Inspectie Leefomgeving en Transport
Ministerie van Infrastructuur en Waterstaat

OPENBAAR

MinIenW BCT PKIoverheid Certificaatprofielen G3

Versie 2.2

Datum	09-12-2019
Status	Definitief

Colofon

Projectnaam	MinIenW PKIoverheid TSP
Documenttitel	MinIenW BCT PKIoverheid Certificaatprofielen G3
Classificatie	**OPENBAAR**
Versienummer	2.2
Status	Definitief
Datum	09-12-2019

Contactpersoon

L. de Jager
TSP
tel: +31 6 4674 8901
dci.csp@minienw.nl
Ministerie van Infrastructuur en Waterstaat
Directie Concern Informatievoorziening
Rijnstraat 8 | 2515 XP | Den Haag
Postbus 20906 | 2500 EX | Den Haag

Bijlage(n)	Geen
Auteur(s)	Dossierhouder BCT

Wijzigingshistorie

Versie	Datum	Samenvatting aanpassing(en)
1.0	26-02-2015	Oplevering vanwege overgang naar de G3 hiërarchie van PKIoverheid
1.1	17-03-2015	Review commentaar van Logius verwerkt. Status definitief.
2.0	15-02-2019	Status review. Aanpassingen vanwege uitfaseren G2 project: 1. Naamgeving MinIenM --> MinIenW, Milieu --> Waterstaat 2. CSP -> TSP, Trust Service Provider; 3. Verwijdering onnodige certificaatprofielen vooruitlopende op het vervallen van in aanvullende eisen 9.17-pkio139, 9.17-pkio140 en 9.17-pkio141; 4. PvE change 332 UserNotice codering als UTF8String expliciet vermeld. Alleen tekstueel; 5. PvE change 333 QcStatements uitgebreid in handtekeningcertificaten inclusief verwijzing naar PKI Disclosure Statement (PDS); 6. PvE change 341 BasicContstraints, Alleen tekstueel verduidelijking van de vereiste codering; 7. PvE change 342 Extended KeyUsages aangepast in authenticiteitscertificaat en toegevoegd in vertrouwelijkheid en handtekeningcertificaat; 8. PvE Change 373, GivenName en surName toegevoegd in Chauffeurs- en Inspectiekaart; 9. Change 376,_Subject.OrganizationIdentifier toegevoegd in Ondernemers- en Keuringskaart; 10. http -> https in link naar CPS in certificatePolicies.PolicyQualifier.cPS.uri en in userNotice.
2.1	07-05-2019	Aanpassingen n.a.v. (final) review: 1. csp.minienm.nl aangepast in **t**sp.minien**w**.nl 2. authorityInfoAccess.caIssuers verwijst in productie naar cert.pkioverheid.nl (ipv tsp.minienw.nl) aangezien de CA certificaten door Logius zijn uitgegeven en dat de officiële publicatie URL is van de TSP CA certificaten. Bestandsnamen zijn aangepast naar naamgevingsconventie Logius; 3. Par. 7.6 opmerking over afwijking subject.title van PvE Logius; 4. H.5 verwerking van aanpassingen in TSP CA certificaten n.a.v. resigning d.d. 16 april 2019; 5. Verwijdering Extended Key Usage EmailProtection uit profiel Gebruikercertificaten. Toepassing niet noodzakelijk in BCT context en daardoor buiten scope van o.a. Mozilla Policy; 6. Verwijdering Extended Key Usage Smart Card Logon uit profiel Gebruikercertificaten. Niet meer toegestaan binnen PKIoverheid en niet meer noodzakelijk; 7. Verwijdering van "Microsoft UPN" (userPrincipalName) uit SAN (SubjectAlternativeName) extensie uit certificaten van boord-computerkaarten. Hierdoor blijft in alle gebruikercertificaten uitsluitend de Permanent Identifier over in de SAN; 8. Opmerking bij Test CA's: er is momenteel geen aparte Test omgeving ingericht; 9. Om verwarring te voorkomen is overal de term 'Referentie' vervangen door 'Acceptatie' omgeving, REF door ACC en IMSIM door IWSIM; 10. OU attributen verwijderd uit CA certificaten van Test en Acceptatie; 11. Toegevoegd formaat certificaatserienummer in eindgebruiker-certificaten: random gegenereerd, uniek, 160 bits, positief integer. 12. Tabel 8: alle links verwijzen naar publicatie adres op pkioverheid site
2.1a	13-05-2019	Aanpassingen n.a.v. review commentaar: 1. Adres van IenW gewijzigd in Rijnstraat 8, 2515 XP 2. tabel 24: http**s** in CPS URL 3. par. 13.6: IVW -> TSP 4. par. 7.8: verwijderd verouderde versienummer bij ETSI EN 319 411-1 5. Tabel 30: typo in CRL DP: minient -> minien**w** 6. Par. 7.2 maximale geldigheid is duidelijker opgenomen 7. Publicatie van CRL's op **bct**.tsp.minienw.nl (o.a. par 4.4.2 en 7.9)
2.1b	17-06-2019	Aanpassingen n.a.v. review commentaar bij implementatie:

		1. Update figuur 1, ontbrekende lijn Services CA toegevoegd 2. Bij alle eindgebruiker certificaatprofielen en CRL profiel de OrganizationIdentifier toegevoegd bij de Issuer DN 3. Geldigheidsduur CRL 24 uur (i.p.v. 48) conform de operationele situatie.
2.1c	12-09-2019	Correctie tabel heading van tabel 5
2.1d	12-09-2019	Verduidelijking aantal posities KvK-nummer par. 7.3 en in tabel 21 en 26
2.2	09-12-2019	Aanpassingen n.a.v. reviewcommentaar: 1. Terminologie: 'leestekens' vervangen door 'karakters'; 2. Terminologie: 'referentiekaarten' vervangen door 'acceptatiekaarten' 3. Hoofdstuk 4: om verwarring te voorkomen is de niet ingerichte testomgeving uit de specificatie verwijderd. BCT heeft alleen een Acceptatie- en een Productie-omgeving ingericht; 4. Par. 7.3 opmerking toegevoegd over formaat P-nummer; 5. Par. 7.4 maximale lengte subject.givenName (16 karakters) en subject.surname (40 karakters) aangepast conform RFC 5280.

De wijzigingen van de laatste release zijn rood in dit document opgenomen.

Inhoud

Lijst met Tabellen

Lijst met Figuren

1 Inleiding

1.1 Doelstelling

Het doel van dit document is het specificeren van alle certificaatprofielen voor de PKIoverheid certificatiedienstverlener (TSP, Trust Service Provider) van het Ministerie van Infrastructuur en Waterstaat ten behoeve van de toepassing "Boordcomputer Taxi" (BCT). Dit document specificeert de certificaatprofielen voor respectievelijk productie-~~, test~~ en acceptatieomgeving onder de derde generatie PKIoverheid (G3).

Dit document is als volgt opgebouwd:

- CA model (hoofdstuk 2)
- Keuzes CA Certificaatprofiel (hoofdstuk 3)
- Naamgeving en URL's voor productie en non–productie CA's (hoofdstuk 4)
- TSP CA certificaatprofielen (hoofdstuk 5)
- Toelichting gebruikercertificaten BCT (hoofdstuk 6)
- Algemene keuzes profielen gebruikercertificaten (hoofdstuk 7)
- Profielen gebruikercertificaten (hoofdstuk 8 t/m 12);
- Het CRL model (hoofdstuk 13)

1.2 Uitgangspunten

Het actuele Programma van Eisen (PvE) van PKI voor de Overheid (PKIoverheid) is de norm voor de certificaat- en CRL-profielen. Zie https://logius.nl/diensten/pkioverheid

In het PvE zijn de referenties opgenomen naar standaardisatiedocumenten vanuit ISO/ITU (bijv. X.509), IETF in de vorm van RFC's en ETSI (met name voor het Qualified Certificate Profile).

OCSP wordt vooralsnog niet gebruikt in de gebruikercertificaten, maar is wel in de G3 Services CA opgenomen.

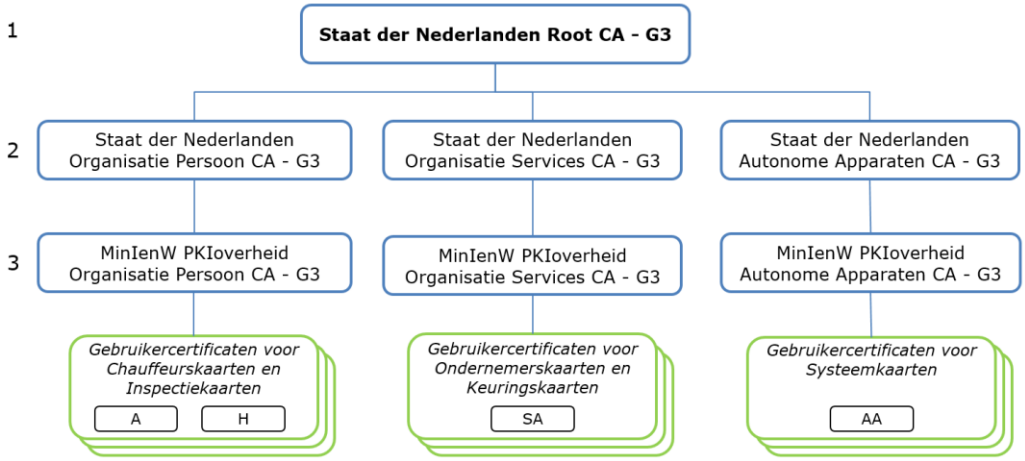
DEEL 1: CA CERTIFICATEN

2 CA model

Dit hoofdstuk beschrijft de CA structuur onder de G3 hiërarchie van PKIoverheid en de naamgeving van de CA's.

2.1 PKI hiërarchie

Figuur 1 toont de G3 PKI hiërarchie die de TSP van het Ministerie van Infrastructuur en Waterstaat gebruikt voor de BCT. De CA certificaten zijn blauw weergegeven en de eindgebruikercertificaten groen.



Figuur 1 - PKI hiërarchie (CommonName CA's) G3

TOELICHTING:

- Voor de G3 hiërarchie heeft de Policy Autoriteit van PKIoverheid besloten om een apart domein voor services certificaten in te richten. Hierdoor is een nieuwe 'tak' ontstaan voor Services certificaten[1].
- Voor de G3 hiërarchie is besloten om direct onder de laag 3 CA's de gebruikercertificaten uit te geven voor de BCT toepassing zoals aangegeven in Figuur 1. Het profiel van alle CA certificaten is daarom bepaald door PKIoverheid.
- De CA's op laag 3 betreffen de TSP CA's van de Trust Service Provider (TSP) van het Ministerie van Infrastructuur en Waterstaat. Van deze CA's specificeert dit document de definitieve invulling van de desbetreffende certificaatprofielen. Zie hoofdstuk 5.
- De verschillende typen eindgebruikercertificaten voor de BCT zijn als volgt:
  - A: Persoonsgebonden certificaat voor authenticiteit;
  - H: Persoonsgebonden certificaat voor gekwalificeerde elektronische handtekening;
  - SA: Organisatiegebonden servicescertificaat voor authenticiteit;
  - AA: (Autonoom) Apparaatgebonden certificaat voor authenticiteit.

1 Services certificaten zijn onder de G2 root nog onderdeel van het domein organisatie waaronder ook persoonsgebonden certificaten worden uitgegeven. Dit is vanwege diverse ontwikkelingen niet langer wenselijk.

2.2 Naamgeving Distinguished Name (DN) van CA's

2.2.1 Staat der Nederlanden CA's

Tabel 1 geeft de naamgeving weer die gebruikt wordt voor de Staat der Nederlanden CA's (lagen 1 en 2).

Omschrijving	Naam
CN NLRootCAG3	Staat der Nederlanden Root CA - G3
CN NLOrganisatiePersoonCAG3	Staat der Nederlanden Organisatie Persoon CA - G3
CN NLOrganisatieServicesCAG3	Staat der Nederlanden Organisatie Services CA - G3
CN NLApparatenCAG3	Staat der Nederlanden Autonome Apparaten CA - G3
O NLOrganisatienaam	Staat der Nederlanden
C NLCountry	NL

Tabel 1 - Naamgeving DN Staat der Nederlanden G3 (laag 1 en 2)

2.2.2 Ministerie van Infrastructuur en Waterstaat CA's

De naamgeving van de CA's van het Ministerie van Infrastructuur en Waterstaat is in deze paragraaf beschreven. De gespecificeerde namen zijn hoofdlettergevoelig. Met betrekking tot de Distinguished Name (DN) van elke CA van het Ministerie van Infrastructuur en Waterstaat geldt, dat uitsluitend de Common Name (CN) de onderscheidende factor is. PKIoverheid schrijft de andere Relative Distinguished Names (RDN's) van een DN voor.

De onderstaande tabel geeft de voorgeschreven DN attributen weer die in iedere TSP CA zijn opgenomen. In de G3 TSP CA's is ook een OrganisationIdentifier opgenomen met de volgende vulling:

- NTRNL: National Trade Register Nederland, gevolgd door
- het 8-cijferige KvK-nummer van het Ministerie van Infrastructuur en Waterstaat

RDN	Voorgeschreven invulling
OrganisationIdentifier	NTRNL-52766179
OrganizationName (O)	Ministerie van Infrastructuur en Waterstaat
CountryName (C)	NL

Tabel 2 - Voorgeschreven DN-attributen voor elke G3 TSP CA (laag 3)

Onderstaande tabel bevat de volledige CommonName van de G3 TSP CA's.

CA	Common Name (CN)
IenWOrganisatiePersoonCAG3	MinIenW PKIoverheid Organisatie Persoon CA - G3
IenWOrganisatieServicesCAG3	MinIenW PKIoverheid Organisatie Services CA - G3
IenWApparatenCAG3	MinIenW PKIoverheid Autonome Apparaten CA - G3

Tabel 3 - Common Name van de G3 TSP CA's (laag 3)

3 Keuzes CA Certificaatprofiel

Dit hoofdstuk beschrijft een aantal attributen op generieke wijze. Vanuit de certificaatprofielen zal hier naar worden verwezen.
De certificaat en CRL profielen zijn gebaseerd op RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
Alle karakters gebruikt dienen te voldoen aan de GBA karakter set zoals gedefinieerd in de bijlage van het "GBA logische ontwerp".

3.1 Codering X.520 attributen van het type DirectoryString

De X.520 attributen van het type DirectoryString (bijv. CN en O) zullen in het subjectDN en issuerDN van CA, en gebruikercertificaten evenals in de CRL's worden gecodeerd als **UTF8String**. Conform RFC 5280 zal Country en subject.SerialNumber als PrintableString worden gecodeerd.

3.2 CertificatePolicies

3.2.1 PolicyIdentifier

Hier zijn vanaf G3 de specifieke OID's opgenomen waarvoor de betreffende CA certificaten uitgeeft. Deze OID's zijn gespecificeerd in het betreffende deel van het PvE van PKIoverheid. Zie voor de specifieke waarden de profielen in hoofdstuk 5.

3.2.2 PolicyQualifier.cPS.uri

Vanuit de CA certificaten is er een verwijzing naar het actuele "certification practice statement" (CPS). Dat CPS publicatiepunt moet via https bereikbaar zijn. De TSP CA certificaten (laag 3 in Figuur 1) bevatten de desbetreffende URL in hun certificaatprofiel zoals opgenomen in de onderstaande tabel. Vanaf G3 is dit een verwijzing naar het CPS van PKIoverheid aangezien dat van toepassing is op de TSP CA's.

CA	CPS URL
Alle MinIenW TSP CA's	https://cps.pkioverheid.nl

Tabel 4 – CPS URL in TSP CA's van MinIenW

3.2.3 PolicyQualifier.UserNotice

Voor alle CA certificaten: Géén User Notice

3.3 CRL Distribution Points

Elke CA van de Staat der Nederlanden en elke CA van het Ministerie van Infrastructuur en Waterstaat houdt (slechts) één CRL bij voor alle mogelijke intrekkingsredenen. Elk van die CRLs is via het hypertext transfer protocol (http) vanaf een vast punt opvraagbaar.

Elk certificaat uitgegeven door het Ministerie van Infrastructuur en Waterstaat bevat de certificaatextensie cRLDistributionPoints met daarin het attribuut distributionPoint.fullName. Dat attribuut is gevuld met de http URL van de CRL (een CRL Distribution Point, ofwel CDP) van de CA die het certificaat uitgaf. Het overzicht van de voor het Ministerie van Infrastructuur en Waterstaat relevante CDPs is opgenomen in de volgende tabel.

CA	URL van CRL's
NLOrganisatiePersoonCAG3	http://crl.pkioverheid.nl/RootLatestCRL-G3.crl
NLOrganisatieServicesCAG3	http://crl.pkioverheid.nl/RootLatestCRL-G3.crl
NLApparatenCAG3	http://crl.pkioverheid.nl/RootLatestCRL-G3.crl
IenWOrganisatiePersoonCAG3	http://crl.pkioverheid.nl/DomOrganisatiePersoonLatestCRL-G3.crl
IenWOrganisatieServicesCAG3	http://crl.pkioverheid.nl/DomOrganisatieServicesLatestCRL-G3.crl
IenWApparatenCAG3	http://crl.pkioverheid.nl/DomAutonomeApparatenLatestCRL-G3.crl

Tabel 5 - CDP URL's van PKIoverheid en van de MinIenW TSP G3

Verdere eisen aan elk CDP:

- Het CRL bestand moet DER-encoded zijn;
- De bestandsnaamextensie moet ".crl" zijn;
- De http server moet als media type voor deze url de waarde "application/pkix-crl" aangeven.

3.4 TSP en CA Object Identifiers (OID)

Binnen PKI overheid worden OIDs toegekend aan elke TSP en diens CA(s). Dit nummer wordt in verschillende velden van het certificaat gebruikt. De door Logius aan het Ministerie van Infrastructuur en Waterstaat toegekende OID registraties zijn opgenomen in de onderstaande tabel.

OID	Geregistreerde OID naam
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 de TSP-CA's toegekende OID's G3

3.5 URL's van CA certificaten

De certificaten van de domein en TSP CA's worden door PKIoverheid op een vaste URL gepubliceerd. De certificaten van de TSP CA's (laag 3) bevatten een verwijzing naar de respectievelijke URL's van de domein CA's.
De gebruikercertificaten bevatten een verwijzing naar het betreffende TSP CA certificaat waaronder het is uitgegeven. Deze URL's zijn opgenomen in Tabel 7.

CA	URL van CA certificaat
NLOrganisatiePersoonCAG3	http://cert.pkioverheid.nl/DomOrganisatiePersoonCA-G3.cer
NLOrganisatieServicesCAG3	http://cert.pkioverheid.nl/DomOrganisatieServicesCA-G3.cer
NLApparatenCAG3	http://cert.pkioverheid.nl/DomAutonomeApparatenCA-G3.cer
IenWOrganisatiePersoonCAG3	http://cert.pkioverheid.nl/MinIenW_PKIoverheid_Organisatie_Persoon_CA-G3.cer
IenWOrganisatieServicesCAG3	http://cert.pkioverheid.nl/MinIenW_PKIoverheid_Organisatie_Services_CA-G3.cer
IenWApparatenCAG3	http://cert.pkioverheid.nl/MinIenW_PKIoverheid_Autonome_Apparaten_CA-G3.cer

Tabel 7 - URL's van de certificaten van Domein en TSP CA's G3

Verdere eisen:

- Het CA certificaatbestand moet DER-encoded zijn;
- De bestandsnaamextensie moet ".cer" zijn;
- De http server moet als media type voor deze url de waarde "application/pkix-cert" aangeven.

3.6 Geldigheidsduur CA-certificaten

3.6.1 DatumTijd waarop het certificaat geldig wordt

De DatumTijd waarop het certificaat geldig wordt is bepaald door het tijdstip van certificeren (sleutelceremonie) door de bovenliggende CA.

Voor de CA certificaten zal het tijd-deel van deze DatumTijd waarde altijd 0:00u UTC (GMT) tijd zijn.

3.6.2 DatumTijd waarna het certificaat ongeldig wordt

De einddatum van de NLRootCA uit generatie 3 (14 november 2028) is bepalend voor de einddatum van alle onderliggende certificaten. Om optimaal gebruik te kunnen maken van de CA's wordt de einddatum van de TSP CA's zoveel gelijk getrokken met de domein CA's (laag 2). Met telkens 1 dag minder dan de bovenliggende CA. De onderstaande tabel geeft de einddatum van alle G3 CA's weer.

Laag	CA	Einddatum
1	NLRootCAG3	14 november 2028
2	NLOrganisatiePersoonCAG3	13 november 2028
2	NLOrganisatieServicesCAG3	13 november 2028
2	NLApparatenCAG3	13 november 2028
3	IenWOrganisatiePersoonCAG3	12 november 2028
3	IenWOrganisatieServicesCAG3	12 november 2028
3	IenWApparatenCAG3	12 november 2028

Tabel 8 - Einddatum CA's PKIoverheid G3 hiërarchie

Voor de CA certificaten van MinIenW zal het tijddeel van deze DatumTijd waarde altijd 0:00u UTC (GMT) tijd zijn.

4 Naamgeving en URL's voor productie en non–productie CA's

4.1 Terminologie met betrekking tot productie en non-productie CA's

De andere hoofdstukken van dit document behandelen configuratiekeuzes zoals die voor de productie CA's gelden. Voor de ondersteuning van de levenscyclus van het systeem zijn naast de productie CA's ook ~~de test CA's~~ acceptatie CA's nodig.

~~Test CA's zijn bedoeld ter ondersteuning van de technisch georiënteerde ontwikkel- en testactiviteiten van één of meer realisatieteams (software- en/of dienstenleveranciers). Omdat de certificaten van test CA's uitsluitend dienen ter ondersteuning van de techniek, worden er aan de beheeromgeving van test CA's minder hoge eisen gesteld. Test CA's moeten worden geïnstalleerd op een andere dan de ICT infrastructuur die bedoeld is voor productie CA's. De met een test CA geproduceerde certificaten worden testcertificaten genoemd.~~

Acceptatie CA's zijn bedoeld om opgeleverde functionaliteit te testen alvorens deze in productie wordt genomen. Om dat laatste proces zo accuraat mogelijk uit te kunnen voeren, dienen de acceptatie CA's zo veel mogelijk gelijk te zijn aan de (beoogde) productie CA's. Acceptatie CA's worden daarom geïnstalleerd op vergelijkbare ICT infrastructuur en vallen onder dezelfde operationele organisatie als de (beoogde) productie CA's. De door de acceptatie CA's gedurende een acceptatie-proces gegenereerde gebruikercertificaten worden acceptatiecertificaten genoemd.

De toepassingseigenaar (dossierhouder) kan de acceptatie CA's inzetten voor het produceren van zogenaamde acceptatiekaarten. Acceptatiekaarten worden door de toepassingeigenaar uitgereikt aan (externe) partijen die geïnteresseerd zijn in het bouwen van vertrouwende toepassingen en/of apparatuur. Acceptatiekaarten, inclusief de bijbehorende CA certificaten en eventueel de relevante CRL's, vinden daarmee hun weg buiten het domein van de TSP (IenW en DH).

Tot slot geldt nog het volgende:

- ~~De gezamenlijke test CA's vormen de drie lagen van de test PKI (overheid-IenW) hiërarchie;~~
- De gezamenlijke acceptie CA's vormen de drie lagen van de acceptatie PKI (overheid-IenW) hiërarchie;
- De gezamenlijke productie CA's vormen de drie lagen van de productie PKI (overheid-IenW) hiërarchie.

Samenvattend bestaan er twee logische hiërarchieën die gerealiseerd zijn op twee of drie fysiek verschillende omgevingen (ICT-infrastructuren):

Omgeving	Doel	CA's
Productie	Operationeel productiesysteem	Productie CA's
Uitwijk	Stand-by productiesysteem	Kloon van productie CA's
Acceptatie	Accepteren ontwikkeling en uitgifte Acceptatiekaarten	Acceptatie CA's
~~Test~~	~~Ontwikkelen en testen~~	~~Test CA's~~

Opmerking: MinIenW heeft momenteel geen Test ICT-infrastructuur.

4.2 PKIoverheid en MinIenW eisen aan productie en non-productie CA's

Om bij vertrouwende partijen geen verwarring te zaaien met betrekking tot de betrouwbaarheid van certificaten stelt PKIoverheid de volgende drie eisen aan non-productie CA's:

1. Elk van de handtekeningsleutels van non-productie CA's dient een andere te zijn dan enige handtekeningsleutel van de productie CA's;
2. De Common Name van elke non-productie CA op lagen 1 en 2 dient duidelijk af te wijken van die van alle productie CA's;
3. Certificaten geproduceerd met non-productie CA's mogen in hun qcStatements extensie nimmer de indicatie "Qualified Certificate" bevatten.

Binnen de Ministerie van Infrastructuur en Waterstaat TSP geldt dat op laag 3 de Distinguished Name (DN) attributen Common Name, Organization, OrganizationIdentifier (OID 2.5.4.97) en Country van elke CA gelijk zijn in alle omgevingen. Op deze lagen wordt het omgevingsonderscheid gemaakt door gebruikmaking van het DN-attribuut Organizational Unit Name (OU). De conventie hiervoor is als volgt:

	Productie en uitwijk	**Acceptatie**	~~**Ontwikkel/test**~~
CN	*Afhankelijk van laag en domein, maar daarbinnen, ongeacht de omgeving, dezelfde naam* ***m.u.v. de term 'PKIoverheid' die alleen in productie voorkomt.***		
O	Ministerie van Infrastructuur en Waterstaat		
O id	NTRNL-52766179		
C	NL		

4.3 Hiërarchieën ondersteund door de MinIenW TSP

Voor de realisatie van een Acceptatie PKI hiërarchie kiest MinIenW bij G3 voor gebruik van een MinIenW PKIoverheid simulator.

~~In subparagraaf 4.3.1 is de naamgeving van de PKI hiërarchie voor test CA's nader gespecificeerd.~~ In subparagraaf 4.3.2 is de naamgeving van de PKI hiërarchie voor acceptatie CA's nader gespecificeerd. In subparagraaf 4.3.3 is voor de volledigheid nog een overzicht gegeven van de naamgeving van de CA's zoals die in de productie hiërarchie van toepassing zijn.

~~*4.3.1 Test CA's onder de MinIenW PKIoverheid simulator*~~

~~Deze PKI hiërarchie is opgebouwd onder een door het Ministerie van Infrastructuur en Waterstaat speciaal voor test CA's opgezette test root CA. De naamgeving luidt als volgt voor de G3 simulator:~~

~~**Laag**~~	~~**CA (Subject DN)**~~	~~**Beheerorganisatie**~~
~~1~~	~~CN = MinIenW SIMULATOR NL Root Test CA - G3 O = Ministerie van Infrastructuur en Waterstaat C = NL~~	~~MinIenW~~
~~2~~	~~CN = MinIenW SIMULATOR NL Organisatie Persoon Test CA - G3 O = Ministerie van Infrastructuur en Waterstaat C = NL~~	~~MinIenW~~

~~Laag~~	~~CA (Subject DN)~~	~~Beheerorganisatie~~
~~3~~	~~CN = MinIenW Organisatie Persoon Test CA - G3 O = Ministerie van Infrastructuur en Waterstaat OrganizationIdentifier = NTRNL-52766179 C = NL~~	~~MinIenW~~
~~2~~	~~CN = MinIenW SIMULATOR NL Organisatie Services Test CA - G3 O = Ministerie van Infrastructuur en Waterstaat C = NL~~	~~MinIenW~~
~~3~~	~~CN = MinIenW Organisatie Services Test CA - G3 O = Ministerie van Infrastructuur en Waterstaat OrganizationIdentifier = NTRNL-52766179 C = NL~~	~~MinIenW~~
~~2~~	~~CN = MinIenW SIMULATOR NL Autonome Apparaten Test CA - G3 O = Ministerie van Infrastructuur en Waterstaat C = NL~~	~~MinIenW~~
~~3~~	~~CN = MinIenW Autonome Apparaten Test CA - G3 O = Ministerie van Infrastructuur en Waterstaat OrganizationIdentifier = NTRNL-52766179 C = NL~~	~~MinIenW~~

~~**Tabel 9 – Naamgeving Test CA's G3**~~

4.3.2 *Acceptatie CA's onder de MinIenW PKIoverheid simulator*

Deze PKI hiërarchie is opgebouwd onder een door het Ministerie van Infrastructuur en Waterstaat speciaal voor acceptatie CA's opgezette root CA. De voor deze hiërarchie voorgeschreven naamgeving is als volgt in G3:

Laag	CA (Subject DN)	Beheerorganisatie
1	CN = MinIenW SIMULATOR NL Root Acceptatie CA - G3 O = Ministerie van Infrastructuur en Waterstaat C = NL	MinIenW
2	CN = MinIenW SIMULATOR NL Organisatie Persoon Acceptatie CA - G3 O = Ministerie van Infrastructuur en Waterstaat C = NL	MinIenW
3	CN = MinIenW Organisatie Persoon Acceptatie CA - G3 O = Ministerie van Infrastructuur en Waterstaat OrganizationIdentifier = NTRNL-52766179 C = NL	MinIenW
2	CN = MinIenW SIMULATOR NL Organisatie Services Acceptatie CA - G3 O = Ministerie van Infrastructuur en Waterstaat C = NL	MinIenW
3	CN = MinIenW Organisatie Services Acceptatie CA - G3 O = Ministerie van Infrastructuur en Waterstaat OrganizationIdentifier = NTRNL-52766179 C = NL	MinIenW
2	CN = MinIenW SIMULATOR NL Autonome Apparaten Acceptatie CA - G3 O = Ministerie van Infrastructuur en Waterstaat C = NL	MinIenW
3	CN = MinIenW Autonome Apparaten Acceptatie CA - G3 O = Ministerie van Infrastructuur en Waterstaat OrganizationIdentifier = NTRNL-52766179 C = NL	MinIenW

Tabel 10 - Naamgeving Acceptatie CA's G3

4.3.3 *Productie CA's in de PKIoverheid productie hiërarchie*

Deze PKI hiërarchie is de hiërarchie zoals die is opgebouwd in de productieomgeving. De voor deze hiërarchie voorgeschreven naamgeving is als volgt in G3:

Laag	CA (Subject DN)	Beheerorganisatie
1	CN = Staat der Nederlanden Root CA - G3 O = Staat der Nederlanden C = NL	PKIoverheid
2	CN = Staat der Nederlanden Organisatie Persoon CA - G3 O = Staat der Nederlanden C = NL	PKIoverheid
3	CN = MinIenW PKIoverheid Organisatie Persoon CA - G3 O = Ministerie van Infrastructuur en Waterstaat OrganizationIdentifier = NTRNL-52766179 C = NL	PKIoverheid
2	CN = Staat der Nederlanden Organisatie Services CA - G3 O = Staat der Nederlanden C = NL	PKIoverheid
3	CN = MinIenW PKIoverheid Organisatie Services CA - G3 O = Ministerie van Infrastructuur en Waterstaat OrganizationIdentifier = NTRNL-52766179 C = NL	PKIoverheid
2	CN = Staat der Nederlanden Autonome Apparaten CA - G3 O = Staat der Nederlanden C = NL	PKIoverheid
3	CN = MinIenW PKIoverheid Autonome Apparaten CA - G3 O = Ministerie van Infrastructuur en Waterstaat OrganizationIdentifier = NTRNL-52766179 C = NL	PKIoverheid

Tabel 11 - Naamgeving Productie CA's G3

4.4 URL's gebruikt binnen de certificaatprofielen

4.4.1 Uitgangspunten

Naast een onderscheid in de Distinguished Names is er een onderscheid in de verschillende URL's benodigd. Hierbij zijn de uitgangspunten de volgende:

1. Voor de TSP CA's (laag 3) wordt een DNS subdomein onder de domeinnaam van het ministerie aangemaakt met daaronder een subdomein "test" voor interne testdoeleinden;
2. De URL's van de ~~(eventuele)~~ Uitwijk CA's zijn exact gelijk aan die van de corresponderende Productie CA's;
3. Onderscheid tussen Acceptatie CA en Productie CA wordt niet gemaakt door verschillen in DNS namen, maar door directory en/of bestandsnamen. Hierdoor kunnen beiden op fysiek dezelfde machine worden geïmplementeerd.
4. ~~Onderscheid tussen Test CA en Productie CA wordt niet gemaakt door verschillen in directory en/of bestandsnamen, maar door DNS namen. Hierdoor kunnen test CA's op fysiek andere machines draaien.~~
5. Voor ~~zowel~~ de Acceptatie CA ~~als voor de Test CA~~ is een PKI testhiërarchie nodig. Voor die situaties waarbij niet wordt gekozen voor een door PKIoverheid beheerde oplossing, wordt deze behoefte ingevuld vanuit dezelfde DNS domeinnamen als genoemd onder de eerste twee punten. De nodige bestanden (CPS, certificaten en CRL's) worden hierbij in eigen directories (niet in eigen DNS domeinnamen) geplaatst:
    - CPS, certificaten en CRL's van gesimuleerde PKIoverheid CA's worden geplaatst in de directory /NLSIM;
    - CPS, certificaten en CRL's van Acceptatie CA's op laag 3 worden geplaatst in de directory /ACC.

Het met deze uitgangspunten beoogde resultaat is een technische infrastructuur waarvan het beheer, inclusief DNS beheer, per toepassing en/of omgeving apart kan worden uitgevoerd en/of uitbesteed.

De volgende subparagraaf geeft de URL's voor de acceptatie- en de productie~~- en test~~hiërarchie.

4.4.2 Acceptatie en Test CA's onder de MinIenW PKIoverheid simulator

De Ministerie van Infrastructuur en Waterstaat TSP exploiteert één webserver~~s~~:

1. **bct.tsp.minienw.nl** met daarop:
   a. in de root directory:
      i. een subdirectory /minienw-cps/ voor het Productie CPS;
      ii. de certificaten en CRL's van de Productie TSP CA's.
   b. een directory /NLSIM met daarin de CPS, certificaten en CRL's van de voor de Acceptatie hiërarchie gesimuleerde PKIoverheid Root en Domein CA's
   c. een directory /ACC met daarin de CPS, certificaten en CRL's van de Acceptatie TSP CA's.

~~2. **test.bct.tsp.minienw.nl** met daarop de eigen testhiërarchie:~~
~~a. in de root directory:~~
~~i. een subdirectory /minienw-cps/ voor de Test CPS's van toepassingen;~~
~~ii. de certificaten en CRL's van de Test TSP CA's.~~
~~b. een directory /NLSIM met daarin de CPS, certificaten en CRL's van de voor de Test hiërarchie gesimuleerde PKIoverheid Root en Domein CA's.~~

URL voor	**Productie CA G3**	**Acceptatie CA G3**	~~**Test CA G3**~~
PKIoverheid Root CA (laag 1)			
DNS-host	www.pkioverheid.nl & crl.pkioverheid.nl	bct.tsp.minienw.nl	~~test.bct.tsp.minienw.nl~~
CPS	https://cps.pkioverheid.nl	/NLSIM/<dezelfde dir>/	~~/NLSIM/<dezelfde dir>/~~
CA cert	n.v.t.	/NLSIM/<dezelfde file>	~~/NLSIM/<dezelfde file>~~
CRL	/RootLatestCRL-G3.crl	/NLSIM/<dezelfde file>	~~/NLSIM/<dezelfde file>~~
PKIoverheid Organisatie Persoon CA G3 (laag 2)			
DNS-host	https://cps.pkioverheid.nl & crl.pkioverheid.nl	bct.tsp.minienw.nl	~~test.bct.tsp.minienw.nl~~
CPS	https://cps.pkioverheid.nl	/NLSIM/<dezelfde dir>/	~~/NLSIM/<dezelfde dir>/~~
CA cert	http://cert.pkioverheid.nl/DomOrganisatiePersoonCA-G3.cer	/NLSIM/<dezelfde file>	~~/NLSIM/<dezelfde file>~~
CRL	/DomOrganisatiePersoonLatestCRL-G3.crl	/NLSIM/<dezelfde file>	~~/NLSIM/<dezelfde file>~~
PKIoverheid Organisatie Services CA G3 (laag 2)			
DNS-host	https://cps.pkioverheid.nl & crl.pkioverheid.nl	bct.tsp.minienw.nl	~~test.bct.tsp.minienw.nl~~
CPS	https://cps.pkioverheid.nl	/NLSIM/<dezelfde dir>/	~~/NLSIM/<dezelfde dir>/~~
CA cert	http://cert.pkioverheid.nl/DomOrganisatieServicesCA-G3.cer	/NLSIM/<dezelfde file>	~~/NLSIM/<dezelfde file>~~

URL voor	**Productie CA G3**	**Acceptatie CA G3**	~~**Test CA G3**~~
CRL	/DomOrganisatieServicesLatestCRL-G3.crl	/NLSIM/<dezelfde file>	~~/NLSIM/<dezelfde file>~~
PKIoverheid Autonome Apparaten CA G3 (laag 2)			
DNS-host	cert.pkioverheid.nl & crl.pkioverheid.nl	bct.tsp.minienw.nl	~~test.bct.tsp.minienw.nl~~
CPS	https://cps.pkioverheid.nl	/NLSIM/<dezelfde dir>/	~~/NLSIM/<dezelfde dir>/~~
CA cert	http://cert.pkioverheid.nl/DomAutonomeApparatenCA-G3.cer	/NLSIM/<dezelfde file>	~~/NLSIM/<dezelfde file>~~
CRL	/DomAutonomeApparatenLatestCRL-G3.crl	/NLSIM/<dezelfde file>	~~/NLSIM/<dezelfde file>~~
MinIenW Organisatie Persoon CA G3 (laag 3)			
DNS-host	cert.pkioverheid.nl & crl.pkioverheid.nl	bct.tsp.minienw.nl	~~test.bct.tsp.minienw.nl~~
CPS	/minienw-cps/	/ACC/<dezelfde dir>/	~~/IWSIM/<dezelfde dir>/~~
CA cert	/MinIenW_PKIoverheid_Organisatie_Persoon_CA-G3.cer	/ACC/<dezelfde file>	~~/IWSIM /<dezelfde file>~~
CRL	/minienw-org-pers-ca-g3.crl	/ACC/<dezelfde file>	~~/IWSIM /<dezelfde file>~~
MinIenW Organisatie Services CA G3 (laag 3)			
DNS-host	cert.pkioverheid.nl & crl.pkioverheid.nl	bct.tsp.minienw.nl	~~test.bct.tsp.minienw.nl~~
CPS	/minienw-cps/	/ACC/<dezelfde dir>/	~~/IWSIM/<dezelfde dir>/~~
CA cert	/MinIenW_PKIoverheid_Organisatie_Services_CA-G3.cer	/ACC/<dezelfde file>	~~/IWSIM /<dezelfde file>~~
CRL	/minienw-org-serv-ca-g3.crl	/ACC/<dezelfde file>	~~/IWSIM /<dezelfde file>~~
MinIenW Autonome Apparaten CA G3 (laag 3)			
DNS-host	cert.pkioverheid.nl & crl.pkioverheid.nl	bct.tsp.minienw.nl	~~test.bct.tsp.minienw.nl~~
CPS	/minienw-cps/	/ACC/<dezelfde dir>/	~~/IWSIM /<dezelfde dir>/~~
CA cert	/MinIenW_PKIoverheid_Autonome_Apparaten_CA-G3.cer	/ACC/<dezelfde file>	~~/IWSIM /<dezelfde file>~~
CRL	/minienw-aa-ca-g3.crl	/ACC/<dezelfde file>	~~/IWSIM /<dezelfde file>~~

Tabel 12 – URL's gebruikt in certificaatprofielen

5 TSP CA certificaatprofielen (laag 3)

Dit hoofdstuk bevat de certificaatprofielen van de TSP CA's (laag 3) van het Ministerie van Infrastructuur en Waterstaat. Dit hoofdstuk specificeert de profielen voor uitsluitend de productieomgeving (en uiteraard de uitwijkomgeving). Voor de opbouw van de namen en URL's voor de andere omgevingen wordt verwezen naar hoofdstuk 4.

5.1 Toelichting

In de CA certificaatprofiel tabellen zijn de volgende kolommen opgenomen:

- Certificaat / Attribuut: Deze bevat de naam van het certificaatveld in de certificaten;
- OID: Hierin is de Object IDentifier opgenomen zoals deze in de RFC's is beschreven. Dit is de standaard naamgeving;
- Waarde: Dit is de waarde die het veld moet krijgen;
- De laatste kolom geeft een verwijzing naar de betreffende paragraaf die een toelichting bij het betreffende attribuut geeft.

De basisstructuur van een certificaat bestaat uit een to-be-signed gedeelte (tbsCertificate) en een handtekening van de uitgever. Het tbsCertificate bestaat uit een aantal verplichte basisvelden gevolgd door extensies.

Met rood is aangegeven dat een extensie critical is.

5.2 Certificaatprofielen van de TSP CA's

5.2.1 Certificaatprofiel van de IenWOrganisatiePersoonCAG3

Certificaat / Attribuut	OID	Waarde	Ref §
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11 { sha256WithRSAEncryption }	
signatureValue		Handtekening gezet door de NLOrganisatiePersoonCAG3	
tbsCertificate			
Version		2 (X509v3)	
serialNumber		Uniek certificaatnummer gegenereerd door de NLOrganisatiePersoonCA G3. Lengte 160 bits.	
signature		1.2.840.113549.1.1.11 (= signatureAlgorithm)	
Issuer			
.countryName	{ id-at 6 }	NL	2.2.1
.organizationName	{ id-at 10 }	Staat der Nederlanden	2.2.1
.commonName	{ id-at 3 }	Staat der Nederlanden Organisatie Persoon CA - G3	2.2.1
Validity			
.notBefore		DatumTijd waarop het certificaat geldig wordt (16 april 2019)	3.6.1
.notAfter		DatumTijd waarna het certificaat **on**geldig wordt (12 november 2028)	3.6.2

Certificaat / Attribuut	OID	Waarde	Ref §
Subject			
.countryName	{ id-at 6 }	NL	2.2.2
.organizationName	{ id-at 10 }	Ministerie van Infrastructuur en Waterstaat	2.2.2
.organizationIdentifier	2.5.4.97	NTRNL-52766179	2.2.2
.commonName	{ id-at 3 }	MinIenW PKIoverheid Organisatie Persoon CA - G3	2.2.2
SubjectPublicKeyInfo			
.algorithm		1.2.840.113549.1.1.1 { rsaEncryption }	
.subjectPublicKey		4096 bits RSA publieke sleutel van IenWOrganisatiePersoonCAG3	
Extensions			
certificatePolicies	{ id-ce 32 }		3.2
.PolicyIdentifier		OID's van Domein Organisatie Persoon (g3): 2.16.528.1.1003.1.2.5.1 Authenticiteit 2.16.528.1.1003.1.2.5.2 Onweerlegbaarheid OPMERKING: vertrouwelijkheid wordt bij BCT niet uitgegeven. Daarom is die PolicyIdentifier OID niet opgenomen.	3.2.1
.PolicyQualifier			
.cPS.uri	{ id-qt 1 }	https://cps.pkioverheid.nl	3.2.2
keyUsage	{ id-ce 15 }	KeyCertSign, cRLSign	
ExtendedKeyUsage	{id-ce 37}	clientAuthentication: 1.3.6.1.5.5.7.3.2 OCSPSigning: 1.3.6.1.5.5.7.3.9 DocumentSigning: 1.3.6.1.4.1.311.10.3.12	
AuthorityInfoAccess	{ id-pe 1 }		
.caIssuers	{ id-ad 2 }	http://cert.pkioverheid.nl/DomOrganisatiePersoonCA-G3.cer	3.5
authorityKeyIdentifier	{ id-ce 35 }		
.KeyIdentifier		NLOrganisatiePersoonCAG3.**subject**KeyIdentifier.KeyIdentifier	
subjectKeyIdentifier .keyIdentifier	{ id-ce 14 }	SHA-1 hash van de publieke sleutel van dit certificaat	
cRLDistributionPoints .distributionPoint. .fullName	{ id-ce 31 }	http://crl.pkioverheid.nl/DomOrganisatiePersoonLatestCRL-G3.crl	3.3
BasicConstraints	{ id-ce 19 }		
.CA		True	
.pathLenConstraint		0 Toelichting: de 'pathLenConstraint' specificeert het maximale aantal volgende CA's dat toegestaan is in het certificeringspad van de betreffende CA tot aan een eindgebruikercertificaat. De waarde '0' betekent dat de gebruikercertificaten direct onder deze CA moeten worden uitgegeven.	
QcStatement2	{ id-qcs-pkixQCSyntax-v2 }	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)	

Tabel 13 - Certificaatprofiel van de IenWOrganisatiePersoonCAG3

5.2.2 Certificaatprofiel van de IenWOrganisatieServicesCAG3

Certificaat / Attribuut	**OID**	**Waarde**	**Ref §**
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11 { sha256WithRSAEncryption }	
signatureValue		Handtekening gezet door de NLOrganisatieServicesCAG3	
tbsCertificate			
Version		2 (X509v3)	
serialNumber		Uniek certificaatnummer gegenereerd door de NLOrganisatieServicesCA G3. Lengte 160 bits.	
signature		1.2.840.113549.1.1.11 (= signatureAlgorithm)	
Issuer			
.countryName	{ id-at 6 }	NL	2.2.1
.organizationName	{ id-at 10 }	Staat der Nederlanden	2.2.1
.commonName	{ id-at 3 }	Staat der Nederlanden Organisatie Services CA - G3	2.2.1
Validity			
.notBefore		DatumTijd waarop het certificaat geldig wordt (16 april 2019)	3.6.1
.notAfter		DatumTijd waarna het certificaat **on**geldig wordt (12 november 2028)	3.6.2
Subject			
.countryName	{ id-at 6 }	NL	2.2.2
.organizationName	{ id-at 10 }	Ministerie van Infrastructuur en Waterstaat	2.2.2
.organizationIdentifier	2.5.4.97	NTRNL-52766179	2.2.2
.commonName	{ id-at 3 }	MinIenW PKIoverheid Organisatie Services CA - G3	2.2.2
SubjectPublicKeyInfo			
.algorithm		1.2.840.113549.1.1.1 { rsaEncryption }	
.subjectPublicKey		4096 bits RSA publieke sleutel van IenWOrganisatieServicesCAG3	
Extensions			
certificatePolicies	{ id-ce 32 }		3.2
.PolicyIdentifier		OID's Domein Organisatie Services (g3): 2.16.528.1.1003.1.2.5.4 Services - Authenticiteit OPMERKING: Vertrouwelijkheid en Onweerlegbaarheid wordt bij BCT niet uitgegeven. Daarom zijn die PolicyIdentifier OID's niet opgenomen.	3.2.1
.PolicyQualifier			
.cPS.uri	{ id-qt 1 }	https://cps.pkioverheid.nl	3.2.2
keyUsage	{ id-ce 15 }	KeyCertSign, cRLSign	
ExtendedKeyUsage	{id-ce 37}	clientAuthentication: 1.3.6.1.5.5.7.3.2 OCSPSigning: 1.3.6.1.5.5.7.3.9 DocumentSigning: 1.3.6.1.4.1.311.10.3.12	
AuthorityInfoAccess	{ id-pe 1 }		
.caIssuers	{ id-ad 2 }	http://cert.pkioverheid.nl/DomOrganisatieServicesCA-G3.cer	3.5
.OCSP	{ id-ad 1 }	http://domorganisatieservicesocsp-g3.pkioverheid.nl	3.5
authorityKeyIdentifier	{ id-ce 35 }		
.KeyIdentifier		NLOrganisatieServicesCAG3.**subject**KeyIdentifier.KeyIdentifier	
subjectKeyIdentifier .keyIdentifier	{ id-ce 14 }	SHA-1 hash van de publieke sleutel van dit certificaat	

Certificaat / Attribuut	OID	Waarde	Ref §
cRLDistributionPoints .distributionPoint. .fullName	{ id-ce 31 }	http://crl.pkioverheid.nl/DomOrganisatieServicesLatestCRL-G3.crl	3.3
BasicConstraints	{ id-ce 19 }		
.CA		True	
.pathLenConstraint		0	
QcStatement2	{ id-qcs-pkixQCSyntax-v2 }	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)	

Tabel 14 - Certificaatprofiel van de IenWOrganisatieServicesCAG3

5.2.3 Certificaatprofiel van de IenWApparatenCAG3

Certificaat / Attribuut	OID	Waarde	Ref §
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11 { sha256WithRSAEncryption }	
signatureValue		Handtekening gezet door de NLApparatenCAG3	
tbsCertificate			
Version		2 (X509v3)	
serialNumber		Uniek certificaatnummer gegenereerd door de NLApparatenCAG3. Lengte 160 bits.	
signature		1.2.840.113549.1.1.11 (= signatureAlgorithm)	
Issuer			
.countryName	{ id-at 6 }	NL	2.2.1
.organizationName	{ id-at 10 }	Staat der Nederlanden	2.2.1
.commonName	{ id-at 3 }	Staat der Nederlanden Autonome Apparaten CA - G3	2.2.1
Validity			
.notBefore		DatumTijd waarop het certificaat geldig wordt (16 april 2019)	3.6.1
.notAfter		DatumTijd waarna het certificaat **on**geldig wordt (12 nov. 2028)	3.6.2
Subject			
.countryName	{ id-at 6 }	NL	2.2.2
.organizationName	{ id-at 10 }	Ministerie van Infrastructuur en Waterstaat	2.2.2
.organizationIdentifier	2.5.4.97	NTRNL-52766179	2.2.2
.commonName	{ id-at 3 }	MinIenW PKIoverheid Autonome Apparaten CA - G3	2.2.2
SubjectPublicKeyInfo			
.algorithm		1.2.840.113549.1.1.1 { rsaEncryption }	
.subjectPublicKey		4096 bits RSA publieke sleutel van de IenWApparatenCAG3	
Extensions			
certificatePolicies	{ id-ce 32 }		3.2
.PolicyIdentifier		OID's Domein autonome apparaten: 2.16.528.1.1003.1.2.6.1 Autonome Apparaten – Authenticiteit Bij BCT wordt alleen Authenticiteit gebruikt. Daarom zijn de PolicyIdentifier OID's van Vertrouwelijkheid en Combinatie certificaten niet opgenomen.	3.2.1
.PolicyQualifier			
.cPS.uri	{ id-qt 1 }	https://cps.pkioverheid.nl	3.2.2
keyUsage	{ id-ce 15 }	KeyCertSign, cRLSign	

ExtendedKeyUsage	{id-ce 37}	clientAuthentication: 1.3.6.1.5.5.7.3.2 OCSPSigning: 1.3.6.1.5.5.7.3.9 DocumentSigning: 1.3.6.1.4.1.311.10.3.12	
AuthorityInfoAccess	{ id-pe 1 }		
.caIssuers	{ id-ad 2 }	http://cert.pkioverheid.nl/DomAutonomeApparatenCA-G3.cer	3.5
authorityKeyIdentifier .KeyIdentifier	{ id-ce 35 }	NLApparatenCAG3.**subject**KeyIdentifier.keyIdentifier	
subjectKeyIdentifier .keyIdentifier	{ id-ce 14 }	SHA-1 hash van de publieke sleutel van dit certificaat	
cRLDistributionPoints .distributionPoint.fullName	{ id-ce 31 }	http://crl.pkioverheid.nl/DomAutonomeApparatenLatestCRL-G3.crl	3.3
BasicConstraints	{ id-ce 19 }		
.CA		True	
.pathLenConstraint		0	
QcStatement2	{ id-qcs-pkixQCSyntax-v2 }	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)	

Tabel 15 - Certificaatprofiel van de IenWApparatenCAG3

DEEL 2: GEBRUIKERCERTIFICATEN

Het tweede deel van dit document specificeert het profiel van elk gebruikercertificaat en elke CRL die een rol speelt bij Boordcomputer Taxi toepassing. De specificaties in dit document omvatten de omgevingen voor respectievelijk productie en acceptatie.

6 Toelichting gebruikercertificaten BCT

Dit hoofdstuk beschrijft de relatie tussen de kaarten van Boordcomputer Taxi (BCT) en de Certificate Policy van PKIoverheid.

6.1 Kaartmodel Boordcomputer Taxi

Boordcomputer Taxi kent 2 verschillende kaartsoorten: boordcomputerkaarten en systeemkaarten.

- De certificaten voor boordcomputerkaarten worden uitgegeven door de IenWOrganisatiePersoonCAG3 of de IenWOrganisatieServicesCAG3;
- De certificaten voor systeemkaarten worden uitgegeven door de IenWApparatenCAG3.

Een systeemkaart is uitgevoerd als een ID 000 smartcard en is bedoeld voor inbouw in en gebruik door een boordcomputereenheid (apparaat).
Boordcomputerkaarten zijn uitgevoerd als ID 1 smartcards en bestaan in 4 verschillende vormen, elk gericht op een specifieke soort boordcomputergebruiker. Daarmee betreft het in totaal 5 hoofdtypen kaarten, elk met een eigen behoefte aan PKIoverheid-certificaten. Elk van deze 5 kaarthoofdtypen valt, afhankelijk van zijn gebruikerssoort, onder een specifiek deel van de Certificate Policy van PKIoverheid.

Voor de G3 root heeft de Policy Autoriteit van PKIoverheid besloten om een apart domein voor services certificaten in te richten. De volgende tabel geeft inzicht in de relatie tussen kaarthoofdtypes, de certificaatbehoefte en PKIoverheid beleid voor de G3 generatie.

Kaarthoofdtype Eigenschappen	Chauffeurs-kaart	Inspectie-kaart	Ondernemers-kaart	Keurings-kaart	Systeemkaart
Certificaten	A, H	A, H	SA	SA	AA
Gebruiker	Bestuurder	Toezicht-houder	Vervoerder	Werkplaats	Boordcomputer
Gebruikertype	Persoon		Organisatie		Apparaat
Drager	Smartcard				
Formaat drager	ID-1				ID-000
Uitgever	IenWOrganisatie PersoonCAG3		IenWOrganisatie ServicesCAG3		IenWApparaten CAG3
PKIoverheid Domein	Organisatie Persoon		Organisatie Services		Autonome Apparaten
PKIoverheid CP	PvE deel 3a		PvE deel 3b		PvE deel 3d

Tabel 16 - Kaarteigenschappen onder de G3 hiërarchie PKIoverheid

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

Het PKIoverheid PvE vereist -in aanvullende eisen 9.17-pkio139, 9.17-pkio140 en 9.17-pkio141- dat een TSP in staat moet zijn om alle in die delen genoemde certificaatprofielen uit te geven. Er is een wijzigingsverzoek ingediend om deze eisen in het eerstvolgende PvE na versie 4.7 te laten vervangen. Dit verzoek is gehonoreerd en er is dispensatie verleend waardoor MinIenW vooruitlopend op deze aanpassing van het PvE onder de G3 geen onnodige certificaatprofielen hoeft te configureren. Deze specificatie bevat alleen de noodzakelijke profielen.

7 Algemene keuzes profielen gebruikercertificaten

Dit hoofdstuk beschrijft een aantal attributen op generieke wijze. Vanuit de specifieke certificaatprofielen zal hier naar verwezen worden.

7.1 Issuer Distinguished Name (DN)

7.1.1 issuer.countryName

Dit attribuut geeft het land van vestiging van de TSP weer. Binnen PKIoverheid is de TSP altijd in Nederland gevestigd. De waarde van dit attribuut is daarmee altijd: *NL*.

7.1.2 issuer.organizationName

Hierin staat de officiële naam van de organisatie onder wiens verantwoordelijkheid de TSP dienstverlening plaatsvindt.

De waarde van dit veld is: *Ministerie van Infrastructuur en Waterstaat*

7.1.3 issuer.commonName

Hierin staat de officiële naam van de zogenaamde issuing CA. Er zijn drie issuing CA's voor het uitgeven van certificaten namelijk de TSP CA's.

Voor de boordcomputerkaarten is dit afhankelijk van het kaarttype.
Voor de Chauffeurskaart en Inspectiekaart is dit de IenWOrganisatiePersoonCAG3 met de volledige naam:
MinIenW PKIoverheid Organisatie Persoon CA - G3

Voor de Ondernemerskaart en Keuringskaart is dit de IenWOrganisatieServicesCAG3 met de volledige naam:
MinIenW PKIoverheid Organisatie Services CA - G3

Voor de Systeemkaarten is dit de IenWApparatenCAG3 met de volledige naam:
MinIenW PKIoverheid Autonome Apparaten CA - G3

7.2 Geldigheidsduur certificaten

De geldigheid van de certificaten is gekoppeld aan de geldigheidsduur van de kaarten. De maximale geldigheidsduur van een kaart, en daarmee diens certificaten, is per kaart hoofd- en subtype verschillend:

- chauffeurs- en inspectiekaarten: maximaal 5 jaar;
- ondernemers- en keuringskaarten: maximaal 5 jaar;
- systeemkaarten: maximaal 10 jaar.

Om te waarborgen dat een certificaat net zo lang geldig blijft als de kaart waarop dat certificaat geplaatst wordt, zal elke certificaataanvraag worden voorzien van een expliciete datum-tijdwaarde voor zowel de gewenste start, als de gewenste einde geldigheid. Het tijddeel van die waarden zal daarbij door de aanvrager op 0:00:00 UTC tijd worden ingesteld. Afhankelijk van de aangevraagde geldigheid, de huidige

tijd en de geldigheid van het CA-certificaat dient de CA een certificaataanvraag in de navolgende volgorde te valideren/verwerken:

1. indien de aangevraagde einde-geldigheid minder dan 24 uur in de toekomst ligt, dient de certificaataanvraag te worden geweigerd, anders;
2. indien de aangevraagde einde-geldigheid later is dan de datum van de einde-geldigheid van het CA-certificaat, dient de certificaataanvraag te worden geweigerd, anders;
3. indien het een certificaataanvraag voor een boordcomputerkaart (chauffeurs-, ondernemers-, keurings- of inspectiekaart) betreft én het verschil tussen de aangevraagde einde-geldigheid en de aangevraagde start-geldigheid is groter dan vijf (5) jaar, dient de certificaataanvraag te worden geweigerd, anders;
4. indien het een certificaataanvraag voor een systeemkaart betreft én het verschil tussen de aangevraagde einde-geldigheid en de aangevraagde start-geldigheid is groter dan tien (10) jaar, dient de certificaataanvraag te worden geweigerd, anders;
5. indien de aangevraagde start-geldigheid in het verleden ligt, dient het certificaat te worden gegenereerd met de huidige tijd als start-geldigheid en de uit de aanvraag overgenomen einde-geldigheid, anders;
6. indien de aangevraagde start-geldigheid niet in het verleden ligt, dient het certificaat te worden gegenereerd met uit de aanvraag overgenomen start- en einde-geldigheid;

Kaarttype	**SA**	**EA**	**GA = EA – SA**	**Actie**	**S**	**E**
irrelevant	irrelevant	eerder dan morgen	irrelevant	weiger	n.v.t.	n.v.t.
irrelevant	irrelevant	later dan E_{MAX}	irrelevant	weiger	n.v.t.	n.v.t.
irrelevant	irrelevant	irrelevant	minder dan 1 dag	weiger	n.v.t.	n.v.t.
C, O, K of I	irrelevant	tussen morgen en E_{MAX}	meer dan 5 jaar	weiger	n.v.t.	n.v.t.
C, O, K of I	voor vandaag	tussen morgen en E_{MAX}	1 dag tot G_{REST}	genereer	vandaag	EA
C, O, K of I	vandaag of later	tussen morgen en E_{MAX}	1 dag tot G_{REST}	genereer	SA	EA
S	irrelevant	tussen morgen en E_{MAX}	meer dan 10 jaar	weiger	n.v.t.	n.v.t.
S	voor vandaag	tussen morgen en E_{MAX}	1 dag tot G_{REST}	genereer	vandaag	EA
S	vandaag of later	tussen morgen en E_{MAX}	1 dag tot G_{REST}	genereer	SA	EA

Tabel 17 - Geldigheidsduur certificaten

Legenda:
SA: Aangevraagde start-geldigheid
EA: Aangevraagde eind-geldigheid
GA: Aangevraagde geldigheidsduur
E_{MAX}: De datum van de einde-geldigheid van de betreffende CA
G_{REST}: De (vanaf vandaag) resterende geldigheidsduur van de betreffende CA

7.2.1 DatumTijd waarop het certificaat geldig wordt

Binnen Boordcomputer Taxi zal het tijd-deel van deze DatumTijd waarde altijd 0:00u UTC (GMT) tijd zijn. De te gebruiken datum zal door het kaartbeheersysteem worden gelijkgesteld aan de start-geldigheid van de bijbehorende kaart en door de CA worden gevalideerd/verwerkt conform Tabel 2. Deze datum kan voor een kaart wél, maar voor een (nieuw gegenereerd) certificaat niet in het verleden liggen.

7.2.2 DatumTijd waarna het certificaat ongeldig wordt

Binnen Boordcomputer Taxi zal het tijd-deel van deze DatumTijd waarde altijd 0:00u UTC (GMT) tijd zijn. De te gebruiken datum zal door het kaartbeheersysteem worden gelijkgesteld aan de eind-geldigheid van de bijbehorende kaart en door de CA worden gevalideerd/verwerkt conform Tabel 2. Deze datum kan noch voor een kaart, noch voor een certificaat later zijn dan de datum van de einde-geldigheid van de CA.

7.3 Subject organizationName, organizationalUnitName en organizationIdentifier

De invulling van subject.organizationName (O) en subject.organizationalUnitName (OU) is afhankelijk van het Kaarthoofdtype en is als volgt:

Kaarthoofdtype	**organizationName**	**organizationalUnitName**
Chauffeurskaart	[Naam certificaathouder]	n.v.t.
Ondernemerskaart	[Naam (taxi)onderneming]	[P-nummer]
Keuringskaart	[Naam keuringsinstantie]	n.v.t.
Inspectiekaart	[Naam inspectiedienst]	n.v.t.
Systeemkaart	[Naam boordcomputerfabrikant]	n.v.t.

Tabel 18 - OrganizationName en OrganizationalUnitName

Het [P-nummer] is gedefinieerd in de *Regeling specificaties en typegoedkeuring boordcomputer taxi* en heeft in de praktijk een waarde bestaande uit de letter "P" direct gevolgd door een nummer van maximaal 7 cijfers.

In ETSI EN 319 412-3 staat een verplichting om het veld Subject.organizationIdentifier te gebruiken voor certificaten uitgegeven aan rechtspersonen. Dit is bij PKIoverheid deel 3b en opgenomen in PvE change 376. In de Ondernemerskaart en Keuringskaart is dit nieuwe attribuut als volgt toegevoegd:

OID 2.5.4.97
Gevuld met waarde: `NTRNL-[KvK-nummer onderneming of keuringsinstantie]`

Waarbij:
- NTR aangeeft dat het een National Trade Register identifier betreft;
- NL het land aangeeft waar het National Trade Register zich bevindt;

- een hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8));
- na de hyphen-minus is als variabele het 8-cijferige KvK-nummer van de onderneming of keuringsinstantie opgenomen afhankelijk van het Kaarthoofdtype.

7.4 Subject commonName, givenName and surName

Subject.commonName bevat de leesbare naam van de certificaathouder (kaarthouder). Dit veld wordt gecodeerd als UTF-8 en mag uitsluitend karakters uit de GBA karakterset bevatten. De opbouw van dit veld is afhankelijk van de gebruikersoort (persoon, organisatie of apparaat). De maximale lengte van dit veld is 64 karakters. Namen dienen zo nodig te worden ingekort om binnen deze 64 posities te vallen. De wijze waarop wordt ingekort, is afhankelijk van de opbouw (gebruikersoort) van de commonName conform onderstaande tabel.

Soort	Opbouw	Inkortingregel
Persoon	{Volledige eerste voornaam}+ [' '+{Initiaal 2e voornaam}+ [' '+{Initiaal 3e voornaam}+ … etc.]]+ [' '+{Tussenvoegsel}]+ ' '+{Geboorteachternaam}	Eerst van rechts naar links net zo veel keren [' '+{Initiaal ne voornaam}] weglaten als nodig is om de volledige reeks kleiner dan 65 karakters te krijgen. Indien er geen initialen meer zijn weg te laten en {Volledige eerste voornaam}+[' '+{Tussenvoegsel}]+ ' '+{Geboorteachternaam} is nog steeds langer dan 64 karakters, dan de gehele reeks afkappen na de 64e positie.
Organisatie	Officiële organisatienaam volgens betrouwbaar register	Naam afkappen na de 64e positie.
Apparaat	Typegoedkeuringsnummer	Naam afkappen na de 64e positie.

Tabel 19 – subject.commonName

Om te voldoen aan ETSI EN 319 412-2 zijn ook de subject.givenName and subject.surname toegevoegd in de chauffeurs- en inspectiekaart. Deze velden worden gecodeerd als UTF-8 en mogen uitsluitend karakters uit de GBA karakterset bevatten. Deze velden komen alleen voor bij de gebruikersoort 'persoon'. De maximale lengte van deze velden is bepaald in RFC 5820:

- subject.givenName maximaal 16 karakters;
- subject.surname maximaal 40 karakters.

Veld (soort)	Opbouw	Inkortingregel
givenName (persoon)	{Volledige eerste voornaam}+ [' '+{Initiaal 2e voornaam}+ [' '+{Initiaal 3e voornaam}+ … etc.]]	Naam afkappen na de 16e positie.
surname (persoon)	[' '+{Tussenvoegsel}]+ ' '+{Geslachtsnaam}	Naam afkappen na de 40e positie.

Tabel 20 – subject.givenName en subject.surname

7.5 Kaart-, houder- en gebruikersgroep-identificerende velden uit CABS

Binnen het datamodel voor de Boordcomputer Taxi wordt er gebruik gemaakt van de velden Kaarthoofdtype, Kaarthoudernummer en Kaartvolgnummer om een specifieke kaart te identificeren. Deze nummers worden door het Card Aanvraag & Beschikking Systeem (CABS) uitgegeven. De combinatie van de velden Kaarthoofdtype en Kaarthoudernummer is daarbij binnen het domein van Boordcomputer Taxi uniek identificerend voor de houder van het certificaat.

CABS registreert daarnaast voor taxichauffeurs een kaartsubtype dat het niveau van een chauffeursopleiding aanduidt.

De subparagrafen van deze paragraaf geven een specificatie van de hierboven genoemde velden. De beschreven velden wordt op meerdere plekken in het certificaat gebruikt.

7.5.1 Kaarthoofdtype

De Kaarthoofdtypes die binnen ILT bekend zijn: Chauffeurskaart, Ondernemerskaart, Keuringskaart, Inspectiekaart en Systeemkaart.

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

Tabel 21 - Kaarthoofdtype

Het Kaarthoofdtype kan gebruikt worden door een boordcomputer om de gebruikersgroep van de kaarthouder vast te stellen.

7.5.2 Kaartsubtype

Het Kaartsubtype is een veld dat gevuld wordt door CABS. De inhoud komt overeen met wat er gebruikt wordt binnen ILT. Dit veld is 3 karakters lang en van het type Text.

Met deze gegevens wordt binnen de boordcomputer niets gedaan maar dient er voor om binnen achterliggende systemen de chauffeurskaarten te kunnen herleiden naar niveau van de vergunning.

NB: Alleen voor de chauffeurskaart is er een kaartsubtype gedefinieerd.

7.5.3 Kaarthoudernummer

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

Kaarthoofdtype	Veldinhoud Kaarthoudernummer	Type en lengte
Chauffeurskaart	BSN of NI-nummer van de chauffeur.	Text 9
Ondernemerskaart	KvK-nummer (8 cijfers) en aansluitend '0000' of een 4 cijferig vestigingsnummer	Text 12
Keuringskaart	RDW-Erkenningsnummer	Text 7
Inspectiekaart	Inspectienummer	Text 10
Systeemkaart	Een door ILT gegenereerd uniek boordcomputernummer	Text 9

Tabel 22 - Kaarthoudernummer

NB 1: Voor de Chauffeurskaart wordt het BSN gebruikt. Indien er geen BSN bekend is van een chauffeur dan kent ILT een eigen nummer aan de houders toe. Dit nummer begint met "NI" en wordt gevolgd door het ILT-nummer.

7.5.4 Kaartvolgnummer

Dit nummer wordt gebruikt om de kaart uniek te identificeren binnen de combinatie Kaarthoofdtype en Kaarthoudernummer. Dit ondersteunt zowel het bestaan van meerdere kaarten per houder op eenzelfde moment in tijd, als vervanging van kaarten. De lengte van dit veld is altijd 5 cijferposities.

Kaartvolgnummers beginnen met 00001 en lopen opvolgend op.

7.5.5 Subject serialNumber

Aanvullend op de PKI-overheid eis dat het subject.serialNumber bruikbaar moet zijn om de certificaathouder uniek te identificeren, gebruikt Boordcomputer Taxi dat nummer ook om de kaart waarvoor het certificaat is uitgegeven, te identificeren. De opbouw van een subject.serialNumber is als volgt:

Kaarthoofdtype + Kaarthoudernummer + "-" + Kaartvolgnummer

7.5.6 Voorbeeld van de inhoud subject.serialNumber

Voorbeeld:
subject.serialNumber = C123456789-00002

In bovenstaand voorbeeld is:
- [Kaarthoofdtype] = C (type: Chauffeurskaart);
- [BSN] = 123456789;
- [Kaartvolgnummer] = 00002 (vervangende of vervolgkaart).

7.6 Subject title

Dit attribuut vermeldt de rol van een kaart/gebruiker. Het kan gebruikt worden in de Boordcomputer Taxi om de gebruikersgroep van de kaarthouder vast te stellen.

De opbouw van dit veld is:
[Kaarthoofdtype] + [Kaartsubtype]

Binnen Boordcomputer Taxi zijn daarmee de volgende waarden mogelijk:

Type	Inhoud
Chauffeurskaart Volledig	CVOL
Chauffeurskaart Beperkt	CBEP
Ondernemerskaart	O
Keuringskaart	K
Inspectiekaart	I
Systeemkaart	S

Tabel 23 - Subject.Title

NB 1: Alleen voor de chauffeurskaart is er een kaartsubtype gedefinieerd.

NB 2: De huidige invulling van de subject.title voldoet niet aan het PvE PKIoverheid. Voor de volgende afwijkingen is tijdelijk een dispensatie verleend:

1. Ondernemerskaarten en Keuringskaarten waar het attribuut is opgenomen, terwijl dat niet is toegestaan conform PvE deel 3b;
2. Chauffeurskaarten en Inspectiekaarten (uitgegeven onder PvE deel 3a) waarin beroepen zijn opgenomen in de subject.title die niet op de limitatieve lijst met erkende beroep staan zoals zijn beschreven zijn in eis 3.2.5-pkio160.

7.7 certificatePolicies extensie

De volgende waarden voor certificatePolicies extensie zullen worden geconfigureerd.

7.7.1 certificatePolicies.policyIdentifier

Tabel 24 geeft een overzicht van de binnen het domein Boordcomputer Taxi relevante PolicyIdentifiers (OID’s).

Certificaatgebruik/kaarttype	PolicyIdentifiers (OID)	Beschrijving
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 Persoon (G3)
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 Persoon (G3)
Services Authenticiteitcertificaten: -Keuringskaart -Ondernemerskaart	2.16.528.1.1003.1.2.5.4	OID van de PKI-overheid Certificate Policy voor servercertificaten in het domein Organisatie Services (G3)
Autonome Apparaten Authenticiteitcertificaten: -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 24 - Waarden PolicyIdentifiers van certificaten

7.7.2 certificatePolicies.PolicyQualifier.cPS.uri

Voor Boordcomputer Taxi is één certification practice statement (CPS) van kracht. Dat CPS zal (uitsluitend) in PDF formaat worden gepubliceerd en via het hypertext transfer protocol (https) opvraagbaar zijn.
Om onafhankelijk te zijn van toekomstige wijzigingen van het CPS, wordt de bestandsnaam niet in de URL opgenomen.
In elk certificaat zal het veld certificatePolicies.PolicyQualifier.cPS.uri worden gevuld met de, als IA5String gecodeerde, URL:

https://bct.tsp.minienw.nl/minienw-bct-cps

7.7.3 certificatePolicies.PolicyQualifier.userNotice.explicitText

Het veld certificatePolicies.PolicyQualifier.userNotice.explicitText wordt gevuld met de volgende tekst. Deze tekst dient als UTF8String gecodeerd te zijn:

Het CPS voor dit certificaat kan worden geraadpleegd op: https://bct.tsp.minienw.nl/minienw-bct-cps

7.8 Qualified Certificates (qcStatements)

Deze extensie komt alleen voor in de persoonsgebonden Handtekeningcertificaten in productieomgeving.

Het qcStatement is uitgebreid door PvE wijziging 333 die samenhangt met het in werking treden van EU Verordening 910/2014. Het bevat nu de volgende qcStatements:

- etsiQcsCompliance. Dit geeft aan dat uitgifte van gekwalificeerd certificaat overeenstemt met annex I van EU Verordening 910/2014[2].
- etsiQcsQcSSCD. Dit geeft aan dat de private sleutel behorende bij de publieke sleutel in het certificaat is opgeslagen op een Qualified Signature Creation Device (QSCD) overeenstemmend met annex II van EU Verordening 910/2015.
- etsiQcsQcType. Dit geeft het type gekwalificeerd certificaat aan overeenstemmend met annex I van EU Verordening 910/2014. In dit geval Type 1: eSigning.
- etsiQcsQcPDS. Dit bevat een verwijzing naar het PKI Dislosure Statement (PDS). Dit is een document dat een samenvatting geeft van de belangrijkste punten uit het CPS. Zie voor een toelichting op het doel en de structuur van een PDS: *ETSI EN 319 411-1, Annex A (informative): Model PKI disclosure statement*.

Onderdeel van het etsiQcsQcPDS is de URL waarop het PDS is gepubliceerd. In elk handtekeningcertificaat is de volgende URL worden opgenomen gecodeerd als IA5String:

https://bct.tsp.minienw.nl/minienw-bct-pds

7.9 CRL Distribution Points

Het veld cRLDistributionPoints van de gebruikerscertificaten kan een of meer publicatiepunten, elk met een bepaald toegangsprotocol, aanduiden. Binnen het domein van Boordcomputer Taxi zullen de uitgevende CA's slechts één CRL bijhouden voor alle mogelijke intrekkingredenen. Bovendien zal die CRL slechts via het hypertext transfer protocol (http) opvraagbaar zijn. In elk certificaat zal het veld cRLDistributionPoints.distributionPoint.fullName worden gevuld met de volgende, als IA5String gecodeerde, URL:

IenWOrganisatiePersoonCAG3:

http://bct.tsp.minienw.nl/minienw-org-pers-ca-g3.crl

BoordcomputerkaartenServicesCAG3:

http://bct.tsp.minienw.nl/minienw-org-serv-ca-g3.crl

IenWApparatenCAG3:

http://bct.tsp.minienw.nl/minienw-aa-ca-g3.crl

Verdere eisen:

- Het CRL bestand moet DER-encoded zijn;
- De bestandsnaamextensie moet ".crl" zijn;
- De http server moet als media type voor deze url de waarde "application/pkix-crl" aangeven.

2 Voorheen gaf dit attribuut aan dat het een certificaat gekwalificeerd betrof zoals beschreven in ETSI TS 101 456 en voldoet aan Bijlage I en II of the EU directive 1999/93/EC.

7.10 SubjectAltName en extKeyUsage

PKIoverheid eist dat de subjectAltName in een eindgebruikercertificaat in minimaal één otherName (in één van de voorgeschreven formaten) de combinatie van de volgende twee elementen vastlegt:

- De OID van de uitgevende CA;
- Een nummer/code die binnen voornoemde CA de certificaathouder uniek identificeert.

Boordcomputer Taxi zal met betrekking tot deze eis in alle eindgebruikercertificaten (inclusief de servicescertificaten) gebruik maken van een otherName in het formaat voor een Permanent Identifier zoals gedefinieerd in RFC 4043, waarbij de subvelden van permanentIdentifier als volgt worden gevuld:

- identifierValue: een UTF8String bestaande uit [Kaarthoofdtype] + [Kaarthoudernummer];
- assigner: de als OID gecodeerde waarde van de OID van de CA.

Bij de overgang naar G3 is de Microsoft User Principal Name (UPN) (die gevuld was met [Kaarthoofdtype] + [Kaarthoudernummer] + '@' + [CA.OID in dotted decimal notatie]) niet meer opgenomen in de certificaten.

Zie voor de OID's van de verschillende CA's par. 3.4.

Specifiek voor die bredere inzetbaarheid van boordcomputerkaarten, wordt aan de authenticiteitcertificaten van die kaarten ook de extensie extKeyUsage toegevoegd. Met PvE update versie 4.2 is de extKeyUsage toegevoegd aan Systeemkaarten. Met de uitvoering van PKIoverheid change 342 is ook een extKeyUsage toegevoegd aan handtekeningcertificaten.

7.11 URL's van CA certificaten

De eindgebruikercertificaten bevatten een verwijzing naar het certificaat van hun uitgever. Daarom publiceert PKIoverheid de TSP CA certificaten op vaste URL's. Zie voor de URL's van de CA certificaten par. 3.5.

7.12 OCSP

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

7.13 Certificaten voor non-productieomgevingen

Voor de ~~test en~~ acceptatieomgeving~~en~~ zijn de profielen van de eindgebruikercertificaten nagenoeg gelijk aan die van de productieomgeving. De verschillen zitten hem voornamelijk in de naamgeving van de CA's (issuer.DN's) en in de URL's voor CA certificaten, CRL's en CPS's. Zie hiervoor hoofdstuk 4. Daarnaast geldt dat **geen enkel** certificaat uit een niet-productieomgeving voorzien zal zijn van de qCStatements extensie die aanduidt dat het een gekwalificeerd certificaat zou betreffen (zie par. 7.8).

Met betrekking tot subject distinguished names gelden vanuit het certificaatprofiel geen verdere beperkingen aan de eindgebruikercertificaten van non-productie-omgevingen. Uiteraard verdient het de voorkeur om in deze soort omgevingen niet met de gegevens van bestaande personen te werken.

7.14 Toelichting bij tabellen eindgebruikercertificaten

In de tabellen voor de profielen is een aantal kolommen opgenomen. Hierna vindt men een uitleg van de kolommen en de benamingen van deze:

- Certificaat / Attribuut: Deze bevat de naam van het certificaatveld in de certificaten;
- OID: Hierin is, voor zover toepasselijk, de Object IDentifier van het attribuut opgenomen zoals deze in de RFC's is beschreven. Dit is de standaard naamgeving;
- Type: dit betreft het gegevenstype van de waarde die het veld moet krijgen;
- Waarde: Dit is de waarde die het veld moet krijgen;
- Referentie: De laatste kolom verwijst naar een beschrijving en/of nadere toelichting op het veld.

Om ruimte te sparen is in het tabellen gebruik gemaakt van de kleur geel om aan te duiden of een attribuut variabel is en van rood om aan te duiden of een extensie kritiek is; de combinatie van variabel met kritiek komt niet voor.

De kleur groen is gebruikt om die attributen aan te duiden, die bepaald worden door de CA die het certificaat uitgeeft.

De basisstructuur van een certificaat bestaat uit een to-be-signed gedeelte (tbsCertificate) en een handtekening van de uitgever. Het tbsCertificate bestaat uit een aantal verplichte basisvelden gevolgd door extensies.

8 Profielen gebruikercertificaten Chauffeurskaart

8.1 Profiel authenticiteitcertificaat Chauffeurskaart

Certificaat/Attribuut	OID	Type	Waarde	Ref. §
Certificate				
signatureAlgorithm		OID	1.2.840.113549.1.1.11 { sha256WithRSAEncryption }	
signatureValue		BIT STRING	*Handtekening van de IenWOrganisatiePersoonCAG3*	
tbsCertificate				
version		INTEGER	2 { X.509v3 }	
serialNumber		INTEGER	*Certificaatserienummer toegekend door de IenWOrganisatiePersoonCAG3 (een random gegenereerd, uniek, 160 bits, positief integer)*	
signature		OID	1.2.840.113549.1.1.11 { signatureAlgorithm }	
Issuer.DN				7.1
.countryName	C { id-at 6 }	PrintableString	*NL*	
.organizationName	O { id-at 10 }	UTF8String	*Ministerie van Infrastructuur en Waterstaat*	
.organizationIdentifier	2.5.4.97	UTF8String	*NTRNL-52766179*	
.commonName	CN { id-at 3 }	UTF8String	*MinIenW PKIoverheid Organisatie Persoon CA - G3*	
Validity				7.2
.notBefore		UTCTime	*Tijdstip waarop het certificaat geldig wordt*	
.notAfter		UTCTime	*Tijdstip waar**na** het certificaat **on**geldig wordt*	
Subject				
.countryName	C { id-at 6 }	PrintableString	NL	
.organizationName	O { id-at 10 }	UTF8String	[Eerste voornaam] [Verdere voorletters] [Voorvoegsel] [Geslachtsnaam]	7.3
.commonName	CN { id-at 3 }	UTF8String	[Eerste voornaam] [Verdere voorletters] [Voorvoegsel] [Geslachtsnaam]	7.4
.givenName	G { id-at 42 }	UTF8String	[Eerste voornaam] [Verdere voorletters]	7.4
.surname	S { id-at 4 }	UTF8String	[Voorvoegsel] [Geslachtsnaam]	7.4
.serialNumber	{ id-at 5 }	PrintableString	[Kaarthoofdtype] + [BSN] + "-" + [Kaartvolgnummer]of[Kaarthoofdtype] + [NI-Nummer] + "-" + [Kaartvolgnummer]	7.5.5
.title	{ id-at 12 }	UTF8String	[Kaarthoofdtype] + [Kaartsubtype]	7.6

Certificaat/Attribuut	OID	Type	Waarde	Ref. §
SubjectPublicKeyInfo				
.algorithm		OID	1.2.840.113549.1.1.1 { rsaEncryption }	
.subjectPublicKey		BIT STRING	*2048 bits RSA publieke sleutel van de certificaathouder*	
Extensions				
certificatePolicies	{ id-ce 32 }			
.PolicyIdentifier		OID	2.16.528.1.1003.1.2.5.1	7.7.1
.PolicyQualifier				
.cPS.uri	{ id-qt 1 }	IA5String	https://bct.tsp.minienw.nl/minienw-bct-cps	7.7.2
.userNotice .explicitText	{ id-qt 2 }	UTF8String	Het CPS voor dit certificaat kan worden geraadpleegd op: https://bct.tsp.minienw.nl/minienw-bct-cps	7.7.3
keyUsage	{ id-ce 15 }	BIT STRING	digitalSignature	
AuthorityInfoAccess	{ id-pe 1 }			
.caIssuers	{ id-ad 2 }	URI - IA5String	http://cert.pkioverheid.nl/MinIenW_PKIoverheid_Organisatie_Persoon_CA-G3.cer	7.11
authorityKeyIdentifier	{ id-ce 35 }			
.keyIdentifier		OCTET STRING	IenWOrganisatiePersoonCAG3.subjectPublicKeyIdentifier.keyIdentifier	
subjectKeyIdentifier .keyIdentifier	{ id-ce 14 }	OCTET STRING	*SHA-1 hash van publieke sleutel van dit certificaat*	
cRLDistributionPoints .distributionPoint .fullName	{ id-ce 31 }	URI – IA5String	http://bct.tsp.minienw.nl/minienw-org-pers-ca-g3.crl	7.9
subjectAltName.othername	{ id-ce 17 }			7.10
.permanentIdentifier	{ id-on 3 }			
.identifierValue		UTF8String	[Kaarthoofdtype] + [BSN]of[Kaarthoofdtype] + [NI-nummer]	
.assigner		OID	2.16.528.1.1003.1.3.10.1.1	3.4
basicConstraints	{ id-ce 19 }			
.cA			Door het CA attribuut weg te laten, geldt de default waarde: CA=False	
.pathLenConstraint			Door het attribuut weg te laten, geldt de default waarde: pathLenConstraint=None	
extKeyUsage	{ id-ce 37 }		clientAuth: 1.3.6.1.5.5.7.3.2 Document_Signing: 1.3.6.1.4.1.311.10.3.12	

Tabel 25 - Profiel authenticiteitcertificaat Chauffeurskaart

8.2 Profiel handtekeningcertificaat Chauffeurskaart

Van de profieldefinitie van het handtekeningcertificaat van een chauffeurskaart zijn in de onderstaande tabel uitsluitend de verschillen met het authenticiteitcertificaat van een chauffeurskaart opgenomen. Naast deze verschillen zijn er uiteraard verschillen in de waarde van attributen die (gebaseerd zijn op) random data zoals publieke sleutel, certificaatserienummer en subjectKeyIdentifier.

Certificaat / Attribuut	OID	Type	Waarde	Ref. §
Extensions				
certificatePolicies.PolicyIdentifier		OID	2.16.528.1.1003.1.2.5.2	7.7.1
keyUsage	{ id-ce 15 }	BIT STRING	nonRepudiation	
qcStatements	{ id-pe 3 }	OID	1.3.6.1.5.5.7.1.3	7.8
.etsiQcsCompliance	{ id-etsi-qcs 1 }	OID	0.4.0.1862.1.1	
.etsiQcsQcSSCD	{ id-etsi-qcs 4 }	OID	0.4.0.1862.1.4	
.etsiQcsQcType	{ id-etsi-qcs-QcType }	OID	0.4.0.1862.1.6	
.Type 1 (esign)	{ id-etsi-qcs-QcType 1 }[3]	OID	0.4.0.1862.1.6.1	
.etsiQcsQcPDS	{ id-etsi-qcs 5 }		0.4.0.1862.1.5	
.url		IA5String	https://bct.tsp.minienw.nl/minienw-bct-pds	
.language		PrintableString	"en"	
subjectAltName.othername			bevat uitsluitend de PermanentIdentifier	7.10
extKeyUsage	{id-ce 37}	OID	document Signing: 1.3.6.1.4.1.311.10.3.12	

Tabel 26 - Profiel handtekeningcertificaat Chauffeurskaart

3Dit geeft aan dat het gekwalificeerd certificaat is voor elektronische handtekeningen overeenstemmend met annex I van EU Verordening 910/2014 (id-etsi-qct-esign).

9 Profielen gebruikercertificaten Ondernemerskaart

9.1 Profiel authenticiteitcertificaat Ondernemerskaart

Certificaat / Attribuut	OID	Type	Waarde	Ref. §
Certificate				
signatureAlgorithm		OID	1.2.840.113549.1.1.11 { sha256WithRSAEncryption }	
signatureValue		BIT STRING	*Handtekening van de IenWOrganisatieServicesCAG3*	
tbsCertificate				
version		INTEGER	2 { X.509v3 }	
serialNumber		INTEGER	*Certificaatnummer toegekend door de IenWOrganisatieServicesCAG3 (een random gegenereerd, uniek, 160 bits, positief integer).*	
signature		OID	1.2.840.113549.1.1.11 { signatureAlgorithm }	
Issuer.DN				7.1
.countryName	C { id-at 6 }	PrintableString	*NL*	
.organizationName	O { id-at 10 }	UTF8String	*Ministerie van Infrastructuur en Waterstaat*	
.organizationIdentifier	2.5.4.97	UTF8String	*NTRNL-52766179*	
.commonName	CN { id-at 3 }	UTF8String	*MinIenW PKIoverheid Organisatie Services CA - G3*	
Validity				7.2
.notBefore		UTCTime	*Tijdstip waarop het certificaat geldig wordt*	
.notAfter		UTCTime	*Tijdstip waar**na** het certificaat **on**geldig wordt*	
Subject				
.countryName	C { id-at 6 }	PrintableString	NL	Altijd NL
.organizationName	O { id-at 10 }	UTF8String	[Naam onderneming]	7.3
.organizationalUnitName		UTF8String	[P-nummer]	7.3
.organizationIdentifier	2.5.4.97	UTF8String	NTRNL-[kvk-nummer onderneming]	7.3
.commonName	CN { id-at 3 }	UTF8String	[Naam onderneming]	7.4
.serialNumber	{ id-at 5 }	PrintableString	[Kaarthoofdtype] + [KvK-nummer 8 cijferig] + [“0000” of 4 cijferig vestigingsnummer] + “-“ + [Kaartvolgnummer]	7.5.5
.title	{ id-at 12 }	UTF8String	[Kaarthoofdtype] + [Kaartsubtype]	7.6

Certificaat / Attribuut	OID	Type	Waarde	Ref. §
SubjectPublicKeyInfo				
.algorithm		OID	1.2.840.113549.1.1.1 { rsaEncryption }	
.subjectPublicKey		BIT STRING	*2048 bits RSA publieke sleutel van de certificaathouder*	
Extentions				
certificatePolicies	{ id-ce 32 }			
.PolicyIdentifier		OID	2.16.528.1.1003.1.2.5.4	7.7.1
.PolicyQualifier				
.**cPS**.uri	{ id-qt 1 }	IA5String	https://bct.tsp.minienw.nl/minienw-bct-cps	7.7.2
.**userNotice** .explicitText	{ id-qt 2 }	UTF8String	Het CPS voor dit certificaat kan worden geraadpleegd op: https://bct.tsp.minienw.nl/minienw-bct-cps	7.7.3
keyUsage	{ id-ce 15 }	BIT STRING	digitalSignature	
AuthorityInfoAccess	{ id-pe 1 }			
.caIssuers	{ id-ad 2 }	URI - IA5String	http://cert.pkioverheid.nl/MinIenW_PKIoverheid_Organisatie_Services_CA-G3.cer	7.11
authorityKeyIdentifier	{ id-ce 35 }			
.keyIdentifier		OCTET STRING	IenWOrganisatieServicesCAG3.subjectPublicKeyIdentifier.keyIdentifier	
subjectKeyIdentifier .keyIdentifier	{ id-ce 14 }	OCTET STRING	*SHA-1 hash van publieke sleutel van dit certificaat*	
cRLDistributionPoints .distributionPoint .fullName	{ id-ce 31 }	URI – IA5String	http://bct.tsp.minienw.nl/minienw-org-serv-ca-g3.crl	7.9
subjectAltName.othername	{ id-ce 17 }			7.10
.**permanentIdentifier**	{ id-on 3 }			
.identifierValue		UTF8String	[Kaarthoofdtype] + [KvK-nummer] + [“0000” of 4 cijferig vestigingsnummer]	
.assigner		OID	2.16.528.1.1003.1.3.11.1.1	3.4
basicConstraints	{ id-ce 19 }			
.cA			Door het CA attribuut weg te laten, geldt de default waarde: CA=False	
.pathLenConstraint			Door het attribuut weg te laten, geldt de default waarde: pathLenConstraint=None	
extKeyUsage	{ id-ce 37 }		clientAuth: 1.3.6.1.5.5.7.3.2 Document_Signing: 1.3.6.1.4.1.311.10.3.12	

Tabel 27 - Profiel authenticiteitcertificaat Ondernemerskaart

10 Profielen gebruikercertificaten Keuringskaart

10.1 Profiel authenticiteitcertificaat Keuringskaart

Certificaat / Attribuut	OID	Type	Waarde	Ref. §
Certificate				
signatureAlgorithm		OID	1.2.840.113549.1.1.11 { sha256WithRSAEncryption }	
signatureValue		BIT STRING	*Handtekening van de IenWOrganisatieServicesCAG3*	
tbsCertificate				
version		INTEGER	2 { X.509v3 }	
serialNumber		INTEGER	*Certificaatnummer toegekend door de IenWOrganisatieServicesCAG3 (een random gegenereerd, uniek, 160 bits, positief integer).*	
signature		OID	1.2.840.113549.1.1.11 { signatureAlgorithm }	
Issuer.DN				7.1
.countryName	C { id-at 6 }	PrintableString	*NL*	
.organizationName	O { id-at 10 }	UTF8String	*Ministerie van Infrastructuur en Waterstaat*	
.organizationIdentifier	2.5.4.97	UTF8String	*NTRNL-52766179*	
.commonName	CN { id-at 3 }	UTF8String	*MinIenW PKIoverheid Organisatie Services CA - G3*	
Validity				7.2
.notBefore		UTCTime	*Tijdstip waarop het certificaat geldig wordt*	
.notAfter		UTCTime	*Tijdstip waar**na** het certificaat **on**geldig wordt*	
Subject				
.countryName	C { id-at 6 }	PrintableString	NL	Altijd NL
.organizationName	O { id-at 10 }	UTF8String	[Naam keuringsinstantie]	7.3
.organizationIdentifier	2.5.4.97	UTF8String	NTRNL-[kvk-nummer keuringsinstantie]	7.3
.commonName	CN { id-at 3 }	UTF8String	[Naam keuringsinstantie]	7.4
.serialNumber	{ id-at 5 }	PrintableString	[Kaarthoofdtype] + [RDW-erkenningsnummer] + "-" + [Kaartvolgnummer]	7.5.5
.title	{ id-at 12 }	UTF8String	[Kaarthoofdtype] + [Kaartsubtype]	7.6
SubjectPublicKeyInfo				
.algorithm		OID	1.2.840.113549.1.1.1 { rsaEncryption }	

Certificaat / Attribuut	OID	Type	Waarde	Ref. §
.subjectPublicKey		BIT STRING	*2048 bits RSA publieke sleutel van de certificaathouder*	
Extentions				
certificatePolicies	{ id-ce 32 }			
.PolicyIdentifier		OID	2.16.528.1.1003.1.2.5.4	7.7.1
.PolicyQualifier				
.**cPS**.uri	{ id-qt 1 }	IA5String	https://bct.tsp.minienw.nl/minienw-bct-cps	7.7.2
.**userNotice** .explicitText	{ id-qt 2 }	UTF8String	Het CPS voor dit certificaat kan worden geraadpleegd op: https://bct.tsp.minienw.nl/minienw-bct-cps	7.7.3
keyUsage	{ id-ce 15 }	BIT STRING	digitalSignature	
authorityInfoAccess	{ id-pe 1 }			
.caIssuers	{ id-ad 2 }	URI - IA5String	http://cert.pkioverheid.nl/MinIenW_PKIoverheid_Organisatie_Services_CA-G3.cer	7.11
authorityKeyIdentifier	{ id-ce 35 }			
.keyIdentifier		OCTET STRING	IenWOrganisatieServicesCAG3.subjectPublicKeyIdentifier.keyIdentifier	
subjectKeyIdentifier .keyIdentifier	{ id-ce 14 }	OCTET STRING	*SHA-1 hash van publieke sleutel van dit certificaat*	
cRLDistributionPoints .distributionPoint .fullName	{ id-ce 31 }	URI – IA5String	http://bct.tsp.minienw.nl/minienw-org-serv-ca-g3.crl	7.9
subjectAltName.othername	{ id-ce 17 }			7.10
.**permanentIdentifier**	{ id-on 3 }			
.identifierValue		UTF8String	[Kaarthoofdtype] + [RDW-erkenningsnummer]	
.assigner		OID	2.16.528.1.1003.1.3.11.1.1	3.4
basicConstraints	{ id-ce 19 }			
.cA			Door het CA attribuut weg te laten, geldt de default waarde: CA=False	
.pathLenConstraint			Door het attribuut weg te laten, geldt de default waarde: pathLenConstraint=None	
extKeyUsage	{ id-ce 37 }		clientAuth: 1.3.6.1.5.5.7.3.2 Document_Signing: 1.3.6.1.4.1.311.10.3.12	

Tabel 28 - Profiel authenticiteitcertificaat Keuringskaart

11 Profielen gebruikercertificaten Inspectiekaart

11.1 Profiel authenticiteitcertificaat Inspectiekaart

Certificaat / Attribuut	OID	Type	Waarde	Ref. §
Certificate				
signatureAlgorithm		OID	1.2.840.113549.1.1.11 { sha256WithRSAEncryption }	
signatureValue		BIT STRING	*Handtekening van de IenWOrganisatiePersoonCAG3*	
tbsCertificate				
version		INTEGER	2 { X.509v3 }	
serialNumber		INTEGER	*Certificaatnummer toegekend door de IenWOrganisatiePersoonCAG3 (een random gegenereerd, uniek, 160 bits, positief integer).*	
signature		OID	1.2.840.113549.1.1.11 { signatureAlgorithm }	
Issuer.DN				7.1
.countryName	C { id-at 6 }	PrintableString	*NL*	
.organizationName	O { id-at 10 }	UTF8String	*Ministerie van Infrastructuur en Waterstaat*	
.organizationIdentifier	2.5.4.97	UTF8String	*NTRNL-52766179*	
.commonName	CN { id-at 3 }	UTF8String	*MinIenW PKIoverheid Organisatie Persoon CA - G3*	
Validity				7.2
.notBefore		UTCTime	*Tijdstip waarop het certificaat geldig wordt*	
.notAfter		UTCTime	*Tijdstip waar**na** het certificaat **on**geldig wordt*	
Subject				
.countryName	C { id-at 6 }	PrintableString	NL	Altijd NL
.organizationName	O { id-at 10 }	UTF8String	[Naam inspectiedienst]	7.3
.commonName	CN { id-at 3 }	UTF8String	[Eerste voornaam] [Verdere voorletters] [Voorvoegsel] [Geslachtsnaam]	7.4
.givenName	G { id-at 42 }	UTF8String	[Eerste voornaam] [Verdere voorletters]	7.4
.surname	S { id-at 4 }	UTF8String	[Voorvoegsel] [Geslachtsnaam]	7.4
.serialNumber	{ id-at 5 }	PrintableString	[Kaarthoofdtype] + [Inspectienummer] + "-" + [Kaartvolgnummer]	7.5.5
.title	{ id-at 12 }	UTF8String	[Kaarthoofdtype] + [Kaartsubtype]	7.6
SubjectPublicKeyInfo				

Certificaat / Attribuut	OID	Type	Waarde	Ref. §
.algorithm		OID	1.2.840.113549.1.1.1 { rsaEncryption }	
.subjectPublicKey		BIT STRING	*2048 bits RSA publieke sleutel van de certificaathouder*	
Extentions				
certificatePolicies	{ id-ce 32 }			
.PolicyIdentifier		OID	2.16.528.1.1003.1.2.5.1	7.7.1
.PolicyQualifier				
.**cPS**.uri	{ id-qt 1 }	IA5String	https://bct.tsp.minienw.nl/minienw-bct-cps	7.7.2
.**userNotice** .explicitText	{ id-qt 2 }	UTF8String	Het CPS voor dit certificaat kan worden geraadpleegd op: https://bct.tsp.minienw.nl/minienw-bct-cps	7.7.3
keyUsage	{ id-ce 15 }	BIT STRING	digitalSignature	
authorityInfoAccess	{ id-pe 1 }			
.caIssuers	{ id-ad 2 }	URI - IA5String	http://cert.pkioverheid.nl/MinIenW_PKIoverheid_Organisatie_Persoon_CA-G3.cer	7.11
authorityKeyIdentifier	{ id-ce 35 }			
.keyIdentifier		OCTET STRING	IenWOrganisatiePersoonCAG3.subjectPublicKeyIdentifier.keyIdentifier	
subjectKeyIdentifier .keyIdentifier	{ id-ce 14 }	OCTET STRING	*SHA-1 hash van publieke sleutel van dit certificaat*	
cRLDistributionPoints .distributionPoint .fullName	{ id-ce 31 }	URI – IA5String	http://bct.tsp.minienw.nl/minienw-org-pers-ca-g3.crl	7.9
subjectAltName.othername	{ id-ce 17 }			7.10
.**permanentIdentifier**	{ id-on 3 }			
.identifierValue		UTF8String	[Kaarthoofdtype] + [Inspectienummer]	
.assigner		OID	2.16.528.1.1003.1.3.10.1.1	3.4
basicConstraints	{ id-ce 19 }			
.cA			Door het CA attribuut weg te laten, geldt de default waarde: CA=False	
.pathLenConstraint			Door het attribuut weg te laten, geldt de default waarde: pathLenConstraint=None	
extKeyUsage	{ id-ce 37 }		clientAuth: 1.3.6.1.5.5.7.3.2 Document_Signing: 1.3.6.1.4.1.311.10.3.12	

Tabel 29 - Profiel authenticiteitcertificaat inspectiekaart

11.2 Profiel handtekeningcertificaat Inspectiekaart

Van de profieldefinitie van het handtekeningcertificaat van een inspectiekaart zijn in de onderstaande tabel uitsluitend de verschillen met het authenticiteitcertificaat van een inspectiekaart opgenomen. Naast deze verschillen zijn er uiteraard verschillen in de waarde van attributen die (gebaseerd zijn op) random data zoals publieke sleutel, certificaatserienummer en subjectKeyIdentifier.

Certificaat / Attribuut	**OID**	**Type**	**Waarde**	**Ref. §**
Extentions				
certificatePolicies.PolicyIdentifier		OID	2.16.528.1.1003.1.2.5.2	7.7.1
keyUsage	{ id-ce 15 }	BIT STRING	nonRepudiation	
qcStatements	{ id-pe 3 }	OID	1.3.6.1.5.5.7.1.3	7.8
.etsiQcsCompliance	{ id-etsi-qcs 1 }	OID	0.4.0.1862.1.1	
.etsiQcsQcSSCD	{ id-etsi-qcs 4 }	OID	0.4.0.1862.1.4	
.etsiQcsQcType	{ id-etsi-qcs-QcType }	OID	0.4.0.1862.1.6	
.Type 1 (esign)	{ id-etsi-qcs-QcType 1 }[4]	OID	0.4.0.1862.1.6.1	
.etsiQcsQcPDS	{ id-etsi-qcs 5 }		0.4.0.1862.1.5	
.url		IA5String	https://bct.tsp.minienw.nl/minienw-bct-pds	
.language		PrintableString	"en"	
subjectAltName.othername			bevat uitsluitend de PermanentIdentifier	7.10
extKeyUsage	{id-ce 37}	OID	document Signing: 1.3.6.1.4.1.311.10.3.12	

Tabel 30 - Profiel handtekeningcertificaat Inspectiekaart

4 Dit geeft aan dat het gekwalificeerd certificaat is voor elektronische handtekeningen overeenstemmend met annex I van EU Verordening 910/2014 (id-etsi-qct-esign).

12 Profielen gebruikercertificaten Systeemkaart

12.1 Profiel authenticiteitcertificaat Systeemkaart

Certificaat / Attribuut	OID	Type	Waarde	Ref. §
Certificate				
signatureAlgorithm		OID	1.2.840.113549.1.1.11 { sha256WithRSAEncryption }	
signatureValue		BIT STRING	*Handtekening van de IenWApparatenCAG3*	
tbsCertificate				
version		INTEGER	2 { X.509v3 }	
serialNumber		INTEGER	*Certificaatnummer toegekend door de IenWApparatenCAG3 (een random gegenereerd, uniek, 160 bits, positief integer).*	
signature		OID	1.2.840.113549.1.1.11 { signatureAlgorithm }	
Issuer.DN				7.1
.countryName	C { id-at 6 }	PrintableString	*NL*	
.organizationName	O { id-at 10 }	UTF8String	*Ministerie van Infrastructuur en Waterstaat*	
.organizationIdentifier	2.5.4.97	UTF8String	*NTRNL-52766179*	
.commonName	CN { id-at 3 }	UTF8String	*MinIenW PKIoverheid Autonome Apparaten CA - G3*	
Validity				7.2
.notBefore		UTCTime	*Tijdstip waarop het certificaat geldig wordt*	
.notAfter		UTCTime	*Tijdstip waar***na** *het certificaat* ***on****geldig wordt*	
Subject				
.countryName	C { id-at 6 }	PrintableString	NL	Altijd NL
.organizationName	O { id-at 10 }	UTF8String	[Naam boordcomputerfabrikant]	7.3
.commonName	CN { id-at 3 }	UTF8String	[Typegoedkeuringsnummer]	7.4
.serialNumber	{ id-at 5 }	PrintableString	[Kaarthoofdtype] + [Boordcomputernummer] + "-" + [Kaartvolgnummer]	7.5.5
.title	{ id-at 12 }	UTF8String	[Kaarthoofdtype] + [Kaartsubtype]	7.6
SubjectPublicKeyInfo				

Certificaat / Attribuut	OID	Type	Waarde	Ref. §
.algorithm		OID	1.2.840.113549.1.1.1 { rsaEncryption }	
.subjectPublicKey		BIT STRING	*2048 bits RSA publieke sleutel van de certificaathouder*	
Extentions				
certificatePolicies	{ id-ce 32 }			
.PolicyIdentifier		OID	2.16.528.1.1003.1.2.6.1	7.7.1
.PolicyQualifier				
.**cPS**.uri	{ id-qt 1 }	IA5String	https://bct.tsp.minienw.nl/minienw-bct-cps	7.7.2
.**userNotice** .explicitText	{ id-qt 2 }	UTF8String	Het CPS voor dit certificaat kan worden geraadpleegd op: https://bct.tsp.minienw.nl/minienw-bct-cps	7.7.3
keyUsage	{ id-ce 15 }	BIT STRING	digitalSignature	
authorityInfoAccess	{ id-pe 1 }			
.caIssuers	{ id-ad 2 }	URI - IA5String	http://cert.pkioverheid.nl/MinIenW_PKIoverheid_Autonome_Apparaten_CA-G3.cer	7.11
authorityKeyIdentifier	{ id-ce 35 }			
.keyIdentifier		OCTET STRING	IenWApparatenCAG3.subjectPublicKeyIdentifier.keyIdentifier	
subjectKeyIdentifier .keyIdentifier	{ id-ce 14 }	OCTET STRING	*SHA-1 hash van publieke sleutel van dit certificaat*	
cRLDistributionPoints .distributionPoint .fullName	{ id-ce 31 }	URI – IA5String	http://bct.tsp.minienw.nl/minienw-aa-ca-g3.crl	7.9
subjectAltName.othername	{ id-ce 17 }			7.10
.**permanentIdentifier**	{ id-on 3 }			
.identifierValue		UTF8String	[Kaarthoofdtype] + [Boordcomputernummer]	
.assigner		OID	2.16.528.1.1003.1.3.6.2.1	
basicConstraints	{ id-ce 19 }			
.cA			Door het CA attribuut weg te laten, geldt de default waarde: CA=False	
.pathLenConstraint			Door het attribuut weg te laten, geldt de default waarde: pathLenConstraint=None	
extKeyUsage	{ id-ce 37 }		clientAuth: 1.3.6.1.5.5.7.3.2 Document_Signing: 1.3.6.1.4.1.311.10.3.12	

Tabel 31 - Profiel authenticiteitcertificaat Systeemkaart

13 CRL Model

13.1 CRL keuzes

Bij het ontwerp van de CRL's zijn de volgende ontwerpkeuzes gemaakt:

- Er is 1 CRL per CA, die certificate.serialNumbers van gebruikercertificaten kan bevatten;
- Er wordt gebruik gemaakt van de zogenaamde 'Reason Code' waarmee de reden van intrekking weergegeven kan worden in de CRL;
- De CRL wordt ondertekend door dezelfde CA als de CA die de certificaten ondertekent met dezelfde sleutel; dit betekent dat er per generatie van een CA een (latest) CRL zal worden bijgehouden; De naam van elke CRL bevat het generatienummer (de sleutelversie) van de CA die de CRL ondertekent. Hierdoor is Boordcomputer Taxi voorbereid op een zogenaamde "CA rollover".
- De ingetrokken certificaten blijven te allen tijde op de CRL staan. Dit is noodzakelijk omdat er na het verlopen van het certificaat nog moet worden nagetrokken of het certificaat geldig was op tijd van ondertekenen gegevens;
- De MinIenW CA's geven alleen volledige CRL's uit.

13.2 CRL van IenWOrganisatiePersoonCAG3

Hierna volgt het CRL profiel voor de IenWOrganisatiePersoonCAG3. Hierop staat informatie over de certificaten van ingetrokken Chauffeurs- en Inspectiekaarten:

CRL veld	Critical	Waarde	Omschrijving
Velden			
Version		1	CRL version 2
Signature		1.2.840.113549.1.1.11	sha-256WithRSAEncryption
Issuer.DN		*CN= MinIenW PKIoverheid Organisatie Persoon CA - G3, O=Ministerie van Infrastructuur en Waterstaat, organizationIdentifier=NTRNL-52766179, C=NL*	DN van de issuer
thisUpdate		Automatisch gegenereerd	Uitgiftetijdstip van de CRL
nextUpdate		Automatisch gegenereerd	Uitgiftetijdstip + 24 uur
revokedCertificates			Lijst van ingetrokken certificaten, per ingetrokken certificaat bestaande uit de drie navolgende velden:
userCertificate		[CertificateSerialNumber]	Serienummer van het ingetrokken certificaat
revocationDate		[UTCTime]	Tijdstip dat de CA de intrekking behandelde
crlEntryExtensions			Een opsomming van de twee navolgende extensies die betrekking hebben op de intrekking
reasonCode		[CRLReason ::= ENUMERATED]	Zie Tabel 26 voor invulling van de reasonCode
invalidityDate		[UTCTime]	OPTIONEEL: Het door de melder gemelde en door de RA geregistreerde vermoedelijke tijdstip waarop de reasonCode van kracht werd. Dit zal

CRL veld	Critical	Waarde	Omschrijving
			eerder zijn dan de hierboven genoemde revocationDate.
Extensies			
authorityKeyIdentifier .keyIdentifier	False	IenWOrganisatiePersoonCAG3. subjectPublicKeyIdentifier. keyIdentifier	
cRLNumber	False	Automatisch gegenereerd	
authorityInformation Access	False	http://cert.pkioverheid.nl/MinIenW_PKIoverheid_Organisatie_Persoon_CA-G3.cer	Zie paragraaf 3.5

Tabel 32 - CRL profiel van IenWOrganisatiePersoonCAG3

13.3 CRL van IenWOrganisatieServicesCAG3

Hierna volgt het CRL profiel voor de IenWOrganisatieServicesCAG3. Hierop staat informatie over de certificaten van ingetrokken Ondernemers- en Keuringskaarten. Alleen de wijzigingen t.o.v. de IenWOrganisatiePersoonCAG3 zijn opgenomen.

CRL veld	Critical	Waarde	Omschrijving
Issuer.CommonName		*CN= MinIenW PKIoverheid Organisatie Services CA - G3*	CommonName van de issuer
Extensies			
authorityKeyIdentifier .keyIdentifier	False	IenWOrganisatieServicesCAG3. subjectPublicKeyIdentifier. keyIdentifier	
authorityInformation Access	False	http://cert.pkioverheid.nl/MinIenW_PKIoverheid_Organisatie_Services_CA-G3.cer	Zie paragraaf 3.5

Tabel 33 - CRL profiel IenWOrganisatieServicesCAG3

13.4 CRL van IenWApparatenCAG3

Hierna volgt het CRL profiel voor de IenWApparatenCAG3. Hierop staat informatie over de certificaten van ingetrokken Systeemkaarten. Alleen de wijzigingen t.o.v. de IenWOrganisatiePersoonCAG3 zijn opgenomen.

CRL veld	Critical	Waarde	Omschrijving
Issuer.CommonName		*CN= MinIenW PKIoverheid Autonome Apparaten CA - G3*	CommonName van de issuer
Extensies			
authorityKeyIdentifier .keyIdentifier	False	IenWApparatenCAG3.subjectPublicKeyIdentifier.keyIdentifier	
authorityInformation Access	False	http://cert.pkioverheid.nl/MinIenW_PKIoverheid_Autonome_Apparaten_CA-G3.cer	Zie paragraaf 3.5

Tabel 34 - CRL profiel SysteemkaartenCA

13.5 CRL Reason Code

Binnen CABS is een aantal redenen om de kaart ongeldig te verklaren. Deze redenen moeten overeenkomen met een reasonCode die in de CRL gebruikt kan worden. De reasonCode geldt voor alle TSP CA's

Van een verlopen kaart wordt het certificaat niet ingetrokken. Het certificaat heeft dezelfde einddatum en tijd als de kaart zelf en is daardoor ongeldig als de kaart verlopen is.

In hierna getoonde tabel staan de redenen en reasonCode gekoppeld.

Reason Code	**CABS(Card Aanvraag & Beschikking Systeem)**
Unspecified (0)	Niet in gebruik.
keyCompromise (1)	1.Gestolen (duplicaatkaart eventueel aangevraagd); 2.Verloren (duplicaatkaart eventueel aangevraagd).
cACompromise (2)	Niet in gebruik.
affiliationChanged (3)	3.Einde dienstverband (Alleen bij Inspectiekaart); 4.Overlijden.
superseded (4)	5.Defect (duplicaatkaart eventueel aangevraagd); 6.Niet succesvol uitgeleverd; 7.Niet succesvol geproduceerd; 8.Naamwijziging (duplicaatkaart eventueel aangevraagd); 9.Omzetten naar ander toelatingseis.
cessationOfOperation (5)	Niet in gebruik
certificateHold (6)	Niet in gebruik
Reserved (7)	Niet in gebruik
removeFromCRL (8)	Niet in gebruik
privilegeWithdrawn (9)	10.Vergunning ingetrokken; 11.Kaarthouder voldoet niet aan de toelatingseisen;
aACompromise (10)	Niet in gebruik

Tabel 35 - CRL Reason Codes

13.6 CRL publicatie

Deze paragraaf geeft toelichting op de publicatiefrequentie van de CRL's en specificeert de tijdstippen van publicatie. Deze informatie is vooral van belang voor applicatieontwikkelaars omdat binnen applicaties vaak de CRL's tijdelijk worden opgeslagen (caching).

Het Programma van Eisen van PKI voor de overheid vereist dat de maximale vertraging tussen een verzoek tot intrekking van een kaart en de publicatie van de aangepaste statusinformatie 4 uur is. Om nog enige marge te hebben, genereert de TSP iedere 3 uur een nieuwe CRL beginnende om 0:00 (GMT).

13.7 CRL overlap voor opvangen van een calamiteit

In het 'nextUpdate' attribuut van de CRL staat dat een volgende CRL maximaal 24

nadat de huidige CRL ontstond zal worden gepubliceerd. In de praktijk zal al na 3 uur een nieuwe CRL gepubliceerd worden. Hiermee realiseert Boordcomputer Taxi een zogenaamde 'CRL overlap' van 21 uur. Overigens staat alleen de laatst gegenereerde CRL per generatie per CA op de website.

De CRL overlap periode is een continuïteitdienst van de CA aan vertrouwende partijen. Die dienst treedt (automatisch) in werking ingeval van een calamiteit waarbij de CA niet in staat is een nieuwe CRL tijdig (3 uur na de vorige publicatie) te publiceren. Zolang de CA binnen 21 uur na optreden van een dergelijke calamiteit haar reguliere dienstverlening kan hervatten, kunnen vertrouwende partijen - die over standaard validatiesoftware beschikken - van de laatst gepubliceerde CRL gebruikmaken.

NB. Standaard validatiesoftware zal een (gedownloade) CRL voor certificaatvalidatie kunnen gebruiken indien die CRL een 'nextUpdate' attribuut met een waarde in de toekomst bevat.

Het advies in normale omstandigheden is om altijd gebruik te maken van de meest actuele CRL. Dit houdt in dat vertrouwende partijen iedere 3 uur een nieuwe CRL op moeten halen en wel enkele minuten na het genoemde publicatieschema.