van het ministerie van Infrastructuur en Waterstaat is het startpunt voor het vertrouwen binnen de hiërarchie van de PKI van dit ministerie.

Dit bepaalt het vertrouwen dat wordt gesteld in alle andere certificaten (zowel dossierhouder- als eindgebruikercertificaten) die zijn uitgegeven binnen de hiërarchie van de PKI van dit ministerie.

Deze TSP vervult de rol van PKIoverheid TSP en is eindverantwoordelijk voor het leveren van alle certificatiediensten die namens het ministerie van Infrastructuur en Waterstaat worden geleverd.

Om van een betrouwbare PKI hiërarchie te kunnen spreken is het van belang dat de TSP managementfunctie op een betrouwbare wijze functioneert. Deze managementfunctie waarborgt de betrouwbaarheid van het TSP certificaat door het toepassen van adequate beveiligingsmaatregelen.

De TSP toont het betrouwbaar functioneren aan door zich te onderwerpen aan het reguliere toezicht door de Policy Autoriteit (PA) van de PKIoverheid.

De PA vereist van de TSP dat deze zich conformeert aan het reguliere toezichtproces door de PA, zoals dat geldt voor elke TSP die is toegetreden tot de hiërarchie van PKIoverheid.

In deze systematiek dient de TSP zich middels een periodieke audit te certificeren. Met de implementatie van de eIDAS Verordening (Elektronische Identificatie en Vertrouwensdiensten voor Elektronische Transacties in de Interne Markt) is de 3 jaarlijkse TTP.nl audit komen te vervallen. Na inwerkingtreding van de Uitvoeringswet van deze Verordening, maar ook als gevolg van eisen vanuit het CAB forum, komt hier een jaarlijkse audit voor terug.

1.3.2 Dossierhouder BCT

De verantwoordelijkheid voor de dienstverlening voor de BCT berust bij de DH BCT. Deze DH BCT voert haar taken uit onder auspiciën van de TSP.

1.3.3 Kaartuitgever

De kaartuitgever zorgt voor de verwerking van certificaataanvragen en alle daarbij behorende taken. De kaartuitgever verzamelt fysiek de identificatiegegevens, controleert en registreert deze en voert de beschreven toetsingscontroles uit.

De kaartuitgever geeft, na de controles, de personalisator opdracht voor het produceren van de BCT kaarten, en de certificaatproducent voor het vervaardigen van certificaten. Nadat de kaarten zijn geproduceerd worden deze door de distributeur aan de certificaathouders uitgereikt.

Verzoeken tot intrekking van een certificaat worden aan de kaartuitgever gericht. De kaartuitgever controleert of het verzoek voldoet aan de van toepassing zijnde voorwaarden en geeft na een positieve beoordeling opdracht aan de certificaatproducent om het betreffende certificaat in te trekken.

1.3.4 Personalisator

De BCT kaarten worden door de personalisator grafisch gepersonaliseerd op basis van productieopdrachten van de kaartuitgever. Deze productieopdrachten dienen verder als basis voor het genereren van het sleutelmateriaal en certificaataanvragen die door de personalisator aan de Certificaatproducent worden verzonden. De resulterende certificaten worden vervolgens op de BCT kaarten geplaatst en aan de distributeur verzonden.

1.3.5 Certificaatproducent

De certificaatproducent verzorgt de productie van aangevraagde certificaten op basis van een geauthenticeerd verzoek van de personalisator. De certificaten worden direct nadat zij zijn aangemaakt aan de personalisator verzonden.

De certificaatproducent publiceert ingetrokken certificaten op de Certificate Revocation List (CRL). Ingetrokken certificaten worden pas op een CRL gepubliceerd nadat de certificaatproducent een bericht voor intrekking van het certificaat heeft ontvangen van de kaartuitgever.

1.3.6 Distributeur

De distributeur verzorgt de fysieke uitgifte van de door de personalisator aangeleverde kaarten, inclusief de activeringsgegevens aan de certificaathouder en/of certificaatbeheerder.

1.3.7 Abonnee, Certificaathouder en Certificaatbeheerder.

De abonnee is de partij die een overeenkomst aangaat met de TSP voor het leveren van certificaten aan de abonnee. Hierbij vertegenwoordigt de abonnee de certificaathouder.

De certificaathouder wordt in het certificaat geïdentificeerd als de houder van de private sleutel die correspondeert met de publieke sleutel die in het certificaat is opgenomen.

Een certificaatbeheerder is bevoegd om namens de abonnee en ten behoeve van de certificaathouder handelingen uit te voeren waartoe de certificaathouder zelf niet in staat is.

In tabel 1 wordt per kaarttype weergegeven wat de relatie tussen de abonnee en de certificaathouder is.

Kaarttype	**Abonnee**	**Certificaathouder**
Chauffeurskaart	Taxichauffeur	Taxichauffeur
Inspectiekaart	Inspectiedienst / controledienst	Inspecteur / controleur
Ondernemerskaart	Taxiondernemer	Taxiondernemer
Keuringskaart	Erkende werkplaats	Erkende werkplaats
Systeemkaart	Fabrikant boordcomputer	Boordcomputer

Tabel 1 – Relatie Abonnee - Certificaathouder

1.3.8 Vertrouwende partijen

Een vertrouwende partij is degene die handelt in vertrouwen op een certificaat. De categorie vertrouwende partijen bestaat in dit geval uit iedereen die handelt in vertrouwen op certificaten van de BCT, met als mogelijke doelen het authenticeren van de kaarthouders, het verifiëren van een elektronische handtekening of het versleutelen van communicatie met die betreffende partij.

1.4 Certificaatgebruik

Het toepassingsgebied van de door de DH BCT uitgegeven persoonsgebonden certificaten is beperkt tot de gebruikersgemeenschap bestaande uit abonnees, certificaathouders en vertrouwende partijen, zoals bedoeld in paragraaf 1.3 van deel 3a van het PvE PKIoverheid.

Persoonsgebonden certificaten zijn onderverdeeld in beroepsgebonden en organisatiegebonden certificaten.

Beroepsgebonden certificaten zijn bedoeld voor gebruik door natuurlijke personen die het certificaat gebruiken uit hoofde van hun beroep.

Organisatiegebonden certificaten worden uitgegeven aan natuurlijke personen die namens de abonnee gebruik maken van het certificaat, waaronder inspecteurs van ILT en medewerkers van andere inspectiediensten.

Naast de persoonsgebonden certificaten, worden niet-persoonsgebonden certificaten gebruikt door keuringsinstanties en taxiondernemers. Deze services certificaten staan beschreven in paragraaf 1.4 deel 3b van het PvE PKIoverheid.

De systeemkaart die in de BCT gebruikt wordt bevat een 'Autonoom Apparaat Certificaat'. Het certificaatgebruik hiervan staat beschreven in paragraaf 1.4 deel 3d van het PvE PKIoverheid.

Daarnaast zijn er vertrouwende partijen, die handelen in vertrouwen op certificaten van de betreffende certificaathouders. Een vertrouwende partij is iedere natuurlijke of rechtspersoon die ontvanger is van een certificaat en die handelt in vertrouwen op dat certificaat

De toepasbaarheid van de certificaten wordt in tabel 2 nader toegelicht:

Type	Gebruik
Persoonsgebonden Authenticiteitcertificaat	Dit certificaat wordt gebruikt om de certificaathouder te authenticeren
Persoonsgebonden Handtekeningcertificaat	Dit certificaat wordt gebruikt om een elektronische handtekening te verifiëren
Persoonsgebonden Vertrouwelijkheidcertificaat	Dit certificaat wordt gebruikt voor het versleutelen van gegevens
Services certificaat (authenticiteit)	Dit certificaat wordt gebruikt om de certificaathouder te authenticeren
Autonoom apparaat certificaat (authenticiteit)	Dit certificaat wordt gebruikt voor authenticatie van de BCT.

Tabel 2 – Toepassingsgebied

Certificaten mogen alleen voor het aangegeven doel (t.b.v. gebruik in de BCT) worden gebruikt. Er zijn geen technische beperkingen aan het gebruik van de certificaten.

De chauffeurskaart BCT is geen erkend identiteitsbewijs en kan derhalve niet als zodanig worden gebruikt.

1.5 CPS-beheer

1.5.1 Contactgegevens

Informatie over dit CPS of de dienstverlening van de DH BCT kan worden verkregen via onderstaande contactgegevens. Commentaar op het onderliggend CPS kan worden gericht aan hetzelfde adres.

Inspectie Leefomgeving en Transport
T.a.v. Dossierhouder BCT, F.G. van Wijnen
Postbus 16191
2500 BD Den Haag

ferry.van.wijnen@ilent.nl
06-55871313

Meer informatie over de dienstverlening van de TSP van het ministerie van Infrastructuur en Waterstaat kan worden verkregen via http://csp.minIenM.nl

1.5.2 Wijziging en goedkeuring CPS

De DH BCT heeft het recht het CPS te wijzigen of aan te vullen. Wijzigingen gelden vanaf het moment dat het nieuwe CPS gepubliceerd is. De procedure voor de wijziging en goedkeuring van het CPS staat beschreven in paragraaf 9.11.

1.6 Definities en afkortingen

Een overzicht van de in dit document gebruikte definities en afkortingen is opgenomen in bijlage A respectievelijk in bijlage B.

2 Verantwoordelijkheid voor publicatie en elektronische opslagplaats

2.1 Elektronische opslagplaats

De elektronische opslagplaats van de DH BCT is publiekelijk bereikbaar via http://bct.csp.minIenM.nl

2.2 Publicatie van TSP informatie

De DH BCT publiceert de volgende TSP informatie:

- Certificate Practice Statement (CPS)
- Algemene voorwaarden
- PKI Disclosure Statement (PDS)
- Certificaten Revocatie Lijsten (CRL's)
- CA certificaten

De DH BCT publiceert geen eindgebruikercertificaten. CA certificaten worden gepubliceerd als onderdeel van het uitgifteproces van deze certificaten.

De onderstaande tabel geeft weer waar de gegevens beschikbaar gesteld zijn:

Soort informatie	URL
CPS	http://bct.csp.minIenM.nl/minIenM-bct-cps/minIenM-bct-cps.pdf
Algemene Voorwaarden	http://bct.csp.minIenM.nl/minIenM-bct-av/minIenM-bct-av.pdf
Boordcomputerkaarten CRL	http://bct.csp.minIenM.nl/minIenM-bc-ca-1.crl
Systeemkaarten CRL	http://bct.csp.minIenM.nl/minIenM-sys-ca-1.crl
Boordcomputerkaarten CA	http://bct.csp.minIenM.nl/minIenM-bc-ca-1.cer
Systeemkaarten CA	http://bct.csp.minIenM.nl/minIenM-sys-ca-1.cer

Tabel 3 – URLs

Informatie van de TSP wordt gepubliceerd via http://csp.minIenM.nl. De CA certificaten van de TSP zijn ook via dit kanaal opvraagbaar.

De in dit CPS aangehaalde wet- en regelgeving is te raadplegen via de website http://wetten.overheid.nl

Voor de Certificate Policies (CP) wordt doorverwezen naar www.pkioverheid.nl. Om de juiste CP te kunnen identificeren geeft de navolgende tabel de samenhang tussen de kaarten, de functies van de certificaten, de toepasselijke CP en de Object Identifier (OID) van de CP.

Soort Certificaat **–** Kaarttype	PolicyIdentifiers (OID)	CP
Persoonsgebonden authenticiteitcertificaten: Chauffeurskaart Inspectiekaart	2.16.528.1.1003.1.2.5.1	OID van de PKI-overheid Certificate Policy voor persoonsgebonden authenticiteitcertificaten in het domein Organisatie.
Persoonsgebonden handtekeningcertificaten: Chauffeurskaart Inspectiekaart	2.16.528.1.1003.1.2.5.2	OID van de PKI-overheid Certificate Policy voor persoonsgebonden handtekeningcertificaten in het domein Organisatie.
Persoonsgebonden vertrouwelijkheid-certificaten: Chauffeurskaart Inspectiekaart	2.16.528.1.1003.1.2.5.3	OID van de PKI-overheid Certificate Policy voor persoonsgebonden vertrouwelijkheidcertificaten in het domein Organisatie.
Services Authenticiteitcertificaten: Keuringskaart Ondernemerskaart	2.16.528.1.1003.1.2.5.4	OID van de PKI-overheid Certificate Policy voor services certificaten voor authenticiteit in het domein Organisatie
Services Vertrouwelijkheidcertificaten Keuringskaart Ondernemerskaart	2.16.528.1.1003.1.2.5.5	OID van de PKI-overheid Certificate Policy voor services certificaten voor authenticiteit in het domein Organisatie
Services Servercertificaten Keuringskaart Ondernermerskaart	2.16.528.1.1003.1.2.5.6	OID van de PKI-overheid Certificate Policy voor services certificaten voor authenticiteit in het domein Organisatie
Autonoom apparaat certificaat: Systeemkaart	2.16.528.1.1003.1.2.6.1	OID van de PKI-overheid Certificate Policy voor Apparaat gebonden Authenticiteit in het domein Autonome Apparaten.

Tabel 4 - Kaarttype en toepasselijke CP

2.3 Tijdstip of frequentie van publicatie

Het publiceren van Certificaten Revocatie Lijsten (CRL's) vindt ieder drie uur plaats. De overige onder 2.2 genoemde informatie wordt in het geval van wijziging zo snel als nodig is geactualiseerd.

2.4 Toegang tot gepubliceerde informatie

De onder 2.2. genoemde gepubliceerde informatie is publiek van aard en vrij toegankelijk. De gepubliceerde informatie kan op elektronische wijze vierentwintig uur per dag en zeven dagen per week worden geraadpleegd, met uitzondering van systeemdefecten en onderhoudswerkzaamheden.

Indien de elektronische opslagplaats niet beschikbaar is wordt de beschikbaarheid binnen 24 uur hersteld.

3 Identificatie en authenticatie

3.1 Naamgeving

Deze paragraaf beschrijft op welke wijze de identificatie en authenticatie van aanvragers plaatsvindt tijdens de initiële registratieprocedure en welke criteria DH BCT stelt ten aanzien van de naamgeving.

3.1.1 Soorten naamformaten

Alle certificaten die door DH BCT worden uitgegeven bevatten gegevens over de organisatie van de aanvrager. Bij chauffeurskaarten en inspectiekaarten worden ook persoonsgebonden naamsgegevens in het certificaat opgenomen.

De naamgeving in de certificaten is opgebouwd zoals beschreven in de volgende tabel:

Attribute (X.500)	Chauffeurskaart	Ondernemerskaart	Keuringskaart	Inspectiekaart	Systeemkaart
issuer.countryName	NL	NL	NL	NL	NL
issuer. organisationName	Ministerie van Infrastructuur en Milieu	Ministerie van Infrastructuur en Milieu	Ministerie van Infrastructuur en Mileu	Ministerie van Infrastructuur en Milieu	Ministerie van Infrastructuur en Milieu
issuer. CommonName	MinIenM Taxi CA Boordcomputerkaarten – G2	MinIenM Taxi CA Boordcomputerkaarten – G2	MinIenM Taxi CA Boordcomputerkaarten – G2	MinIenM Taxi CA Boordcomputerkaarten – G2	MinIenM Taxi CA Systeemkaarten – G2
Subject.CountryName	NL	NL	NL	NL	NL
subject.organizationName	[Eerste voornaam] [Verdere voorletters] [Voorvoegsel] [Geslachtsnaam]	[Naam onderneming]	[Naam keuringsinstantie]	[Naam Inspectiedienst]	[Naam Boordcomputerfabrikant]
Subject. organizationIdentifier	Nvt	NTRNL-KVK-nummer	kvk-nummer keuringsinstantie	Nvt	Nvt
Subject. CommonName	[Eerste voornaam] [Verdere voorletters] [Voorvoegsel] [Geslachtsnaam]	[Naam onderneming]	[Naam keuringsinstantie]	[Eerste voornaam] [Verdere voorletters] [voorvoegsel] [Geslachtsnaam]	[Typegoedkeuringsnummer]
Subject.givenName	[Eerste voornaam] [Verdere voorletters]	Nvt	[Eerste voornaam] [Verdere voorletters]	[Eerste voornaam] [Verdere voorletters]	Nvt
Subject.surName	[Voorvoegsel] [Geslachtsnaam]	Nvt	[Voorvoegsel] [Geslachtsnaam]	[Voorvoegsel] [Geslachtsnaam]	Nvt
Subject. SerialNumber	[Kaarthoofdtype] + [BSN] + "-" + [Kaartvolgnummer] of Kaarthoofdtype + [NI-Nummer] + "-" [Kaartvolgnummer]	[Kaarthoofdtype] + [KvKnummer] + "-"+ [Kaartvolgnummer]	[Kaarthoofdtype] + [RDW-erkenningsnummer] + "-" + [Kaartvolgnummer]	[Kaarthoofdtype] + [Inspectienummer] + "-" + [Kaartvolgnummer]	[Kaarthoofdtype] + [Boordcomputernummer] + "-" + [Kaartvolgnummer]
Subject.Title	[Kaarthoofdtype] + [Kaartsubtype]	[Kaarthoofdtype] + [Kaartsubtype]	[Kaarthoofdtype] + [Kaartsubtype]	[Kaarthoofdtype] + [Kaartsubtype]	[Kaarthoofdtype] + [Kaartsubtype]
subjectAltName. PermanentIdentifier. identifierValue	[Kaarthoofdtype] + [BSN] of [Kaarthoofdtype] + [NI-Nummer]	[Kaarthoofdtype] + [KvK-nummer]	[Kaarthoofdtype] + [RDW-erkenningsnummer]	[Kaarthoofdtype] + [Inspectienummer]	[Kaarthoofdtype] + [Boordcomputernummer]
PermanentIdentifier. assigner	2.16.528.1.1003.1.3.5.1.2	2.16.528.1.1003.1.3.5.1.2	2.16.528.1.1003.1.3.5.1.2	2.16.528.1.1003.1.3.5.1.2	2.16.528.1.1003.1.3.6.1.2
subjectAltName. UserPrincipalName	[Kaarthoofdtype] + [BSN] of [NI-Nummer] + "@2.16.528.1.1003.1.3.5.1.2"	[Kaarthoofdtype] + [KvK-nummer] + '@' + "2.16.528.1.1003.1.3.5.1.2"	[Kaarthoofdtype] + [RDW-erkenningsnummer] + "@" + "2.16.528.1.1003.1.3.5.1.2"	[Kaarthoofdtype] + [Inspectienummer] + '@' + "2.16.528.1.1003.1.3.5.1.2"	Nvt
certificatePolicies. PolicyIdentifier	2.16.528.1.1003.1.2.5.1	2.16.528.1.1003.1.2.5.4	2.16.528.1.1003.1.2.5.4	2.16.528.1.1003.1.2.5.1	2.16.528.1.1003.1.2.6.1

Tabel 5 - Gegevens in certificaten

De door de aanvrager aangeleverde gegevens worden geverifieerd aan de hand van betrouwbare bronnen. De aangeleverde gegevens bestaan uit karakters uit de Gemeentelijke Basis Administratie (GBA) karakterset, gecodeerd als UTF8.

Binnen PKIoverheid worden unieke OID nummers toegekend aan de TSP. Dit nummer wordt in verschillende velden van de verschillende certificaten gebruikt.

De volgende OID's zijn door de Policy Autoriteit van PKIoverheid toegekend aan het ministerie van Infrastructuur en Waterstaat. De OID's zijn uitgegeven voor respectievelijk de organisatie van het ministerie van Infrastructuur en Waterstaat en de daaronder uitgegeven CA Certificaten voor de TSP en de DH.

OID	Betekenis
2.16.528.1.1003.1.3.5.1	Ministerie van Infrastructuur en Milieu
2.16.528.1.1003.1.3.5.1.1	Ministerie van Infrastructuur en Milieu CSP CA
2.16.528.1.1003.1.3.5.1.2	MinIenM BCTCA
2.16.528.1.1003.1.3.6.1	minIenM
2.16.528.1.1003.1.3.6.1.1	minIenM.autonome-apparaten-csp-ca
2.16.528.1.1003.1.3.6.1.2	minIenM.taxi-svsteemkaarten-ca

Tabel 6 - Door PKIoverheid aan het ministerie van Infrastructuur en Waterstaat uitgegeven OIDs

3.1.2 Velddefinitie

a) Kaarthoudernummer

Hierna getoonde tabel geeft de lengtes en types van de velden aan die gebruikt worden in de certificaten van alle kaarttypen:

Kaarttype	Veldinhoud	Type en lengte
Chauffeurskaart	BSN of NI-nummer van de chauffeur	Text 9
Ondernemerskaart	KvK-Nummer	Text 12
Keuringskaart	RDW-Erkenningsnummer	Text 7
Inspectiekaart	Inspectienummer	Text 10
Systeemkaart	Een door de DH BCT gegenereerd uniek boordcomputernummer	Text 9

Tabel 7 - Kaarthoudernummer veldinhoud

Voor de chauffeurskaart wordt het Burgerservicenummer (BSN) gebruikt voor personen die een BSN hebben. Voor personen die niet over een BSN beschikken wordt een Niet Ingezetene Nummer (NI-nummer) gegenereerd.

b) Kaarttype

De Kaarttypes die door de DH BCT gebruikt worden zijn:
- **C**hauffeurskaart
- **O**ndernemerskaart
- **K**euringskaart
- **I**nspectiekaart
- **S**ysteemkaart

Voor de kaarten zijn verschillende Kaartsubtypes mogelijk.

Kaarttype	Gebruikersgroep	Inhoud
Chauffeurskaart	Bestuurder	C
Ondernemerskaart	Vervoerder	O
Keuringskaart	Werkplaats	K
Inspectiekaart	Toezichthouder	I
Systeemkaart	Boordcomputer	S

Tabel 8 – Kaarttype

Het kaarttype wordt binnen de BCT gebruikt om de toegangsrechten en werkingsmodus vast te stellen.

c) Kaartsubtype

Binnen het kaarttype chauffeurskaart komen twee subtypes voor, die worden aangeduid met een kaartsubtype. Het subtype geeft aan of de houder van de chauffeurskaart gerechtigd is om volledig of beperkt taxivervoer te verrichten. De inhoud van het veld is dan respectievelijk VOL of BEP.

d) Kaartvolgnummer

Dit nummer wordt gebruikt om de kaart uniek te identificeren binnen de combinatie kaarthoudernummer en kaarttype. Dit dient zowel het bestaan van meerdere kaarten per kaarthouder op eenzelfde moment in tijd (voor ondernemerskaart en keuringskaart), als vervanging van kaarten. Dit veld is 5 karakters lang en van het type tekst.

Kaartvolgnummers beginnen met 00001 en lopen opvolgend op.

3.1.3 Noodzaak betekenisvolle benaming

Naamgeving die in de uitgegeven certificaten wordt gehanteerd is zodanig, dat het voor de vertrouwende partij mogelijk is de identiteit van de certificaathouder of abonnee onomstotelijk vast te stellen.

3.1.4 Anonimiteit pseudoniem en wildcards in certificaten

De DH BCT staat het gebruik van pseudoniemen en wildcards niet toe.

3.1.5 Richtlijnen voor het interpreteren van de diverse naamvormen

Voor de interpretatie van de benaming zijn de volgende punten relevant:

1. De commonName in certificaten op de chauffeurskaart en inspectiekaart bevat de geslachtsnaam van de houder inclusief voorvoegsels en voornamen, zoals opgenomen in het bij registratie voorgelegde identificatiedocument. Als identificatiedocument gelden bij artikel 1 van de Wet op de identificatieplicht (Wid) aangewezen geldige documenten.

2. In de onder punt 1 genoemde commonName worden alleen de eerste voornaam volledig vermeld, de overige namen worden afgekort conform het

bij registratie overlegde identificatiedocument. Als de zo ontstane commonName meer karakters bevat dan technisch mogelijk is, worden één of meer initialen weggelaten, te beginnen bij de laatste initiaal, net zo lang tot de op deze wijze ontstane commonName wel past.

3. De commonName in certificaten op de ondernemerskaart en keuringskaart bevat de organisatienaam zoals deze op het bij registratie overlegde document voor identificatie van de organisatie voorkomt.

4. De commonName in het certificaat op de systeemkaart bevat het door RDW afgegeven typegoedkeuringsnummer voor het betreffende type boordcomputer.

5. De organizationName in de certificaten van alle kaarttypen komt overeen met in punt 3 bedoelde organisatienaam, met uitzondering van de chauffeurskaart waar de organizationName en commonName hetzelfde zijn.

De DH BCT behoudt zich het recht voor om bij registratie de aangevraagde naam aan te passen als dit juridisch of technisch noodzakelijk is.

3.1.6 *Uniciteit van namen*
De DH BCT garandeert dat de uniciteit van het 'subject'-veld wordt gewaarborgd. Dit betekent dat de onderscheidende naam die is gebruikt in een uitgegeven certificaat, nooit kan worden toegewezen aan een ander subject. Dit gebeurt door middel van het kaarttype, kaarthoudernummer en kaartvolgnummer dat is opgenomen in het veld subject.serialNumber.

3.2 Initiële identiteitsvalidatie

3.2.1 *Bewijs van bezit 'private sleutel behorend bij het uit te geven certificaat'*
De DH BCT levert geen certificaten voor sleutelparen die niet door haar zelf zijn gegenereerd. De sleutelparen worden door de personalisator in een gecontroleerde en afgeschermde ruimte, als onderdeel van de personalisatieprocedure in een beveiligde cryptografische module gegenereerd. Via een beveiligd communicatieprotocol worden de certificaataanvragen vervolgens aan de certificaatproducent verzonden. Na verwerking en retourzending van de certificaten worden certificaten en private sleutels vervolgens via een beveiligde communicatiesessie in de kaart geïnjecteerd. De private sleutel kan de kaart niet verlaten.

3.2.2 *Authenticatie van organisatorische identiteit*
Tijdens de aanvraag van een kaart wordt door de abonnee gegevens overlegd waaruit de identiteit van de in de certificaten op te nemen organisatie blijkt. De uitzondering hierop is de chauffeurskaart. Hierin is de identiteit van de kaarthouder gelijk aan de organisatorische identiteit.

De volgende gegevens, en het daarbij behorende bewijs, worden tijdens het aanvraagproces aangeleverd en vastgelegd:

Gegevens	Kaarttype
Kamer van Koophandel nummer	Keuringkaart, ondernemerskaart, systeemkaart
Taxivergunningsnummer	Ondernemingkaart
RDW-erkenningsnummer	Keuringkaart
ILT-nummer	Inspectiekaart
Typegoedkeuringsnummer	Systeemkaart

Tabel 9 – Aanvraaggegevens organisatorische entiteit

Op basis van de aangeleverde gegevens wordt door de DH BCT met behulp van betrouwbare registers vastgesteld of de organisatie bestaat en tot een aanvraag geautoriseerd is. De in het certificaat op te nemen informatie betreffende de organisatie, zoals organisatienaam, wordt overgenomen uit de betrouwbare registers.

3.2.3 Authenticatie van persoonlijke identiteit

Bij de vaststelling van een persoonlijke identiteit kunnen certificaathouder en certificaatbeheerder worden onderscheiden. Bij de chauffeurs- en inspectiekaart wordt de persoonlijke identiteit van de certificaathouder vastgesteld. Voor de ondernemers-, keuring-, inspectie- en systeemkaart betreft deze controle de certificaatbeheerder.

Tijdens de aanvraag van een kaart worden de volgende gegevens betreffende de certificaathouder aangeleverd door de abonnee:

Gegevens	Kaarttype
BSN	Chauffeurskaart, Inspectiekaart
Geboortedatum	Chauffeurskaart, Inspectiekaart
ILT-nummer	Inspectiekaart
Inspectienummer (BOA)	Inspectiekaart

Tabel 10 – Aanvraaggegevens certificaathouder

Indien een beoogde certificaathouder niet over een BSN beschikt zal de abonnee tijdens de aanvraag van een kaart de gegevens aanleveren die op de certificaatbeheerder van toepassing zijn.

Een abonnee levert over de certificaatbeheerder de volgende gegevens, en het daarbij behorende bewijs aan:

Gegevens	Kaarttype
Volledige naam, met inbegrip van achternaam, eerste voornaam, initialen of overige voorna(a)m(en) (indien van toepassing) en tussenvoegsels (indien van toepassing);	Chauffeurskaart*, inspectiekaart, ondernemerskaart, keuringskaart, systeemkaart
Geboortedatum en -plaats, een nationaal passend registratienummer, of andere eigenschappen van de certificaathouder of –beheerder die kunnen worden gebruikt om, voor zover mogelijk, de persoon van andere	Chauffeurskaart*, inspectiekaart, ondernemerskaart, keuringskaart, systeemkaart

personen met dezelfde naam te kunnen onderscheiden	
Bewijs dat de Certificaatbeheerder gerechtigd is voor een Certificaathouder een Certificaat te ontvangen namens de rechtspersoon of andere organisatorische entiteit	Inspectiekaart, ondernemerskaart, keuringskaart, systeemkaart

Tabel 11 – Aanvraaggegevens certificaatbeheerder

De Distributeur valideert in het geval van de chauffeurskaart en inspectiekaart de identiteit van de certificaathouder op basis van een persoonlijke controle van de certificaathouder in combinatie met een in artikel 1 van de Wet op de Identificatieplicht genoemd identiteitsdocument.

Bij de ondernemerskaart, keuringskaart en systeemkaart wordt de identiteit van de certificaatbeheerder gevalideerd op basis van het bij de aanvraag meegezonden bewijs.

Deze validatie vindt plaats op de door de certificaathouder/certificaatbeheerder afgesproken tijd en plaats met de distributeur.

3.2.4 Niet geverifieerde gegevens

De DH BCT verifieert de naam van de abonnee aan de hand van erkende documenten en betrouwbare registers. Ook worden alle aanvraaggegevens die worden opgenomen in het certificaat geverifieerd.

Gegevens die alleen voor correspondentiedoeleinden worden vastgelegd, zoals correspondentieadres, en telefoonnummers worden niet geverifieerd. Gegevens die niet worden geverifieerd, neemt de DH BCT over uit het door een gemachtigd aanvrager namens de abonnee ondertekend aanvraagformulier.

3.2.5 Autorisaties certificaataanvrager

Gedurende een aanvraag voor een BCT kaart wordt door de DH BCT vastgesteld of een aanvrager geautoriseerd is om de aanvraag namens de abonnee te doen.

3.3 Identificatie en authenticatie bij vernieuwing van het Certificaat

3.3.1 Routinematige vernieuwing van het certificaat

Door de DH BCT wordt geen routinematige vernieuwing van het certificaat aangeboden. Als een BCT kaart op het punt staat te verlopen zal de certificaathouder of certificaatbeheerder hiervoor opnieuw een aanvraag moeten doen.

3.4 Identificatie en authenticatie bij verzoeken tot intrekking

Verzoeken tot intrekking van certificaten zijn gekoppeld aan de intrekkingprocedure van de BCT kaarten.

Een verzoek tot intrekking van een BCT kaart wordt op echtheid gecontroleerd met behulp van de intrekkingscode. Deze code wordt aan de certificaathouder of certificaatbeheerder verstrekt als onderdeel van het uitgifteproces. De code is uniek met de BCT kaart verbonden.

Houders van een chauffeurskaart hebben de mogelijkheid een vervangende kaart aan te vragen. Voordat een vervangende chauffeurskaart wordt verstrekt, worden de certificaten van de oude kaart ingetrokken. De certificaathouder behoeft hiervoor geen apart verzoek in te dienen.

4 Operationele eisen certificaatlevenscyclus

4.1 Aanvraag van certificaten

Aanvragen voor certificaten maken onderdeel uit van de aanvraag voor een kaart. Deze aanvragen kunnen alleen worden gedaan door abonnees.

4.1.1 Registratieproces abonnee

Het registratieproces voor een abonnee kent twee varianten, afhankelijk van het type kaart dat wordt aangevraagd.

Bij de kaarttypen chauffeurskaart , ondernemerskaart en keuringskaart maakt de registratie van de abonnee onderdeel uit van het aanvraagproces van de kaart.

De registratie van de abonnee maakt geen onderdeel uit van het aanvraagproces van de inspectiekaart en de systeemkaart. Voor deze twee kaarttypen dient de abonnee zich voorafgaand aan de kaartaanvraag te laten registreren bij de DH BCT. Hiervoor wordt het corresponderende formulier ingevuld, ondertekend en voorzien van de benodigde bewijsstukken schriftelijk bij de DH BCT ingediend.

De abonnee registratie dient in alle gevallen door de bevoegd vertegenwoordiger van de abonnee te worden gedaan. Bij aanvragen voor de systeemkaart en boordcomputerkaarten anders dan de chauffeurskaart kan door de bevoegd vertegenwoordiger een certificaatbeheerder worden aangewezen.

Door het indienen van een registratieaanvraag gaat de beoogd abonnee akkoord met de inhoud van dit CPS, de Regeling gebruik Boordcomputer en boordcomputerkaarten, en de algemene voorwaarden.

4.1.2 Aanvraagproces Kaarten

Een aanvraag voor een chauffeurskaart, ondernemerskaart of keuringskaart wordt gedaan door de beoogd abonnee. Het corresponderende aanvraagformulier wordt hiertoe ingevuld, ondertekend en voorzien van de benodigde bewijsstukken schriftelijk bij de DH BCT ingediend.

De door de Abonnee aangewezen contactpersoon kan een aanvraag voor een Inspectiekaart per mail indienen via vergunningen@kiwa.nl .

In deze mail worden van de betreffende certificaathouder de volgende gegevens opgenomen:

- Volledige naam (voornamen voluit)
- Geboortedatum
- BOA aktenummer
- Het inspectienummer van de Abonnee

De Leverancier stuurt de Abonnee per post en voor elke aangevraagde Inspectiekaart een aanvraagset. Deze aanvraagset bestaat uit:

- Begeleidend schrijven
- Aanvraagformulier (op naam van de betreffende Certificaathouder) met ruimte voor pasfoto
- Toelichting op aanvraag
- Antwoordenvelop

De contactpersoon van de Abonnee draagt er zorg voor dat de betreffende Certificaathouder het aanvraagformulier in bezit krijgt, zijn/haar foto volgens de aanwijzingen hierin plaatst, het formulier ondertekent en deze binnen 4 weken retour zendt aan KIWA.

De verschuldigde vergoeding voor de Inspectiekaart wordt voldaan door middel van de gesloten overeenkomst 'achteraf betalen'.

Zodra de aanvraagset door Leverancier is ontvangen neemt zij deze aanvraag in behandeling. Na goedkeuring van de aanvraag wordt de Inspectiekaart geproduceerd.

Wanneer de Inspectiekaart gereed is ontvangt de Certificaathouder thuis een bezorgbericht. De Certificaathouder plant via www.mijnafspraak.nl een afspraak in.

Bij afleveren van de Inspectiekaart controleert AMP de identiteit van de Certificaathouder.

Bij het aanvragen van een systeemkaart wordt door de certificaatbeheerder alleen aangegeven hoeveel systeemkaarten gewenst zijn. De overige gegevens worden overgenomen uit de abonnee registratie.

Door het indienen van een kaartaanvraag gaat de beoogd certificaathouder / certificaatbeheerder akkoord met de inhoud van dit CPS, de Regeling gebruik Boordcomputer en boordcomputerkaarten, en de Algemene Voorwaarden.

4.2 Verwerking certificaataanvraag

De kaartuitgever neemt de kaartaanvraag in ontvangst en beoordeelt de volledigheid en de juistheid van deze aanvraag. Tijdens deze beoordeling vindt een vaststelling van de identiteit van de Aanvrager plaatst conform paragraaf 3.2 van dit CPS. Wanneer de aanvrager voldoet aan de gestelde eisen wordt de kaartaanvraag goedgekeurd.

4.3 Uitgifte van Certificaten

Na de goedkeuring van de kaartaanvraag plaatst de kaartuitgever een productieorder voor de betreffende kaart bij de personalisator.

Op basis van deze productieorder wordt door de personalisator een sleutelpaar aangemaakt voor de betreffende kaart. Vervolgens doet de personalisator een certificaataanvraag bij de certificaatproducent op basis van de gegevens uit de productieorder en de aangemaakte publieke sleutel van het sleutelpaar.

De certificaatproducent geeft hierop een certificaat uit conform de certificaataanvraag en retourneert het resultaat aan zowel de personalisator als de kaartuitgever.

De personalisator neemt het certificaat in ontvangst en plaatst dit met de corresponderende private sleutel op een kaart. Hiertoe worden activeringsgegevens voor de desbetreffende kaart aangemaakt. Vervolgens wordt de kaart grafisch gepersonaliseerd op basis van de gegevens uit de productieorder.

Na productie van alle typen BCT kaarten worden deze door de distributeur in bewaring genomen. De certificaathouder of abonnee krijgt een positieve beschikking toegezonden, met daarop:

- de gebruikersinstructie intrekking
- het bezorgbericht met de mogelijkheid via www.mijnafspraak.nl een afspraak te maken met de distributeur voor de tijd en plaats van gewenste levering.

De ondernemerskaart, keuringskaart en systeemkaart worden in ontvangst genomen door een personeelslid van de abonnee, waarbij de naam van het personeelslid door de distributeur wordt vastgelegd.

Alvorens de kaart in ontvangst te nemen is de ontvanger gehouden de op de kaart vermelde gegevens op juistheid te controleren. Zijn deze niet juist, dan dient de Distributeur deze kaarten mee terug te nemen, hiervan onverwijld melding te maken bij de Kaartuitgever en af te leveren de Kaartuitgever.

In alle gevallen wordt voor de ontvangst van de kaart getekend, waarmee de certificaathouder / certificaatbeheerder aangeeft akkoord te gaan met de inhoud van dit CPS, de Regeling gebruik boordcomputer en boordcomputerkaarten, en de Algemene Voorwaarden, voor zover dit niet reeds is gebeurd.

De activeringsgegevens worden in alle gevallen door de personalisator direct aan de certificaathouder/certificaatbeheerder verzonden.

4.4 Acceptatie van certificaten

Acceptatie van certificaten wordt geacht plaats te hebben gevonden na de overdracht van de boordcomputerkaart aan de certificaathouder / certificaatbeheerder.

4.5 Sleutelpaar en certificaatgebruik

De verantwoordelijkheden en met name de bijbehorende verplichtingen van de abonnee, de certificaathouder/certificaatbeheerder en vertrouwende partijen zijn beschreven in het stelsel van de Regeling gebruik Boordcomputer en boordcomputerkaarten, het CPS en de Algemene Voorwaarden.

4.5.1 *Verantwoordelijkheden en verplichtingen abonnee*

De abonnee is verantwoordelijk voor het juist, tijdige en volledig aanleveren van alle benodigde gegevens voor het aanmaken en leveren en voor het correct gebruik van de certificaten. De abonnee garandeert de DH BCT en vertrouwende partijen dat zij zich conformeert aan de juiste, tijdige en volledige naleving van de gestelde richtlijnen in dit CPS en de Algemene Voorwaarden.

4.5.2 *Verantwoordelijkheden en verplichtingen certificaathouder/certificaatbeheerder*

De certificaathouder/certificaatbeheerder treedt op als houder van het certificaat dat namens de abonnee voor de certificaathouder is aangevraagd. Tevens is hij verantwoordelijk voor het correct aanleveren van alle benodigde gegevens voor het aanmaken en leveren van certificaten, evenals voor het correcte gebruik van de certificaten. De certificaathouder garandeert de DH BCT en de overige belanghebbenden dat zich conformeert aan de juiste, tijdige en volledige naleving van de gestelde richtlijnen in dit CPS en de Algemene Voorwaarden.

4.5.3 Verantwoordelijkheden en verplichtingen vertrouwende partijen

De vertrouwende partij is verantwoordelijk voor het op correcte wijze vertrouwen op een certificaat en garandeert de DH BCT en de overige belanghebbenden dat zij zich conformeert aan de juiste, tijdige en volledige naleving van de gestelde richtlijnen in dit CPS en de Algemene Voorwaarden.

De volgende verplichtingen van de vertrouwende partij zijn van toepassing:

- de geldigheid van het certificaat door middel van de meest recent gepubliceerde Certificaten Revocatie Lijst (CRL) te verifiëren;
- kennis te nemen van alle verplichtingen over het gebruik van het certificaat zoals vermeld in voorliggend CPS en de vertrouwende partij voorwaarden, hieronder uitdrukkelijk mede begrepen alle beperkingen over het gebruik van het certificaat;
- alle overige voorzorgsmaatregelen te nemen die in redelijkheid door vertrouwende partijen genomen kunnen worden;
- zich ervan bewust te zijn dat voorgaande controles slechts de integriteit van de gegevens en de identiteit van de certificaathouder authenticeren, wat uitdrukkelijk geen oordeel inhoudt over de inhoud van de gegevens.

4.6 Vernieuwing van certificaten

De DH BCT biedt geen mogelijkheid tot vernieuwing van PKIoverheid certificaten. Een verzoek tot vernieuwing zal worden behandeld als een verzoek voor een nieuw certificaat, waarbij een nieuw sleutelpaar gegenereerd zal worden.

4.7 Re-key van certificaten

Sleutels van certificaathouders zullen na het verstrijken van de geldigheidsduur of na het intrekken van de bijbehorende certificaten niet opnieuw worden gebruikt.

4.8 Aanpassing van certificaten

De DH BCT biedt geen mogelijkheden tot aanpassing van de inhoud van PKIoverheid certificaten. Indien de gegevens in het certificaat niet meer overeenstemmen met de werkelijkheid is de abonnee verplicht onmiddellijk een verzoek tot intrekking in te dienen. Indien gewenst kan een nieuwe kaart aangevraagd worden.

4.9 Intrekking en opschorting van certificaten

4.9.1 Omstandigheden die leiden tot intrekking

In de volgende gevallen is de abonnee en/of de certificaathouder gehouden per direct en zonder vertraging een verzoek om intrekking van het certificaat in te dienen bij de DH BCT:

- verlies, diefstal of onklaar raken van de boordcomputerkaart;
- geconstateerd of vermoed misbruik of compromittering van het certificaat;
- definitieve blokkering van de boordcomputerkaart na driemaal invoer van een onjuiste PUK-code;
- onjuistheden in de inhoud van het certificaat;
- wijziging van de in het certificaat vermelde gegevens;
- wijziging van de voor de betrouwbaarheid van het certificaat noodzakelijke gegevens;
- overlijden van de certificaathouder (bij persoonsgebonden of beroepsgebonden certificaten);
- beëindiging van de relatie tussen abonnee en certificaathouder;
- beëindiging van de organisatorische eenheid (bij services certificaten);
- ontbinding of faillissement van de rechtspersoon van abonnee (bij services certificaten).

Indien de abonnee aangeeft dat het oorspronkelijke verzoek voor een certificaat niet was toegestaan en de abonnee verleend met terugwerkende kracht ook geen toestemming wordt het certificaat door de DH BCT ingetrokken.

Als de certificaathouder een vermoeden heeft dat zijn PIN-code bekend is geworden, maar tevens de zekerheid heeft dat de Boordcomputerkaart niet uit zijn bezit is geweest kan de certificaathouder zelf de PIN wijzigen, waardoor de kaart niet hoeft worden ingetrokken.

Certificaten kunnen door de DH BCT zonder nadere tussenkomst worden ingetrokken wanneer:

- de DH BCT beschikt over voldoende bewijs dat de privésleutel van de abonnee is aangetast of er is het vermoeden van compromittatie, of er is sprake van inherente beveiligingszwakheid, of dat het certificaat op een andere wijze is misbruikt. Een sleutel wordt in elk geval als aangetast beschouwd in geval van

ongeautoriseerde toegang of vermoede ongeautoriseerde toegang tot de private sleutel, verloren of vermoedelijk verloren private sleutel of SSCD, gestolen of vermoedelijk gestolen sleutel of SSCD of vernietigde sleutel of SSCD;
- indien de abonnee, de certificaathouder en/of de certificaatbeheerder zich niet houdt aan de verplichtingen in dit CPS, de Regeling gebruik Boordcomputer en boordcomputerkaarten, de Algemene Voorwaarden of de overeenkomst die met de abonnee is gesloten;
- de DH BCT op de hoogte wordt gesteld of anderszins zich bewust wordt van een wezenlijke verandering in de informatie, die in het certificaat staat;
- de DH BCT bepaalt dat het certificaat niet is uitgegeven in overeenstemming met dit CPS, de Regeling gebruik Boordcomputer en boordcomputerkaarten, de Algemene Voorwaarden of de overeenkomst die met de abonnee is gesloten;
- de DH BCT bepaalt dat informatie in het certificaat niet juist of misleidend is;
- de DH BCT haar werkzaamheden staakt en de CRL dienstverlening niet wordt overgenomen door een andere TSP;
- De technische inhoud van het certificaat een onverantwoord risico met zich mee brengt voor abonnees, vertrouwende partijen en derden (b.v.browserpartijen).

Intrekking door de DH BCT vindt in ieder geval plaats in de volgende omstandigheden;
- Na in kennisstelling door het GBA van het overlijden van de certificaathouder.
- Na aantasting van de private sleutel van de DH BCT, TSP IenW of PKIoverheid. Hierbij worden de certificaten van alle bij de DH BCT bekende abonnees en certificaathouders ingetrokken.
- Als de kaart niet binnen de gestelde termijn van 12 weken is afgehaald.
- Na definitieve intrekking of schorsing van de BCT-kaart.

De beweegreden voor elke door de DH BCT zelfstandig uitgevoerde intrekking wordt door haar geregistreerd.

De DH BCT zorgt ervoor dat datum en tijdstip van intrekking van (services) certificaten precies kunnen worden vastgesteld. In geval van twijfel geldt het door de DH BCT vastgestelde tijdstip als moment van intrekking. Als een certificaat is ingetrokken, kan het niet opnieuw geldig worden verklaard.

4.9.2 Wie mag een verzoek tot intrekking doen?

De DH BCT trekt een certificaat in na een geautoriseerd verzoek daartoe van de abonnee, de certificaathouder of de certificaatbeheerder. De DH BCT mag ook zelf een verzoek tot intrekking initiëren. Een vertrouwendepartij kan geen verzoek tot intrekking doen, maar kan wel melding maken van het vermoeden van een omstandigheid die aanleiding kan zijn tot het intrekken van een certificaat. De DH BCT zal een dergelijke melding onderzoeken en, als daar aanleiding toe is, het certificaat intrekken.

4.9.3 Procedure voor een verzoek tot intrekking

Verzoeken tot intrekking van certificaten kunnen door een daartoe bevoegd persoon van de abonnee of door de certificaathouder/certificaatbeheerder telefonisch of elektronisch worden gedaan. Nadrukkelijk wordt erop gewezen dat, in geval met de intrekking een spoedeisend belang gediend is, dit elektronisch via de website van Kiwa Register B.V. (https://intrekken.kiwabctkaart.nl) dient te geschieden. Deze vorm van intrekking is vierentwintig uur per dag beschikbaar, zeven dagen per week.

Bij elektronische intrekking vult de aanvrager het kaartnummer van de in te trekken boordcomputerkaart en de bijbehorende intrekkingscode in op de website van de DH BCT. Als de combinatie van de intrekkingcode en het kaartnummer correct is, worden de certificaten op de boordcomputerkaart ingetrokken. De aanvrager krijgt hiervan op website een melding. Als de intrekkingcode en kaartnummer niet correct zijn, wordt teruggemeld dat de intrekking niet wordt uitgevoerd. De DH BCT heeft maatregelen genomen om te
voorkomen dat onbeperkt foutieve intrekkingverzoeken kunnen worden gedaan.

Bij telefonische intrekking worden geen documenten overlegd. De indiener van het intrekkingverzoek dient een aantal vooraf vastgestelde vragen te beantwoorden. Aan de hand van deze vragen dient de DH BCT voldoende zekerheid te verkrijgen over de identiteit van de aanvrager van de intrekking en de boordcomputerkaart waarvoor intrekking wordt aangevraagd. Na het vaststellen van de identiteit van de indiener van het intrekkingverzoek en van de boordcomputerkaart, controleert de DH BCT of de indiener bevoegd is de aanvraag tot intrekking te doen. Na uitvoering van de controles trekt de DH BCT de certificaten op de boordcomputerkaart in en plaatst deze op de Certificate Revocation List (CRL). Een bevestiging van de afhandeling of melding van de afwijzing van het verzoek tot intrekking wordt schriftelijk aan de abonnee en certificaathouder gemeld.

De telefonische intrekkingdienst is beschikbaar gedurende kantoortijden op telefoonnummer **088-9984888**.

Een melding door een vertrouwendepartij van het vermoeden van een omstandigheid die kan leiden tot de intrekking van een certificaat kan uitsluitend telefonisch plaatsvinden.

De DH BCT zorgt ervoor dat datum en tijdstip van intrekking van certificaten precies kunnen worden vastgesteld. In geval van twijfel geldt het door de DH BCT vastgestelde tijdstip als moment van intrekking. Als een certificaat is ingetrokken, kan het niet opnieuw geldig worden verklaard.

4.9.4 Noodprocedure voor een verzoek tot intrekking

In het geval dat de website voor elektronische intrekking niet beschikbaar is treedt de noodprocedure voor een verzoek tot intrekking in werking.

De aanvrager van de intrekking stuurt via e-mail een intrekkingverzoek naar het e-mail adres intrekkenBCT@kiwa.nl . In het intrekkingverzoek neemt de aanvrager de volgende gegevens op:

- de kaartsoort;
- het kaartnummer;
- de intrekkingcode;
- de reden voor intrekking;
- de naam van de aanvrager, en;
- het telefoonnummer waaronder de aanvrager te bereiken is.

4.9.5 Tijdsduur voor de verwerking van intrekkingverzoek

De maximale verwerkingstermijn van een intrekkingsverzoek is vier (4) uur.

4.9.6 Controlevoorwaarden

De controleverplichtingen van de vertrouwende partijen zijn opgenomen in paragraaf 4.5.3 van dit CPS en de Algemene Voorwaarden.

Ingetrokken certificaten blijven ook na het verstrijken van de oorspronkelijke geldigheidsdatum op de CRL vermeld staan.

4.9.7 CRL uitgiftefrequentie & maximale vertraging

De CRL-uitgifte frequentie van de MinIenW CA vindt eens per drie maanden plus 1 dag plaats.

De CRL-uitgifte frequentie is eens per drie uur, waarbij de CRL een geldigheidsduur heeft van vierentwintig uur. Maximaal vier uur nadat een geautoriseerd online verzoek om intrekking is ontvangen, zal de DH BCT een CRL publiceren met de statuswijziging van dit certificaat.

In het geval dat een kaart wordt ingetrokken via de noodprocedure wordt de CRL onmiddellijk na de verwerking door de CA gepubliceerd.

4.9.8 Online intrekking/statuscontrole

De DH BCT biedt geen online intrekking/statuscontrole (OCSP) dienst aan.

4.9.9 Opschorten van certificaten

Het opschorten van certificaten wordt door de DH BCT niet aangeboden.

4.10 Certificaat status dienst

De status van certificaten wordt door de DH BCT bekend gemaakt door middel van een CRL. De CRL is 7 dagen per week 24 uur beschikbaar. In het geval van systeemdefecten of andere oorzaken die buiten het bereik van de DH BCT liggen, zal de DH BCT al het mogelijke doen om de niet-beschikbaarheid van de CRL niet langer te laten duren dan vier uur.

4.11 Beëindiging abonnee relatie

Indien een abonnee het abonnement wil beëindigen kan deze contact op te nemen met de DH BCT. De abonnee is gehouden alle nog niet verlopen certificaten in te trekken, voordat tot beëindiging van het abonnement kan worden overgegaan.

4.12Key Escrow en Key Recovery

De private sleutels van de DH BCT worden niet aan een derde in key escrow gegeven.

Er wordt door de DH BCT geen key recovery aangeboden voor de private sleutels gerelateerd aan uitgegeven certificaten.

5 Fysieke, procedurele en personele beveiliging

De beheersmaatregelen in hoofdstuk 5 zijn bepaald op grond van de risicoanalyse en beveiligingsplannen op BCT kaartaanvragen en uitgifteprocessen.

De genomen maatregelen waarborgen een afgeschermd en goed beveiligd registratie-, personalisatie-, certificatie-, uitgifte- en intrekkingproces, waarbij ongeautoriseerde toegang tot of inbreuk op deze processen of de locaties waar deze processen worden uitgevoerd, wordt tegengegaan.

5.1 Fysieke beveiliging

5.1.1 *Locatie*

De dienstverlening van de DH BCT wordt door verschillende partijen uitgevoerd en vindt op verschillende locaties plaats.

De registratiewerkzaamheden en werkzaamheden met betrekking tot de verstrekking en intrekking van kaarten vinden plaats op de locatie van de kaartuitgever. Het centrale registratiesysteem bevindt zich in het rekencentrum van een hiertoe gespecialiseerde partij.

De productie van de boordcomputerkaarten, te weten de grafische personalisatie en de generatie van sleutelmateriaal, vindt plaats op de vestigingslocatie van de personalisator.

Het daadwerkelijk produceren van certificaten wordt bij de certificaatproducent uitgevoerd.

De uitgifte van persoonsgebonden boordcomputerkaarten vindt plaats op de gewenste locatie van de kaartaanvrager. Hiervoor wordt een afspraak gemaakt tussen de kaartaanvrager en de distributeur.

5.1.2 *Fysieke toegangscontrole*

Voor alle locaties zijn passende fysieke beveiligingsmaatregelen getroffen. Deze maatregelen zijn genomen op basis van risicoanalyses en beveiligingsplannen.

5.1.3 *Opslag van media*

Opslagmedia van systemen die worden gebruikt, worden veilig behandeld om de opslagmedia tegen schade, diefstal en ongeautoriseerde toegang te beschermen. Opslagmedia worden zorgvuldig vernietigd wanneer zij niet meer nodig zijn.

5.1.4 *Afvalverwerking*

In alle locaties zijn maatregelen genomen om op een veilige wijze met (vertrouwelijk) afval om te gaan.

5.1.5 *Back-up buiten de locatie*

Data noodzakelijk voor het waarborgen van de dienstverlening door de DH BCT bij een calamiteit wordt door de verschillende partijen op een adequate wijze veilig gesteld.

5.2 Procedurele beveiliging

5.2.1 *Vertrouwelijke rollen*
Alle functies die een rol spelen in de dienstverlening binnen de DH BCT zijn aangewezen als vertrouwensfuncties, conform de Uitvoeringsbepalingen Vertrouwensfuncties.

5.2.2 *Aantal personen benodigd per taak*
Voor het uitvoeren van bepaalde, vooraf gedefinieerde, activiteiten op het gebied van sleutel-, certificaatmanagement, systeemontwikkeling, -onderhoud en -beheer zijn meerdere medewerkers nodig. De noodzaak om met meerdere mensen een bepaalde activiteit uit te voeren, wordt afgedwongen o.a. met behulp van technische voorzieningen, autorisaties in combinatie met identificatie/authenticatie en aanvullende procedures.

5.2.3 *Functiescheiding*
De DH BCT hanteert een strikte scheiding tussen uitvoerende, beslissende, registrerende, bewarende en controlerende taken. Er is sprake van functiescheiding tussen systeembeheer en bediening van de TSP systemen, alsmede tussen Security Officer(s), Systeem auditor(s), systeembeheerder(s) en TSP operator(s).

5.3 Personele beveiliging

5.3.1 *Kwalificaties, ervaring en screening*
De DH BCT zet voldoende personeel in dat beschikt over voldoende vakkennis, ervaring en kwalificaties die noodzakelijk zijn voor de certificatiediensten. Vastgesteld is over welke kennis, kunde en ervaring een medewerker voor de betreffende functie moet kunnen beschikken.

5.3.2 *Antecedentenonderzoek*
Alle medewerkers die betrokken zijn bij personalisatie en certificatiewerkzaamheden zijn onderwerp van antecedentenonderzoek. De DH BCT vraagt van alle aan dit onderzoek onderworpen medewerkers een Verklaring Omtrent Gedrag (VOG).

De DH BCT conformeert zich aan bepaling artikel 24 lid 2 onder b eIDAS omtrent het in dienst nemen van personen. Personeel voert geen werkzaamheden uit voordat zij in dienst treden. Deze eisen gelden eveneens voor organisaties waaraan de DH BCT activiteiten heeft uitbesteed.

5.3.3 *Opleidingseisen*
De opleidingseisen van de medewerkers zijn vastgelegd in de functieomschrijvingen. Voor iedere rol is beschreven over welke kennis, kunde en ervaring de functionaris dient te beschikken.

5.3.4 *Sancties op ongeautoriseerd handelen*
Na het vaststellen van een ongeautoriseerde handeling op een systeem wordt de medewerker die deze handeling heeft ondernomen direct de toegang tot het betreffende systeem ontnomen. De verantwoordelijk manager beslist over de duur en de voorwaarden van de ontzegging en de verder te nemen disciplinaire maatregelen.

5.3.5 Inhuur van personeel
Voor personeel dat is ingehuurd gelden onverkort de eisen uit paragraaf 5.3.

5.3.6 Beschikbaar stellen van documentatie aan personeel
De taakbeschrijvingen van de medewerkers van de DH BCT die als actor de systemen bedienen, zijn vastgelegd in de Administratieve Organisatie en de bijbehorende werkinstructies.

5.4 Procedures ten behoeve van audit logging

5.4.1 Vastleggen van gebeurtenissen
Binnen de systemen en applicaties voor de certificatiediensten worden automatisch of handmatig gebeurtenissen gelogd, die relevant zijn voor de kwaliteit van deze dienstverlening. Deze gebeurtenissen vallen in verschillende categorieën.

1. Registratiehandelingen in het kaartuitgiftesysteem met betrekking tot het aanvragen van boordcomputerkaarten en eventuele latere wijzigingen van de registratiegegevens;
2. Gebeurtenissen in de levenscyclus van sleutels van de CA's zelf en van de sleutels die door de DH BCT ten behoeve van de BCT kaarthouders zijn vervaardigd;
3. Gebeurtenissen in de levenscyclus van certificaten en CRL's, waaronder intrekkingsverzoeken en de naar aanleiding van deze verzoeken ondernomen activiteiten;
4. Gebeurtenissen in de levenscyclus van BCT kaarten;
5. Gebeurtenissen in de infrastructuur voor de certificatiediensten, waaronder:
    - inbreuken op de systemen en pogingen daartoe;
    - aan- en afmelden door systeembeheerders;
    - handelingen door systeembeheerders, die relevant zijn voor de betrouwbaarheid van de certificatiediensten;
    - wijzigingen van autorisaties (beveiligingsprofielen) en van accounts van actoren;
    - afsluiten en (her)starten van de systemen;
    - foutmeldingen van de hard- of software van de systemen;
    - installatie van nieuwe of gewijzigde software;
    - wijzigingen van de hardware;
    - handelingen met betrekking tot de logbestanden of logfunctionaliteit, etc.

5.4.2 Frequentie van het behandelen van de audit-logbestanden
Logbestanden worden periodiek geanalyseerd conform de Beheerprotocollen, zoals opgesteld voor de certificatiedienst.

5.4.3 Bewaartermijn van de audit-logbestanden
Het archiveringssysteem bewaart de gearchiveerde audit-logbestanden gedurende een periode van tenminste zeven jaar en verwijdert deze daarna.

Het archiveringssysteem bewaart de gearchiveerde security-logbestanden gedurende een periode van tenminste 18 maanden en verwijdert deze daarna.

5.4.4 Bescherming van de audit-logbestanden
Gebeurtenissen die op elektronische- en handmatige wijze worden opgenomen in audit log files worden beschermd tegen niet geautoriseerde inzage, wijziging,

verwijdering, of andere ongewenste aanpassingen door middel van fysieke en logische toegangscontrole middelen.

5.4.5 *Back-up procedures van de audit-logbestanden*
Standaard worden dagelijks volledige back-ups gemaakt.

5.4.6 *Bewaren van audit logs*
De audit logbestanden worden intern bewaard op de systemen waarop zij betrekking hebben. Daarnaast wordt de logging off-site gearchiveerd.

5.4.7 *Kwetsbaarhedenanalyse*
De DH BCT stelt een nader onderzoek in als de analyse van de auditlogbestanden op een mogelijk kwaadwillende actie of beveiligingsincident wijst.

5.5 Archiveringsprocedures

5.5.1 *Soorten gearchiveerde gegevens*
De DH BCT legt alle relevante registratie-informatie vast, waaronder tenminste:
- het (certificaat)aanvraagformulier;
- de gegevens van/over het identiteitsdocument dat door de certificaathouder of certificaatbeheerder is getoond;
- de bevindingen en het besluit over de aanvraag;
- de identiteit van de validatiemedewerker die de certificaataanvraag heeft behandeld respectievelijk heeft goedgekeurd;
- de methode om identiteitsdocumenten te valideren en identiteiten vast te stellen;
- het bewijs van identificatie en ontvangst.

5.5.2 *Bewaartermijn archief*
De elektronisch gearchiveerde gegevens worden evenals het papieren archief tenminste zeven jaar bewaard.

5.5.3 *Bescherming van het archief*
De kaartuitgever hanteert een passend stelsel van maatregelen voor de bescherming van de gearchiveerde gegevens, conform de Wbp en het DH BCT-beveiligingsbeleid. Hieronder vallen onder meer de volgende maatregelen:
- de logging wordt redundant gearchiveerd;
- het archief is beveiligd voor de aspecten authenticiteit en integriteit;
- de audit-trail wordt bij archivering voorzien van een elektronische handtekening;
- slechts een selecte groep functionarissen heeft toegang tot het archief.

5.5.4 *Back-up procedures van het archief*
Standaard worden dagelijks volledige back-ups gemaakt. Van het papieren archief wordt geen back-up gemaakt.

5.5.5 *Eisen gesteld aan time-stamping van de logrecords*
De logrecords zijn voorzien van de datum en tijd van het verwerkend systeem waarop de handeling is verricht. De verwerkende systemen worden aan een betrouwbare tijdsbron gesynchroniseerd.

5.5.6 *Positionering van het verzamelsysteem van archiefbestanden*
Het archiveringssysteem bevindt zich in het rekencentrum van de kaartuitgever.

5.5.7 Procedures voor het verkrijgen en verifiëren van gearchiveerde informatie
Het archiveringssysteem en de overige archieven, die van belang zijn voor de certificatiediensten zijn slechts benaderbaar door geautoriseerde functionarissen.

5.6 Procedures voor vernieuwing van de TSP-sleutel

Het genereren en installeren van de sleutels van de DH BCT vindt plaats in het rekencentrum van de certificaatproducent volgens een tevoren vastgesteld draaiboek.

5.7 Aantasting en continuïteit

5.7.1 Procedures voor afhandeling incidenten en aantasting
Incidenten kunnen worden gemeld bij het call center van de kaartuitgever (**088-9984888**) en worden conform het reguliere incidentenbeheer afgehandeld. Als wordt voorzien dat een incident escaleert, wordt een calamiteit aangemeld bij de TSP. Op dat moment kan besloten worden om het business continuity plan van de TSP / DH BCT van kracht te laten worden.

Compromittering van de private sleutel van de DH BCT wordt beschouwd als een calamiteit. De DH BCT neemt in deze situatie minimaal de volgende acties:

- de DH BCT stelt vertrouwende partijen en BCT kaarthouders hiervan zo spoedig mogelijk op de hoogte door de informatie te publiceren via het internet;
- de DH BCT trekt de betrokken certificaten direct in en publiceert deze op de toepasselijke CRL volgens het normale publicatieschema;
- De DH BCT stelt via de TSP het Business Continuity Plan (calamiteitenplan) in werking.

5.7.2 Herstelprocedures IT-omgevingen
In het kader van het incidentenbeheer en het calamiteitenplan van de DH BCT vindt herstel van de IT-omgevingen plaats. Hierbij inbegrepen is de mogelijkheid om de dienstverlening op uitwijklocaties voort te zetten.

5.7.3 Herstelprocedures gecompromitteerde sleutels van de certificaathouders
Compromittering van de sleutels van een BCT kaart of systeemkaart leidt tot een intrekkingsverzoek, zoals beschreven. Na intrekking kan een nieuwe kaart worden aangevraagd, waarvoor nieuwe sleutels worden gegenereerd.

5.8 Beëindiging van de TSP-diensten

Als het voornemen is om de certificatiedienstverlening BCT te beëindigen, zal de DH BCT zich naar beste vermogen inzetten om te zorgen dat de dienstverlening binnen het Ministerie zelf of door een andere dienstverlener onder de hiërarchie van de PKI voor de Overheid wordt overgenomen.

Als dit niet mogelijk is, zal de DH BCT de abonnees en certificaathouders informeren tenminste drie maanden voordat de dienstverlening daadwerkelijk wordt beëindigd. Vanaf dit moment zal KIWA Register geen BCT-kaarten meer uitgeven.

Bij het beëindigen van de certificatiedienstverlening zal het KIWA Register alle geldige certificaten intrekken en deze opnemen in de CRL's. De revocation status

service met de CRL's zal tot ten minste zes maanden na het tijdstip waarop de dienstverlening is beëindigd in stand worden gehouden.

Er zijn geen voorzieningen getroffen voor het geval de Staat der Nederlanden niet langer financieel in staat is om de Certificatiediensten te continueren. Zie evenwel het bepaalde in 9.2 Financiële verantwoordelijkheid en aansprakelijkheid.

De DH BCT neemt daarbij alle redelijkerwijs mogelijke maatregelen om de schade voor BCT kaarthouders en vertrouwende partijen te beperken en zal er zorg voor dragen dat bewijzen van certificatie die eventueel nodig zijn in gerechtelijke procedures blijven bestaan.

Concrete activiteiten zijn tenminste:

- Onderzoek of overname van de dienstverlening door een andere geregistreerde certificatiedienstverlener mogelijk is;
- Indien dit mogelijk is, de door hem afgegeven gekwalificeerde certificaten aan deze dienstverlener overdragen;
- Het informeren van abonnees, certificaathouders en/of certificaatbeheerders, vertrouwende partijen en andere partijen, waarmee overeenkomsten zijn gesloten, over de voorgenomen overdracht of beëindiging van de dienstverlening;
- Indien overdracht van de dienstverlening redelijkerwijs niet mogelijk is:
  - het beëindigen van autorisaties van onderaannemers die namens de DH BCT betrokken zijn bij het leveren van certificatiediensten, daartoe wordt ook het verbreken van externe koppelingen gerekend;
  - alle autorisaties van onderaannemers die namens de DH BCT werkzaam zijn in het proces van het uitgeven van BCT certificaten worden beëindigd.
  - het intrekken van alle geldige certificaten;
  - het buiten gebruik stellen c.q. vernietigen van de private sleutels op een zodanig wijze dat deze niet meer kunnen worden teruggehaald of opnieuw in gebruik kunnen worden genomen.;
  - het bewaren van registratie-informatie, audit-logbestanden (archief, 7 jaar bewaren) en CRL's conform de eisen die daaraan zijn gesteld:
    - de bewaartermijn m.b.t. registratie-informatie en audit-logbestanden zijn te vinden in het PvE (deel 3 basis eisen) onder 5.4.3-pkio81.
    - De bewaartermijn m.b.t. CRL's is te vinden in de ETSI EN 319 411-2, onder 7.3.6.i.

6 Technische beveiliging

6.1 Genereren en installeren van sleutelparen

Bij het genereren van sleutelparen maakt de DH BCT gebruik van veilige middelen en betrouwbare systemen. De betrouwbaarheid en de veiligheid van deze systemen voldoen in ieder geval aan internationaal erkende standaards en nationale wetgeving.

Het genereren van de sleutels van certificaathouders (c.q. gegevens voor het aanmaken van elektronische handtekeningen) vindt plaats in een middel dat voldoet aan de eisen genoemd in {7} CWA 14169 Secure signature-creation devices "EAL 4+" of gelijkwaardige beveiligingscriteria.

6.1.1 Genereren van sleutelparen

Bij het genereren van sleutelparen gebruikt de DH BCT een betrouwbare omgeving en de juiste procedures, die voldoen aan erkende standaarden.

De generatie van de sleutelparen voor de uitgevende CA's van de DH BCT vindt plaats in een FIPS 140-2 level 3 gecertificeerde Hardware Security Module (HSM) op de locatie van de Certificaatproducent. De sleutels van de sleutelparen zijn 4096 bits asymmetrisch RSA.

De sleutelgeneratie voor de BCT kaarten en systeemkaarten vindt plaats in een FIPS 140-2 level 3 gecertificeerde HSM op de locatie van de personalisator. Hierbij wordt gebruik gemaakt van het signature algoritme 'sha256WithRSAEncryption'. De sleutels van de sleutelparen zijn 2048 bits asymmetrisch RSA. De sleutels worden, na ontvangst van de door de CA uitgegeven certificaten, via een beveiligd communicatiekanaal door de personalisator in de kaart (SSCD) geïnjecteerd.

6.1.2 Overdracht van private sleutels en SSCD naar de gebruiker

De kaarten met sleutels en certificaten worden:

- persoonlijk overhandigd aan de kaarthouder in geval van een chauffeurskaart of een inspectiekaart. De PIN-code en PUK-code worden in de vorm van een PIN-mailer separaat naar de certificaathouder gestuurd.
- persoonlijk overhandigd aan een vast te leggen personeelslid van de abonnee in geval van een 'niet op naam gestelde' kaart (ondernemerskaart, keuringskaart en systeemkaart). De PIN-code en PUK-code worden in de vorm van een PIN-mailer separaat naar de certificaatbeheerder gestuurd.

Alle sleutels worden via de kaart verstrekt. Softwarematig gegenereerde sleutels worden niet verwerkt.

6.1.3 Overdracht van publieke sleutels naar de CA

De sleutelparen voor kaarten worden door de personalisator gegenereerd. De publieke sleutel worden via een beveiligde verbinding door middel van een ondertekend productieberichten naar de CA verstuurd ter verwerking.

6.1.4 Overdracht van de publieke sleutel van de TSP naar eindgebruikers

De publieke sleutels van de TSP CA's van het ministerie van Infrastructuur en Waterstaat zijn door de corresponderende Domein Overheid CA's van de Policy Autoriteit van PKIoverheid getekend. De sleutels van de uitgevende CA's van de DH

BCT zijn op haar beurt getekend door de TSP CA's van het ministerie van Infrastructuur en Waterstaat. Door deze tekenhandeling zijn de integriteit en herkomst van deze publieke sleutels gewaarborgd.

De bovenstaande sleutels worden in de vorm van een certificaat beschikbaar gesteld via de uitgegeven kaarten en de website.

6.1.5 Sleutellengten

De sleutellengte voor certificaten voor BCT kaarten is 2048 bits RSA. De BCT kaarten worden getekend met het MinIenW Taxi CA BCT kaarten - G2 Sleutelpaar met een sleutellengte van 4096 bits RSA.

De sleutellengte voor certificaten voor systeemkaarten is 2048 bits RSA. De systeemkaarten worden getekend met het MinIenW Taxi CA Systeemkaarten - G2 Sleutelpaar met een sleutellengte van 4096 bits RSA.

6.1.6 Hardware / software sleutelgeneratie

Sleutels worden uitsluitend in hardware gegenereerd.

6.1.7 Doelen van sleutelgebruik (zoals bedoeld in X.509 v3)

De certificaten, inclusief de daarbij behorende sleutelparen, zijn uitsluitend bedoeld voor de doeleinden die beschreven zijn in dit CPS. De doelen waarvoor een sleutel gebruikt mag worden zijn opgenomen in het certificaat. Hiervoor is het attribuut KeyUsage en eventueel Extended KeyUsage in het certificaat opgenomen.

6.2 Private sleutel bescherming

6.2.1 Standaarden voor crytografische modulen

Voor operationeel gebruik worden de cryptografische gegevens opgeslagen in een Hardware Security Module (HSM). De HSM voldoet aan de eisen zoals beschreven FIPS 140-2 niveau 3 of hoger.

6.2.2 Functiescheiding beheer private sleutels

De toegang tot de HSM's en daarmee de private sleutels van de CA's is beperkt tot houders van een vertrouwende rol, waar nodig op basis van het principe van 'dual control'.

Daarnaast wordt een back-up gemaakt van de private sleutels van de CA's van de DH BCT. De back-up wordt in meerdere versleutelde delen bewaard in cryptografische modules. De back-up kan alleen in gebruik genomen worden wanneer de houders van deze modules aanwezig zijn met hun deel van de sleutel.

De private sleutels van de CA's worden door de DH BCT niet extern in escrow gegeven.

6.2.3 Escrow van private sleutels van kaarthouders

De DH BCT biedt geen escrow dienstverlening aan de kaarthouders aan.

6.2.4 Back-up van de private sleutels van certificaathouders

De DH BCT maakt geen back up van de private sleutels van certificaathouders.

6.2.5 Archivering van private sleutels van certificaathouders

Private sleutels van certificaathouders worden niet gearchiveerd. Technische en organisatorische maatregelen zijn getroffen zodat de archivering van deze sleutels niet mogelijk is.

6.2.6 Toegang tot private sleutels in cryptografische module

De DH BCT CA's slaat de eigen private sleutels gedurende de gehele levensduur beveiligd in een HSM op, op een zodanige wijze dat gebruik uitsluitend mogelijk is onder dual control.

De BCT kaarten en systeemkaarten bevatten ook private sleutels. De toegang hiertoe is afgeschermd met behulp van een PIN code.

6.2.7 Opslag private sleutels

De private sleutels van de DH BCT CA's zijn versleuteld opgeslagen in een HSM. Hierbij wordt toegangsbeveiliging gebruikt die zeker stelt dat de sleutels niet buiten de module kunnen worden gebruikt.

De private sleutels van certificaathouders worden zodanig op de kaart opgeslagen dat deze alleen op de kaart kunnen worden gebruikt.

6.2.8 Activeren private sleutels

Slechts door middel van een sleutelceremonie en de daarvoor noodzakelijk aanwezige functionarissen worden de private sleutels van de uitgevende CA's van de DH BCT geactiveerd. De DH BCT zorgt voor een zorgvuldige procedure in een beveiligde omgeving.

Voor het activeren van private sleutels van eindgebruikers wordt een activeringscode (PIN code) verstrekt.

6.2.9 Methode voor deactiveren private sleutels

De private sleutels die door de DH BCT CA's worden gebruikt om certificaten mee uit te geven worden normaal gesproken niet gedeactiveerd. Deze sleutels blijven in een beveiligde omgeving in productie.

6.2.10 Methode voor vernietigen private sleutels

De private sleutels waarmee certificaten worden ondertekend kunnen na het einde van hun levenscyclus niet meer kunnen worden gebruikt. De DH BCT zorgt voor een adequate vernietiging waarbij wordt voorkomen dat het mogelijk is de vernietigde sleutels te herleiden uit de restanten.

6.2.11 Veilige middelen voor het aanmaken van elektronische handtekeningen

Toegepaste Hardware Security Modules binnen de systemen van de DH BCT zijn gecertificeerd conform FIPS 140-2 level 3. Hierdoor kan cryptografisch materiaal niet ongemerkt wordt gewijzigd tijdens opslag, gebruik en vervoer. De HSM's worden door de leverancier aangeleverd in een verpakking die elke vorm van corruptie van de inhoud toonbaar maakt.

De combinatie van microprocessor en besturingssysteem van de BCT kaart en systeemkaart is onafhankelijk gecertificeerd tegen de Common Criteria for Security Evaluation standaard. Het hierbij toegepaste garantieniveau is EAL5+.

6.3 Aanvullende aspecten van sleutelpaar management

Alle aspecten van het sleutelmanagement worden door de DH BCT uitgevoerd door toepassing van zorgvuldige procedures die in overeenstemming zijn met het beoogde doel.

6.3.1 Archiveren van publieke sleutels

Publieke sleutels worden door de DH BCT gedurende een periode van tenminste zeven jaar na het verstrijken van de oorspronkelijke geldigheidsduur van een certificaat gearchiveerd. Deze archivering vindt plaats in de fysiek veilige omgeving van de CA.

6.3.2 Gebruiksduur publieke/private sleutel

De sleutelparen en certificaten die worden gebruikt door de TSP en de DH BCT zijn steeds 1 dag minder lang geldig dan de bovenliggende CA. Hierdoor zijn de MinIenW TSP CA's een dag minder lang geldig dan het einde van de geldigheid van de bovenliggende CA van PKI Overheid, terwijl de DH BCT CA's een dag minder lang geldig zijn dan de bovenliggende TSP CA's.

Voor de certificaten op de BCT kaarten, inclusief de bijbehorende sleutelparen, wordt verwezen naar paragraaf 1.1.2.

6.4 Activeringsgegevens

6.4.1 Generatie van activeringsgegevens

Voor het gebruik van de private sleutel op de kaart zijn activeringsgegevens nodig. Deze gegevens bestaan uit een PIN code en een PUK code. De activeringsgegevens worden bij de aanmaak van het sleutelpaar door de personalisator op veilige wijze aangemaakt.

De PIN-code bestaat uit minimaal vier cijfers en de PUK-code bestaat in alle gevallen uit twaalf cijfers, de PUK-code voor systeemkaarten bestaat uit 64 karakters. De PIN-code en de PUK-code worden alleen beschikbaar gesteld aan de certificaathouder.

6.4.2 Bescherming activeringsgegevens

De verspreiding van de activeringsgegevens vindt zodanig plaats dat het voor derden onmogelijk is ongezien kennis te nemen van deze gegevens. Hiertoe wordt gebruik gemaakt van een PIN-mailer. De distributie van deze PIN-mailer gebeurt altijd gescheiden van de kaart. Na overdracht van de activeringsgegevens is de certificaathouder verantwoordelijk voor de bescherming van deze gegevens.

De kaart blokkeert na de zesde ingave van een foutieve PIN-code. De kaart kan worden gedeblokkeerd met behulp van de PUK-code. Hierbij wordt een nieuwe PIN-code gekozen. Als de PUK-code drie maal onjuist is ingevoerd, is de BCT kaart definitief geblokkeerd en daarmee onbruikbaar gemaakt.

6.5 Toegangsbeveiliging van TSP-systemen

6.5.1 Algemene systeem beveiligingsmaatregelen

De DH BCT beschikt over een informatiebeveiligingsbeleid en treft conform dit beleid maatregelen om de beschikbaarheid, integriteit en exclusiviteit van de gebruikte

systemen te waarborgen. Computersystemen worden op passende wijze beveiligd tegen ongeautoriseerde toegang en andere bedreigingen. Met de verschillende operationele partijen worden de maatregelen uitgewerkt in Service Level Agreements (SLA's). De beheerwerkzaamheden worden gelogd.

6.5.2 *Specifieke systeem beveiligingsmaatregelen*
In de registratiesystemen van de DH BCT zijn passende controles en beveiligingsmaatregelen opgenomen, waarbij minimaal het vereist niveau uit het PvE PKIoverheid wordt aangehouden. Mede hierdoor is het onmogelijk dat een kaartaanvraag door één medewerker van de DH BCT wordt afgehandeld.

6.5.3 *Beheer en classificatie van middelen*
De DH BCT classificeert de gebruikte middelen op basis van een risicoanalyse.

6.6 Beheersingsmaatregelen technische levenscyclus

6.6.1 *Beheersingsmaatregelen systeemontwikkeling*
Voor de door de DH BCT ontwikkelde systemen wordt door een geaccrediteerde EDP auditor een auditverklaring afgegeven op basis van CWA 14167-1. De DH BCT voert testen uit voordat systemen in gebruik worden genomen. Deze testen vinden plaats op basis van vooraf opgestelde testplannen.

6.6.2 *Beheersmaatregelen beveiligingsmanagement*
De DH BCT beschikt over gescheiden test/acceptatie- en productiesystemen. Het overbrengen van programmatuur van de ene omgeving naar de andere vindt beheerst plaats via een change management procedure. Deze procedure omvat onder andere het bijhouden en vastleggen van versies, wijzigingen en noodreparaties van alle operationele software.

De integriteit van de systemen en informatie van de DH BCT wordt beschermd tegen virussen, schadelijke en niet-geautoriseerde software en andere mogelijk bronnen die kunnen leiden tot verstoring van de dienstverlening, door middel van een samenstel van passende fysieke, logische en organisatorische maatregelen. Deze maatregelen zijn preventief, repressief en correctief van aard. Voorbeelden van maatregelen zijn: logging, firewalls, intrusion detection en redundantie van systemen, systeemonderdelen en netwerkcomponenten.

De verschillende operationele partijen zijn zelf verantwoordelijk voor het op juiste wijze toepassen van de noodzakelijke maatregelen binnen het bereik van de eigen dienstverlening.

Opslagmedia van systemen die worden gebruikt worden veilig behandeld om de opslagmedia tegen schade, diefstal en niet-geautoriseerde toegang te beschermen. Opslagmedia worden zorgvuldig verwijderd wanneer zij niet meer nodig zijn.

6.6.3 *Levenscyclus van beveiligingsclassificatie*
Classificatie wordt periodiek beoordeeld en zo nodig aangepast.

6.7 Netwerkbeveiliging

De beschikbaarheid, integriteit en exclusiviteit van de gegevens die tussen de verschillende operationele partijen worden uitgewisseld wordt geborgd met behulp van maatregelen op het gebied van netwerkbeveiliging. Communicatie over publieke netwerken tussen systemen van de operationele partijen vindt in vertrouwelijke vorm plaats. De koppeling tussen enerzijds de publieke netwerken, en anderzijds de netwerken van de kaartuitgever, personalisator en certificaatproducent zijn voorzien van stringente veiligheidsmaatregelen (actuele firewall, virusscanners, proxy).

6.8 Time-stamping

De DH BCT biedt geen time-stamping dienstverlening aan derden aan.

7 Certificaat en CRL profielen

7.1 Certificaatprofielen

De certificaten die worden uitgegeven voor gebruik op de BCT kaarten en systeemkaarten voldoen aan de profielen in het document "Certificaatprofielen en CRL Model BCT Kaarten versie 1.3".

7.2 CRL profiel

Het profiel van de CRL die door de DH BCT wordt uitgegeven wordt beschreven in het document "Certificaatprofielen en CRL model BCT Kaarten versie 1.3".

7.3 OCSP profiel

Na een wijziging in de EU regelgeving dient de DH BCT een OCSP functie te ondersteunen. De implementatie hiervan wordt momenteel voorbereid. Zodra de functie beschikbaar is, wordt dit CPS op dit punt aangepast.

8 Conformiteitsbeoordeling

De TSP dienstverlening van het Ministerie van Infrastructuur en Waterstaat is per 20-2-2012 gecertificeerd tegen 'Scheme for certification of Certification Authorities tegen ETSI EN 319 411-2 en ETSI TS 102 042 en voldoet daarmee aan de eisen zoals gesteld aan Certificatiedienstverleners in ETSI EN 319 411-2 en daarmee aan de eisen uit de Wet elektronische handtekening (Weh). De norm ETSI TS 101 456 is opgevolgd door ETSI EN 319 411-2 (in combinatie met ETSI EN 319 401).
Een vernieuwing van deze certificering heeft plaatsgevonden op 16-1-2017 door BSI Group The Netherlands B.V. (hierna: BSI).

Verordening elektronische identiteiten en vertrouwensdiensten (eIDAS)
Op 1 juli 2016 is de Europese Verordening (VERORDENING (EU) Nr. 910/2014 VAN HET EUROPEES PARLEMENT EN DE RAAD van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG) van kracht geworden. Deze verordening vervangt de Wet Elektronische Handtekening.

Omdat in deze verordening de eisen t.a.v. frequentie van de audit en de accreditatie zijn opgenomen is het TTP.NL Scheme per die datum vervallen.

Ook zijn de eerdere ETSI certificeringen in februari 2015 ETSI TS 101 456 vervangen door ETSI ETSI EN 319 411-2 en een nieuw certificaat voor ETSI TS 102 042.

Het Ministerie van Infrastructuur en Waterstaat voldoet tevens aan de relevante onderdelen van het Programma van Eisen van de PKIoverheid zoals gesteld in het Programma van Eisen(zie hiervoor https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-tsp/programma-van-eisen/). Dit is aantoonbaar met behulp van een door BSI Group The Netherlands B.V. afgegeven auditverklaring.

Een afschrift van het ETSI TS 102 042 en het ETSI EN 319 411-2-certificaat staan vermeld op de site van de Trust Service Provider (http://csp.minIenM.nl/) en DH BCT (http://bct.csp.minIenM.nl/ en zie certificeringsbeleid).

De door de betreffende auditors opgestelde auditrapporten zijn vanuit beveiligingsoogpunt geheim. Ze worden niet beschikbaar gesteld aan derden en zijn alleen op verzoek en onder strikte geheimhouding in te zien.

Met ingang van 10 maart 2017 is Agentschap Telecom (hierna AT) aangewezen als wettelijk toezichthouder op de eIDAS verordening.
Per 16-01-2017 is het Ministerie van Infrastructuur en Waterstaat voor ETSI EN 319 411-2 en ETSI TS 102 042.).

Per 1 juli 2017 wordt tevens gecertificeerd tegen Verordening eIDAS (elektronische identificatie en vertrouwensdiensten voor elektronische transacties) [1].

Binnen de TSP is de DH BCT verantwoordelijk voor de eigen dienstverlening. Deze verantwoordelijkheid komt tot uiting in het eigenstandig behalen van een

deelcertificering conform de eIDAS en de ETSI normen (zie hiervoor gaande opgenomen voetnoot).[2]

8.1 Auditcyclus

In Uitvoeringswet verordening eIDAS is onder andere verwoord met welke frequentie de audit wordt uitgevoerd, aan welke eisen de certificerende instelling moet voldoen en hoe omgegaan wordt met zogenaamde non-conformities. Een certificerende instelling moet alvorens te kunnen certificeren geaccrediteerd zijn door een IAF-lid (International Accreditation Forum) tegen ISO 17065.

De auditcyclus wordt uitgevoerd volgens ETSI EN 319 403 certificatieschema. De TSP en DH BCT ondergaan eenmaal per 2 jaar een certificatieaudit. In de tussenliggende jaren wordt jaarlijks een volledige controle audit uitgevoerd. Als op beleidsmatig of technisch vlak grotere wijzigingen worden doorgevoerd, kan een tussentijdse conformiteitsaudit worden uitgevoerd.
Naast deze audits laat de TSP gezamenlijk met DH BCT een interne audits uitvoeren.

Naast deze audits houdt de TSP toezicht op de DH BCT. De DH BCT houdt op zijn beurt, deels via de kaartuitgever, toezicht op de operationele partijen die gezamenlijk de dienstverlening vormgeven.

8.2 Certificerende instelling

Certificatieaudit en controle audits worden uitgevoerd door een geaccrediteerde organisatie. Deze organisatie dient geaccrediteerd te zijn door een IAF lid (International Accreditation Form) tegen ISO 17065.

8.3 Relatie met certificerende instelling

De auditoren die de audits uitvoeren zijn onafhankelijk. Er is geen verdere relatie tussen het MinIenW en de certificerende instelling.

8.4 Onderwerp van audit

Tijdens de audits wordt beoordeeld in hoeverre het managementsysteem voor het uitgeven van (gekwalificeerde) certificaten blijvend voldoet aan de eisen in de normen:

- ETSI EN 319 411-1, (ten behoeve van de ondernemerskaart, keuringskaart en systeemkaart niet op naam), inclusief de hierin verwezen normen in de CABforum Baseline Requirements en de Network Security Controls.
- ETSI EN 319 411-2, (ten behoeve van de chauffeurskaart en inspectiekaart op naam)
- eisen uit de Verordening elektronische identiteiten en vertrouwensdiensten (de eIDAS-Verordening)
- het Programma van Eisen PKIoverheid delen 3a, 3b en 3d.

De audit is uitgevoerd op de volgende onderwerpen en processen:

- Registration Service;
- Certificate Generation Service;
- Dissemination Service;
- Revocation Management Service;
- Subject Device Provision Service;
- Revocation Status Service

8.5 Resultaten audit

Als bij de audit tekortkomingen worden geconstateerd, stelt de TSP en DH BCT binnen 15 dagen na ontvangst van het definitieve auditrapport een plan van aanpak op om de geconstateerde afwijkingen te analyseren en doeltreffende corrigerende maatregelen te nemen.

8.6 Beschikbaarheid conformiteitcertificaten

De conformiteitcertificaten van de meest recente audits zullen beschikbaar zijn op de website van het Trust Service Provider (BCT) en in de elektronische opslagplaats van de Policy Authority van de PKI voor de overheid. De TSP en DH BCT voldoen tevens aan het normenkader van de PKI voor de overheid zoals gesteld in het Programma van Eisen (zie hiervoor http://www.logius.nl).

9 Algemene en juridische bepalingen

Het ministerie van IenW is de eindverantwoordelijke certificatiedienstverlener en eveneens verantwoordelijk voor de delen die zijn uitbesteed aan andere organisaties. De ILT, als DH BCT, heeft de feitelijke kaartuitgifte uitbesteed aan Kiwa Register B.V. De personalisatie van de BCT kaarten en het aanmaken van de sleutelparen wordt verzorgd door Morpho, terwijl de productie van de certificaten is uitbesteed aan KPN.

9.1 Tarieven

In dit CPS zijn geen tarieven opgenomen. Informatie over de tarieven is te vinden in de 'Regeling vergoeding documenten Wet personenvervoer 2000'.

9.2 Financiële verantwoordelijkheid en aansprakelijkheid

De DH BCT heeft adequate regelingen getroffen om aansprakelijkheden die verband houden met onderhavige dienstverlening af te dekken. De verhaalbaarheid van aansprakelijkheidsclaims betreffende deze dienstverlening is geborgd door de financiële positie van de DH BCT, het Ministerie van IenW en in breder verband de Staat der Nederlanden (Rijksoverheid).

De DH BCT heeft voor de certificatiedienstverlening geen aparte verzekering afgesloten. Het is immers overheidsbeleid dat de Staat zich niet verzekert.

Zie voor aansprakelijkheid verder paragraaf 9.6.

9.3 Vertrouwelijkheid van bedrijfsgegevens

Op basis van de Wet openbaarheid van bestuur (Wob) kan een ieder een verzoek doen aan de DH BCT om documenten te overleggen.

Bij de beoordeling van een verzoek om openbaarmaking van documenten wordt getoetst aan hetgeen bepaald is in de Wob.

9.4 Vertrouwelijkheid van persoonsgegevens

Alle uitgevoerde handelingen die van belang zijn in het registratieproces worden vastgelegd. Hierbij worden zo min mogelijk persoonsgegevens vastgelegd. In ieder geval worden geen (persoons)gegevens vastgelegd die niet van belang zijn voor het registratieproces.

De certificaathouders hebben recht op inzage en correctie van hun persoonsgegevens. Ook kan de certificaathouder bij de DH BCT nagaan of en zo ja wie inzage heeft gehad in deze gegevens.

9.4.1 Vertrouwelijke informatie

De informatie die door de DH BCT wordt verkregen over een persoon, zijnde een natuurlijk persoon of rechtspersoon, wordt vertrouwelijk behandeld. De eisen gesteld in de Wet bescherming persoonsgegevens (Wbp) zijn hierop uitdrukkelijk van toepassing.

Tenminste de volgende documenten bevatten informatie die als vertrouwelijk worden beschouwd en worden dan ook niet aan derden verstrekt:

- informatie in het kader van de registratie en certificering van partijen;
- overeenkomsten met (toe)leveranciers en dienstverleners;
- beveiligingsprocedures en maatregelen;
- procedures Administratieve Organisatie (AO);
- audit rapporten.

9.4.2 Niet-vertrouwelijke informatie

De inhoud van certificaten is vrij raadpleegbaar. Echter, de door de DH BCT uitgegeven certificaten worden niet gepubliceerd. De informatie die is opgenomen in een certificaat en wordt verstrekt met betrekking tot ingetrokken certificaten is beperkt tot hetgeen in hoofdstuk 7 'Certificaat-, CRL- en OCSP-profielen' van voorliggend CPS vermeld is.

Informatie met betrekking tot intrekking van certificaten is beschikbaar via de CRL. De CRL bevat alleen informatie over ingetrokken certificaten. De daar gegeven informatie betreft per certificaat het certificaatnummer, het moment van intrekking, de reden van intrekking en optioneel het vermoedelijke tijdstip waarop de intrekkingsreden van kracht is geworden.

9.4.3 Vrijgeven van informatie

Als in het kader van een straf- of tuchtrechtelijk onderzoek niet-openbare informatie uit het DH BCT register wordt opgevraagd door een bevoegde opsporingsambtenaar, dan wordt deze informatie door de DH BCT vrijgegeven. De eisen gesteld in de Wbp zijn hierop uitdrukkelijk van toepassing.

Als door een abonnee of certificaathouder in een civiele procedure niet-openbare informatie uit het DH BCT register wordt opgevraagd ten behoeve voor het leveren van bewijs van certificatie, dan wordt deze informatie vrijgegeven door de DH BCT, als naar het oordeel van deze laatste er geen sprake is van een zwaarwegend belang dat zich verzet tegen de genoemde gegevensverstrekking. Als tot gegevensverstrekking zal worden overgegaan, wordt de betrokkene hiervan op de hoogte gesteld.

Vertrouwelijke gegevens zullen slechts ter bewijsvoering aan andere partijen dan de abonnee of certificaathouder worden verstrekt met voorafgaande schriftelijke toestemming van de abonnee of de certificaathouder.

Behoudens het hiervoor gestelde worden geen gegevens behorende bij certificaathouders of abonnees vrijgegeven aan derden, zonder dat dit uit nadere wet- en regelgeving blijkt of dat de abonnees of certificaathouders hier uitdrukkelijk toestemming voor hebben gegeven.

9.5 Intellectuele eigendomsrechten

Dit CPS is eigendom van de DH BCT. Ongewijzigde kopieën van deze CPS mogen zonder toestemming verspreid en gepubliceerd worden zolang dit met bronvermelding geschiedt.

Eigendomsrechten met betrekking tot certificaten, de BCT kaarten en systeemkaarten blijven ook na uitgifte berusten bij de Staat der Nederlanden, inclusief rechten van intellectueel eigendom.

De DH BCT garandeert jegens haar abonnees, certificaathouders en -beheerders dat de door haar uitgegeven certificaten en dragers van de private en publieke sleutel, inclusief de daarbij behorende en geleverde apparatuur en documentatie, geen inbreuk maakt op intellectuele eigendomsrechten, waaronder auteursrechten, merkenrechten en gebruikte programmatuur waarvan deze berusten bij haar (toe)leveranciers.

9.6 Aansprakelijkheid en garanties

In de Algemene Voorwaarden PKIoverheid Certificaten is de wijze opgenomen waarop de DH BCT en betrokken partijen om gaan met aansprakelijkheid en garanties.

9.7 Beperkingen in garanties

In de Algemene Voorwaarden PKIoverheid Certificaten is de wijze opgenomen waarop de DH BCT en betrokken partijen om gaan met beperkingen in garanties.

9.8 Schadeloosstelling

Niet van toepassing.

9.9 Geldigheidstermijn CPS

Het CPS is geldig vanaf de datum van publicatie. Het CPS is geldig zolang de dienstverlening van de DH BCT voortduurt of totdat het CPS wordt vervangen door een nieuwere versie. Nieuwere versies worden gepubliceerd via de elektronische opslagplaats, als beschreven in hoofdstuk 2.

9.10 Communicatie met betrokken partijen

Geen nadere bepalingen.

9.11 Wijzigingen

De DH BCT heeft het recht het CPS te wijzigingen en/of aan te vullen. De werking van het geldende CPS wordt jaarlijks beoordeeld door de TSP.

Abonnees, certificaathouders, certificaatbeheerders en vertrouwende partijen kunnen op- en aanmerkingen plaatsen met de betrekking tot de inhoud van het CPS en deze indienen bij de DH BCT. De contactgegevens van de DH BCT staan vermeld in paragraaf 1.5.1. Indien de DH BCT, evt. in overleg met de TSP, op grond van de op- en aanmerkingen vaststelt dat wijzigingen in het CPS noodzakelijk zijn, worden deze wijzigingen doorgevoerd.

Bij wijziging van het CPS wordt de impact bepaald voor de handhavingapplicatie van ILT. Indien noodzakelijk kunnen hier dan tijdig aanpassingen worden gedaan.

Wijzigingen van tekstuele aard of correcties van schrijf- en/of spelfouten kunnen zonder voorafgaande bekendmaking in werking treden en zijn herkenbaar doordat het versienummer met 0.1.1 wordt opgehoogd. Bij wijzigingen in de PvE-delen wordt het versienummer van PKIoverheid gebruikt.

De nieuwe versie van het CPS wordt gepubliceerd op de website van de DH BCT.

9.12 Geschillenbeslechting

De DH BCT kent een klachtenprocedure en een bezwaar- en beroepprocedure.

Bezwaar tegen een beslissing over de afgifte van een BCT kaart of systeemkaart kan worden gemaakt bij:

Inspectie Leefomgeving en Transport
T.a.v. Bezwaar en Beroep
Postbus 16191
2500 BD Den Haag

Overige klachten over de dienstverlening kunnen worden gericht aan:

Kiwa Register B.V.
T.a.v. het kwaliteitsteam
Postbus 4
2280 AA, Rijswijk (ZH)
Mail: vergunningen@kiwa.nl
Tel: +31 88 9984888

9.13 Toepasselijk recht

Op de diensten van de DH BCT, voorliggend CPS en door de DH BCT vanwege de certificatiedienstverlening gesloten overeenkomsten is het Nederlands recht van toepassing.

9.14 Naleving relevante wetgeving

Overige relevante wetgeving wordt door de DH BCT in letter en geest van de wet nageleefd.

9.15 Overige bepalingen

Geen nadere bepalingen.

10 Revisies

10.1 Revisie 4.5 → 4.5.1

4.5.1	29 jan 2018	Actualisatie CPS als gevolg van ontbreken volledige beschrijving van diverse gegevens en uitkomsten BSI audit november 2017

Verantwoording wijzigingen aan CPS PvE 4.5 → 4.5.1						
nr	Eis afkomstig uit	Omschrijving	Van toepassing	Reden	Wijziging in CPS[3]	Gewijzigd / toelichting
1	Nvt	Naamswijziging Min IenW naar Min IenW doorgevoerd	ja	Actueel maken	ja	Door hele document heen
2	Nvt	Figuur 1 PKI Overheid Hiërarchie aangepast	ja	Kloppend maken	ja	Paragraaf 1.1.4
3	Nvt	Tabel 12 - Kaarttype en toepasselijke CP aangepast	ja	In lijn brengen met certificaatprofiel.	ja	Paragraaf 2.2
4	Nvt	Tabel 13 - Gegevens in certificaten aangepast	ja	In lijn brengen met certificaatprofiel.	ja	Paragraaf 3.1.1
5	Nvt	Aanvraagproces Inspectiekaarten geactualiseerd	ja	Kloppend maken	ja	Paragraaf 4.1.2 en 4.9.1
6	Nvt	Reden intrekking certificaat door DH BCT toegevoegd.	ja	Kloppend maken	ja	Paragraaf 4.9.1
7	ETSI	OCSP functie dient te worden geïmplementeerd.	ja	In lijn brengen met ETSI.	ja	Paragraaf 7.3

[3] Actuele wijzigingen zijn in rood weergegeven in dit CPS

10.2Revisie 4.4 → 4.5

4.5	6 nov 2017	Actualisatie CPS als gevolg van ontbreken volledige beschrijving van diverse gegevens Wijzigingen nav implementatie eIDAS en PvE wijzigiging 4.4 → 4.5

Verantwoording wijzigingen aan CPS PvE 4.4 → 4.5						
nr	Eis afkomstig uit	Omschrijving	Van toepassing	Reden	Wijziging in CPS[4]	Gewijzigd / toelichting
1	PvE delen 1,2 en 4	Nieuwe regelgeving eIDAS	Ja	Per 1 juli 2017 van kracht	Ja	Correcties in Hoofdstuk 8 Conformiteitsbeoordeling
2	nvt	Gecertificeerde dienst 'Revocation Status Service' toegevoegd	Ja	Suggestie auditor	Ja	H 8.4
3	nvt	Datum revisie 4.3 → 4.4 aangepast	Ja	Suggestie auditor	Ja	H 10.2
4	Nvt	Beschrijving geaccrediteerde organisatie aangepast	Ja	Bevinding auditor	ja	H 8.2

10.3 Revisie 4.3 → 4.4

4.4	20 mrt 2017	Actualisatie CPS als gevolg van ontbreken volledige beschrijving van diverse gegevens Wijzigingen nav PvE wijzigiging 4.3 → 4.4

Verantwoording wijzigingen aan CPS PvE 4.3 → 4.4						
nr	Eis afkomstig uit	Omschrijving	Van toepassing	Reden	Wijziging in CPS	Gewijzigd / toelichting
1	PvE 3b	Geldigheid services BCT kaarten naar drie jaar	Ja	De vrijstelling loopt per 23-3-2017 af.	Ja	Correctie in CPS paragraaf 1.1.2 en 6.3.2
2	BSI-audit	Toevoeging OiD's van de van issuing CA's van CSP en systeemkaarten	Ja	OiD-gegevens ontbraken in paragraaf 3.1.1, tabel 6	Ja	Correctie in CPS paragraaf 3.1.1.
3	Nvt	Post NL is AMP geworden	Ja	Distributie BCT kaarten anders geregeld.	Ja	Correctie in CPS paragraaf 3.2.3, 4.3 en 5.1.1
4	BSI-audit	Beschrijving aanvraag Inspectiekaart	Ja	Beschrijving niet overeenkomstig de werkelijkheid.	Ja	Correctie in CPS paragraaf 4.1.2
5	BSI-audit	Betere omschrijving verplichtingen vertrouwende partijen	Ja	Betere omschrijving verplichtingen vertrouwende partijen	Ja	Correctie in CPS paragraaf 4.5.3 en 4.9.6.
6	BSI-audit	Uitgiftefrequentie en geldigheidsduur	Ja	Nu wel beschreven	Ja	Correctie in CPS paragraaf 4.9.7

[4] Actuele wijzigingen zijn in rood weergegeven in dit CPS

		subordinate CA's niet beschreven				
7	BSI audit 2015	Bij audit 2015 bleek de CA termination plan niet geregeld te zijn. Na overleg is besloten geen convenant met een andere CSP te sluiten, maar om wel de te nemen maatregelen bij beëindiging te verduidelijken in het CPS.	Ja	Betere beschrijving bij beëindiging TSP dienstverlening.	Ja	Correctie in CPS paragraaf 5.8
8	BSI audit	Niet alle BCT ketenpartijen beschikken over testomgeving.	Ja	Wordt nog met keten besproken.		
9	BSI audit	Accreditatie van de certificerende instelling is gewijzigd.	Ja	Certificerende instelling moet IAF lid zijn.	ja	Correctie in CPS hoofdstuk 8

10.4Revisie 4.2 → 4.3

4.3	28-07-2016	Actualisatie gegevens Enkele redactionele wijzigingen Wijzigingen nav PvE wijzigiging 4.2 → 4.3

Verantwoording wijzigingen aan CPS PvE 4.2 → 4.3						
nr	Eis afkomstig uit	Omschrijving	Van toepassing	Reden	Wijziging in CPS	Gewijzigd / toelichting
1	ABC	Toevoeging Issuer.organizationalIdentifier in het certificaatprofiel	Ja	Nieuw	Nee	Leidt wel tot wijziging van het certificaatprofiel. (uiterlijke ingangsdatum 1 juli 2016)
2	B	Pkio153: het stellen van nadere eisen aan het gebruik van gekwalificeerde zegels	Nee	Nieuw	Nee	Dossierhouder BCT geeft geen gekwalificeerde zegels uit. (uiterlijke ingangsdatum 1 juli 2016)
3	B	Nieuwe policyidentifier en profielaanpassingen voor gebruik van gekwalificeerde zegels	Nee	Nieuw	Nee	Dossierhouder BCT geeft geen gekwalificeerde zegels uit. (uiterlijke ingangsdatum 1 juli 2016)
4	ABD	Beschrijving bij het attribuut CertificatePolicies	Ja	Aanpassing	Nee	Leidt wel tot wijziging van het certificaatprofiel. (uiterlijke ingangsdatum 1 juli 2016)
5	ABD	Verwijdering optioneel gebruik KeyAgreement bij Key Usage	Ja	Aanpassing	Nee	Leidt wel tot wijziging van het certificaatprofiel. (uiterlijke ingangsdatum 28 juli 2016)
6	A	Opname QcStatement gekwalificeerd certificaat verplicht	Ja	Aanpassing	Nee	Leidt wel tot wijziging van het certificaatprofiel. (uiterlijke ingangsdatum 1 juli 2016)
7	ABD	ETSI TS 102 176-1 vervangen door ETSI TS 119 312	Nee	Aanpassing	Nee	ETSI TS 102 176-1 is niet van toepassing op de Dossierhouder BCT
8	ABD	Gebruik van waarden binnen het BasicConstraints veld niet meer toegestaan in eindgebruikerscertificaten	Ja	Aanpassing	Nee	Leidt wel tot wijziging van het certificaatprofiel. (uiterlijke ingangsdatum 1 juli 2016)

9	A	Gebruik van “Any ExtendedKeyUsage” in eindgebruikerscertificaten niet meer toegestaan	Ja	Aanpassing	Nee	Leidt wel tot wijziging van het certificaatprofiel. (uiterlijke ingangsdatum 1 november 2016)
10	BD	Vervallen eis pkio95 ivm dubbeling met ETSI EN 319 411-1	Ja	Aanpassing	Nee	Eis pkio95 is niet opgenomen in dit CPS
11	BD	ETSI TS 102 042 is vervangen door ETSI EN 319 411-1	Ja	Aanpassing	Ja	Ingangsdatum 1-7-2016 of zoveel later als de accreditatie aan de certificerende instelling is verleend met een uiterste datum van 30 juni 2017.
12	B	Eis 7.1-pkio150 aangepast (niet toegestane EKU verwijderd)	Ja	Aanpassing	Nee	Leidt wel tot wijziging van het certificaatprofiel. (uiterlijke ingangsdatum 1 november 2016)
13	ABD	Verwijzingen naar G1 (verlopen) verwijderd en naar G3 (domeinen) verduidelijkt.	Ja	Redactioneel	Nee	Verwijzing naar G1 niet opgenomen in CPS
14	DH BCT	Adres contactgegevens DH BCT en bezwaar en beroep gewijzigd.	Ja	Redactioneel	Ja	
15	DH BCT	Versienummering aangepast aan nummering PvE wijziging	Ja	Redactioneel	Ja	Ter verduidelijking
16	DH BCT	Certificering TTP.nl verwijderd en certificering ihkv Uitvoeringswet eIDAS verordening aangekondigd.	Ja	Redactioneel	Ja	Op pagina 15 geactualiseerd naar huidige juridische status
17	DH BCT	Telefoonnummer KIWA gewijzigd	Ja	Redactioneel	Ja	Op pagina 32, 38 en 52
18	DH BCT	Artikel 2 Besluit elekronische handtekening vervangen door artikel 24 eIDAS	Ja	Aanpassing	Ja	Op pagina 35

10.5Revisie 4.1 → 4.2

4.2	28-01-2016	Actualisatie gegevens Enkele redactionele wijzigingen Wijzigingen nav PvE wijzigiging 4.1 → 4.2

Verantwoording wijzigingen aan CPS PvE 4.1 → 4.2						
nr	Eis afkomstig uit	Omschrijving	Van toepassing	Reden	Wijziging in CPS	Gewijzigd / toelichting
1	A	Eis 7.1-pkio149	Ja	Nieuw	Nee	Uiterlijke ingangsdatum 1 juli 2016
2	B	Eis 6.3.2-pkio148	Ja	Nieuw	Nee	Uiterlijke ingangsdatum direct na publicatie PvE. Deze eis stelt dat services certificaten nog maar voor een periode van 3 jaar mogen worden uitgegeven. N.a.v. deze change (die stevige gevolgen zou hebben voor de taxibranche) is door de CSP een verzoek

						ingediend bij de PA om de services certificaten toch voor 5 jaar te mogen blijven uitgeven. Dit verzoek is voor de duur van 1 jaar (tot 10 oktober 2016) gehonoreerd. Jaarlijks wordt een nieuw verzoek hieromtrent ingediend. Om deze reden is deze change ook niet verwerkt in dit CPS.
3	B	Eis 7.1-pkio150	Ja	Nieuw	Nee	Uiterlijke ingangsdatum 1 juli 2016
4	D	Eis 7.1-pkio151	Ja	Nieuw	Nee	Uiterlijke ingangsdatum 1 juli 2016
5	B	Certificaatprofiel: gebruik van subjectAltName van “niet toegestaan” naar “optioneel” veranderd.	Ja	Aanpassing	Nee	Leidt wel tot wijziging van het certificaatprofiel.
6	B	Verbod op uitgifte van 5 jarige services certificaten naar 3 jarige, hierdoor is eis 6.3.2-pkio109 verwijderd en 6.3.2-pkio148 toegevoegd.	Ja	Aanpassing	Nee	Zie opmerking onder 2.

10.6Revisie 4.0 → 4.1

4.1[5]	28-07-2015	Actualisatie gegevens Enkele redactionele wijzigingen Wijzigingen nav PvE wijzigiging 4.0 → 4.1

Verantwoording wijzigingen aan CPS PvE 4.0 → 4.1						
nr	Eis afkomstig uit	Eisnummer	Van toepassing	Reden	Wijziging in CPS	Gewijzigd / toelichting
1	ABD	Certificering tegen ETSI TS 102 042	Ja	Nieuw	Ja	Zie H 8 Conformiteitsbeoordeling
2	A	Beschrijving bij het attribuut Subject.organizationName	Ja	Aanpassing	Nee	Leidt wel tot wijziging van het certificaatprofiel.
3	B	Eis 6.3.2-pkio109	Nee	Aanpassing	Nee	
4	A	Eis 3.1.3-pkio11	Ja	Redactioneel	Nee	
5	A	Eis 3.2.5-pkio32	Ja	Redactioneel	Nee	
6	ABD	Eis 5.7.4-pkio86	Ja	Redactioneel	Nee	
7	A	Eis 5.5.1-pkio82	Ja	Redactioneel	Nee	

10.7Revisie 3.7 → 4.0

Verantwoording wijzigingen aan CPS PvE 3.7 → 4.0						
nr	Eis afkomstig uit	Eisnummer	Van toepassing	Reden	Wijziging in CPS	Gewijzigd / toelichting
1	A	Eis 5.5.1-pkio82	Ja	Nieuw	nee	

[5] Vanaf deze versie de nummering van de PvE wijzigingen aangehouden

2	B	Certificering tegen EN319-411-3	Ja	Nieuw	ja	Zie H 8 Conformiteitsbeoordeling
3	ABD	PvE eisen zijn omgenummerd volgens een nieuwe naming convention;	Ja	aanpassing	nee	In CPS staan PvE eisen niet genummerd weergegeven
5	ABD	De creatie van een baseline en een aanvullende eisen document;		aanpassing	nee	
6	ABD	Inhoudelijke wijzigingen aan eisen zijn terug te vinden in de baseline en het aanvullende eisen document.		aanpassing	nee	
7	B	Voormalig deel B is nu opgedeeld in 2 delen, services (deel B) en server (deel E)		aanpassing	nee	Alleen deel B is/blijft van toepassing, server certificaten worden niet uitgegeven.
8	ABD	Redactionele wijzigingen aan eisen zijn terug te vinden in de baseline en het aanvullende eisen document. Deze hebben echter geen gevolgen voor de inhoud van de informatie.	ja	Redactioneel	nee	Wijzigingen hebben geen gevolgen voor de inhoud van de informatie.

10.8Revisie 3.6 → 3.7

Verantwoording wijzigingen aan CPS PvE 3.6 → 3.7						
nr	Eis afkomstig uit	Eisnummer	Van toepassing	Reden	Wijziging in CPS	Gewijzigd / toelichting
1	B	6.1.1-5	Nee	Redactioneel	Nee	
2	A	6.2.11-1	Ja	Redactioneel	Nee	
3	A	Voor de extensie subjectDirectoryAttributes in het certificaatprofiel in Bijlage A is de kolom 'Critical?' gevuld met het woord 'Nee'.	Nee	Aanpassing	Nee	Jacob zoekt uit ivm Server certificaten Niet in gebruik, geen aanpassing nodig in Certificaatprofiel.
4	B	De volgende PKIo eisen zijn aangepast naar aanleiding van het rechstreeks toesten tegen de normen van de Baseline Requirements via ETSI TS 102 042 PTC-BR: 2.2-5, 2.4-1, 4.1-1, 4.9.1-1, 4.9.3-4, 4.9.7-1, 4.9.9-2, 4.9.9-6, 5.3.2-1, 5.4.1-1, 5.7.4-1, 6.1.1-1, 7.3-1	Nee	Aanpassing	Nee	Idem Geen impact aangezien de Baseline Requirements gaan over services server en geen betrekking hebben op services Aut. en Vertr. Zie PvE deel 3b par. 1.1.1 Ter info: dit wordt in PvE versie 4 duidelijker omdat dan de volgende splitsing komt in PvE delen: • Deel 3a persoonsgebonden certificaten in het domein organisatie • Deel 3b services authenticiteits- en vertrouwelijkheidcertificaten in het domein organisatie • n.v.t. Deel 3c persoonsgebonden certificaten in het domein burger

						• Deel 3d service en server certificaten in het domein autonome apparaten • n.v.t. Deel 3e website en server certificaten in het domein organisatie • n.v.t. Deel 3f Extended Validation certificaten onder het EV stamcertificaat • n.v.t. Deel 3g services authenticiteit- en vertrouwelijkheidcertificaten in het domein private services • n.v.t. Deel 3h server certificaten in het domein private services • n.v.t. Deel 3i persoonsgebonden certificaten in het domein private personen
5	B	De volgende eisen zijn verwijderd als PKIoverheid eisen en worden nu getoest tegen de normen van de Baseline Requirements via ETSI TS 102 042 PTC-BR: 2.2-4, 3.2.5-3, 4.9.9-3, 4.9.9-7, 4.9.9-8, 4.10.1-15.3.1-1, 5.5.1-2, 5.5.2-2, 6.3.2-2		Aanpassing	Nee	Idem Zie hierboven

10.9Revisie 1.0 t/m 2.1

Versie	Datum	Samenvatting aanpassing(en)
1.0	20-12-2012	Definitief vastgesteld
1.1	06-02-2014	Actualisatie gegevens Wijzigingen nav PvE wijzigiging 3.4 → 3.5
2.0	20-11-2014	Actualisatie gegevens Enkele redactionele wijzigingen Wijzigingen nav PvE wijzigiging 3.5 → 3.6 en 3.7
2.1	28-01-2015	Actualisatie gegevens Enkele redactionele wijzigingen Wijzigingen nav PvE wijzigiging 3.7 → 4.0

Bijlage A Definities

Term	Definitie
Aanvrager	een natuurlijke persoon (Beroepsgebonden Certificaten) of rechtspersoon (Organisatiegebonden Certificaten) die een Certificaataanvraag tot uitgifte van een Certificaat indient bij de Dossierhouder BCT. De Aanvrager hoeft niet dezelfde partij te zijn als de Abonnee of de Certificaathouder, maar is wel één van beide.
Abonnee	de natuurlijke persoon (Beroepsgebonden Certificaten) of rechtspersoon (Organisatiegebonden Certificaten) die een overeenkomst aangaat met de Dossierhouder BCT om uitgifte van PKIoverheid Certificaten aan door de Abonnee aangewezen Certificaathouders te bewerkstelligen.
Sleutelpaar	een Publieke Sleutel en Private Sleutel binnen de public key cryptografie die wiskundig zodanig met elkaar zijn verbonden dat de Publieke Sleutel en de Private Sleutel elkaars tegenhanger zijn. Wordt de ene sleutel gebruikt om te versleutelen, dan móet de andere gebruikt worden om te ontsleutelen en omgekeerd.
Authenticatie	(1) Het controleren van een identiteit voordat informatieoverdracht plaatsvindt; (2) het controleren van de juistheid van een boodschap of afzender.
Authenticiteitcertificaat	Certificaat waarin de Publieke Sleutel wordt gecertificeerd van het Sleutelpaar dat voor identificatie- en authenticatiediensten wordt gebruikt.
Autonoom Apparaat Certificaat	een op een SSCD opgeslagen Niet-Gekwalificeerd Certificaat dat de functie van authenticiteit ondersteunt en uitsluitend wordt uitgegeven aan apparaten die in hun operationele levensfase zelfstandig de integriteit en authenticiteit van (meet)gegevens waarborgen ten behoeve van (een specifiek doel binnen een kerntaak van) een bepaalde overheidsinstantie. Het Certificaat voldoet aan de volgende vereisten: a) ze zijn uitgegeven aan een bovengenoemd apparaat, en; b) ze zijn uitgegeven op basis van de binnen de PKIoverheid geldende „Certificate Policy Domein Autonome Apparaten”.
Beroepsgebonden Certificaat	een op een SSCD opgeslagen combinatie een Niet-Gekwalificeerd Certificaat dat de functie van authenticiteit ondersteunt, en een Gekwalificeerd Certificaat dat de functie van Onweerlegbaarheid ondersteunt, en die uitsluitend worden uitgegeven aan een beoefenaar van een Erkend Beroep. De Certificaten voldoen aan de volgende vereisten: a) ze zijn uitgegeven aan een natuurlijke persoon, die het Certificaat gebruikt of gaat gebruiken uit hoofde van zijn/haar beroep, en; b) ze zijn uitgegeven op basis van de binnen de PKIoverheid geldende „Certificate Policy Domein Overheid/Bedrijven en Organisatie”.
Bevoegd	De vertegenwoordiger van de Abonnee die bevoegd is de

Term	Definitie
Vertegenwoordiger	Abonnee te vertegenwoordigen als het Certificatiediensten betreft.
CA-Certificaat	een Certificaat van een Certification Authority.
CA-Sleutels	het Sleutelpaar, de Private en de Publieke Sleutel van een Certification Authority.
Certificaat	de Publieke Sleutel van een Eindgebruiker, samen met aanvullende gegevens. Een Certificaat is vercijferd met de Private Sleutel van de Certification Authority die de Publieke Sleutel heeft uitgegeven, waardoor het Certificaat onvervalsbaar is.
Certificaataanvraag	de door een Aanvrager ingediend verzoek om uitgifte van een Certificaat door de Dossierhouder BCT.
Certificaatbeheerder	een natuurlijke persoon die bevoegd is om namens de Abonnee en ten behoeve van de Certificaathouder een Certificaat aan te vragen, te installeren, te beheren en/of in te trekken. De Certificaatbeheerder voert handelingen uit waartoe de Certificaathouder zelf niet in staat is.
Certificaathouder	een entiteit die geïdentificeerd wordt in een Certificaat als de houder van de Private Sleutel behorende bij de Publieke Sleutel die in het Certificaat gegeven wordt.
Certificaatprofiel	een beschrijving van de inhoud van een Certificaat. Ieder soort Certificaat (handtekening, vertrouwelijkheid, e.d.) heeft een eigen invulling en daarmee een eigen beschrijving – hierin staan bijvoorbeeld afspraken omtrent naamgeving e.d.
Certificate Policy (CP)	een benoemde verzameling regels die de toepasbaarheid van een Certificaat aangeeft voor een bepaalde gemeenschap en/of toepassingsklasse met gemeenschappelijke beveiligingseisen. Met behulp van een CP kunnen Abonnees en Vertrouwende partijen bepalen hoeveel vertrouwen zij kunnen stellen in het verband tussen de Publieke Sleutel en de identiteit van de houder van de Publieke Sleutel. De van toepassing zijnde CP's zijn opgenomen in het PvE van de PKIoverheid. Het betreft hier het deel 3a Certificate Policy – Domein Overheid/Bedrijven en Organisatie, het deel 3b Certificate Policy – Services en het deel 3d Certificate Policy – Autonome Apparaten, bijlagen bij CP Domein Overheid/Bedrijven en Organisatie
Certificaten Revocatie Lijst (CRL)	een openbaar toegankelijke en te raadplegen lijst van ingetrokken Certificaten, ondertekend en beschikbaar gesteld door de uitgevende TSP.
Dossierhouder BCT (CA)	een organisatie die Certificaten genereert en intrekt. Het functioneren als CA is een deelactiviteit die onder de verantwoordelijkheid van de TSP wordt uitgevoerd.
Certificatiediensten	het afgeven, beheren en intrekken van Certificaten door Certificatiedienstverleners.
Certificate Practice Statement (CPS)	een document dat de door een TSP gevolgde procedures en getroffen maatregelen ten aanzien van alle aspecten van de dienstverlening beschrijft. Het CPS beschrijft daarmee op welke wijze de TSP voldoet aan de eisen zoals gesteld in de van toepassing zijnde CP.
Certificate Practice Statement PKIoverheid (CPS PKIoverheid)	de onderhavige CPS, zoals van toepassing op de uitgifte door de Dossierhouder BCT van PKIoverheid Certificaten alsmede het gebruik daarvan.

Term	Definitie
Certificatie-dienstverlener	een natuurlijke persoon of rechtspersoon die als functie heeft het verstrekken en beheren van Certificaten en sleutelinformatie, met inbegrip van de hiervoor voorziene drager (SSCD). De Certificatiedienstverlener heeft tevens de eindverantwoordelijkheid voor het leveren van de Certificatiediensten waarbij het niet uit maakt of het de feitelijke werkzaamheden zelf uitvoert of deze uitbesteedt aan anderen.
Trust Service Provider (TSP)	zie Certificatiedienstverlener.
Eindgebruiker	een natuurlijke persoon of rechtspersoon die binnen de PKIoverheid één of meer van de volgende rollen vervult: Abonnee, Certificaathouder of VertrouwendePartij.
Elektronische Handtekening	elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie. Door het plaatsen van een Elektronische Handtekening staat vast dat iemand die zegt een document te hebben ondertekend, dat ook daadwerkelijk heeft gedaan.
Elektronische Opslagplaats	locatie waar relevante informatie ten aanzien van de dienstverlening van de Dossierhouder BCT is te vinden.
Erkend beroep	Voor beroepsgebonden Certificaathouders gelden dat zij een erkend beroep moeten uitoefenen om Certificaten binnen de PKIoverheid te kunnen aanvragen. Een erkend beroep is in dit verband een beroep waarbij sprake is van: · een door de betreffende beroepsgroep erkend (beroeps)register waarbij een wettelijk geregeld tuchtrecht van toepassing is en waarbij inschrijving in het register verplicht is om het beroep uit te mogen oefenen; · wettelijke eisen voor het uitoefenen van het beroep, waarbij een geldig bewijs (bv. een vergunning) moet worden verkregen om het beroep te mogen uitoefenen.
Escrow (Key-Escrow)	Een methode om tijdens uitgifte van een Certificaat een kopie te genereren van de Private Sleutel ten behoeve van toegang tot versleutelde gegevens door daartoe bevoegde partijen, alsmede de beveiligde bewaarneming daarvan.
Gegevens voor het aanmaken van Elektronische Handtekeningen	zie Signature Creation Data.
Gegevens voor het verifiëren van een Elektronische Handtekening	zie Signature Verification Data.
Gekwalificeerd Certificaat	een Certificaat dat voldoet aan de eisen, gesteld krachtens artikel 18.15, tweede lid van de Telecommunicatiewet, en is afgegeven door een Certificatiedienstverlener die voldoet aan de eisen gesteld krachtens artikel 18.15, eerste lid van de Telecommunicatiewet. Het Certificaat dient tevens te strekken tot toepassing van de Gekwalificeerde Elektronische Handtekening.

Term	Definitie
Gekwalificeerde Elektronische Handtekening	een Elektronische Handtekening die voldoet aan de volgende eisen: a) het is op unieke wijze aan de ondertekenaar verbonden; b) het maakt het mogelijk de ondertekenaar te identificeren; c) het komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; d) het is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord; e) het is gebaseerd op een Gekwalificeerd Certificaat als bedoeld in artikel 1.1 onderdeel dd van de Telecommunicatiewet; f) het is gegenereerd door een veilig middel voor het aanmaken van Elektronische Handtekeningen als bedoeld in artikel 1.1 onderdeel gg van de Telecommunicatiewet.
Groepscertificaat	een op een SSCD opgeslagen combinatie van twee Niet-Gekwalificeerde Certificaten die tezamen de functies van vertrouwelijkheid en authenticiteit ondersteunen en die voldoen aan de volgende vereisten: a) ze zijn uitgegeven aan een dienst of een functie, deel uitmakend van de Abonnee (organisatorische entiteit), en b) ze zijn uitgegeven op basis van de binnen de PKIoverheid geldende Certificate Policy Services
Hardware Security Module	De randapparatuur dat wordt gebruikt aan de server kant om cryptografische processen te versnellen. Met name dient hierbij gedacht te worden aan het aanmaken van sleutels.
Veilig middel voor het aanmaken van Elektronische Handtekeningen	zie Signature Creation Device.
Niet-Gekwalificeerd Certificaat	een Certificaat dat niet voldoet aan de aan een Gekwalificeerd Certificaat gestelde eisen.
Object Identifier (OID)	een rij van getallen die op unieke wijze en permanent een object aanduidt.
Online Certificate Status Protocol (OCSP)	een methode om de geldigheid van Certificaten online (en real time) te controleren. Deze methode kan worden gebruikt als alternatief voor het raadplegen van de CRL.
Onweerlegbaarheid	de eigenschap van een bericht om aan te tonen dat bepaalde gebeurtenissen of handelingen hebben plaatsgevonden, zoals het verzenden en ontvangen van elektronische documenten.
Organisatiegebonden Certificaat	een op een SSCD opgeslagen combinatie van twee Niet-Gekwalificeerde Certificaten die tezamen de functies van authenticiteit en vertrouwelijkheid ondersteunen, alsmede een Gekwalificeerd Certificaat dat de functie van Onweerlegbaarheid ondersteunt, en die voldoen aan de volgende vereisten: a) ze zijn uitgegeven aan een natuurlijke persoon, die het Certificaat gebruikt of gaat gebruiken namens de

Term	Definitie
	Abonnee (organisatorische entiteit), en b) ze zijn uitgegeven op basis van de binnen de PKIoverheid geldende „Certificate Policy Domein Overheid/Bedrijven en Organisatie”
Policy Authority van PKIoverheid	de hoogste beleidsbepalende autoriteit binnen de hiërarchie van de PKIoverheid die de regie over de Root CA voert.
Persoonsgebonden Certificaat	een certificaat dat is uitgegeven aan een Natuurlijk Persoon. Hierbij wordt een onderscheid gemaakt tussen Organisatiegebonden en Beroepsgebonden Certificaten. Voor Organisatiegebonden Certificaten geldt dat de Certificaten worden aangevraagd door een organisatorische entiteit, die Abonnee is bij de Dossierhouder BCT, voor een Certificaathouder die onderdeel is van of een relatie onderhoudt met die organisatorische entiteit. De Certificaathouder gebruikt het Certificaat namens de organisatie. Voor Beroepsgebonden Certificaten geldt dat deze worden aangevraagd door een beoefenaar van een Erkend Beroep, die in die hoedanigheid zelf een Abonnee, maar tegelijk ook Certificaathouder is. De Certificaathouder gebruikt het Certificaat uit hoofde van zijn beroep.
PKI voor de overheid, de Public Key Infrastructure van de Staat der Nederlanden (ook wel PKIoverheid)	een afsprakenstelsel dat generiek en grootschalig gebruik mogelijk maakt van de Elektronische Handtekening, en faciliteert voorts identificatie op afstand en vertrouwelijke communicatie. Het afsprakenstelsel is eigendom van de Minister van Binnenlandse Zaken en Koninkrijksrelaties en wordt beheerd door de Policy Authority PKIoverheid.
PKIoverheid Certificaat	een onder de PKIoverheid door de Dossierhouder BCT uitgegeven Certificaat
Policy Management Authority	de organisatorische entiteit binnen de Dossierhouder BCT die verantwoordelijk is voor ontwikkelen, onderhouden en formeel vaststellen van aan de dienstverlening verwante documenten, inclusief het CPS.
Private key	zie Private Sleutel.
Private Sleutel	de sleutel van een Sleutelpaar die alleen bekend dient te zijn bij de houder ervan en strikt geheim moet worden gehouden. In het kader van de PKIoverheid wordt de Private Sleutel door de Certificaathouder gebruikt om zich elektronisch te identificeren, zijn Elektronische Handtekening te zetten of om een vercijferd bericht te ontcijferen.
Public key	zie Publieke Sleutel.
Public Key Infrastructure (PKI)	het geheel van organisatie, procedures en techniek, benodigd voor het uitgeven, gebruiken en beheer van Certificaten.
Publieke Sleutel	de sleutel van een Sleutelpaar die publiekelijk kan worden bekendgemaakt. De Publieke Sleutel wordt gebruikt voor de controle van de identiteit van de eigenaar van het Sleutelpaar, voor de controle van de Elektronische Handtekening van de eigenaar van het Sleutelpaar en voor het vercijferen van informatie voor een derde.
Regeling gebruik boordcomputer en Boordcomputerkaarten	De regeling die van toepassing zijn op alle bij de uitgifte en het gebruik van PKIoverheid Certificaten betrokken partijen.

Term	Definitie
Root	het centrale gedeelte van een (PKI-)hiërarchie waaraan de gehele hiërarchie en haar betrouwbaarheidsniveau is opgehangen.
Root Certificate	zie Stamcertificaat
Root Certification Authority (Root-CA)	een CA die het centrum van het gemeenschappelijk vertrouwen in een PKI-hiërarchie is. Het Certificaat van de Root-CA (de Root Certificate of Stamcertificaat) is self-signed, waardoor het niet mogelijk is de bron van de handtekening op dit Certificaat te authenticeren, alleen de integriteit van de inhoud van het Certificaat. De Root-CA wordt echter vertrouwd op basis van bijvoorbeeld de CP en andere documenten. De Root-CA hoeft niet noodzakelijkerwijs aan de top van een hiërarchie te zijn gepositioneerd.
Secure Signature Creation Device (SSCD):	een middel voor het aanmaken van Elektronische Handtekeningen dat voldoet aan de eisen gesteld krachtens artikel 18.17, eerste lid van de Telecommunicatiewet. Een SSCD wordt ingezet t.b.v persoonsgebonden en beroepsgebonden Certificaten. Een SSCD kan bijvoorbeeld een smartcard of een USB token zijn.
Services Certificaat	zie Groepscertificaat .
Signature Creation Data	unieke gegevens, zoals codes of private cryptografische sleutels, die door de ondertekenaar worden gebruikt om een Elektronische Handtekening te maken.
Signature Creation Device	geconfigureerde software of hardware die wordt gebruikt voor het implementeren van de gegevens voor het aanmaken van Elektronische Handtekeningen.
Signature Verification Data	gegevens, zoals codes of cryptografische Publieke Sleutels, die worden gebruikt voor het verifiëren van een Elektronische Handtekening
Sleutelpaar	unieke combinatie van Private Sleutel en Publieke Sleutel
Stamcertificaat	het Certificaat van de Root-CA. Dit is het Certificaat behorend bij de plek waar het vertrouwen in alle binnen de PKIoverheid uitgegeven Certificaten zijn oorsprong vindt. Er is geen hoger liggende CA waaraan het vertrouwen wordt ontleend. Dit Certificaat wordt door de Certificaathouder (binnen de PKIoverheid is dat de Overheids-CA) zelf ondertekend. Alle onderliggende Certificaten worden uitgegeven door de houder van het Stamcertificaat
Veilig Middel voor het aanmaken van Elektronische Handtekeningen	zie Secure Signature Creation Device.
Vertrouwelijkheid-certificaat	Certificaat waarin de Publieke Sleutel wordt gecertificeerd van het Sleutelpaar dat voor vertrouwelijkheidsdiensten wordt gebruikt.
VertrouwendePartij	de natuurlijke persoon of rechtspersoon die ontvanger is van een Certificaat en die handelt in vertrouwen op dat Certificaat.
X.509	een ISO standaard die een basis voor de elektronische opmaak van Certificaten definieert.

Bijlage B Afkortingen

Afkorting	Betekenis
BCT	Boordcomputer Taxi
BOA	Buitengewoon Opsporingsambtenaar
BSN	Burgerservicenummer
CA	Dossierhouder BCT (Certification Authority)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificaten Revocatie Lijst
ETSI	European Telecommunication Standardisation Institute
FIPS	Federal Information Processing Standards
GBA	Gemeentelijke Basis Administratie
HSM	Hardware Security Module
ILT	Inspectie Leefomgeving en Transport
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Autoriteit
PIN	Persoonlijk Identificatie Nummer
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PUK	Persoonlijk Unlock Kengetal
RFC	Request for Comments
SLA	Service Level Agreement
SSCD	Secure Signature Creation Device
TSP	Trust Service Provider ofwel Certificatiedienstverlener
VGB	Verklaring geen bezwaar
VOG	Verklaring omtrent gedrag
Weh	Wet elektronische handtekeningen
Wbp	Wet bescherming persoonsgegevens
Wid	Wet op de identificatieplicht