Inspectie Leefomgeving en Transport
Ministerie van Infrastructuur en Waterstaat

OPENBAAR

MinIenW TSP Naamgevingsdocument Acceptatieomgeving BCT G3

Versie 2.5

Datum	21-10-2020
Status	Definitief

Colofon

Documenttitel	MinIenW TSP Naamgevingsdocument Acceptatieomgeving BCT G3
Classificatie	**OPENBAAR**
Versienummer	2.5
Status	Definitief
Datum	21-10-2020

Contact **dci.csp@minienw.nl**

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

Bijlage(n)	Geen
Auteur(s)	MinIenW TSP

Wijzigingshistorie

Versie	Datum	Samenvatting aanpassing(en)
2.4	1-09-2020	Eerste oplevering n.a.v. ontvlechten van de Acceptatie- en Productieomgeving. Nieuwe base url: acceptatie.bct.tsp.minienw.nl Overige aanpassingen: - User notice tekst uitgebreid
2.5	21-10-2020	- AIA OCSP toegevoegd in Tabel 8 MinIenW SIMULATOR NL Organisatie Services Acceptatie CA - G3 - Fingerprints CA toegevoegd in Tabel 5

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 zaken die in de BCT Acceptatieomgeving afwijken van de Productieomgeving. Dit betreft vooral de naamgeving van de CA's en de gebruikte URL's.

Voor toelichting en motivatie van ontwerpkeuzes wordt verwezen naar de specificaties van de Productieomgeving: "MinIenW TSP PKIoverheid Certificaatprofielen BCT G3".

1.2 Doel Acceptatieomgeving

De BCT Acceptatieomgeving is 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 IenW TSP kan de acceptatie CA's inzetten voor het produceren van zogenaamde acceptatiekaarten. Acceptatiekaarten worden door de toepassing eigenaar 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 IenW TSP.

DEEL 1: CA CERTIFICATEN ACCEPTATIEOMGEVING

2 CA model Acceptatieomgeving

Dit hoofdstuk beschrijft de CA structuur van de Acceptatieomgeving BCT G3.

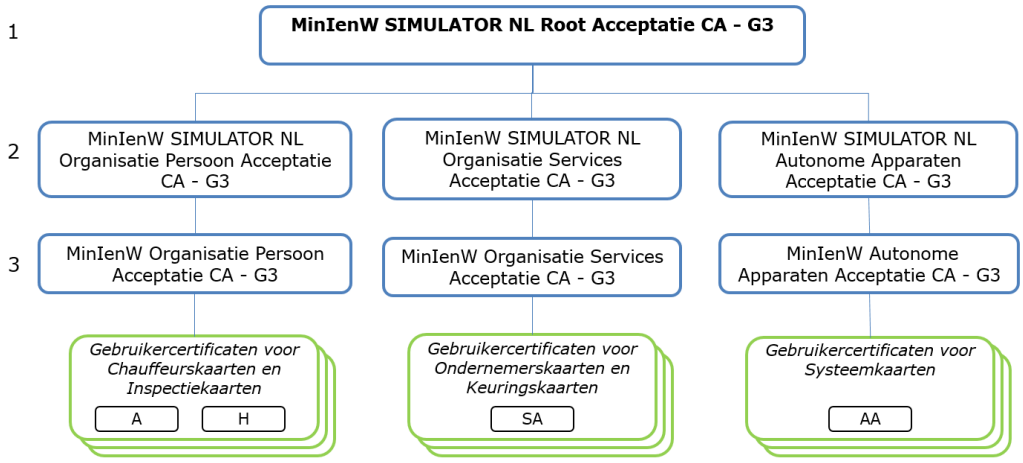
2.1 PKIoverheid en MinIenW eisen aan non-productie CA's

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.

2.2 PKI hiërarchie Acceptatieomgeving BCT G3

Figuur 1 toont de PKI hiërarchie die de TSP van het Ministerie van Infrastructuur en Waterstaat gebruikt voor de Acceptatieomgeving BCT G3. De CA certificaten zijn blauw weergegeven en de eindgebruikercertificaten groen. De naamgeving van de CA's (subject.CommonName van de betreffende CA certificaten, case sensitive) is opgenomen in de figuur.



Figuur 1 - PKI hiërarchie Acceptatieomgeving BCT G3

2.3 Naamgeving Acceptatie CA's BCT G3

Laag 1 en 2 van de CA's zijn niet gespecificeerd voor de Productieomgeving aangezien die volledig onder beheer van Logius zijn ingericht. Voor de Acceptatieomgeving zijn die wel gespecificeerd aangezien de IenW TSP zelf een 'simulator' heeft gerealiseerd die representatief is voor de PKIoverheid Productieomgeving. De voor deze hiërarchie voorgeschreven naamgeving is opgenomen in de volgende tabel.

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 1 - Naamgeving Acceptatie CA's BCT G3

3 Keuzes CA Certificaatprofiel Acceptatieomgeving

Dit hoofdstuk beschrijft een aantal attributen op generieke wijze. Deze attributen zijn ook opgenomen in de certificaatprofielen in Hoofdstuk 4.

3.1 Hostname Acceptatie webserver

De Ministerie van Infrastructuur en Waterstaat TSP exploiteert één webserver voor de Acceptatieomgeving. De hostname van de webserver in de acceptatie omgeving is: **acceptatie.bct.tsp.minienw.nl**

3.2 CertificatePolicies

3.2.1 PolicyIdentifier

In de acceptatieomgeving zijn dezelfde Policy OID's gebruikt als in de productieomgeving.

3.2.2 PolicyQualifier.cPS.uri

Vanuit de laag 2 en 3 CA certificaten is er een verwijzing naar het actuele "Certification Practice Statement" (CPS).

CA	CPS URL Acceptatieomgeving
Alle Laag 2 en 3 Acceptatie CA's	https://acceptatie.bct.tsp.minienw.nl/minienw-bct-cps

Tabel 2 – CPS URL in Laag 2 en 3 Acceptatie CA's BCT G3

3.2.3 PolicyQualifier.UserNotice

Voor alle CA certificaten geldt: Géén User Notice

3.3 CRL Distribution Points Acceptatieomgeving

Het overzicht van de CDPs in de Acceptatieomgeving is opgenomen in de volgende tabel.

Naam Acceptatie CA	CRL Distributiepunt opgenomen in betreffende Acceptatie CA
MinIenW SIMULATOR NL Root Acceptatie CA - G3	CDP ontbreekt in Root CA.
MinIenW SIMULATOR NL Organisatie Persoon Acceptatie CA - G3	http://acceptatie.bct.tsp.minienw.nl/RootLatestCRL-G3.crl
MinIenW SIMULATOR NL Organisatie Services Acceptatie CA - G3	http://acceptatie.bct.tsp.minienw.nl/RootLatestCRL-G3.crl
MinIenW SIMULATOR NL Autonome Apparaten Acceptatie CA - G3	http://acceptatie.bct.tsp.minienw.nl/RootLatestCRL-G3.crl
MinIenW Organisatie Persoon Acceptatie CA - G3	http://acceptatie.bct.tsp.minienw.nl/DomOrganisatiePersoonLatestCRL-G3.crl
MinIenW Organisatie Services Acceptatie CA - G3	http://acceptatie.bct.tsp.minienw.nl/DomOrganisatieServicesLatestCRL-G3.crl

Naam Acceptatie CA	CRL Distributiepunt opgenomen in betreffende Acceptatie CA
MinIenW Autonome Apparaten Acceptatie CA - G3	http://acceptatie.bct.tsp.minienw.nl/DomAutonomeApparatenLatestCRL-G3.crl

Tabel 3 - CDP URL's van Acceptatieomgeving BCT G3

3.4 TSP en Acceptatie CA Object Identifiers (OID)

In de Acceptatieomgeving zijn dezelfde OID's in gebruik voor de CA's als in de productieomgeving.

3.5 URL's van Acceptatie CA certificaten

De certificaten van de domein en TSP CA's worden 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 laag 3 CA certificaat waaronder het is uitgegeven. Deze URL's zijn opgenomen in de volgende tabel. Voor de volledigheid is ook de URL van de Root CA opgenomen hoewel deze niet gebruikt wordt in andere certificaten.

Naam Acceptatie CA	URL van CA certificaat
MinIenW SIMULATOR NL Root Acceptatie CA - G3	http://acceptatie.bct.tsp.minienw.nl/RootCA-G3.cer
MinIenW SIMULATOR NL Organisatie Persoon Acceptatie CA - G3	http://acceptatie.bct.tsp.minienw.nl/DomOrganisatiePersoonCA-G3.cer
MinIenW SIMULATOR NL Organisatie Services Acceptatie CA - G3	http://acceptatie.bct.tsp.minienw.nl/DomOrganisatieServicesCA-G3.cer
MinIenW SIMULATOR NL Autonome Apparaten Acceptatie CA - G3	http://acceptatie.bct.tsp.minienw.nl/DomAutonomeApparatenCA-G3.cer
MinIenW Organisatie Persoon Acceptatie CA - G3	http://acceptatie.bct.tsp.minienw.nl/MinIenW_Organisatie_Persoon_Acceptatie_CA-G3.cer
MinIenW Organisatie Services Acceptatie CA - G3	http://acceptatie.bct.tsp.minienw.nl/MinIenW_Organisatie_Services_Acceptatie_CA-G3.cer
MinIenW Autonome Apparaten Acceptatie CA - G3	http://acceptatie.bct.tsp.minienw.nl/MinIenW_Autonome_Apparaten_Acceptatie_CA-G3.cer

Tabel 4 – URL's van CA certificaten Acceptatieomgeving BCT G3

3.6 Geldigheidsduur CA certificaten in Acceptatieomgeving

De geldigheidsduur van de Acceptatie CA certificaten is gelijk aan de Productieomgeving.

3.7 Controle juistheid van CA certificaten in Acceptatieomgeving

Op de BCT kaarten uit de Acceptatieomgeving staat de complete CA hiërarchie. De juistheid van de Acceptatie CA certificaten is met behulp van volgende tabel vast te stellen op basis van de zogenaamde 'thumbprint'. Dit is de SHA-1 hash-waarde van het certificaat en deze is met de standaard microsoft certificate viewer als volgt te verifiëren:

- Dubbelklik het certificaatbestand;
- Klik op Tab 'details';
- Klik op 'Thumbprint'.

De onderstaande tabel bevat de Thumbprints van de CA certificaten van de resigning d.d. 30 september 2020.

Naam Acceptatie CA	SHA-1 thumbprint CA certificaat
MinIenW SIMULATOR NL Root Acceptatie CA - G3	f246db9deac5fc2e5c212b21e7d2ad113e1f0452
MinIenW SIMULATOR NL Organisatie Persoon Acceptatie CA - G3	e379729091d81e8537b96c051afbb8fda25f0b3d
MinIenW SIMULATOR NL Organisatie Services Acceptatie CA - G3	d9d981fb5ef03e9265b5d1e6448cfeb7e2345f5b
MinIenW SIMULATOR NL Autonome Apparaten Acceptatie CA - G3	e8f320e8c4bbd3087ce335ea0b2983c8756d046b
MinIenW Organisatie Persoon Acceptatie CA - G3	58cc660282817 56b314c36564d1ca1b17cbf8aba
MinIenW Organisatie Services Acceptatie CA - G3	c352da357c9650e529484fc4a24fb416b01fb0fa
MinIenW Autonome Apparaten Acceptatie CA - G3	476208bc278490c0f7851ffc4ee1f2ff7a656281

Tabel 5 – Thumbprints CA certificaten Acceptatieomgeving BCT G3

4 CA certificaatprofielen (laag 1, 2 en 3)

Dit hoofdstuk specificeert de profielen/naming documents voor alle CA certificaten van de acceptatieomgeving BCT G3.

4.1 Certificaatprofiel van de Root CA (laag 1)

4.1.1 Certificaatprofiel MinIenW SIMULATOR NL Root Acceptatie CA - G3

Certificaat / Attribuut	**OID**	**Waarde**
Certificate		
signatureAlgorithm		1.2.840.113549.1.1.11 { sha256WithRSAEncryption }
signatureValue		Self-signed handtekening
tbsCertificate		
Version		2 (X509v3)
serialNumber		Uniek certificaatnummer. Lengte 160 bits.
signature		1.2.840.113549.1.1.11 (= signatureAlgorithm)
Issuer		
.commonName	{ id-at 3 }	MinIenW SIMULATOR NL Root Acceptatie CA - G3
.organizationName	{ id-at 10 }	Ministerie van Infrastructuur en Waterstaat
.countryName	{ id-at 6 }	NL
Validity		
.notBefore		DatumTijd waarop het certificaat geldig wordt (15 mei 2019)
.notAfter		DatumTijd waarna het certificaat **on**geldig wordt (14 november 2028)
Subject		
.commonName	{ id-at 3 }	**MinIenW SIMULATOR NL Root Acceptatie CA - G3**
.organizationName	{ id-at 10 }	**Ministerie van Infrastructuur en Waterstaat**
.countryName	{ id-at 6 }	**NL**
SubjectPublicKeyInfo		
.algorithm		1.2.840.113549.1.1.1 { rsaEncryption }
.subjectPublicKey		4096 bits RSA publieke sleutel van de CA
Extensions		
authorityKeyIdentifier	{ id-ce 35 }	
.KeyIdentifier		KeyIdentifier ondertekenende CA
subjectKeyIdentifier .keyIdentifier	{ id-ce 14 }	SHA-1 hash van de publieke sleutel van dit certificaat
BasicConstraints	{ id-ce 19 }	
.CA		True (Betreft CA certificaat)
.pathLenConstraint		None (Geen beperking)
keyUsage	{ id-ce 15 }	KeyCertSign, cRLSign

Tabel 6 - MinIenW SIMULATOR NL Root Acceptatie CA - G3

4.2 Certificaatprofielen van de domein CA's (laag 2)

4.2.1 Certificaatprofiel MinIenW SIMULATOR NL Organisatie Persoon Acceptatie CA - G3

Certificaat / Attribuut	OID	Waarde
Certificate		
signatureAlgorithm		1.2.840.113549.1.1.11 { sha256WithRSAEncryption }
signatureValue		Handtekening gezet door de MinIenW SIMULATOR NL Root Acceptatie CA - G3
tbsCertificate		
Version		2 (X509v3)
serialNumber		Uniek certificaatnummer. Lengte 160 bits.
signature		1.2.840.113549.1.1.11 (= signatureAlgorithm)
Issuer		
.commonName	{ id-at 3 }	MinIenW SIMULATOR NL Root Acceptatie CA - G3
.organizationName	{ id-at 10 }	Ministerie van Infrastructuur en Waterstaat
.countryName	{ id-at 6 }	NL
Validity		
.notBefore		DatumTijd waarop het certificaat geldig wordt (30 september 2020)
.notAfter		DatumTijd waarna het certificaat **on**geldig wordt (13 november 2028)
Subject		
.commonName	{ id-at 3 }	**MinIenW SIMULATOR NL Organisatie Persoon Acceptatie CA - G3**
.organizationName	{ id-at 10 }	**Ministerie van Infrastructuur en Waterstaat**
.countryName	{ id-at 6 }	**NL**
SubjectPublicKeyInfo		
.algorithm		1.2.840.113549.1.1.1 { rsaEncryption }
.subjectPublicKey		4096 bits RSA publieke sleutel van CA
Extensions		
authorityKeyIdentifier	{ id-ce 35 }	
.KeyIdentifier		KeyIdentifier ondertekenende CA
certificatePolicies	{ id-ce 32 }	
.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 2.16.528.1.1003.1.2.5.3 Vertrouwelijkheid
.PolicyQualifier		
.cPS.uri	{ id-qt 1 }	https://acceptatie.bct.tsp.minienw.nl/minienw-bct-cps
cRLDistributionPoints .distributionPoint. .fullName	{ id-ce 31 }	http://acceptatie.bct.tsp.minienw.nl/RootLatestCRL-G3.crl
subjectKeyIdentifier .keyIdentifier	{ id-ce 14 }	SHA-1 hash van de publieke sleutel van dit certificaat
BasicConstraints	{ id-ce 19 }	
.CA		True (Betreft CA certificaat)
.pathLenConstraint		None (Geen beperking)
keyUsage	{ id-ce 15 }	KeyCertSign, cRLSign

Tabel 7 - MinIenW SIMULATOR NL Organisatie Persoon Acceptatie CA - G3

4.2.2 Certificaatprofiel MinIenW SIMULATOR NL Organisatie Services Acceptatie CA - G3

Certificaat / Attribuut	**OID**	**Waarde**
Certificate		
signatureAlgorithm		1.2.840.113549.1.1.11 { sha256WithRSAEncryption }
signatureValue		Handtekening gezet door de MinIenW SIMULATOR NL Root Acceptatie CA - G3
tbsCertificate		
Version		2 (X509v3)
serialNumber		Uniek certificaatnummer. Lengte 160 bits.
signature		1.2.840.113549.1.1.11 (= signatureAlgorithm)
Issuer		
.commonName	{ id-at 3 }	MinIenW SIMULATOR NL Root Acceptatie CA - G3
.organizationName	{ id-at 10 }	Ministerie van Infrastructuur en Waterstaat
.countryName	{ id-at 6 }	NL
Validity		
.notBefore		DatumTijd waarop het certificaat geldig wordt (30 september 2020)
.notAfter		DatumTijd waarna het certificaat **on**geldig wordt (13 november 2028)
Subject		
.commonName	{ id-at 3 }	**MinIenW SIMULATOR NL Organisatie Services Acceptatie CA - G3**
.organizationName	{ id-at 10 }	**Ministerie van Infrastructuur en Waterstaat**
.countryName	{ id-at 6 }	**NL**
SubjectPublicKeyInfo		
.algorithm		1.2.840.113549.1.1.1 { rsaEncryption }
.subjectPublicKey		4096 bits RSA publieke sleutel van IenWOrganisatieServicesCAG3
Extensions		
authorityKeyIdentifier	{ id-ce 35 }	
.KeyIdentifier		KeyIdentifier ondertekenende CA
AuthorityInfoAccess	{ id-pe 1 }	
.OCSP	{ id-ad 1 }	http://ocsp-acc1.minienw.nl/
certificatePolicies	{ id-ce 32 }	
.PolicyIdentifier		OID's Domein Organisatie Services (g3): 2.16.528.1.1003.1.2.5.4 Services – Authenticiteit 2.16.528.1.1003.1.2.5.5 Services - Vertrouwelijkheid 2.16.528.1.1003.1.2.5.6 Services - Server
.PolicyQualifier		
.cPS.uri	{ id-qt 1 }	https://acceptatie.bct.tsp.minienw.nl/minienw-bct-cps
cRLDistributionPoints .distributionPoint. .fullName	{ id-ce 31 }	 http://acceptatie.bct.tsp.minienw.nl/RootLatestCRL-G3.crl
subjectKeyIdentifier .keyIdentifier	{ id-ce 14 }	 SHA-1 hash van de publieke sleutel van dit certificaat
BasicConstraints	{ id-ce 19 }	
.CA		True (Betreft CA certificaat)
.pathLenConstraint		None (Geen beperking)
keyUsage	{ id-ce 15 }	KeyCertSign, cRLSign

Tabel 8 - MinIenW SIMULATOR NL Organisatie Services Acceptatie CA - G3

4.2.3 Certificaatprofiel MinIenW SIMULATOR NL Autonome Apparaten Acceptatie CA - G3

Certificaat / Attribuut	**OID**	**Waarde**
Certificate		
signatureAlgorithm		1.2.840.113549.1.1.11 { sha256WithRSAEncryption }
signatureValue		Handtekening gezet door de MinIenW SIMULATOR NL Root Acceptatie CA - G3
tbsCertificate		
Version		2 (X509v3)
serialNumber		Uniek certificaatnummer. Lengte 160 bits.
signature		1.2.840.113549.1.1.11 (= signatureAlgorithm)
Issuer		
.commonName	{ id-at 3 }	MinIenW SIMULATOR NL Root Acceptatie CA - G3
.organizationName	{ id-at 10 }	Ministerie van Infrastructuur en Waterstaat
.countryName	{ id-at 6 }	NL
Validity		
.notBefore		DatumTijd waarop het certificaat geldig wordt (30 september 2020)
.notAfter		DatumTijd waarna het certificaat **on**geldig wordt (13 nov. 2028)
Subject		
.commonName	{ id-at 3 }	**MinIenW SIMULATOR NL Autonome Apparaten Acceptatie CA - G3**
.organizationName	{ id-at 10 }	**Ministerie van Infrastructuur en Waterstaat**
.countryName	{ id-at 6 }	**NL**
SubjectPublicKeyInfo		
.algorithm		1.2.840.113549.1.1.1 { rsaEncryption }
.subjectPublicKey		4096 bits RSA publieke sleutel van deze CA
Extensions		
authorityKeyIdentifier .KeyIdentifier	{ id-ce 35 }	KeyIdentifier ondertekenende CA
certificatePolicies	{ id-ce 32 }	
.PolicyIdentifier		OID's Domein autonome apparaten: 2.16.528.1.1003.1.2.6.1 Autonome Apparaten – Authenticiteit 2.16.528.1.1003.1.2.6.2 Autonome Apparaten – Vertrouwelijkheid 2.16.528.1.1003.1.2.6.3 Autonome Apparaten – Combinatie
.PolicyQualifier		
.cPS.uri	{ id-qt 1 }	https://acceptatie.bct.tsp.minienw.nl/minienw-bct-cps
cRLDistributionPoints .distributionPoint.fullName	{ id-ce 31 }	http://acceptatie.bct.tsp.minienw.nl/RootLatestCRL-G3.crl
subjectKeyIdentifier .keyIdentifier	{ id-ce 14 }	SHA-1 hash van de publieke sleutel van dit certificaat
BasicConstraints	{ id-ce 19 }	
.CA		True (Betreft CA certificaat)
.pathLenConstraint		None (Geen beperking)
keyUsage	{ id-ce 15 }	KeyCertSign, cRLSign

Tabel 9 - MinIenW SIMULATOR NL Autonome Apparaten Acceptatie CA - G3

4.3 Certificaatprofielen van de TSP CA's (laag 3)

4.3.1 Certificaatprofiel MinIenW Organisatie Persoon Acceptatie CA - G3

Certificaat / Attribuut	**OID**	**Waarde**
Certificate		
signatureAlgorithm		1.2.840.113549.1.1.11 { sha256WithRSAEncryption }
signatureValue		Handtekening gezet door MinIenW SIMULATOR NL Organisatie Persoon Acceptatie CA - G3
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		
.commonName	{ id-at 3 }	MinIenW SIMULATOR NL Organisatie Persoon Acceptatie CA - G3
.organizationName	{ id-at 10 }	Ministerie van Infrastructuur en Waterstaat
.countryName	{ id-at 6 }	NL
Validity		
.notBefore		DatumTijd waarop het certificaat geldig wordt (30 september 2020)
.notAfter		DatumTijd waarna het certificaat **on**geldig wordt (12 november 2028)
Subject		
.commonName	{ id-at 3 }	**MinIenW Organisatie Persoon Acceptatie CA - G3**
.organizationIdentifier	2.5.4.97	**NTRNL-52766179**
.organizationName	{ id-at 10 }	**Ministerie van Infrastructuur en Waterstaat**
.countryName	{ id-at 6 }	**NL**
SubjectPublicKeyInfo		
.algorithm		1.2.840.113549.1.1.1 { rsaEncryption }
.subjectPublicKey		4096 bits RSA publieke sleutel van deze CA
Extensions		
authorityKeyIdentifier	{ id-ce 35 }	
.KeyIdentifier		KeyIdentifier ondertekenende CA
AuthorityInfoAccess	{ id-pe 1 }	
.caIssuers	{ id-ad 2 }	http://acceptatie.bct.tsp.minienw.nl/DomOrganisatiePersoonCA-G3.cer
certificatePolicies	{ id-ce 32 }	
.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.
.PolicyQualifier		
.cPS.uri	{ id-qt 1 }	https://acceptatie.bct.tsp.minienw.nl/minienw-bct-cps
ExtendedKeyUsage	{id-ce 37}	clientAuthentication: 1.3.6.1.5.5.7.3.2 DocumentSigning: 1.3.6.1.4.1.311.10.3.12 OCSPSigning: 1.3.6.1.5.5.7.3.9
QcStatement2	{ id-qcs-pkixQCSyntax-v2 }	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)

Certificaat / Attribuut	OID	Waarde
cRLDistributionPoints .distributionPoint. .fullName	{ id-ce 31 }	http://acceptatie.bct.tsp.minienw.nl/DomOrganisatiePersoonLatestCRL-G3.crl
subjectKeyIdentifier .keyIdentifier	{ id-ce 14 }	SHA-1 hash van de publieke sleutel van dit certificaat
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.
keyUsage	{ id-ce 15 }	KeyCertSign, cRLSign

Tabel 10 - MinIenW Organisatie Persoon Acceptatie CA - G3

4.3.2 Certificaatprofiel MinIenW Organisatie Services Acceptatie CA - G3

Certificaat / Attribuut	**OID**	**Waarde**	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11 { sha256WithRSAEncryption }	
signatureValue		Handtekening gezet door MinIenW SIMULATOR NL Organisatie Services Acceptatie CA - G3	
tbsCertificate			
Version		2 (X509v3)	
serialNumber		Uniek certificaatnummer. Lengte 160 bits.	
signature		1.2.840.113549.1.1.11 (= signatureAlgorithm)	
Issuer			
.commonName	{ id-at 3 }	MinIenW SIMULATOR NL Organisatie Services Acceptatie CA - G3	
.organizationName	{ id-at 10 }	Ministerie van Infrastructuur en Waterstaat	
.countryName	{ id-at 6 }	NL	
Validity			
.notBefore		DatumTijd waarop het certificaat geldig wordt (30 september 2020)	
.notAfter		DatumTijd waarna het certificaat **on**geldig wordt (12 november 2028)	
Subject			
.commonName	{ id-at 3 }	**MinIenW Organisatie Services Acceptatie CA - G3**	
.organizationIdentifier	2.5.4.97	**NTRNL-52766179**	
.organizationName	{ id-at 10 }	**Ministerie van Infrastructuur en Waterstaat**	
.countryName	{ id-at 6 }	**NL**	
SubjectPublicKeyInfo			
.algorithm		1.2.840.113549.1.1.1 { rsaEncryption }	
.subjectPublicKey		4096 bits RSA publieke sleutel van CA	
Extensions			
authorityKeyIdentifier	{ id-ce 35 }		
.KeyIdentifier		KeyIdentifier ondertekenende CA	
AuthorityInfoAccess	{ id-pe 1 }		
.caIssuers	{ id-ad 2 }	http://acceptatie.bct.tsp.minienw.nl/DomOrganisatieServicesCA-G3.cer	
.OCSP	{ id-ad 1 }	http://ocsp-acc2.minienw.nl	
certificatePolicies	{ id-ce 32 }		
.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.	
.PolicyQualifier			
.cPS.uri	{ id-qt 1 }	https://acceptatie.bct.tsp.minienw.nl/minienw-bct-cps	
ExtendedKeyUsage	{id-ce 37}	clientAuthentication: 1.3.6.1.5.5.7.3.2 DocumentSigning: 1.3.6.1.4.1.311.10.3.12 OCSPSigning: 1.3.6.1.5.5.7.3.9	
QcStatement2	{ id-qcs-pkixQCSyntax-v2 }	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)	

Certificaat / Attribuut	OID	Waarde	
cRLDistributionPoints .distributionPoint. .fullName	{ id-ce 31 }	http://acceptatie.bct.tsp.minienw.nl/DomOrganisatieServicesLatestCRL-G3.crl	
subjectKeyIdentifier .keyIdentifier	{ id-ce 14 }	SHA-1 hash van de publieke sleutel van dit certificaat	
BasicConstraints	{ id-ce 19 }		
.CA		True	
.pathLenConstraint		0	
keyUsage	{ id-ce 15 }	KeyCertSign, cRLSign	

Tabel 11 - MinIenW Organisatie Services Acceptatie CA - G3

4.3.3 Certificaatprofiel MinIenW Autonome Apparaten Acceptatie CA - G3

Certificaat / Attribuut	**OID**	**Waarde**	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11 { sha256WithRSAEncryption }	
signatureValue		Handtekening gezet door MinIenW SIMULATOR NL Autonome Apparaten Acceptatie CA - G3	
tbsCertificate			
Version		2 (X509v3)	
serialNumber		Uniek certificaatnummer. Lengte 160 bits.	
signature		1.2.840.113549.1.1.11 (= signatureAlgorithm)	
Issuer			
.commonName	{ id-at 3 }	MinIenW SIMULATOR NL Autonome Apparaten Acceptatie CA - G3	
.organizationName	{ id-at 10 }	Ministerie van Infrastructuur en Waterstaat	
.countryName	{ id-at 6 }	NL	
Validity			
.notBefore		DatumTijd waarop het certificaat geldig wordt (30 september 2020)	
.notAfter		DatumTijd waarna het certificaat **on**geldig wordt (12 nov. 2028)	
Subject			
.commonName	{ id-at 3 }	**MinIenW Autonome Apparaten Acceptatie CA - G3**	
.organizationIdentifier	2.5.4.97	**NTRNL-52766179**	
.organizationName	{ id-at 10 }	**Ministerie van Infrastructuur en Waterstaat**	
.countryName	{ id-at 6 }	**NL**	
SubjectPublicKeyInfo			
.algorithm		1.2.840.113549.1.1.1 { rsaEncryption }	
.subjectPublicKey		4096 bits RSA publieke sleutel van deze CA	
Extensions			
authorityKeyIdentifier .KeyIdentifier	{ id-ce 35 }	keyIdentifier van ondertekenende CA	
AuthorityInfoAccess	{ id-pe 1 }		
.caIssuers	{ id-ad 2 }	http://acceptatie.bct.tsp.minienw.nl/DomAutonomeApparatenCA-G3.cer	
certificatePolicies	{ id-ce 32 }		
.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.	
.PolicyQualifier			
.cPS.uri	{ id-qt 1 }	https://acceptatie.bct.tsp.minienw.nl/minienw-bct-cps	
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	
QcStatement2	{ id-qcs-pkixQCSyntax-v2 }	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)	
cRLDistributionPoints .distributionPoint.fullName	{ id-ce 31 }	http://acceptatie.bct.tsp.minienw.nl/DomAutonomeApparatenLatestCRL-G3.crl	
subjectKeyIdentifier .keyIdentifier	{ id-ce 14 }	SHA-1 hash van de publieke sleutel van dit certificaat	

Certificaat / Attribuut	OID	Waarde	
BasicConstraints	{ id-ce 19 }		
.CA		True	
.pathLenConstraint		0	
keyUsage	{ id-ce 15 }	KeyCertSign, cRLSign	

Tabel 12 - MinIenW Autonome Apparaten Acceptatie CA - G3

DEEL 2: GEBRUIKERCERTIFICATEN ACCEPTATIEOMGEVING

Het tweede deel van dit document specificeert de verschillen in het profiel van gebruikercertificaten en CRL's in de acceptatieomgeving.

5 Toelichting gebruikercertificaten BCT Acceptatieomgeving

Dit hoofdstuk specificeert op welke punten de gebruikercertificaten in de Acceptatieomgeving afwijken van de productieomgeving.

5.1 Issuer

De issuer.commonName zal in de Acceptatieomgeving de naam van de betreffende Acceptatie CA bevatten.

5.2 ETSI QC statement (handtekeningscertificaten)

Er wordt GEEN ETSI QC statement opgenomen in de handtekeningcertificaten die door de acceptatieomgeving worden uitgegeven.

5.3 certificatePolicies.PolicyQualifier.cPS.uri

In de Acceptatieomgeving is een andere link naar het CPS opgenomen in de gebruikercertificaten.

CA	CPS URL
Alle gebruikercertificaten	https://acceptatie.bct.tsp.minienw.nl/minienw-bct-cps

Tabel 13 – CPS URL in gebruikercertificaten Acceptatieomgeving

5.4 certificatePolicies.PolicyQualifier.userNotice.explicitText

Het veld certificatePolicies.PolicyQualifier.userNotice.explicitText wordt in Acceptatieomgeving gevuld met de volgende tekst.

Certificaat uitsluitend gebruiken ten behoeve van de TESTEN van BCT toepassingen. Het CPS voor dit certificaat kan worden geraadpleegd op: https://acceptatie.bct.tsp.minienw.nl/minienw-bct-cps

5.5 CRL distribution Point

Het veld cRLDistributionPoints van de gebruikerscertificaten verwijst naar de CRL die uitgegeven wordt door de CA die het gebruikercertificaat ondertekent en is dus afhankelijk van het kaarttype:

CRL distributiepunt certificaten van Chauffeurs-/Inspectiekaarten:

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

CRL distributiepunt certificaten van Ondernemers-/Keuringskaarten:

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

CRL distributiepunt certificaten van Systeemkaarten:

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

5.6 URL's van CA certificaten (Authority Info Access)

De gebruikercertificaten bevatten een verwijzing naar het certificaat van de uitgevende CA in het attribuut AuthorityInfoAccess.caIssuers.

caIssuers link in certificaten van Chauffeurs-/Inspectiekaarten:

http://acceptatie.bct.tsp.minienw.nl/MinIenW_Organisatie_Persoon_Acceptatie_CA-G3.cer

caIssuers link in certificaten van Ondernemers-/Keuringskaarten:

http://acceptatie.bct.tsp.minienw.nl/MinIenW_Organisatie_Services_Acceptatie_CA-G3.cer

caIssuers link in certificaten van Systeemkaarten:

http://acceptatie.bct.tsp.minienw.nl/MinIenW_Autonome_Apparaten_Acceptatie_CA-G3.cer

6 CRL profielen

De CRL profielen en publicatiefrequentie zijn in de Acceptatieomgeving volledig identiek aan de Productieomgeving. Uiteraard is wel de Issuer informatie anders omdat de Acceptatie CA's deze CRL's uitgeven.