Inspectie Leefomgeving en Transport
Ministerie van Infrastructuur en Waterstaat

Uitgiftebeleid Boordcomputerkaarten en Systeemkaart, Certification Practice Statement (CPS)

Trust Service Provider IenW

Boordcomputer Taxi (BCT)

Datum	13 juli 2020
Status	Definitief
Versie	4.8.2 G3

Inhoud

Lijst met Tabellen

Lijst met Figuren

1 Introductie

Een Certification Practice Statement (CPS) is een schriftelijk vastgelegde verzameling regels die de door een certificaatdienstverlener of Trust Service Provider (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 Waterstaat, in dit document verder genoemd 'IenW TSP'.

De IenW TSP heeft als functie het verstrekken en beheren van Certificaten en cryptografische sleutels, met inbegrip van de hiervoor voorziene drager (QSCD). De IenW TSP heeft tevens de eindverantwoordelijkheid voor het leveren van de Vertrouwensdiensten waarbij het niet uitmaakt of het de feitelijke werkzaamheden zelf uitvoert of deze uitbesteedt aan anderen. De door de IenW TSP gevolgde procedures en getroffen maatregelen ten aanzien van alle aspecten van de Public Key Infrastructuur (PKI) staan beschreven in dit document. De werkzaamheden en verantwoordelijkheden van de IenW TSP gelden voor het uitgeven van kaarten en Certificaten voor gebruik in de Boordcomputer Taxi (BCT).

1.1 Overzicht~~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.

- **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 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 persoonsgebonden BCT-kaarten (Chauffeurs- en Inspectiekaart) en BCT-services kaarten (Ondernemers- en Keuringskaart) is vijf jaar.

De Systeemkaart heeft een geldigheidsduur van minimaal 5 jaar en maximaal tien jaar. De daadwerkelijke geldigheidsduur wordt begrensd door de verloopdatum van de CA hiërarchie.

De geldigheidsduur van de certificaten op de kaarten is in alle gevallen beperkt door de verloopdatum van de CA hiërarchie. Voor de G3 is dat 14 november 2028 voor het Root CA certificaat. Dit betekent dat een eindgebruikercertificaat maximaal tot en met 11 november 2028 geldig is.

De LWT kaart is vier maanden geldig, opgevolgd door een BCT Chauffeurskaart van 5 jaar.

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 zogenaamde IenW TSP.

De BCT-kaarten en systeemkaarten worden onder verantwoordelijkheid van de IenW TSP uitgegeven door Kiwa Register B.V. (KIWA). KIWA geeft onder mandaat van de minister van Infrastructuur en Waterstaat vergunningen uit ten behoeve van meerdere modaliteiten, zo ook de BCT-kaarten.

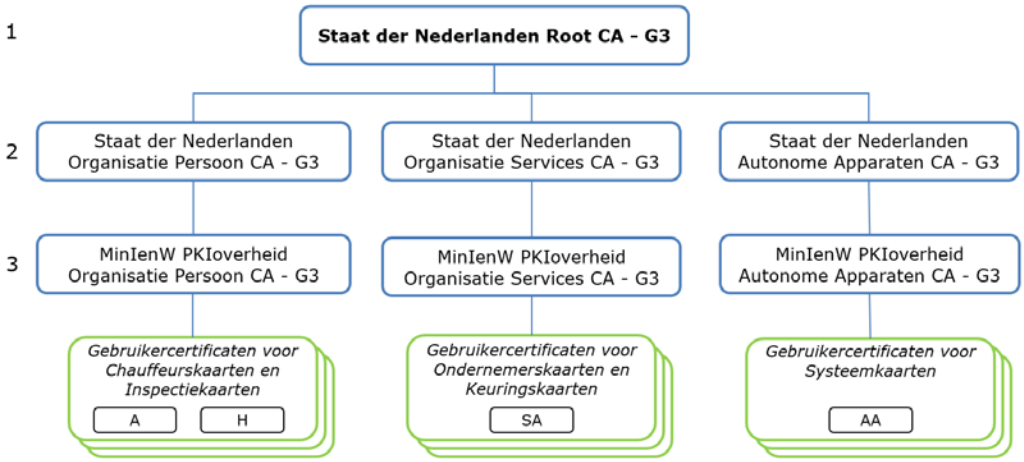
1.1.4 PKIoverheid

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 zijn verschillende domein CA's uitgegeven. Deze domein CA's zijn getekend door de Root CA en tekenen op hun beurt de TSP CA's. Deze TSP CA's ondertekenen de certificaten voor gebruikers en systemen.

De volgende figuur geeft aan voor welke domeinen de TSP van het ministerie van Infrastructuur en Waterstaat certificaten uitgeeft onder de G3 Root CA. Voor de volledigheid zijn ook de verschillende typen eindgebruikercertificaten opgenomen:

- A: Persoonsgebonden certificaat voor authenticiteit
- H: Persoonsgebonden certificaat voor gekwalificeerde elektronische handtekening
- SA: Organisatiegebonden servicescertificaat voor authenticiteit
- AA: (Autonoom) Apparaatgebonden certificaat voor authenticiteit



Figuur 1 – PKIoverheid hiërarchie G3

De hiërarchie van PKIoverheid staat beschreven in het Programma van Eisen (PvE) van PKIoverheid (deel 1, Introductie PvE). De Root CA (niveau 1) en de domein CA's (niveau 2) worden beheerd door PKIoverheid. De TSP CA's (niveau 3) zijn uitgegeven door PKIoverheid maar worden beheerd door de TSP.
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 https://www.logius.nl/diensten/pkioverheid.

1.2 Documentnaam en –identificatie~~Doel en verwijzingen CPS~~

Het CPS van de IenW TSP 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 IenW TSP 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, Certification Practice Statement', kortweg CPS.

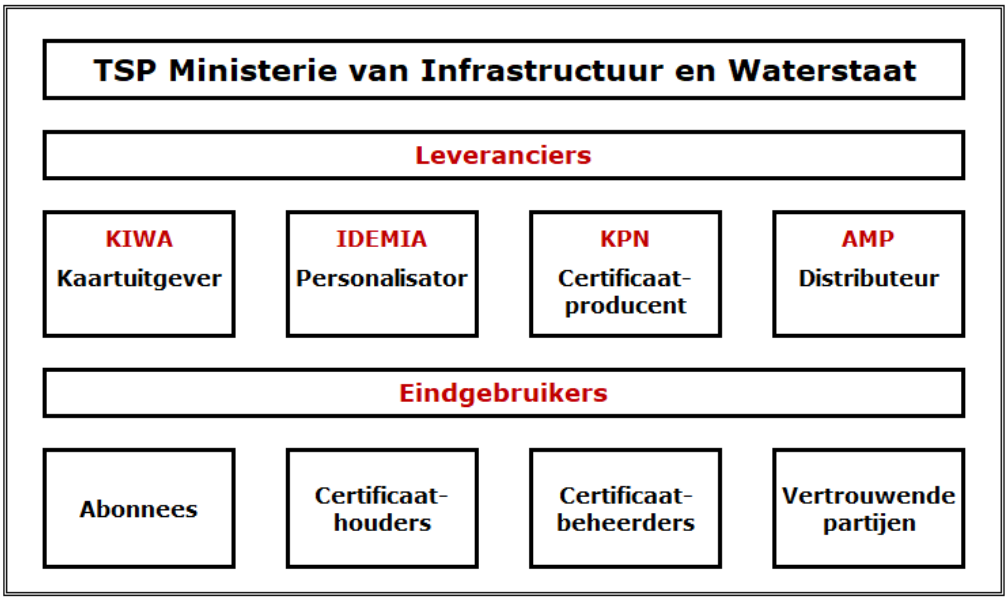
1.3 PKI betrokken partijen

~~De volgende partijen zijn betrokken bij de uitgifte van kaarten:~~
IenW TSP (belegd bij domein Rail en Wegvervoer van de ILT, die onderdeel is van ministerie van Infrastructuur en Waterstaat) is verantwoordelijk voor de uitgifte van kaarten, waarbij de volgende leveranciers van diensten en producten betrokken zijn:

- Kaartuitgever (Kiwa Register B.V.)
- Personalisator (IDEMIA The Netherlands B.V.)
- Certificaatproducent (KPN B.V.)
- Distributeur (AMP Logistics B.V.)

De volgende PKI eindgebruikers (rollen) met betrekking tot het gebruik van certificaten worden onderkend:

- Abonnees
- Certificaathouders
- Certificaatbeheerders
- Vertrouwende partijen



Figuur 2 –PKI betrokken partijen

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

De TSP CA certificaten van het ministerie van Infrastructuur en Waterstaat zijn het startpunt voor het vertrouwen binnen de hiërarchie van de PKI van dit ministerie. Dit bepaalt het vertrouwen dat wordt gesteld in alle eindgebruikercertificaten die zijn uitgegeven onder verantwoordelijk van het ministerie Infrastructuur en Waterstaat.

De 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 de TSP CA-certificaten door het toepassen van adequate beveiligingsmaatregelen.

De TSP toont het betrouwbaar functioneren aan door zich te onderwerpen aan het reguliere toezicht door de Policy Authority (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 vindt bij de TSP en gedelegeerde derden een jaarlijkse conformiteitsbeoordeling plaats.

Met de implementatie van de eIDAS Verordening (Elektronische Identificatie en Vertrouwensdiensten voor Elektronische Transacties in de Interne Markt), de nieuwe Telecommunicatiewet en de NetSec-eisen vanuit het CAB-forum wordt de auditcyclus uitgevoerd volgens het ETSI EN 319 403 certificatieschema. De IenW TSP ondergaat eenmaal per 2 jaar een certificatieaudit. In het tussenliggende jaar wordt jaarlijks een volledige controle audit uitgevoerd.

1.3.2 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 maakt gebruik van multi-factor authenticatie voor het systeem of alle gebruikersaccounts waarmee uitgifte of goedkeuring van certificaten kan worden verricht.

Wel heeft de kaartuitgever technische maatregelen geïmplementeerd, waardoor een gebruikersaccount slechts certificaataanvragen kan valideren op basis van een vooraf geaccordeerde lijst van domeinen of e-mailadressen.
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.

1.3.3 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.

1.3.4 Certificaatproducent

De certificaatproducent verzorgt de productie van aangevraagde certificaten op basis van een geauthentiseerd 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.

1.3.5 Distributeur

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

1.3.6 *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

1.3.7 *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 authentiseren 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 IenW TSP 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 authentiseren
Persoonsgebonden Handtekeningcertificaat	Dit certificaat wordt gebruikt om een elektronische handtekening te verifiëren
Services certificaat (authenticiteit)	Dit certificaat wordt gebruikt om de certificaathouder te authentiseren
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 Beheer CPS en uitgiftebeleid ~~beheer~~

1.5.1 Contactgegevens

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

Inspectie Leefomgeving en Transport
T.a.v. Trust Service Provider IenW
Postbus 20901
2500 EX Den Haag

dci.csp@minienw.nl

Meer informatie over de dienstverlening van de TSP van het ministerie van Infrastructuur en Waterstaat kan worden verkregen via https://bct.tsp.minienw.nl

1.5.2 Wijziging en goedkeuring CPS

De IenW TSP 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 Publicatie- en Bewaarverplichtingen~~Verantwoordelijkheid voor publicatie en elektronische opslagplaats~~

2.1 Elektronische opslagplaats

De elektronische opslagplaats van de IenW TSP is publiekelijk bereikbaar via https://bct.tsp.minienw.nl/

2.2 Publicatie van TSP informatie

De IenW TSP publiceert de volgende TSP-informatie:

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

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

Soort informatie	URL
CPS	https://bct.tsp.minienw.nl/minienw-bct-cps
Algemene Voorwaarden	https://bct.tsp.minienw.nl/minienw-bct-av/minienw-bct-av.pdf
CRL Chauffeurs- en Inspectiekaarten	https://bct.tsp.minienw.nl/minienw-org-pers-ca-g3.crl
CRL Ondernemers- en Keuringskaarten	https://bct.tsp.minienw.nl/minienw-org-serv-ca-g3.crl
CRL Systeemkaarten	https://bct.tsp.minienw.nl/minienw-aa-ca-g3.crl
CA Chauffeurs- en Inspectiekaarten	https://cert.pkioverheid.nl/MinIenW_PKIoverheid_Organisatie_Persoon_CA-G3.cer
CA Ondernemers- en Keuringskaarten	https://cert.pkioverheid.nl/MinIenW_PKIoverheid_Organisatie_Services_CA-G3.cer
Systeemkaarten CA	https://cert.pkioverheid.nl/MinIenW_PKIoverheid_Autonome_Apparaten_CA-G3.cer

Tabel 3 – URLs G3

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

Voor de Certificate Policies (CP) wordt doorverwezen naar https://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.

Soort Certificaat – Kaarttype	PolicyIdentifiers (OID)	CP
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.
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
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 (I&A)

3.1 Naamgeving

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

3.1.1 Soorten naamformaten

Alle certificaten die door de IenW TSP 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 Waterstaat	Ministerie van Infrastructuur en Waterstaat	Ministerie van Infrastructuur en Waterstaat	Ministerie van Infrastructuur en Waterstaat	Ministerie van Infrastructuur en Waterstaat
issuer. organizationIdentifier	NTRNL-52766179	NTRNL-52766179	NTRNL-52766179	NTRNL-52766179	NTRNL-52766179
issuer. CommonName	MinIenW PKIoverheid Organisatie Persoon CA - G3	MinIenW PKIoverheid Organisatie Services CA - G3	MinIenW PKIoverheid Organisatie Services CA - G3	MinIenW PKIoverheid Organisatie Persoon CA - G3	MinIenW PKIoverheid Autonome Apparaten CA - G3
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 onderneming]	NTRNL-[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	Nvt	[Eerste voornaam] [Verdere voorletters]	Nvt
Subject.surName	[Voorvoegsel] [Geslachtsnaam]	Nvt	Nvt	[Voorvoegsel] [Geslachtsnaam]	Nvt
Subject. SerialNumber	[Kaarthoofdtype] + [BSN] + "-" + [Kaartvolgnummer] of Kaarthoofdtype + [NI-Nummer] + "-" [Kaartvolgnummer]	[Kaarthoofdtype] + [KvK-nummer] + "-"+ [Kaartvolgnummer]	[Kaarthoofdtype] + [RDW-erkenningsnummer] + "-" + [Kaartvolgnummer]	[Kaarthoofdtype] + [Inspectienummer] + "-" + [Kaartvolgnummer]	[Kaarthoofdtype] + [Boordcomputernummer] + "-" + [Kaartvolgnummer]
Subject.Title	CVOL of CBEP	O	K	I	S
subjectAltName.otherName PermanentIdentifier. identifierValue	[Kaarthoofdtype] + [BSN] of [Kaarthoofdtype] + [NI-Nummer]	[Kaarthoofdtype] + [KvK-nummer]	[Kaarthoofdtype] + [RDW-erkenningsnummer]	[Kaarthoofdtype] + [Inspectienummer]	[Kaarthoofdtype] + [Boordcomputernummer]
PermanentIdentifier. assigner	2.16.528.1.1003.1.3.10.1.1	2.16.528.1.1003.1.3.11.1.1	2.16.528.1.1003.1.3.11.1.1	2.16.528.1.1003.1.3.10.1.1	2.16.528.1.1003.1.3.6.2.1
certificatePolicies. PolicyIdentifier	2.16.528.1.1003.1.2.5.1 (Aut) 2.16.528.1.1003.1.2.5.2 (EH)	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 2.16.528.1.1003.1.2.5.2	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.

Bij lange namen kan het voorkomen dat de IenW TSP genoodzaakt is om inkortingsregels toe te passen voor de commonName, givenName en surName.

Deze inkortingsregels zijn in detail gespecificeerd in de “MinIenW TSP PKIoverheid Certificaatprofielen BCT G3”.

Binnen PKIoverheid worden unieke OID-nummers (Object Identifiers) 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 IenW TSP.

OID	Betekenis
2.16.528.1.1003.1.3.10.1	minienw (PKIO domein organisatie persoon)
2.16.528.1.1003.1.3.10.1.1	minienw.organisatie-persoon-tsp.ca
2.16.528.1.1003.1.3.11.1	minienw (PKIO domein organisatie services)
2.16.528.1.1003.1.3.11.1.1	minienw.organisatie-services-tsp.ca
2.16.528.1.1003.1.3.6.2	minienw (PKIO domein autonome apparaten)
2.16.528.1.1003.1.3.6.2.1	minienw.autonome-apparaten-tsp.ca

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

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 IenW TSP 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 IenW TSP gebruikt worden zijn:
- **C**hauffeurskaart
- **O**ndernemerskaart
- **K**euringskaart
- **I**nspectiekaart
- **S**ysteemkaart

Voor de kaarten zijn verschillende Kaarttypes mogelijk.

Kaarttype	Gebruikersgroep	Inhoud
Chauffeurskaart	Bestuurder	CVOL of CBEP
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) 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.

3.1.2 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.

3.1.3 Anonimiteit pseudoniem en wildcards in certificaten

De IenW TSP staat het gebruik van pseudoniemen en wildcards niet toe.

3.1.4 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 IenW TSP behoudt zich het recht voor om bij registratie de aangevraagde naam aan te passen als dit juridisch of technisch noodzakelijk is.

3.1.5 *Uniciteit van namen*

De IenW TSP 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.

3.1.6 *Erkenning, authenticatie en de rol van handelsmerken*

De naam van een organisatorisch verband zoals geregistreerd in het KvK Handelsregister wordt overgenomen bij registratie en gebruikt in de certificaten. De abonnees dragen de volledige verantwoordelijkheid voor eventuele juridische gevolgen van het gebruik van de door hen opgegeven naam. De IenW TSP neemt bij het gebruik van merknamen de nodige zorgvuldigheid in acht maar is niet gehouden een onderzoek in te stellen naar mogelijke inbreuken op handelsmerken als gevolg van het gebruik van een naam die deel uitmaakt van de in het certificaat opgenomen gegevens. De IenW TSP behoudt zich het recht voor om de aangevraagde naam aan te passen als deze in strijd zou kunnen zijn met het merkenrecht.

3.2 Initiële Identiteitsvalidatie

3.2.1 *Bewijs van bezit 'private sleutel behorend bij het uit te geven certificaat'*

De IenW TSP 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	Ondernemerskaart
RDW-erkenningsnummer	Keuringkaart
ILT-nummer	Inspectiekaart
Typegoedkeuringsnummer	Systeemkaart

Tabel 9 – Aanvraaggegevens organisatorische entiteit

Op basis van de aangeleverde gegevens wordt door de IenW TSP 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 personen met dezelfde naam te kunnen onderscheiden	Chauffeurskaart*, inspectiekaart, ondernemerskaart, keuringskaart, systeemkaart

Gegevens	Kaarttype
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 IenW TSP 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 IenW TSP 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 IenW TSP vastgesteld of een aanvrager geautoriseerd is om de aanvraag namens de abonnee te doen.

3.2.6 *Verzoeken tot cross-certification en andere vormen van interoperation*

Niet van toepassing. De BCT maakt geen gebruik van cross-certification of andere vormen van interoperation.

3.3 Identificatie en Authenticatie voor Re-key-verzoeken ~~bij vernieuwing van het Certificaat~~

3.3.1 *Routinematige vernieuwing van het certificaat*

Door de IenW TSP 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~~ voor Intrekkingsverzoeken

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

Een elektronisch 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.

Bij een telefonisch verzoek tot intrekking dient de indiener van het intrekkingsverzoek een aantal vooraf vastgestelde vragen te beantwoorden. Dit stelt de IenW TSP in staat om voldoende zekerheid te verkrijgen over de identiteit van de aanvrager van de intrekking en de boordcomputerkaart waarvoor intrekking wordt aangevraagd.

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 IenW TSP. Hiervoor wordt het corresponderende formulier ingevuld, ondertekend en voorzien van de benodigde bewijsstukken schriftelijk bij de IenW TSP 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 en de algemene voorwaarden. De abonnee is gehouden aan de Regeling gebruik Boordcomputer en boordcomputerkaarten.

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 IenW TSP ingediend.
De door de Abonnee aangewezen contactpersoon kan een aanvraag voor een Inspectiekaart per mail indienen via **NL.Wegvervoer@kiwa.nl** ~~**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 kaartuitgever 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

- retourenvelop

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 kaartuitgever is ontvangen neemt zij deze aanvraag in behandeling. Na goedkeuring van de aanvraag wordt de Inspectiekaart geproduceerd.

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 en de Algemene Voorwaarden. De certificaathouder / certificaatbeheerder is gehouden aan de Regeling gebruik Boordcomputer en boordcomputerkaarten.

4.1.3 *Vernieuwing kaarten op initiatief TSP en kaartuitgever*
Als er technische noodzaak is kan de TSP besluiten om kaarten te vernieuwen en deze te ‘pushen’ naar de certificaathouders. De kaartuitgever zal zich baseren op de reeds ontvangen gegevens en op basis daarvan een kaart produceren met startdatum gerelateerd aan productiedatum en einddatum gelijk aan einddatum van de te vervangen kaart. Uitgifte inclusief identiteitsvaststelling zal conform het reguliere proces plaatsvinden.

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 **https://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 aangewezen personeelslid van de abonnee, die bevoegd is om namens de abonnee de rol van certificaatbeheerder voor betreffende kaarten en certificaten te vervullen. De naam van het personeelslid wordt door de distributeur vastgelegd.

Alvorens de kaart te overhandigen, controleert de Distributeur de juistheid van de op de kaart vermelde gegevens. Alvorens de kaart in ontvangst te nemen heeft de de ontvanger de gelegenheid en verantwoordelijkheid om 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 Algemene Voorwaarden en de juistheid van de op de kaart vermelde gegevens 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

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

4.4.2 *Publicatie van eindgebruikercertificaten*
De IenW TSP publiceert geen eindgebruikercertificaten. Certificaten worden gedistribueerd als onderdeel van het uitgifteproces van de boordcomputer- en systeemkaarten.

4.4.3 *Notificatie van certificaatuitgifte aan derden*
Tijdens het productieproces deelt de certificaatproducent de certificaten met de personalisator en de kaartuitgever. Er vindt geen verdere notificatie van certificaatuitgifte plaats aan derden.

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 IenW TSP 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 IenW TSP 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 IenW TSP 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 Algemene 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 IenW TSP 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 IenW TSP 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 IenW TSP:

- 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 certificaten);
- Als de IenW TSP een melding van overlijden ontvangt betreffende de certificaathouder van beroepsgebonden certificaten dan voert de IenW TSP een verificatie uit bij de GBA. Wanneer de GBA het overlijden bevestigt, gaat IenW TSP over tot de intrekkingsprocedure[1];
- 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 IenW TSP 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.

[1] Drie maanden voor verlenging van een chauffeurskaart verifieert de IenW TSP de eigenaar van een chauffeurskaart bij de GBA. Wanneer de GBA terugkoppelt dat de persoon is overleden, wordt er geen verlengingsverzoek uitgestuurd.

Certificaten kunnen door de IenW TSP zonder nadere tussenkomst worden ingetrokken wanneer:

- De IenW TSP 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 QSCD, gestolen of vermoedelijk gestolen sleutel of QSCD of vernietigde sleutel of QSCD;
- 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 IenW TSP op de hoogte wordt gesteld of anderszins zich bewust wordt van een wezenlijke verandering in de informatie, die in het certificaat staat;
- De IenW TSP 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 IenW TSP bepaalt dat informatie in het certificaat niet juist of misleidend is;
- De IenW TSP 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 IenW TSP 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 IenW TSP of PKIoverheid. Hierbij worden de certificaten van alle bij de IenW TSP bekende abonnees en certificaathouders ingetrokken.
- Als de kaart niet binnen de gestelde termijn van 12 weken is afgehaald[2].
- Na definitieve intrekking of schorsing van de BCT-kaart.

De beweegreden voor elke door de IenW TSP zelfstandig uitgevoerde intrekking wordt door haar geregistreerd.

De IenW TSP zorgt ervoor dat datum en tijdstip van intrekking van (services) certificaten precies kunnen worden vastgesteld. In geval van twijfel geldt het door de IenW TSP 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 IenW TSP trekt een certificaat in na een geautoriseerd verzoek daartoe van de abonnee, de certificaathouder of de certificaatbeheerder. De IenW TSP mag ook zelf een verzoek tot intrekking initiëren. Een vertrouwende partij 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 IenW TSP zal een dergelijke melding onderzoeken en, als daar aanleiding toe is, het certificaat intrekken.

[2] ~~In de periode eind januari 2020 tot en met 10 april 2020 is het intrekken vanwege overschrijding van de afhaaltermijn tijdelijk opgeschort tijdens de grootschalige vervanging van de G2 BCT kaarten. Vanwege de coronacrisis is deze periode verlengd tot 24 april 2020.~~

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 (**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 IenW TSP. Als de combinatie van de intrekkingscode en het kaartnummer correct is, worden de certificaten op de boordcomputerkaart ingetrokken. De aanvrager krijgt hiervan op website een melding. Als de intrekkingscode en kaartnummer niet correct zijn, wordt terug gemeld dat de intrekking niet wordt uitgevoerd. De IenW TSP heeft maatregelen genomen om te voorkomen dat onbeperkt foutieve intrekkingsverzoeken kunnen worden gedaan.

Bij telefonische intrekking worden geen documenten overlegd. De indiener van het intrekkingsverzoek dient een aantal vooraf vastgestelde vragen te beantwoorden. Aan de hand van deze vragen dient de IenW TSP 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 intrekkingsverzoek en van de boordcomputerkaart, controleert de IenW TSP of de indiener bevoegd is de aanvraag tot intrekking te doen. Na uitvoering van de controles trekt de IenW TSP 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 intrekkingsdienst is beschikbaar gedurende kantoortijden op telefoonnummer **088-9984888**.

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

De IenW TSP zorgt ervoor dat datum en tijdstip van intrekking van certificaten precies kunnen worden vastgesteld. In geval van twijfel geldt het door de IenW TSP 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 intrekkingsverzoek naar het e-mail adres **intrekkenBCT@kiwa.nl**. In het intrekkingsverzoek neemt de aanvrager de volgende gegevens op:

- De kaartsoort;
- Het kaartnummer;
- De intrekkingscode;
- 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 intrekkingsverzoek*
De maximale verwerkingstermijn van een intrekkingsverzoek is vier (4) uur. In normale omstandigheden zal de statusverandering als gevolg van een elektronische of telefonische intrekking verwerkt zijn in de eerstvolgende CRL, zie par. 4.9.7.

Bij gebruik van de noodprocedure zorgt KIWA ervoor dat binnen 1 uur via de Major Incident procedure het intrekkingsverzoek bij KPN wordt gemeld via de telefonisch Helpdesk van KPN. KIWA stuurt binnen 2 uur na ontvangst van het intrekkingsverzoek de getekende formulieren met de intrekkingsinformatie naar KPN. KPN heeft daarmee 3 uur na ontvangst van het verzoek en nog 2 uur na ontvangst van de intrekkingsinformatie de noodintrekking uit te voeren.

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. Dit geldt voor certificaten die verlopen zijn na 1 oktober 2019.

4.9.7 *CRL-uitgiftefrequentie & maximale vertraging*
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 IenW TSP 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*
Online Certificate Status Protocol (OCSP) wordt niet gebruikt in de gebruikercertificaten, maar is wel in de G3 Services CA opgenomen.

4.9.9 *Opschorten van certificaten*
Het opschorten van certificaten wordt door de IenW TSP niet aangeboden.

4.10 Certificaat Status Dienst

De status van certificaten wordt door de IenW TSP 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 IenW TSP liggen, zal de IenW TSP 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 IenW TSP. De abonnee is gehouden alle nog niet verlopen certificaten in te trekken, voordat tot beëindiging van het abonnement kan worden overgegaan.

4.12 Key Escrow en ~~Key~~ Recovery

De private sleutels van de IenW TSP worden niet aan een derde in key escrow gegeven.

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

5 Faciliteiten-~~ysieke~~, Beheer- en ~~procedurele en personele~~ Operationele 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 intrekkingsproces, waarbij ongeautoriseerde toegang tot of inbreuk op deze processen of de locaties waar deze processen worden uitgevoerd, wordt tegengegaan.

5.1 Fysieke Beveiligingsmaatregelen

5.1.1 *Locatie*

De dienstverlening van de IenW TSP 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 boordcomputerkaarten vindt plaats op de gewenste locatie van de certificaathouder / certificaatbeheerder. Hiervoor wordt een afspraak gemaakt tussen de certificaathouder / certificaatbeheerder 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 IenW TSP bij een calamiteit wordt door de verschillende partijen op een adequate wijze veiliggesteld.

5.2 Procedurele Maatregelen~~beveiliging~~

5.2.1 *Vertrouwelijke rollen*

Alle functies die een rol spelen in de dienstverlening binnen de IenW TSP zijn aangewezen als vertrouwensfuncties, conform de Uitvoeringsbepalingen Vertrouwensfuncties. De IenW TSP kent in ieder geval de volgende aangewezen functionarissen:

- Trust Service Provider Manager (TSP-manager);
- Plaatsvervangend Trust Service Provider Manager (plv. TSP-manager);
- Trust Service Provider Operationele Manager (operationele TSP-manager);
- Plaatsvervangend Trust Service Provider Operationele Manager (plv. operationele TSP-manager).

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 IenW TSP 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 Maatregelen~~beveiliging~~

5.3.1 *Kwalificaties, ervaring en screening*

De IenW TSP 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 IenW TSP vraagt van alle aan dit onderzoek onderworpen medewerkers een Verklaring Omtrent Gedrag (VOG).

De IenW TSP 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 IenW TSP 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 IenW TSP die als actor de systemen bedienen, zijn vastgelegd in de Administratieve Organisatie en de bijbehorende werkinstructies.

5.4 Audit Logging 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 IenW TSP 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 logfiles 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 IenW TSP stelt een nader onderzoek in als de analyse van de auditlogbestanden op een mogelijk kwaadwillende actie of beveiligingsincident wijst.

5.5 Archivering documenten~~sprocedures~~

5.5.1 *Soorten gearchiveerde gegevens*
De IenW TSP 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*
Papieren formulieren en documenten worden ingescand. 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 AVG en het Beveiligingsbeleid IenW. 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 IenW TSP vindt plaats in het rekencentrum van de certificaatproducent volgens een tevoren vastgesteld draaiboek.

5.7 Aantasting en Herstel dienstverlening ~~continuïteit~~

5.7.1 *Procedures voor afhandeling incidenten en aantasting*
Incidenten kunnen worden gemeld bij het callcenter 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 IenW TSP. Op dat moment kan besloten worden om het business continuity plan van de IenW TSP van kracht te laten worden.

Compromittering van de private sleutel van de IenW TSP wordt beschouwd als een calamiteit. De IenW TSP neemt in deze situatie minimaal de volgende acties:
- De IenW TSP stelt vertrouwende partijen en BCT-kaarthouders hiervan zo spoedig mogelijk op de hoogte door de informatie te publiceren via het internet;
- De IenW TSP trekt de betrokken certificaten direct in en publiceert deze op de toepasselijke CRL volgens het normale publicatieschema;
- De IenW TSP 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 IenW TSP 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 CA of RA Beëindiging ~~van de TSP-diensten~~

Als het voornemen is om de certificatiedienstverlening te beëindigen, zal de IenW TSP 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 IenW TSP de abonnees en certificaathouders informeren tenminste drie maanden voordat de dienstverlening daadwerkelijk wordt beëindigd. Vanaf dit moment zal KIWA geen BCT-kaarten meer uitgeven.

Bij het beëindigen van de certificatiedienstverlening zal KIWA 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 even wel het bepaalde in 9.2 Financiële verantwoordelijkheid en aansprakelijkheid.

De IenW TSP 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 Vertrouwensdienstverlener 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 IenW TSP betrokken zijn bij het leveren van certificatiediensten, daartoe wordt ook het verbreken van externe koppelingen gerekend;
  - Alle autorisaties van onderaannemers die namens de IenW TSP 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 basiseisen) 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 Beveiligingsmaatregelen

6.1 Genereren en Installeren van sleutelparen

Bij het genereren van sleutelparen maakt de IenW TSP 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.

6.1.1 *Genereren van sleutelparen*

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

De generatie van de sleutelparen voor de (uitgevende) TSP CA's van de IenW TSP 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 signatuur 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 (QSCD) geïnjecteerd dat voldoet aan de eisen genoemd in ETSI EN 419 211 voor Qualified Electronic Signature Creation Device (QSCD).

De IenW TSP zal ieder kwartaal de status van de QSCD controleren als onderdeel van het levencyclus beheer van de QSCD. De IenW TSP zal via reguliere beheerprocessen tijdig overstappen op een vervangende QSCD als de certificering afloopt volgens planning. Bij vroegtijdig en onverwacht sneller vervallen van de QSCD certificering zal de IenW TSP betrokken partijen informeren en zo snel mogelijk met een alternatief komen.

6.1.2 *Overdracht van private sleutels en QSCD 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 (uitgevende) 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. 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 certificaten van Boordcomputerkaarten worden getekend door de 'MinIenW PKIoverheid Organisatie Persoon CA - G3' of 'MinIenW PKIoverheid Organisatie Services CA - G3' met een sleutellengte van 4096 bits RSA.

De sleutellengte voor certificaten voor systeemkaarten is 2048 bits RSA. De systeemkaarten worden getekend met de 'MinIenW PKIoverheid Autonome Apparaten CA - G3' 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 Extended KeyUsage in het certificaat opgenomen.

6.2 ~~Private sleutel b~~Beschermingen Private sleutel en Technische Maatregelen Cryptografische Module

6.2.1 *Standaarden voor cryptografische 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 IenW TSP. 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 IenW TSP niet extern in escrow gegeven.

6.2.3 *Escrow van private sleutels van kaarthouders*
De IenW TSP biedt geen escrow dienstverlening aan de kaarthouders aan.

6.2.4 *Back-up van de private sleutels van certificaathouders*
De IenW TSP 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 IenW TSP 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 IenW TSP 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. Gedurende het productieproces heeft de personalisator de gegenereerde versie van de private sleutels van de certificaathouder, zie ook paragraaf 6.1.1 *Genereren van sleutelparen*. Technische en organisatorische maatregelen maken onopgemerkt oneigenlijk gebruik van deze private sleutels onmogelijk en waarborgen dat deze uitsluitend in bruikbare vorm beschikbaar komen voor de certificaathouder. De personalisator vernietigt aansluitend op verzending -maar uiterlijk 10 werkdagen na genereren van een sleutelpaar- iedere kopie van de private sleutels uit zijn systemen.

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) TSP CA's van de IenW TSP geactiveerd. De IenW TSP 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 IenW TSP 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 IenW TSP 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 IenW TSP 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 fabrikant aangeleverd in een verpakking die elke vorm van corruptie van de inhoud toonbaar maakt.

De volledige QSCD van de BCT kaart en systeemkaart is onafhankelijk gecertificeerd tegen de Common Criteria for Security Evaluation standaard. Het hierbij toegepaste garantieniveau is EAL5+. Uitgangspunt is dat deze QSCD certificering geldig is gedurende de hele gebruiksduur van de BCT kaart.

6.3 ~~Aanvullende~~ Andere Aspecten van Sleutelpaar Beheer~~Management~~

Alle aspecten van het sleutelmanagement worden door de IenW TSP 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 IenW TSP 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 IenW TSP 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 domein CA van PKI Overheid.

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 driemaal onjuist is ingevoerd, is de BCT kaart definitief geblokkeerd en daarmee onbruikbaar gemaakt.

6.5 Computer Beveiligingsmaatregelen ~~Toegangsbeveiliging van TSP-systemen~~

6.5.1 *Algemene systeem beveiligingsmaatregelen*

De IenW TSP 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 IenW TSP 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 IenW TSP wordt afgehandeld.

6.5.3 *Beheer en classificatie van middelen*

De IenW TSP classificeert de gebruikte middelen op basis van een risicoanalyse.

6.6 Be~~heers~~veiligings**maatregelen** ~~technische~~ L**evenscyclus**

6.6.1 *Beheersingsmaatregelen systeemontwikkeling*

Voor de door de IenW TSP ontwikkelde systemen wordt door een geaccrediteerde EDP-auditor een auditverklaring afgegeven op basis van CEN TS 419 261. De IenW TSP 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 IenW TSP 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 IenW TSP 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.

Daarnaast is het verplicht de beveiligingsissues in de markt te volgen en alle software en hardware up to date te houden. Dit betekent dat men geen gebruik mag maken van software en hardware die niet meer wordt voorzien van beveiligingsupdates. Het wordt echter aangeraden alle beschikbare nieuwe versies te implementeren, die ter verbetering van de systeemveiligheid worden uitgebracht.

De verschillende operationele partijen zijn zelf verantwoordelijk voor het op juiste wijze toepassen van de noodzakelijke maatregelen binnen het bereik van de eigen dienstverlening en beschikken over een test/acceptatie- en productiesysteem.

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 Netwerk Beveiligingsmaatregelen

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 IenW TSP biedt geen time-stamping dienstverlening aan derden aan.

7 Certificaat, ~~en~~ CRL- en OCSP-profielen

7.1 Certificaatprofiel~~en~~

De certificaten die worden uitgegeven voor gebruik op de BCT-kaarten en systeemkaarten voldoen aan de profielen in de actuele versie van het document “MinIenW TSP PKIoverheid Certificaatprofielen BCT G3”.

7.2 CRL-profiel

Het profiel van de CRL die door de IenW TSP wordt uitgegeven wordt beschreven in de actuele versie van het document “MinIenW TSP PKIoverheid Certificaatprofielen BCT G3”.

7.3 OCSP-profiel

Online Certificate Status Protocol (OCSP) wordt niet gebruikt in de gebruikercertificaten, maar is wel in de G3 Services CA opgenomen.

8 ~~Conformiteits~~Nalevingsaudit en andere beoordeling

De TSP dienstverlening van het Ministerie van Infrastructuur en Waterstaat is gecertificeerd tegen 'Scheme for certification of Certification Authorities tegen ETSI EN 319 411-2 en ETSI EN 319 411-1 en voldoet daarmee aan de eisen zoals gesteld aan Vertrouwensdienstverleners (beiden in combinatie met ETSI EN 319 401).

NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS (NetSec)

Toelichting:
De netwerk- en certificaatsysteembeveiligingsvereisten (Vereisten) zijn van toepassing op alle publiek vertrouwde certificeringsinstanties (CA's) en zijn goedgekeurd met de bedoeling dat al dergelijke CA's en Gedelegeerde Derden worden gecontroleerd op conformiteit.

M.b.t. deze vereisten is de CA verantwoordelijk voor alle taken die door gedelegeerde derde worden uitgevoerd.

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.

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/diensten/pkioverheid/aansluiten-als-tsp/pogramma-van-eisen). Dit is aantoonbaar met behulp van een door BSI Group The Netherlands B.V. afgegeven auditverklaring.

Een afschrift van het ETSI EN 319 411-1 en het ETSI EN 319 411-2-certificaat staan op de site van de IenW TSP (https://bct.tsp.minienw.nl/).

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. Daarom wordt tevens gecertificeerd tegen Verordening eIDAS (elektronische identificatie en vertrouwensdiensten voor elektronische transacties).
De Trust Service Provider van het Ministerie van Infrastructuur en Waterstaat is gecertificeerd voor ETSI EN 319 411-1 en ETSI EN 319 411-2.

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 IenW TSP ondergaat eenmaal per 2 jaar een certificatieaudit. In het tussenliggende jaar wordt 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 IenW TSP interne audits uitvoeren.

De IenW TSP houdt deels via de kaartuitgever, toezicht op de operationele partijen die gezamenlijk de dienstverlening leveren.

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 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 wordt 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 IenW TSP 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 zijn beschikbaar 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 IenW TSP voldoet tevens aan het normenkader van de PKI voor de overheid zoals gesteld in het Programma van Eisen (zie hiervoor https://www.logius.nl).

9 ~~Algemene~~Overige zakelijke en juridische bepalingen

Het ministerie van Infrastructuur en Waterstaat is de eindverantwoordelijke vertrouwensdienstverlener en eveneens verantwoordelijk voor de delen die zijn uitbesteed aan andere organisaties. De ILT, als IenW TSP, 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 IDEMIA The Netherlands B.V., terwijl de productie van de certificaten is uitbesteed aan KPN B.V..

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 IenW TSP 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 het Ministerie van IenW en in breder verband de Staat der Nederlanden (Rijksoverheid).

De IenW TSP 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 bedrijfsinformatie~~gegevens~~

Op basis van de Wet openbaarheid van bestuur (Wob) kan eenieder een verzoek doen aan de IenW TSP 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 persoonsinformatie~~gegevens~~

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 IenW TSP nagaan of en zo ja wie inzage heeft gehad in deze gegevens.

9.4.1 Vertrouwelijke informatie

De informatie die door de IenW TSP wordt verkregen over een persoon, zijnde een natuurlijk persoon of rechtspersoon, wordt vertrouwelijk behandeld. De eisen gesteld in de Algemene Verordening Gegevensbescherming (AVG) 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;
- Audit rapporten.

9.4.2 Niet-vertrouwelijke informatie

De inhoud van certificaten is vrij raadpleegbaar. Echter, de door de IenW TSP 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 IenW TSP registratie wordt opgevraagd door een bevoegde opsporingsambtenaar, dan wordt deze informatie door de IenW TSP vrijgegeven. De eisen gesteld in de AVG zijn hierop uitdrukkelijk van toepassing.

Als door een abonnee of certificaathouder in een civiele procedure niet-openbare informatie uit het IenW TSP registratie wordt opgevraagd ten behoeve voor het leveren van bewijs van certificatie, dan wordt deze informatie vrijgegeven door de IenW TSP, 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 IenW TSP. 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 IenW TSP 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 Vertegenwoordigingen en garanties

Geen nadere bepalingen van toepassing.

9.7 ~~Aansprakelijkheid~~Uitsluitingen en garanties

In de Algemene Voorwaarden PKIoverheid Certificaten is de wijze opgenomen waarop de IenW TSP en betrokken partijen om gaan met ~~aansprakelijkheid~~ uitsluitingen en garanties.

9.8 Aansprakelijkheidsbeperkingen ~~in garanties~~

In de Algemene Voorwaarden PKIoverheid Certificaten is de wijze opgenomen waarop de IenW TSP en betrokken partijen om gaan met aansprakelijkheidsbeperkingen ~~in garanties~~.

9.9 Schadeloosstelling

Geen nadere bepalingen~~Niet~~ van toepassing.

9.10Geldigheidstermijn ~~CPS~~

Het CPS is geldig vanaf de datum van publicatie. Het CPS is geldig zolang de dienstverlening van de IenW TSP voortduurt of totdat het CPS wordt vervangen door een nieuwere versie.

Indien één of meer bepalingen van dit CPS naar recht of anderszins niet van toepassing wordt verklaard, laat dit de geldigheid en toepasselijkheid van alle andere bepalingen onverlet. Partijen zullen in dat geval zijn gebonden aan een bepaling van zoveel mogelijke overeenkomstige strekking die niet aan vernietiging blootstaat.

Nieuwere versies worden gepubliceerd via de elektronische opslagplaats, als beschreven in hoofdstuk 2.

9.11 Individuele mededelingen en communicatie met betrokken partijen

Geen nadere bepalingen van toepassing.

9.12 Wijzigingen

9.12.1 *Wijzigingsprocedure*

De werking van het geldende CPS wordt ten minste jaarlijks beoordeeld en geactualiseerd door IenW TSP. Wijzigingen gelden vanaf het moment dat het nieuwe CPS is gepubliceerd.

De IenW TSP biedt een aangepaste CPS-versie altijd ter goedkeuring aan het TSP management.

9.12.2 *Wijzigings- en classificatieverzoeken*

De IenW TSP heeft het recht het CPS te wijzigingen en/of aan te vullen.

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 IenW TSP. De contactgegevens van de IenW TSP staan vermeld in paragraaf 1.5.1. Indien de IenW TSP, 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.

De IenW TSP zal de wijzigingsverzoeken classificeren. Waar nodig, wordt hierbij gespecialiseerde juridische of technische kennis betrokken. Bij classificatie wordt tevens de urgentie van het verzoek tot wijziging bepaald.

Bij wijziging van het CPS wordt de impact bepaald voor de handhavingsapplicatie 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.

9.12.3 *Publicatie van wijzigingen*

De nieuwe versie van het CPS wordt na goedkeuring gepubliceerd op de website van de IenW TSP.

9.13 Procedures voor Geschillenbeslechting

De IenW TSP kent een klachtenprocedure en een bezwaar- en beroepsprocedure.

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: **NL.Wegvervoer@kiwa.nl** ~~vergunningen@kiwa.nl~~
Tel: +31 88 9984888

9.14 Toepasselijk recht

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

9.15 Naleving toepasselijke ~~relevante~~ wetgeving

Overige relevante wetgeving wordt door de IenW TSP in letter en geest van de wet nageleefd.

9.16 Diverse bepalingen

Geen nadere bepalingen van toepassing.

9.17 Overige bepalingen

Geen nadere bepalingen van toepassing.

10 Revisies

10.1 Revisie 4.8.1 → 4.8.2 G3

4.8.2 G3	13 juli 2020	Aanpassingen: o Het CPS van de TSP MOET de hoofdstukindeling volgens RFC 3647 volgen. Alle hoofdstukken en paragrafen zoals gedefinieerd in RFC3647 MOETEN in het CPS worden opgenomen. Lege hoofdstukken zijn niet toegestaan. o Het emailadres voor vergunningaanvraag bij KIWA is gewijzigd van vergunningen@kiwa.nl in NL.Wegvervoer@kiwa.nl. o Par. 4.9.1 de voetnoot met betrekking tot de opschorting van de afhaaltermijn is verwijderd.

10.2 Revisie 4.8 → 4.8.1 G3

4.8.1 G3	3 april 2020	Aanpassing: o Par. 4.9.1: update voetnoot bij 12 weken afhaaltermijn: periode verlengd tot 24 april 2020 ivm coronacrisis.

10.3 Revisie 4.7.4a → 4.8 G3

4.8 G3	1 april 2020	Aanpassingen: o er is niet langer een onderscheiden rol van 'Dossierhouder BCT'. Alle taken worden uitgevoerd door de 'IenW TSP' die is ondergebracht bij de Inspectie Leefomgeving en Transport (ILT); o H1 introductie: toegevoegd IenW TSP omschrijving; o Par. 1.5.1: Update contactinformatie; o Par. 1.3.3: Kaartuitgever gebruikt multi-factor authenticatie; o Par. 3.1.1: vermelding van inkortingsregels voor commonName/givenName/surName bij lange namen; o Terminologie: 'Certificatiedienstverlener vervangen door Vertrouwensdienstverlener' ook bij definities; o Par. 3.2.6: toegevoegd voor alignment met RFC 3647; o Par. 4.4: uitgebreid voor alignment met RFC 3647; o Par. 5.2.1: toegevoegd aangewezen functionarissen (rollen).

10.4 Revisie 4.7.4 → 4.7.4a G3

4.7.4a G3	27 januari 2020	Tijdelijke aanpassing: o Par. 4.9.1: voetnoot bij 12 weken afhaaltermijn.

10.5 Revisie 4.7.3 → 4.7.4 G3

4.7.4 G3	9 december 2019	Correcties en wijzigingen op basis van audit bevindingen: o Heading 3.1.2 niet meer genummerd, toegevoegd par. 3.1.6 conform RFC 3647 n.a.v. review commentaar KIWA; o Par. 3.4: verduidelijking authenticatie bij telefonische intrekking; o Par. 4.1.2: leverancier → kaartuitgever;

		o Par. 4.1.1, 4.1.2 en 4.3 verduidelijkt dat men tekent voor akkoord CPS en AV en gehouden is aan Regeling n.a.v. review commentaar KIWA; o Par. 4.1.3: verduidelijkt 'dezelfde geldigheidsduur' n.a.v. review commentaar KIWA; o Par. 4.3: verduidelijkt uitgifte keuringskaarten, onder-nemerskaart en systeemkaart aan certificaatbeheerder; o Par. 4.3: verduidelijkt proces aan voordeur n.a.v. reviewcommentaar AMP; o Par. 4.5.3: 'vertrouwende partij voorwaarden' → 'Algemene Voorwaarden'; o Par. 4.9.5 verduidelijking verwerkingstijd intrekking normale procedure en noodprocedure; o Par. 4.9.6: ingangsdatum toegevoegd voor blijven opnemen van verlopen certificaten op CRL; o Par. 5.1.1: uitgiftelocatie beschreven voor alle boordcomputerkaarten; o Par. 5.5.2: toegevoegd: inscannen papieren documenten; o Par. 6.1.1: QSCD monitoring procedure toegevoegd; o Par. 6.2.7: verduidelijking beveiliging private sleutels certificaathouder tijdens proces; o Par. 4.6.5 en 5.8: uniforme verwijzing naar 'KIWA'; o Par. 9.11 toegevoegd goedkeuringsproces van CPS door TSP management.

10.6 Revisie 4.7.2 → 4.7.3 G3

4.7.3 G3	18 september 2019	Kleine correcties en aanvullingen: o Title, footer, document: Certificate Practice Statement aangepast in officiële term Certification Practice Statement; o Inhoudsopgave: toegevoegd lijst tabellen en figuren; o Par. 1.1.2, na een LWT kaart ontvangt men een Chauffeurskaart die 5 jaar geldig is; o Tabel 5, correctie vulling surName, givenName in Keuringskaart; o Par. 4.9.1 toelichting uitgebreid procedure bij overlijden.

10.7 Revisie 4.7 G3 → 4.7.2 G3

4.7.2 G3	6 augustus 2020	Eerste versie voor overgang naar de PKIoverheid G3 Root CA, geschikt gemaakt voor externe distributie.

10.8 Revisie 4.7 → 4.7 G3

4.7.2 G3	13 juli 2019	Eerste versie voor overgang naar de PKIoverheid G3 Root CA

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 door de IenW TSP. 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 door de IenW TSP 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 QSCD 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 QSCD 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 Vertegenwoordiger	De vertegenwoordiger van de Abonnee die bevoegd is de Abonnee te vertegenwoordigen als het Certificatiediensten betreft.

Term	Definitie
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 door de IenW TSP.
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 CA.
Vertrouwensdiensten	het afgeven, beheren en intrekken van Certificaten door Vertrouwensdienstverleners.
Certification 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.
Certification Practice Statement PKIoverheid (CPS PKIoverheid)	de onderhavige CPS, zoals van toepassing op de uitgifte van PKIoverheid Certificaten door de IenW TSP alsmede het gebruik daarvan.
Trust Service Provider (TSP)	Een natuurlijke of rechtspersoon die certificaten afgeeft of andere diensten in verband met elektronische handtekeningen verleent. De TSP heeft als functie het verstrekken en beheren van Certificaten en sleutelinformatie, met inbegrip van de hiervoor voorziene drager (QSCD). De TSP heeft tevens

Term	Definitie
	de eindverantwoordelijkheid voor het leveren van de Vertrouwensdiensten waarbij het niet uit maakt of het de feitelijke werkzaamheden zelf uitvoert of deze uitbesteedt aan anderen. De door de TSP gevolgde procedures en getroffen maatregelen ten aanzien van alle aspecten van de Public Key Infrastructuur (PKI) staan beschreven in het Certification Practice Statement (CPS).
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 IenW TSP 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 Vertrouwensdienstverlener 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.
Gekwalificeerde Elektronische Handtekening	een Elektronische Handtekening die voldoet aan de volgende eisen: a) het is op unieke wijze aan de ondertekenaar

Term	Definitie
	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 QSCD 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 Qualified Signature Creation Device (QSCD).
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 QSCD 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 Abonnee (organisatorische entiteit), en b) ze zijn uitgegeven op basis van de binnen de PKIoverheid geldende „Certificate Policy Domein Overheid/Bedrijven en Organisatie”

Term	Definitie
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 IenW TSP, 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 IenW TSP uitgegeven Certificaat
Policy Management Authority	de organisatorische entiteit binnen de IenW TSP 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.
QSCD	Een QSCD is een Secure Signature Creation Device dat gecertificeerd en goedgekeurd is voor het genereren van gekwalificeerde elektronische handtekeningen (QES). Het maakt gebruik van technische en procedurele middelen om dit te waarborgen dat: - Ondertekeningssleutels worden geheim gehouden - Ondertekeningssleutels worden gemaakt met behulp van gevestigde cryptografische technieken.

Term	Definitie
	- Ondertekeningssleutels kunnen alleen door de juiste eigenaar worden gebruikt. - Naleving van de strenge normen voor QES. Een QSCD kan bijvoorbeeld een smartcard of een USB token zijn.
Regeling gebruik boordcomputer en Boordcomputerkaarten	De regeling die van toepassing zijn op alle bij de uitgifte en het gebruik van PKIoverheid Certificaten betrokken partijen.
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.
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.
Vertrouwende Partij	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
AP	Autoriteit Persoonsgegevens
AT	Agentschap Telecom
AVG	Algemene Verordening Gegevensbescherming
BCT	Boordcomputer Taxi
BOA	Buitengewoon Opsporingsambtenaar
BSN	Burgerservicenummer
CA	Certification Authority
CI	Certificerende Instantie
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificaten Revocatie Lijst
eIDAS	Verordening Elektronische Identificatie en Vertrouwensdiensten voor Elektronische Transacties in de Interne Markt
ETSI	European Telecommunication Standardisation Institute
FIPS	Federal Information Processing Standards
GBA	Gemeentelijke Basis Administratie
HSM	Hardware Security Module
ILT	Inspectie Leefomgeving en Transport
NetSec	Network Security Controls
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PIN	Persoonlijk Identificatie Nummer
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PUK	Persoonlijk Unlock Kengetal
QSCD	Qualified Signature Creation Device
RA	Registration Authority
RFC	Request for Comments
SLA	Service Level Agreement
TSP	Trust Service Provider ofwel Vertrouwensdienstverlener
VOG	Verklaring omtrent gedrag
Wid	Wet op de identificatieplicht