CIBG
Ministerie van Volksgezondheid, Welzijn en Sport

Naamgevingsdocument

ACCEPTATIEOMGEVING CIBG Zorg CSP

Versie : 10.1 Definitief

Datum : 21 mei 2021
Bestandsnaam : 20210521 Naamgevingsdocument Acceptatieomgeving CIBG Zorg CSP v10_1.docx

Inhoudsopgave

Lijst met Tabellen

Lijst met Figuren

1 Inleiding

1.1 Doelstelling

Dit document specificeert alle zaken die in de acceptatieomgeving van de Zorg CSP afwijken van de specificatie *CA model pasmodel Certificaatprofielen* voor de productieomgeving. Dit betreft vooral de naamgeving, URL's en Object IDentifiers (OID). De profielen zijn zoveel mogelijk ongewijzigd gebleven. Alle afwijkingen ten opzichte van de productieomgeving zijn in dit document opgenomen.

De 'Zorg CSP' omvat het UZI-register (doelgroep zorgverleners) en ZOVAR (doelgroep zorgverzekeraars). In deze specificatie is expliciet aangegeven wanneer bepaalde configuraties voor het UZI-register en ZOVAR van elkaar afwijken.

1.2 Versie historie

Versie	Datum	Status	Omschrijving
5.0	26 oktober 2016	Definitief	Wijzigingen: • Verwijdering eerste en tweede generatie (SHA-1) • Uitfasering G2 Staat der Nederlanden • Naamgeving CSP organisatie gewijzigd in CIBG
6.0	19 januari 2017	Definitief	Wijzigingen: • Aanpassing naar 3 niveaus CA's
6.1	27 januari 2017	Definitief	Wijzigingen: • Toegevoegd Hoofdstuk 7 met profielen/naming documents van alle CA certificaten
6.2	1 februari 2017	Definitief	Wijzigingen n.a.v. review commentaar: • Link naar Acceptatie OCPS: http://ocsp.uzi-register-test.nl (Tabel 26 en 30) • Link CDP Tabel 29 • Link CPS Tabel 32 https://acc.zorgcsp.nl/cps/zovar.html
6.3	17 februari 2017	Definitief	Wijzigingen n.a.v. review commentaar: • **acc**.zorgcsp.nl gewijzigd in **acceptatie**.zorgcsp.nl
6.4	12 juli 2017	Definitief	Wijzigingen: • Thumbprints CA certificaten G3 en G1 generatie toegevoegd • Spatie (typo) verwijderd uit ZOVAR URL in tabel 4 • Specificatie Policy OID in OCSP certificaat in par. 4.3 • In titel toegevoegd 'CIBG'
6.5	6 mei 2019	Definitief	Wijzigingen: • Tabel 3: nieuwe URL's G3 CA's na resigning. • Tabel 6: fingerprints van resigned CA's toegevoegd • Tabel 28, 29, 30: 160 bits serienummer in G3 issuing CA's na resigning
10.0	3 april 2020	Definitief	Aanpassing: - Verwijdering SHA-2/G21 generatie; - Toegevoegd ExpiredCertsOnCRL - Versienummering gelijk met productieomgeving - Correctie OID CA in voorbeelden par. 5.8.1
10.1	21 mei 2021	Definitief	Verwijdering afdelingsnaam

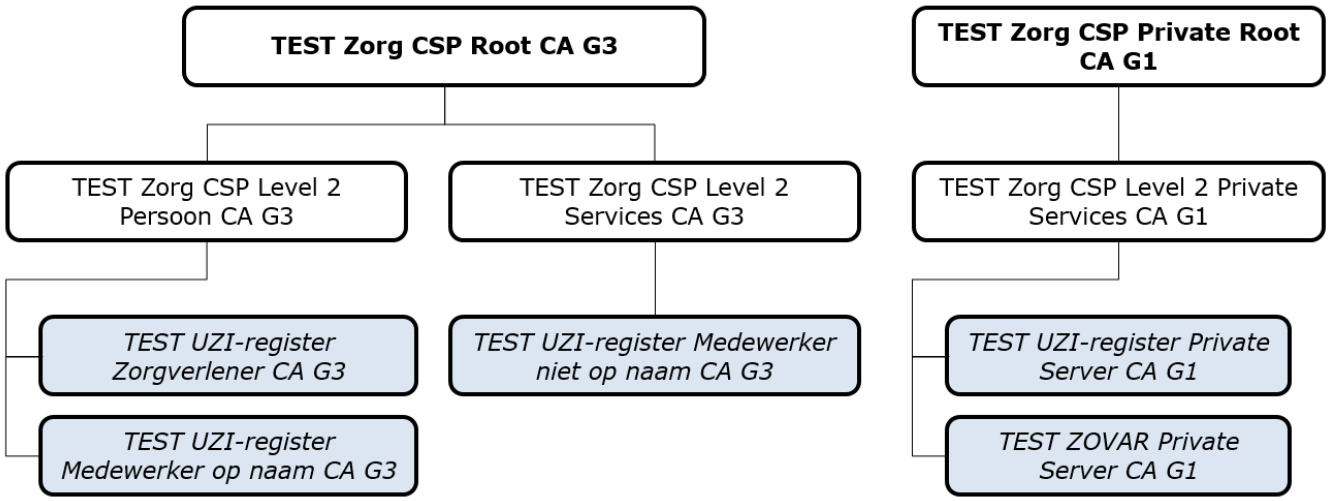
Tabel 1 Versie historie

2 CA model acceptatieomgeving

2.1 Naamgeving

Onderstaande figuur geeft het CA model weer voor de Generatie Public G3/Private G1 van de acceptatieomgeving van de Zorg CSP. De naamgeving (subject.CommonName in de betreffende CA certificaten) van de CA's is opgenomen in de figuur.

OPMERKING: de naamgeving is Case Sensitive.



Figuur 1: CA model acceptatieomgeving generatie Public G3/Private G1

2.2 URL's van CA certificaten in acceptatieomgeving

De CA certificaten in de acceptatieomgeving zijn te vinden via de URL's in de volgende tabellen.

Naam CA	URL van CA certificaat
TEST Zorg CSP Root CA G3	http://www.uzi-register-test.nl/cacerts/test_zorg_csp_root_ca_g3.cer
TEST Zorg CSP Level 2 Persoon CA G3	http://www.uzi-register-test.nl/cacerts/test_zorg_csp_level_2_persoon_ca_g3.cer
TEST UZI-register Zorgverlener CA G3	http://www.uzi-register-test.nl/cacerts/test_uzi-register_zorgverlener_ca_g3.cer *na resigning in mei 2019:* http://www.uzi-register-test.nl/cacerts/20190501_test_uzi-register_zorgverlener_ca_g3.cer
TEST UZI-register Medewerker op naam CA G3	http://www.uzi-register-test.nl/cacerts/test_uzi-register_medewerker_op_naam_ca_g3.cer *na resigning in mei 2019:* http://www.uzi-register-test.nl/cacerts/20190501_test_uzi-register_medewerker_op_naam_ca_g3.cer
TEST Zorg CSP Level 2 Services CA G3	http://www.uzi-register-test.nl/cacerts/test_zorg_csp_level_2_services_ca_g3.cer
TEST UZI-register Medewerker niet op naam CA G3	http://www.uzi-register-test.nl/cacerts/test_uzi-register_medewerker_niet_op_naam_ca_g3.cer *na resigning in mei 2019:* http://www.uzi-register-test.nl/cacerts/20190501_test_uzi-register_medewerker_niet_op_naam_ca_g3.cer

Tabel 2 URL's van CA certificaten in acceptatieomgeving generatie public G3

Naam CA	URL van CA certificaat
TEST Zorg CSP Private Root CA G1	http://www.uzi-register-test.nl/cacerts/test_zorg_csp_private_root_ca_g1.cer
TEST Zorg CSP Level 2 Private Services CA G1	http://www.uzi-register-test.nl/cacerts/test_zorg_csp_level_2_private_services_ca_g1.cer
TEST UZI-register Private Server CA G1	http://www.uzi-register-test.nl/cacerts/test_uzi-register_private_server_ca_g1.cer
TEST ZOVAR Private Server CA G1	http://www.csp.zovar-test.nl/cacerts/test_zovar_private_server_ca_g1.cer

Tabel 3 URL's van CA certificaten in acceptatieomgeving generatie private G1

2.3 Controle juistheid van CA certificaten in acceptatieomgeving

Op de uzi-testpassen staat de complete CA hiërarchie van de betreffende testpas. De juistheid van de CA certificaten is met behulp van volgende tabellen vast te stellen op basis van de zogenaamde 'thumbprint'[1]. 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'.

Naam CA	SHA-1 thumbprint CA certificaat
TEST Zorg CSP Root CA G3	d9 d4 a8 97 d4 b5 99 a5 d0 37 a3 2b 76 b6 38 70 95 10 c3 c8
TEST Zorg CSP Level 2 Persoon CA G3	72 2b 48 95 84 64 41 ac 20 d4 03 a2 6b 02 2d bd 24 63 b4 6c
TEST UZI-register Zorgverlener CA G3	00 9a 67 77 4b 16 63 62 df 3d 34 b0 42 68 c8 59 91 5c 55 98
TEST UZI-register Zorgverlener CA G3 (resigned mei 2019)	1c 0f 40 24 f0 d1 e8 ff 82 d6 64 42 30 85 12 34 ee 61 4a ad
TEST UZI-register Medewerker op naam CA G3 (resigned mei 2019)	eb a5 0f f2 31 c9 1c ac 16 e5 ae 46 a1 01 bd 60 62 8e d7 32
TEST UZI-register Medewerker op naam CA G3	5a f5 f0 58 92 cc a8 21 2c eb 5f 5c 77 91 c6 23 a3 10 e5 6e
TEST Zorg CSP Level 2 Services CA G3	63 2a e5 08 84 37 cd f9 69 08 25 28 44 4e e0 0a f5 17 0b c0
TEST UZI-register Medewerker niet op naam CA G3	0a bb 10 b8 63 62 02 ff a1 39 89 2f b2 08 06 8c 8d 96 a7 62
TEST UZI-register Medewerker niet op naam CA G3 (resigned mei 2019)	ca 1a e3 27 e4 5f b0 18 cf 1e 46 82 db b5 a5 32 3a 55 4b 17

Tabel 4 Thumbprints van CA certificaten in acceptatieomgeving generatie public G3

Naam CA	SHA-1 thumbprint CA certificaat
TEST Zorg CSP Private Root CA G1	ad 5e a1 1f 99 c9 dc ac ba d4 b1 a6 7b bf ab 9d 24 74 9a 8b
TEST Zorg CSP Level 2 Private Services CA G1	3f f6 03 35 44 43 47 16 09 02 0a ed 8e 0a 0c ee 5a bc 72 38
TEST UZI-register Private Server CA G1	c6 97 a1 92 75 17 d4 3b 80 85 91 25 be b0 3f 99 21 56 4b 21
TEST ZOVAR Private Server CA G1	f9 b1 93 5b d8 25 be 8c 87 fd a8 40 59 0f fc 5f e1 40 af a3

Tabel 5 Thumbprints van CA certificaten in acceptatieomgeving generatie private G1

[1] In productie omgeving wordt dit geregeld door automatische distributie van het Staat der Nederlanden Root CA certificaat.

3 Pasmodel acceptatieomgeving

3.1 Portfolio testpassen en -certificaten

Het portfolio in de acceptatieomgeving is identiek aan de productieomgeving. Alleen de naamgeving is veranderd. De toegepaste codering is ongewijzigd.

Naam UZI-testpastype	Codering testpastype
Zorgverlenertestpas	Z
Medewerkertestpas op naam	N
Medewerkertestpas niet op naam	M
UZI-register Servertestcertificaat	S
ZOVAR Servertestcertificaat	V

Tabel 6 Naamgeving en codering testpassen en -certificaten

Tabel 7 geeft een overzicht van de specifieke kenmerken van de verschillende testpastypen. In de beschrijving van de diverse processen wordt hiernaar verwezen.

Pastype ---------- Eigenschappen	Zorgverlener-testpas	Medewerker-testpas op naam	Medewerkertestpas niet op naam	UZI-register test Servercertificaat	ZOVAR test Servercertificaat
Certificaten	A,H,V	A,H,V	A,V	Server	Server
Drager	smartcard	smartcard	smartcard	divers	divers
Issuing CA Common Name generatie Public G3/Private G1	TEST UZI-register Zorgverlener CA G3	TEST UZI-register Medewerker op naam CA G3	TEST UZI-register Medewerker niet op naam CA G3	TEST UZI-register Private Server CA G1	TEST ZOVAR Private Server CA G1

Tabel 7 Overzicht kenmerken testpassen en -certificaten

4 Algemene keuzes certificaatprofielen

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

4.1 UZI-nummer en abonneenummer

De volgende reeksen UZI-nummers zijn gereserveerd voor testdoeleinden:

- 000000001 t/m 000009999
- 900000000 t/m 999999999.

In de subjectAltName.otherName van de testcertificaten van het UZI-register is een abonneenummer opgenomen. De volgende reeksen abonneenummers zijn gereserveerd voor testdoeleinden:

- 00000001 t/m 00010000
- 90000000 t/m 99999999.

4.2 subject.serialNumber in ZOVAR Servercertificaat

Voor de ZOVAR Servercertificaten wordt het subject.SerialNumber als volgt gevuld:
`<UZOVI-nummer><ZOVAR-nummer>`

In de acceptatieomgeving komt het unieke nummer `ZOVAR-nummer` komt uit dezelfde nummerreeks als het UZI-nummer in de acceptatieomgeving.

4.3 Waarden van certificatePolicies extensie

De volgende waarden voor certificatePolicies extensie zullen worden geconfigureerd.

4.3.1 certificatePolicies.policyIdentifier

CA certificaten generatie Public G3/Private G1

In alle CA certificaten (m.u.v. de Root CA certificaten) zijn de policyIdentifiers opgenomen van de Policy waarvoor de CA gebruikercertificaten uitgeeft. Deze zijn gespecificeerd in de volgende tabellen.

Gebruikertestcertificaten

Tabel 8 geeft een overzicht PolicyIdentifiers (OID's) van de verschillende pastypen.

Naam testpas/-certificaat	OID (PolicyIdentifier)	Omschrijving
Authenticiteitcertificaten: • Zorgverlenertestpas • Medewerkertestpas op naam	2.16.528.1.1007.99.211	OID van de CIBG Certificate Policy voor authenticiteitscertificaten in de UZI-register acceptatieomgeving.
Onweerlegbaarheidcertificaten • Zorgverlenertestpas • Medewerkertestpas op naam	2.16.528.1.1007.99.212	OID van de CIBG Certificate Policy voor onweerlegbaarheidcertificaten in de UZI-register acceptatieomgeving.
Vertrouwelijkheidcertificaten • Zorgverlenertestpas • Medewerkertestpas op naam	2.16.528.1.1007.99.213	OID van de CIBG Certificate Policy voor vertrouwelijkheidcertificaten in de UZI-register acceptatieomgeving.
Authenticiteitcertificaten • Medewerkertestpas niet op naam	2.16.528.1.1007.99.214	OID van de CIBG Certificate Policy voor Services authenticiteitcertificaten in de UZI-register acceptatieomgeving.
Vertrouwelijkheidcertificaten • Medewerkertestpas niet op naam	2.16.528.1.1007.99.215	OID van de CIBG Certificate Policy voor Services vertrouwelijkheidcertificaten in de UZI-register acceptatieomgeving.

Naam testpas/-certificaat	OID (PolicyIdentifier)	Omschrijving
UZI-register Servertestcertificaat	2.16.528.1.1007.99.12	OID van de CIBG Certificate Policy voor private server certificaten in de UZI-register acceptatieomgeving.
ZOVAR Servertestcertificaat	2.16.528.1.1007.98.4	OID van de CIBG Certificate Policy voor private server certificaten in de ZOVAR acceptatieomgeving.

Tabel 8 Waarden PolicyIdentifier voor gebruikertestcertificaten en CA certificaten

In G3 OCSP responders is de volgende Policy OID opgenomen: 2.16.528.1.1007.99.214. In de G1 OCSP responders is in de acceptatieomgeving opgenomen: 2.16.528.1.1007.99.13. Dit is de Policy OID voor services authenticiteit in acceptatieomgeving.

4.3.2 User Notice (certificatePolicies.PolicyQualifier.userNotice.explicitText)

CA-testcertificaten

Voor alle CA certificaten in de acceptatieomgeving geldt: **géén User Notice**.

Gebruikertestcertificaten UZI-register

Voor alle gebruikertestcertifcaten van het UZI-register is in de acceptatieomgeving de volgende User Notice toegepast:
Certificaat uitsluitend gebruiken ten behoeve van de TEST van het UZI-register. Het UZI-register is in geen geval aansprakelijk voor eventuele schade.

Gebruikertestcertificaten ZOVAR

Voor alle gebruikertestcertifcaten van ZOVAR is in de acceptatieomgeving de volgende User Notice toegepast:
Certificaat uitsluitend gebruiken ten behoeve van de TEST van ZOVAR. Het CIBG is in geen geval aansprakelijk voor eventuele schade.

4.3.3 certificatePolicies.PolicyQualifier.cPS.uri

CA-certificaten en Gebruikercertificaten UZI-register generatie Public G3/Private G1

In alle CA certificaten en in de gebruikercertificaten is bij de generatie Public G3/Private G1 de volgende certificatePolicies.PolicyQualifier.cPS.uri opgenomen in de acceptatieomgeving:
https://acceptatie.zorgcsp.nl/cps/uzi-register.html

CA-certificaat en Gebruikercertificaat ZOVAR generatie Public G3/Private G1

In het ZOVAR Server CA certificaat en de ZOVAR Servercertificaten is bij generatie Public G3/Private G1 de volgende certificatePolicies.PolicyQualifier.cPS.uri opgenomen in de acceptatieomgeving:
https://acceptatie.zorgcsp.nl/cps/zovar.html

4.4 Waarden cRLDistributionPoints.distributionPoint.fullName

4.4.1 CA certificaten TEST Zorg CSP

In de CA certificaten zijn de volgende cRLDistributionPoint (CDP) waarden geconfigureerd:

Naam CA	Waarde CRL Distribution Point in certificaat
TEST Zorg CSP Root CA G3	GEEN ATTRIBUUT CRL DISTRIBUTION POINT
TEST Zorg CSP Level 2 Persoon CA G3	http://www.uzi-register-test.nl/cdp/test_zorg_csp_root_ca_g3.crl
TEST UZI-register Zorgverlener CA G3 TEST UZI-register Medewerker op naam CA G3	http://www.uzi-register-test.nl/cdp/test_zorg_csp_level_2_persoon_ca_g3.crl
TEST Zorg CSP Level 2 Services CA G3	http://www.uzi-register-test.nl/cdp/test_zorg_csp_root_ca_g3.crl
TEST UZI-register Medewerker niet op naam CA G3	http://www.uzi-register-test.nl/cdp/test_zorg_csp_level_2_services_ca_g3.crl

Tabel 9 CRL Distribution points in CA testcertificaten generatie public G3

Naam CA	Waarde CRL Distribution Point in certificaat
TEST Zorg CSP Private Root CA G1	GEEN ATTRIBUUT CRL DISTRIBUTION POINT
TEST Zorg CSP Level 2 Private Services CA G1	http://www.uzi-register-test.nl/cdp/test_zorg_csp_private_root_ca_g1.crl
TEST UZI-register Private Server CA G1 TEST ZOVAR Private Server CA G1	http://www.uzi-register-test.nl/cdp/test_zorg_csp_level_2_private_services_ca_g1.crl

Tabel 10 CRL Distribution points in CA testcertificaten generatie private G1

4.4.2 Gebruikertestcertificaten Acceptatieomgeving

Bij de gebruikertestcertificaten verschilt het CDP per certificaattype afhankelijk van de CA die het certificaat uitgeeft. De volgende tabellen geven een overzicht van de CDP's per pastype in de verschillende generaties van de Acceptatieomgeving.

Naam UZI-pastype	CRL Distribution Point
Zorgverlenertestpas	http://www.uzi-register-test.nl/cdp/test_uzi-register_zorgverlener_ca_g3.crl
Medewerkertestpas op naam	http://www.uzi-register-test.nl/cdp/test_uzi-register_medewerker_op_naam_ca_g3.crl
Medewerkertestpas niet op naam	http://www.uzi-register-test.nl/cdp/test_uzi-register_medewerker_niet_op_naam_ca_g3.crl
UZI-register Servertestcertificaat	http://www.uzi-register-test.nl/cdp/test_uzi-register_private_server_ca_g1.crl
ZOVAR Servertestcertificaat	http://www.csp.zovar-test.nl/cdp/test_zovar_private_server_ca_g1.crl

Tabel 11 CRL Distribution points in gebruikertestcertificaten generatie public G3/Private G1

5 Profiel gebruikertestcertificaten

Dit hoofdstuk bevat uitsluitend de wijzigingen in de profielen van de gebruikerstestcertificaten ten opzichte van de productieomgeving. Dit geldt voor alle gebruikerscertificaatprofielen tenzij expliciet anders is vermeld.

5.1 Issuer

De issuer.commonName zal in de gebruikerstestcertificaten de naam van de betreffende TEST CA bevatten. Zie voor de relatie tussen UZI-testpassen en de TEST CA's: tabel 7.

5.2 ETSI QC statement (handtekeningscertificaten)

Er wordt **GEEN** ETSI QC statement opgenomen in de handtekeningcertificaten die door de acceptatieomgeving worden uitgegeven. Dit attribuut geeft aan dat een certificaat gekwalificeerd en voldoet aan EU Verordening 910/2014. Dit is voor de testcertificaten niet het geval.

5.3 AuthorityInfoAccess

Dit attribuut bevat de URL naar de OCSP dienstverlening in de acceptatieomgeving van het UZI-register.

Certificaatveld / attribuut	Critical	Waarde	Omschrijving / toelichting
AuthorityInfoAccess			
AuthorityInfoAccess. uniformResourceIndicator		http://ocsp.uzi-register-test.nl OF http://ocsp.zovar-test.nl	Op deze URL is de OCSP dienstverlening beschikbaar voor de acceptatieomgeving van het UZI-register.
AuthorityInfoAccess. accessMethod		1.3.6.1.5.5.7.48.1	OCSP: {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) ocsp(1)}

Tabel 12 AuthorityInfoAccess in gebruikertestcertificaten van het UZI-register

5.4 certificatePolicies.PolicyIdentifier

Zie. Par. 4.3.

5.5 certificatePolicies.PolicyQualifier.cPS.uri

Zie. Par. 4.3.

5.6 certificatePolicies.PolicyQualifier.userNotice.explicitText

Zie. Par. 4.3.

5.7 CRL distribution Point

Zie. Par. 4.4.

5.8 SubjectAltName.otherName

De syntax van de subjectAltName.othername is in de acceptatieomgeving volledig identiek aan de productieomgeving. Alleen de waarden van de <OID CA> wijken af.

Waarden <OID CA>
Onderstaande tabel geeft de <OID CA> weer.

CA type	<OID CA> waarde voor bijbehorende gebruikerstestcertificaten
TEST UZI-register Zorgverlener	2.16.528.1.1007.99.217
TEST UZI-register Medewerker op naam	2.16.528.1.1007.99.218
TEST UZI-register Medewerker niet op naam	2.16.528.1.1007.99.219
TEST UZI-register Server	2.16.528.1.1007.99.2110
TEST ZOVAR Server	2.16.528.1.1007.98.212

Tabel 13 <OID CA> in gebruikertestscertificaten

5.8.1 Voorbeelden SubjectAltName.otherName

Zorgverlenertestpas van een cardioloog
<OID CA>-<versie-nr>-<UZI-nr>-<pastype>-<Abonnee-nr>-<rol>-<AGB-code>
`2.16.528.1.1007.99.217-1-000000789-Z-00000078-01.010-12345678`

In bovenstaand voorbeeld:
- <OID CA> = `2.16.528.1.1007.99.217` (OID van de TEST UZI-register Zorgverlener CA)
- <versie-nr> = `1`
- <UZI-nr> = `000000789`
- <pastype> = `Z`
- <Abonnee-nr> = `00000078`
- <rol> = `01.010` (Beroepstitel: 01=arts; specialisme: 010=cardiologie)
- <AGB-code> = `12345678` (AGB-code van de betreffende zorgverlener.)

ZOVAR Servertestcertificaat
<OID CA>-<versie-nr>-<subject-nr>-<pastype>-<UZOVI-nr>-<Erkenning>
`2.16.528.1.1007.98.212-1-8643000000789-V-8643-ZV`

In bovenstaand voorbeeld is:
- <OID CA> = `2.16.528.1.1007.98.212` (OID van de TEST ZOVAR Server CA)
- <versie-nr> = `1`
- <subject-nr> = `8643000000789`
- <pastype> = `V`
- <UZOVI-nr> = `8643` (uniek identificerend nummer van de zorgverzekeraar.)
- <Erkenning> = `ZV` (ZorgVerzekeraar)

6 CRL profielen

6.1 CRL profiel van Root CA's acceptatieomgeving

Dit is een CRL die in de productieomgeving wordt uitgegeven door de PKI voor de Overheid en daarom niet in de certificaatprofielen van de productieomgeving van de Zorg CSP is gedocumenteerd. Op deze CRL komen alleen entries voor als een onderliggend CA certificaat is ingetrokken. Het profiel specificeert alle generaties.

CRL profiel van TEST UZI-register/Zorg CSP Root CA's			
CRL veld	**Critical**	**Waarde**	**Omschrijving / Toelichting**
TBSCertList			
version		1	CRL version 2
signature		1.2.840.113549.1.1.11	De waarde is de OID die het algoritme specificeert van de handtekening over de CRL: sha256WithRSAEncryption
Issuer.commonName (CN)		*Public G3/Private G1 generatie afhankelijk van pastype:* • TEST Zorg CSP Root CA G3 • TEST Zorg CSP Private Root CA G1	
Issuer.organizationName (O)		*Public G3/Private G1 generatie:* **CIBG**	
Issuer.country (C)		NL	
thisUpdate		Automatisch gegenereerd	Uitgiftetijdstip van de CRL.
nextUpdate		Automatisch gegenereerd	**Uitgiftetijdstip + 48 uur**.
revokedCertificates			Lijst van ingetrokken certificaten bestaande uit het serienummer van het certificaat en de datum van revocatie.
crlExtensies			
authorityKeyIdentifier. keyIdentifier	FALSE	SHA-1 hash van publieke CA sleutel.	Dit attribuut bevat het controle getal voor de publieke sleutel van de CA die de CRL ondertekent.
cRLNumber	FALSE	Automatisch gegenereerd	Volgnummer CRL voor deze CA.
ExpiredCertsOnCRL	FALSE	OID 2 5 29 60	Ingetrokken certificaten blijven op CRL ook na verlopen geldigheidsduur.
date		mm/dd/jjjj	Datum hangt mogelijk af van implementatie moment, maar het effect zal zijn dat alle ingetrokken Public G1/Private G3 certificaten op de CRL zullen blijven.
CertificateList			
signatureAlgorithm		1.2.840.113549.1.1.11	De waarde is de OID die het algoritme specificeert van de handtekening over de CRL: sha256WithRSAEncryption
signatureValue		Handtekening van CA over het tbsCertificateList.	

Tabel 14 CRL profiel van Root CA's acceptatieomgeving

6.2 CRL profiel van TEST UZI-register/Zorg CSP Level 2 CA's

Dit is een CRL die in de productieomgeving wordt uitgegeven door de PKI voor de Overheid. Op deze CRL komen alleen entries voor als er een onderliggend CA certificaat is ingetrokken. In het onderstaande profiel zijn alleen de afwijkingen ten opzichte van het CRL profiel van de TEST UZI-register Root CA weergegeven. Het profiel specificeert alle generaties.

CRL profiel van TEST UZI-register Level 2 CA		
CRL veld	**Critical**	**Waarde**
Velden		
Issuer.commonName (CN)		*Public G3/Private G1 generatie afhankelijk van pastype:* • TEST Zorg CSP Level 2 Persoon CA G3 • TEST Zorg CSP Level 2 Services CA G3 • TEST Zorg CSP Level 2 Private Services CA G1
Issuer.organizationName (O)		*Public G3/Private G1 generatie:* **CIBG**

Tabel 15 CRL profiel van Level 2 CA's acceptatieomgeving

6.3 CRL profiel van CA's voor eindgebruikertestcertificaten

In de onderstaande tabel zijn alleen de afwijkingen ten opzichte van het CRL profiel van de TEST UZI-register Root CA weergegeven. Het betreft hier de 5 sub CA's die testcertificaten uitgeven voor eindgebruikers.

CRL profiel van TEST CA's eindgebruikercertificaten			
CRL veld	**Waarde**		**Omschrijving / Toelichting**
Velden			
issuer.CN	*Generatie Public G3:*	TEST UZI-register Zorgverlener CA G3	CRL met de ingetrokken Zorgverlener testcertificaten.
issuer.CN	*Generatie Public G3:*	TEST UZI-register Medewerker op naam CA G3	CRL met de ingetrokken Medewerker op naam testcertificaten.
issuer.CN	*Generatie Public G3:*	TEST UZI-register Medewerker niet op naam CA G3	CRL met de ingetrokken Medewerker niet op naam testcertificaten.
issuer.CN	*Generatie Private G1:*	TEST UZI-register Private Server CA G1	CRL met de ingetrokken UZI-register Servertestcertificaten.
issuer.CN	*Generatie Private G1:*	TEST ZOVAR Private Server CA G1	CRL met de ingetrokken ZOVAR Servertestcertificaten.
issuer.O	*Public G3/Private G1 generatie:* **CIBG**		

Tabel 16 CRL profiel van CA's voor eindgebruikertestcertificaten

6.4 CRL publicatieschema en publicatiefrequentie

Het CRL publicatieschema en de publicatiefrequentie zijn in de acceptatieomgeving identiek aan de productieomgeving.

De onderhoudswerkzaamheden voor de acceptatieomgeving zullen binnen kantoortijden worden uitgevoerd, waardoor publicatie soms een lagere frequentie heeft.

7 BIJLAGE: Profielen CA certificaten G3/G1

Deze bijlage bevat de profielen/naming documents voor alle CA certificaten in de acceptatieomgeving. Deze zijn volledige gebaseerd op de productie profielen van PKIoverheid met daarin de waarden opgenomen van namen, URL's en OID's zoals in dit document zijn gespecificeerd.

7.1 Profielen Root CA's

7.1.1 TEST Zorg CSP Root CA G3

PROFIEL TEST Zorg CSP Root CA G3			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd CA	Uniek certificaatnummer.
signature		1.2.840.113549.1.1.11	OID van het algoritme waarmee handtekening onder het certificaat is gezet: sha256WithRSAEncryption
issuer.commonName (CN)		**TEST Zorg CSP Root CA G3**	UTF8String
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.countryName (C)		**NL**	PrintableString
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**14 november 2028** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Gelijk aan G3 productie Root CA
subject.commonName (CN)		**TEST Zorg CSP Root CA G3**	UTF8String
subject.organization Name (O)		**CIBG**	UTF8String
subject.countryName (C)		**NL**	PrintableString
subjectPublicKeyInfo. algorithm		1.2.840.113549.1.1.1	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden. In dit geval het RSA algoritme (rsaEncryption).
SubjectPublicKeyInfo. subjectPublic.Key		4096 bits publieke RSA sleutel	Dit attribuut bevat de publieke sleutel.
Standard Extension			
subjectKeyIdentifier		SHA-1 hash van subject public key	-
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint			Geen beperking (none)
keyUsage	TRUE	Certificate Signing, Off-line CRL Signing, CRL Signing	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11	Algoritme waarmee de handtekening onder het certificaat is gezet: sha256WithRSAEncryption
signatureValue		Selfsigned handtekening (ASN.1 DER)	

Tabel 17 Profiel TEST Zorg CSP Root CA G3

7.1.2 TEST Zorg CSP Private Root CA G1

PROFIEL TEST Zorg CSP Private Root CA G1			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd door CSP CA	Uniek certificaatnummer.
signature		1.2.840.113549.1.1.11	OID van het algoritme waarmee handtekening onder het certificaat is gezet: sha256WithRSAEncryption
issuer.commonName (CN)		**TEST Zorg CSP Private Root CA G1**	UTF8String
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.countryName (C)		**NL**	PrintableString
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**14 november 2028** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Gelijk aan G3 productie Root CA
subject.commonName (CN)		**TEST Zorg CSP Private Root CA G1**	UTF8String
subject.organization Name (O)		**CIBG**	UTF8String
subject.countryName (C)		**NL**	PrintableString
subjectPublicKeyInfo. algorithm		1.2.840.113549.1.1.1	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden. In dit geval het RSA algoritme (rsaEncryption).
SubjectPublicKeyInfo. subjectPublic.Key		4096 bits publieke RSA sleutel	Dit attribuut bevat de publieke sleutel.
Standard Extension			
subjectKeyIdentifier		SHA-1 hash van subject public key	-
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint			Geen beperking (none)
keyUsage	TRUE	Certificate Signing, Off-line CRL Signing, CRL Signing	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11	Algoritme waarmee de handtekening onder het certificaat is gezet: sha256WithRSAEncryption
signatureValue		Selfsigned Handtekening (ASN.1 DER)	

Tabel 18 Profiel TEST Zorg CSP Private Root CA G1

7.2 Profielen Level 2 CA's

7.2.1 TEST Zorg CSP Level 2 CA Persoon CA G3

PROFIEL TEST Zorg CSP Level 2 Persoon CA G3			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd door CA	Uniek certificaat serienummer.
signature		1.2.840.113549.1.1.11	OID van algoritme waarmee handtekening onder het certificaat is gezet: sha256WithRSAEncryption
issuer.commonName (CN)		**TEST Zorg CSP Root CA G3**	UTF8String
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.countryName (C)		**NL**	PrintableString
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**13 november 2028** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is.
subject.commonName (CN)		**TEST Zorg CSP Level 2 Persoon CA G3**	UTF8String
subject.organizationName (O)		**CIBG**	UTF8String
subject.countryName (C)		**NL**	PrintableString
subjectPublicKeyInfo. algorithm		1.2.840.113549.1.1.1	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden. In dit geval het RSA algoritme (rsaEncryption).
SubjectPublicKeyInfo. subjectPublic.Key		4096 bits publieke RSA sleutel	Dit attribuut bevat de publieke sleutel.
Standard Extension			
certificatePolicies			
.PolicyIdentifier		**2.16.528.1.1007.99.211** **2.16.528.1.1007.99.212** **2.16.528.1.1007.99.213**	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3.1). Deze OID's verschillen per level 2 CA
.PolicyQualifier.cPS.uri		**https://acceptatie.zorgcsp.nl/cps/uzi-register.html**	Dit attribuut bevat de URL voor het Certificate Practice Statement van het UZI-register (Zie Par. 4.3.3)
authorityKeyIdentifier. KeyIdentifier		SHA-1 hash van issuer public key.	sha-1 hash van authority key (=publieke sleutel van de Root CA) waarmee de handtekening onder dit CA certificaat gevalideerd kan worden.
cRLDistributionPoints. distributionPoint. fullName		**http://www.uzi-register-test.nl/cdp/test_zorg_csp_root_ca_g3.crl**	Zie Par. 4.4.1: URI van CRL distribution point van CRL ondertekend door: TEST Zorg CSP Root CA G3
subjectKeyIdentifier		SHA-1 hash van subject public key	-
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint			Geen beperking (none)
keyUsage	TRUE	Certificate Signing, Off-line CRL Signing, CRL Signing	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11	Algoritme waarmee de handtekening onder het certificaat is gezet: sha256WithRSAEncryption
signatureValue		Handtekening door Root CA (ASN.1 DER)	

Tabel 19 Profiel TEST Zorg CSP Level 2 Persoon CA G3

7.2.2 TEST Zorg CSP Level 2 Services CA G3

PROFIEL TEST Zorg CSP Level 2 Services CA G3			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd door CA	Uniek certificaat serienummer.
signature		1.2.840.113549.1.1.11	OID van algoritme waarmee handtekening onder het certificaat is gezet: sha256WithRSAEncryption
issuer.commonName (CN)		**TEST Zorg CSP Root CA G3**	UTF8String
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.countryName (C)		**NL**	PrintableString
validity.notBefore		UTCTime	Tijdstip vanaf wanneer het certificaat geldig is.
validity.notAfter		**13 november 2028** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is.
subject.commonName (CN)		**TEST Zorg CSP Level 2 Services CA G3**	UTF8String
subject.organizationName (O)		**CIBG**	UTF8String
subject.countryName (C)		**NL**	PrintableString
subjectPublicKeyInfo. algorithm		1.2.840.113549.1.1.1	Algoritme waarmee de publieke sleutel gebruikt dient te worden: rsaEncryption.
SubjectPublicKeyInfo. subjectPublic.Key		4096 bits publieke RSA sleutel	Dit attribuut bevat de publieke sleutel.
Standard Extension			
certificatePolicies			
.PolicyIdentifier		**2.16.528.1.1007.99.214** **2.16.528.1.1007.99.215** **2.16.528.1.1007.99.216**	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3.1). Deze OID's verschillen per level 2 CA. 2.16.528.1.1007.99.216 (services server) wordt niet gebruikt vanwege overgang naar de private omgeving maar is opgenomen voor maximale conformiteit met de productie omgeving.
.PolicyQualifier.cPS.uri		**https://acceptatie.zorgcsp.nl/cps/uzi-register.html**	Dit attribuut bevat de URL voor het Certificate Practice Statement van UZI-register (Zie Par. 4.3.3)
authorityInfoAccess			**Alleen Public G3/Private G1 generatie**
.accessMethod (OCSP)		1.3.6.1.5.5.7.48.1	
.uniformResourceIndicator		**http://ocsp.uzi-register-test.nl**	Op deze URL is de OCSP dienstverlening beschikbaar.
authorityKeyIdentifier. KeyIdentifier		SHA-1 hash van issuer public key.	sha-1 hash van authority key (=publieke sleutel van de Root CA).
cRLDistributionPoints. distributionPoint. fullName		**http://www.uzi-register-test.nl/cdp/test_zorg_csp_root_ca_g3.crl**	Zie Par. 4.4.1: URI van CRL distribution point van CRL ondertekend door: TEST Zorg CSP Root CA G3
subjectKeyIdentifier		SHA-1 hash van subject public key	-
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint			Geen beperking (none)
keyUsage	TRUE	Certificate Signing, Off-line CRL Signing, CRL Signing	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11	Algoritme waarmee de handtekening onder het certificaat is gezet: sha256WithRSAEncryption
signatureValue		Handtekening Root CA (ASN.1 DER)	

Tabel 20 Profiel TEST Zorg CSP Level 2 Services CA G3

7.2.3 TEST Zorg CSP Level 2 Private Services CA G1

PROFIEL TEST Zorg CSP Level 2 Private Services CA G1			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd door CA	Uniek certificaat serienummer.
signature		1.2.840.113549.1.1.11	OID van algoritme waarmee handtekening onder het certificaat is gezet: sha256WithRSAEncryption
issuer.commonName (CN)		**TEST Zorg CSP Private Root CA G1**	UTF8String
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.countryName (C)		**NL**	PrintableString
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**13 november 2028** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is.
subject.commonName (CN)		**TEST Zorg CSP Level 2 Private Services CA G1**	UTF8String
subject.organizationName (O)		**CIBG**	UTF8String
subject.countryName (C)		**NL**	PrintableString
subjectPublicKeyInfo. algorithm		1.2.840.113549.1.1.1	Algoritme waarmee de publieke sleutel gebruikt dient te worden: rsaEncryption
SubjectPublicKeyInfo. subjectPublic.Key		4096 bits publieke RSA sleutel	Dit attribuut bevat de publieke sleutel.
Standard Extension			
certificatePolicies			
.PolicyIdentifier		**2.16.528.1.1007.99.12** **2.16.528.1.1007.98.4**	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3.1). Deze OID's verschillen per level 2 CA
.PolicyQualifier.cPS.uri		**https://acceptatie.zorgcsp.nl/cps/uzi-register.html**	De URL voor het Certificate Practice Statement van het UZI-register (Zie Par. 4.3.3)
authorityInfoAccess			
authorityInfoAccess. accessMethod		1.3.6.1.5.5.7.48.2 (Certification Authority Issuer)	Verwijzing bevat naar het CA certificaat waaronder het certificaat is uitgegeven.
.accessLocation		**http://www.uzi-register-test.nl/cacerts/test_zorg_csp_private_root_ca_g1.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 2.2
authorityKeyIdentifier. KeyIdentifier		SHA-1 hash van issuer public key.	sha-1 hash van authority key (=publieke sleutel van de Root CA).
cRLDistributionPoints. distributionPoint. fullName		**http://www.uzi-register-test.nl/cdp/test_zorg_csp_private_root_ca_g1.crl**	Zie Par. 4.4.1: URI van CRL distribution point van CRL ondertekend door: TEST Zorg CSP Private Root CA G1
subjectKeyIdentifier		SHA-1 hash van subject public key	-
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint			Geen beperking (none)
keyUsage	TRUE	Certificate Signing, Off-line CRL Signing, CRL Signing	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11	Algoritme waarmee de handtekening onder het certificaat is gezet: sha256WithRSAEncryption
signatureValue		Handtekening Root CA (ASN.1 DER)	

Tabel 21 Profiel TEST Zorg CSP Level 2 Private Services CA G1

7.3 Profielen issuing CA's

7.3.1 TEST UZI-register Zorgverlener CA G3

PROFIEL TEST UZI-register Zorgverlener CA G3			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd door CA	Een door de CA random gegenereerd uniek certificaatnummer (160 bits positief integer na resigning mei 2019).
signature		1.2.840.113549.1.1.11	OID van het algoritme waarmee handtekening onder het certificaat is gezet: sha256WithRSAEncryption
issuer.commonName (CN)		**TEST Zorg CSP Level 2 Persoon CA G3**	UTF8String
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.countryName (C)		**NL**	PrintableString
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**12 november 2028** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Gelijk aan productie hiërarchie.
subject.commonName (CN)		**TEST UZI-register Zorgverlener CA G3**	UTF8String
subject.organizationIdentifier		**NTRNL-50000535**	UTF8String
subject.organization Name (O)		**CIBG**	UTF8String
subject.countryName (C)		**NL**	PrintableString
subjectPublicKeyInfo. algorithm		1.2.840.113549.1.1.1	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden. In dit geval het RSA algoritme (rsaEncryption).
SubjectPublicKeyInfo. subjectPublic.Key		4096 bits publieke RSA sleutel	Dit attribuut bevat de publieke sleutel.
Standard Extension			
authorityInfoAccess			**Alleen Public G3/Private G1 generatie**
.accessMethod		1.3.6.1.5.5.7.48.2 (Certification Authority Issuer)	In G3 heeft Logius een extensie toegevoegd die een verwijzing bevat naar het CA certificaat waaronder het certificaat is uitgegeven.
.accessLocation		**http://www.uzi-register-test.nl/cacerts/test_zorg_csp_level_2_persoon_ca_g3.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 2.2
subjectKeyIdentifier		SHA-1 hash van subject public key	-
authorityKeyIdentifier. KeyIdentifier		SHA-1 hash van issuer public key.	sha-1 hash van authority key (=publieke sleutel van de Level 2 CA).
certificatePolicies			
.PolicyIdentifier		**2.16.528.1.1007.99.211** **2.16.528.1.1007.99.212** **2.16.528.1.1007.99.213**	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3.1). Deze OID's verschillen per level 2 CA
.PolicyQualifier.cPS.uri		**https://acceptatie.zorgcsp.nl/cps/uzi-register.html**	Dit attribuut bevat de URL voor het Certificate Practice Statement van het UZI-register (Zie Par. 4.3.3)

PROFIEL TEST UZI-register Zorgverlener CA G3			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
cRLDistributionPoints. distributionPoint. fullName		**http://www.uzi-register-test.nl/cdp/test_zorg_csp_level_2_persoon_ca_g3.crl**	URI van CRL distribution point van level 2 CA. Zie. Par. 4.4.
extKeyUsage		Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4) Document Signing (1.3.6.1.4.1.311.10.3.12) Encrypting File System (1.3.6.1.4.1.311.10.3.4) OCSP Signing (1.3.6.1.5.5.7.3.9)	
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint		0	Hieronder kunnen geen CA's meer gecreëerd worden.
keyUsage	TRUE	Certificate Signing, Off-line CRL Signing, CRL Signing	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11	Algoritme waarmee de handtekening onder het certificaat is gezet: sha256WithRSAEncryption
signatureValue		Handtekening door CSP CA (ASN.1 DER)	

Tabel 22 Profiel TEST UZI-register Zorgverlener CA G3

7.3.2 TEST UZI-register Medewerker op naam CA G3

PROFIEL TEST UZI-register Medewerker op naam CA G3			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd door CA	Een door de CA random gegenereerd uniek certificaatnummer (160 bits positief integer na resigning mei 2019).
signature		1.2.840.113549.1.1.11	OID van het algoritme waarmee handtekening onder het certificaat is gezet: sha256WithRSAEncryption
issuer.commonName (CN)		**TEST Zorg CSP Level 2 Persoon CA G3**	UTF8String
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.countryName (C)		**NL**	PrintableString
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**12 november 2028** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Gelijk aan productie hiërarchie.
subject.commonName (CN)		**TEST UZI-register Medewerker op naam CA G3**	UTF8String
issuer.organizationIdentifier		**NTRNL-50000535**	UTF8String
subject.organization Name (O)		**CIBG**	UTF8String
subject.countryName (C)		**NL**	PrintableString
subjectPublicKeyInfo. algorithm		1.2.840.113549.1.1.1	Het algoritme waarmee de publieke sleutel gebruikt dient te worden: (rsaEncryption).
SubjectPublicKeyInfo. subjectPublic.Key		4096 bits publieke RSA sleutel	Dit attribuut bevat de publieke sleutel.
Standard Extension			
authorityInfoAccess			**Alleen Public G3/Private G1 generatie**
.accessMethod		1.3.6.1.5.5.7.48.2 (Certification Authority Issuer)	Bevat verwijzing naar het CA certificaat waaronder het certificaat is uitgegeven.
.accessLocation		**http://www.uzi-register-test.nl/cacerts/test_zorg_csp_level_2_persoon_ca_g3.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 2.2
subjectKeyIdentifier		SHA-1 hash van subject public key	-
authorityKeyIdentifier. KeyIdentifier		SHA-1 hash van issuer public key.	sha-1 hash van authority key (=publieke sleutel van de Level 2 CA) voor validatie van dit CA certificaat.
certificatePolicies			
.PolicyIdentifier		**2.16.528.1.1007.99.211** **2.16.528.1.1007.99.212** **2.16.528.1.1007.99.213**	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3.1). Deze OID's verschillen per level 2 CA
.PolicyQualifier.cPS.uri		**https://acceptatie.zorgcsp.nl/cps/uzi-register.html**	Dit attribuut bevat de URL voor het Certificate Practice Statement van het UZI-register (Zie Par. 4.3.3)
cRLDistributionPoints. distributionPoint. fullName		**http://www.uzi-register-test.nl/cdp/test_zorg_csp_level_2_persoon_ca_g3.crl**	URI van CRL distribution point van Level 2 CA. Zie. Par. 4.4.

PROFIEL TEST UZI-register Medewerker op naam CA G3			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
extKeyUsage		Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4) Document Signing (1.3.6.1.4.1.311.10.3.12) Encrypting File System (1.3.6.1.4.1.311.10.3.4) OCSP Signing (1.3.6.1.5.5.7.3.9)	
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint		0	Hieronder kunnen geen CA's meer gecreëerd worden.
keyUsage	TRUE	Certificate Signing, Off-line CRL Signing, CRL Signing	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11	Algoritme waarmee de handtekening onder het certificaat is gezet: sha256WithRSAEncryption
signatureValue		Handtekening door CSP CA (ASN.1 DER)	

Tabel 23 Profiel TEST UZI-register Medewerker op naam CA G3

7.3.3 TEST UZI-register Medewerker niet op naam CA G3

PROFIEL TEST UZI-register Medewerker niet op naam CA G3			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd door CA	Een door de CA random gegenereerd uniek certificaatnummer (160 bits positief integer na resigning mei 2019).
signature		1.2.840.113549.1.1.11	OID van het algoritme waarmee handtekening onder het certificaat is gezet: sha256WithRSAEncryption
issuer.commonName (CN)		**TEST Zorg CSP Level 2 Services CA G3**	UTF8String
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.countryName (C)		**NL**	PrintableString
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**12 november 2028** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Gelijk aan productie hiërarchie.
subject.commonName (CN)		**TEST UZI-register Medewerker niet op naam CA G3**	UTF8String
subject.organizationIdentifier		**NTRNL-50000535**	UTF8String
subject.organization Name (O)		**CIBG**	UTF8String
subject.countryName (C)		**NL**	PrintableString
subjectPublicKeyInfo. algorithm		1.2.840.113549.1.1.1	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden. In dit geval het RSA algoritme (rsaEncryption).
SubjectPublicKeyInfo. subjectPublic.Key		4096 bits publieke RSA sleutel	Dit attribuut bevat de publieke sleutel.
Standard Extension			
authorityInfoAccess			**Alleen Public G3/Private G1 generatie**
authorityInfoAccess. accessMethod		1.3.6.1.5.5.7.48.2 (Certification Authority Issuer)	Bevat een verwijzing naar het CA certificaat waaronder het certificaat is uitgegeven.
.accessLocation		**http://www.uzi-register-test.nl/cacerts/test_zorg_csp_level_2_services_ca_g3.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 2.2
.accessMethod (OCSP)		1.3.6.1.5.5.7.48.1	
.uniformResourceIndicator		**http://ocsp.uzi-register-test.nl**	Op deze URL is de OCSP dienstverlening beschikbaar.
subjectKeyIdentifier		SHA-1 hash van subject public key	-
authorityKeyIdentifier. KeyIdentifier		SHA-1 hash van issuer public key.	sha-1 hash van authority key (=publieke sleutel van de Level 2 CA) ter validatie van dit CA certificaat.
certificatePolicies			
.PolicyIdentifier		**2.16.528.1.1007.99.214** **2.16.528.1.1007.99.215**	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3.1). Deze OID's verschillen per level 2 CA
.PolicyQualifier.cPS.uri		**https://acceptatie.zorgcsp.nl/cps/uzi-register.html**	Dit attribuut bevat de URL voor het Certificate Practice Statement van het UZI-register (Zie Par. 4.3.3)
cRLDistributionPoints. distributionPoint. fullName		**http://www.uzi-register-test.nl/cdp/test_zorg_csp_level_2_services_ca_g3.crl**	URI van CRL distribution point van Level 2 CA. Zie. Par. 4.4.

PROFIEL TEST UZI-register Medewerker niet op naam CA G3			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
extKeyUsage		Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4) Document Signing (1.3.6.1.4.1.311.10.3.12) Encrypting File System (1.3.6.1.4.1.311.10.3.4) OCSP Signing (1.3.6.1.5.5.7.3.9)	
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint		0	Hieronder kunnen geen CA's meer gecreëerd worden.
keyUsage	TRUE	Certificate Signing, Off-line CRL Signing, CRL Signing	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11	Algoritme waarmee de handtekening onder het certificaat is gezet: sha256WithRSAEncryption
signatureValue		Handtekening door CSP CA (ASN.1 DER)	

Tabel 24 Profiel TEST UZI-register Medewerker niet op naam CA G3

7.3.4 TEST UZI-register Private Server CA G1

PROFIEL TEST UZI-register Private Server CA G1			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd door CA	Een door de CA gegenereerd uniek certificaatnummer.
signature		1.2.840.113549.1.1.11	OID van het algoritme waarmee handtekening onder het certificaat is gezet: sha256WithRSAEncryption
issuer.commonName (CN)		**TEST Zorg CSP Level 2 Private Services CA G1**	UTF8String
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.countryName (C)		**NL**	PrintableString
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**12 november 2028** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Gelijk aan productie hiërarchie.
subject.commonName (CN)		**TEST UZI-register Private Server CA G1**	UTF8String
subject.organizationIdentifier		**NTRNL-50000535**	UTF8String
subject.organization Name (O)		**CIBG**	UTF8String
subject.countryName (C)		**NL**	PrintableString
subjectPublicKeyInfo. algorithm		1.2.840.113549.1.1.1	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden. In dit geval het RSA algoritme (rsaEncryption).
SubjectPublicKeyInfo. subjectPublic.Key		4096 bits publieke RSA sleutel	Dit attribuut bevat de publieke sleutel.
Standard Extension			
authorityInfoAccess			
authorityInfoAccess. accessMethod		1.3.6.1.5.5.7.48.2 (Certification Authority Issuer)	In G3 heeft Logius een extensie toegevoegd die een verwijzing bevat naar het CA certificaat waaronder het certificaat is uitgegeven.
.accessLocation		**http://www.uzi-register-test.nl/cacerts/test_zorg_csp_level_2_private_services_ca_g1.cer**	HTTP URI naar DER encoded Level 2 CA certificaat. Zie par. 2.2
subjectKeyIdentifier		SHA-1 hash van subject public key	-
authorityKeyIdentifier. KeyIdentifier		SHA-1 hash van issuer public key.	sha-1 hash van authority key (=publieke sleutel van de Level 2 CA) voor validatie dit CA certificaat.
certificatePolicies			
.PolicyIdentifier		**2.16.528.1.1007.99.12** **2.16.528.1.1007.98.4**	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3.1). Deze OID's verschillen per level 2 CA
.PolicyQualifier.cPS.uri		**https://acceptatie.zorgcsp.nl/cps/uzi-register.html**	Dit attribuut bevat de URL voor het Certificate Practice Statement van het UZI-register (Zie Par. 4.3.3)
cRLDistributionPoints. distributionPoint. fullName		**http://www.uzi-register-test.nl/cdp/test_zorg_csp_level_2_private_services_ca_g1.crl**	URI van CRL distribution point van Level 2 CA. Zie. Par. 4.4.
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint		0	Hieronder kunnen geen CA's meer gecreëerd worden.

PROFIEL TEST UZI-register Private Server CA G1			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
keyUsage	TRUE	Certificate Signing, Off-line CRL Signing, CRL Signing	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11	Algoritme waarmee de handtekening onder het certificaat is gezet: sha256WithRSAEncryption
signatureValue		Handtekening door CSP CA (ASN.1 DER)	

Tabel 25 Profiel TEST UZI-register Private Server CA G1

7.3.5 TEST ZOVAR Private Server CA G1

PROFIEL TEST ZOVAR Private Server CA G1			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd door CA	Een door de CA gegenereerd uniek certificaatnummer.
signature		1.2.840.113549.1.1.11	OID van het algoritme waarmee handtekening onder het certificaat is gezet: sha256WithRSAEncryption
issuer.commonName (CN)		**TEST Zorg CSP Level 2 Private Services CA G1**	UTF8String
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.countryName (C)		**NL**	PrintableString
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**12 november 2028** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Gelijk aan productie hiërarchie.
subject.commonName (CN)		**TEST ZOVAR Private Server CA G1**	UTF8String
subject.organizationIdentifier		**NTRNL-50000535**	UTF8String
subject.organization Name (O)		**CIBG**	UTF8String
subject.countryName (C)		**NL**	PrintableString
subjectPublicKeyInfo. algorithm		1.2.840.113549.1.1.1	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden. In dit geval het RSA algoritme (rsaEncryption).
SubjectPublicKeyInfo. subjectPublic.Key		4096 bits publieke RSA sleutel	Dit attribuut bevat de publieke sleutel.
Standard Extension			
authorityInfoAccess			
.accessMethod		1.3.6.1.5.5.7.48.2 (Certification Authority Issuer)	In G3 heeft Logius een extensie toegevoegd die een verwijzing bevat naar het CA certificaat waaronder het certificaat is uitgegeven.
.accessLocation		**http://www.uzi-register-test.nl/cacerts/test_zorg_csp_level_2_private_services_ca_g1.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 2.2
subjectKeyIdentifier		SHA-1 hash van subject public key	-
authorityKeyIdentifier. KeyIdentifier		SHA-1 hash van issuer public key.	sha-1 hash van authority key (=publieke sleutel van de CSP CA) voor validatie van dit CA certificaat.
certificatePolicies			
.PolicyIdentifier		**2.16.528.1.1007.99.12** **2.16.528.1.1007.98.4**	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3.1). Deze OID's verschillen per level 2 CA
.PolicyQualifier.cPS.uri		**https://acceptatie.zorgcsp.nl/cps/zovar.html**	Dit attribuut bevat de URL voor het Certificate Practice Statement van het UZI-register (Zie Par. 4.3.3)
cRLDistributionPoints. distributionPoint. fullName		**http://www.uzi-register-test.nl/cdp/test_zorg_csp_level_2_private_services_ca_g1.crl**	URI van CRL distribution point van Level 2 CA. Zie. Par. 4.4.
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint		0	Hieronder kunnen geen CA's meer gecreëerd worden.
keyUsage	TRUE	Certificate Signing, Off-line CRL Signing, CRL Signing	

PROFIEL TEST ZOVAR Private Server CA G1			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11	Algoritme waarmee de handtekening onder het certificaat is gezet: sha256WithRSAEncryption
signatureValue		Handtekening door CSP CA (ASN.1 DER)	

Tabel 26 Profiel TEST ZOVAR Private Server CA G1