CIBG
Ministerie van Volksgezondheid, Welzijn en Sport

Naamgevingsdocument

ACCEPTATIEOMGEVING Zorg CSP G4

Versie : 1.7 Definitief

Datum : 5 november 2026
Bestandsnaam : 20261105 Naamgevingsdocument Acceptatieomgeving CIBG Zorg CSP G4 v1_7.docx

Inhoudsopgave

1 Inleiding 4
1.1 Doelstelling 4
1.2 Terminologie 4
1.3 Versie historie 4
2 CA model acceptatieomgeving Zorg CSP G4 6
2.1 Naamgeving acceptatieomgeving 6
2.2 URL's van CA certificaten in acceptatieomgeving 7
2.3 Controle juistheid van CA certificaten in acceptatieomgeving (fingerprints) 8
3 Pasmodel acceptatieomgeving Zorg CSP G4 10
3.1 Portfolio testpassen en -certificaten 10
4 Algemene keuzes certificaatprofielen acceptatieomgeving Zorg CSP G4 11
4.1 UZI-nummer en abonneenummer 11
4.2 subject.serialNumber in ZOVAR Servercertificaat 11
4.3 Waarden van certificatePolicies extensie 11
4.4 Waarden cRLDistributionPoints.distributionPoint.fullName 14
5 Profiel gebruikertestcertificaten acceptatieomgeving Zorg CSP G4 16
5.1 Issuer 16
5.2 ETSI QC statements 16
5.3 AuthorityInfoAccess 16
5.4 certificatePolicies.PolicyIdentifier 16
5.5 certificatePolicies.PolicyQualifier.cPS.uri 16
5.6 certificatePolicies.PolicyQualifier.userNotice.explicitText 16
5.7 CRL distribution Point 17
5.8 SubjectAltName.otherName 17
6 CRL profielen acceptatieomgeving Zorg CSP G4 18
6.1 CRL profiel van ACCEPTATIE Zorg CSP G4 Root CA's 18
6.2 CRL profiel van ACCEPTATIE Zorg CSP G4 Intermediate CA's 19
6.3 CRL profiel van ACCEPTATIE G4 CA's voor eindgebruikercertificaten 19
6.4 CRL publicatieschema en publicatiefrequentie acceptatieomgeving 20
7 OCSP acceptatieomgeving Zorg CSP G4 21
8 Profielen CA certificaten acceptatieomgeving Zorg CSP G4 22
8.1 Profielen ACCEPTATIE Zorg CSP CA's G4 G-Sigs 22
8.2 Profielen ACCEPTATIE Zorg CSP CA's G4 S-CIBG 27
8.3 Profielen ACCEPTATIE Zorg CSP CA's G4 G-TLS 36

Lijst met Tabellen

Tabel 1 Versie historie 5
Tabel 2 URL's van CA certificaten in acceptatieomgeving generatie G4 (G-Sigs) 7
Tabel 3 URL's van CA certificaten in acceptatieomgeving generatie G4 (S-CIBG) 7
Tabel 4 URL's van CA certificaten in acceptatieomgeving generatie G4 (G-TLS) 8
Tabel 5 Fingerprints van CA certificaten in acceptatieomgeving generatie G4 (G-Sigs) 8
Tabel 6 Fingerprints van CA certificaten in acceptatieomgeving generatie G4 (S-CIBG) 9
Tabel 7 Fingerprints van CA certificaten in acceptatieomgeving generatie G4 (G-TLS) 9
Tabel 8 Naamgeving en codering testpassen en -certificaten 10
Tabel 9 Overzicht kenmerken testpassen en test-servercertificaten 10
Tabel 10 Waarden PolicyIdentifier in TSP CA certificaten acceptatieomgeving G4 12
Tabel 11 Waarden PolicyIdentifier voor gebruikertestcertificaten in acceptatieomgeving G4 13
Tabel 12 CRL Distribution points in CA certificaten acceptatieomgeving generatie G4 (G-Sigs) 14
Tabel 13 CRL Distribution points in CA certificaten acceptatieomgeving generatie G4 (S-CIBG) 15
Tabel 14 CRL Distribution points in CA certificaten acceptatieomgeving generatie G4 (G-TLS) 15
Tabel 15 CRL Distribution points in gebruikertestcertificaten generatie G4 15
Tabel 16 AuthorityInfoAccess in gebruikertestcertificaten acceptatieomgeving Zorg CSP G4 16
Tabel 17 <OID CA> in gebruikertestscertificaten 17
Tabel 18 CRL profiel van ACCEPTATIE Zorg CSP G4 Root CA's 18

Tabel 19 CRL profiel van ACCEPTATIE Zorg CSP G4 Intermediate CA's 19
Tabel 20 CRL profiel van ACCEPTATIE G4 CA's voor eindgebruikercertificaten 19
Tabel 21 Waarden CommonName in delegated OCSP signer certificaten 21
Tabel 22 Profiel ACCEPTATIE Zorg CSP - G4 Root G-Sigs - 2024 23
Tabel 23 Profiel ACCEPTATIE Zorg CSP - G4 Intm G-Sigs NP - 2024 24
Tabel 24 Profiel ACCEPTATIE UZI Zorgverlener HND - G4 G-Sigs NP - 2025 25
Tabel 25 Profiel ACCEPTATIE UZI Medw op naam HND - G4 G-Sigs NP - 2025 27
Tabel 26 Profiel ACCEPTATIE Zorg CSP - G4 Root Priv S-CIBG - 2024 28
Tabel 27 Profiel ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG NP - 2024 29
Tabel 28 Profiel ACCEPTATIE UZI Zorgverlener - G4 Priv S-CIBG NP - 2025 31
Tabel 29 Profiel ACCEPTATIE UZI Medw op naam - G4 Priv S-CIBG NP - 2025 33
Tabel 30 Profiel ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG LP - 2024 34
Tabel 31 Profiel ACCEPTATIE UZI Medw niet op naam - G4 Priv S-CIBG LP - 2025 36
Tabel 32 Profiel ACCEPTATIE Zorg CSP - G4 Root Priv G-TLS - 2024 37
Tabel 33 Profiel ACCEPTATIE Zorg CSP - G4 Intm Priv G-TLS SYS - 2024 38
Tabel 34 Profiel ACCEPTATIE UZI Server - G4 Priv G-TLS SYS - 2025 39
Tabel 35 Profiel ACCEPTATIE ZOVAR Server - G4 Priv G-TLS SYS - 2025 41

Lijst met Figuren

Figuur 1: CA model acceptatieomgeving generatie G4 UZI-testpassen 6
Figuur 2: CA model acceptatieomgeving generatie G4 test-servercertificaten 6

Copyright CIBG © te Den Haag
Niets uit deze uitgave mag verveelvoudigd en/of openbaar worden gemaakt (voor willekeurig welke doeleinden) door middel van druk, fotokopie, microfilm, geluidsband, elektronisch of op welke andere wijze dan ook zonder voorafgaande schriftelijke toestemming van CIBG.

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 Terminologie

Deze specificatie betreft de acceptatieomgeving van de Zorg CSP. Desondanks is er sprake van testpassen en test-servercertificaten en bevatten sommige URL's 'test' als naam component. Dit is zo gelaten omdat in de externe communicatie de producten uit deze acceptatieomgeving worden aangeduid als Testmiddelen en testomgeving | Softwareleveranciers | UZI-register (uziregister.nl). In de OTAP(U) systematiek (Ontwikkel, Test, Acceptatie, Productie, Uitwijk) betreft het echter de Acceptatieomgeving van de Zorg CSP.

1.3 Versie historie

Versie	Datum	Status	Omschrijving
0.1	5 november 2024	Work in Progress	Eerste interne review versie voor inrichting Acceptatieomgeving G4.
0.2	7 november 2024	REVIEW	Eerste versie voor externe review.
1.0	14 november 2024	Definitief	Verwerking review commentaar: - update figuur 1: weergave uzi-passen duidelijker - par. 2.2 + profielen: geen aparte map voor g4 CA's - par. 4.4 + profielen: geen aparte map voor de g4 crls - par. 4.3.3 aanpassing cpsURI zodat er geen redirect meer nodig is - par. 6.3 geen wijziging in OCSP link
1.1	25 januari 2025	Definitief	Correcties n.a.v. review KPN: - Tabel 4: CA publicatie ZOVAR van http://www.uzi-register-test.nl/ --> http://www.csp.zovar-test.nl/ - Tabel 15: CDP ZOVAR van http://www.uzi-register-test.nl/ --> http://www.csp.zovar-test.nl/
1.2	13 februari 2025	Definitief	Correcties n.a.v. review KPN: - Tabellen van alle Issuing CA's: pathLengthContraint van none → 0

Versie	Datum	Status	Omschrijving
1.3	30 juni 2025	Review	Aanpassingen n.a.v. re-key TSP CA certificaten in 2025 en PoR 5.3: - hele document: commonName Issuing CA's '2024' --> '2025' - update Fig. 1 en Fig. 2 - Tabel 10, 21 en tabellen van TSP CA's: verwijderd OCSP certificatePolicies - Tabel 21: Update Common Names OCSP signer certificaten conform PKIo naamgeving - Tabellen TSP CA certificaten: toegevoegd organizationIdentifier NTRNL-50000535 - par. 6.2.2 toegevoegd m.b.t. etsi-qcs-SemanticsId-Legal
1.4	28 juli 2025	Definitief	- Hoofdstuk 5 verwijderd (bestond uit verwijzing naar Hoofdstuk 9) - Tabel 24, 25, 28, 29, 31, 34, en 35: correcties link CA issuer, link CDP (2025 --> 2024)
1.5	19 februari 2026	Definitief	- Tabel 11, verwijdering authenticity certificate Policies uit alle authenticiteitcertificaten van UZI-passen. - Update status fig. 1 en 2 naar definitief
1.6	23 april 2026	Definitief	- Tabel 5, 6, 7: fingerprints CA certificaten opgenomen - Par. 6.3.1: implementatie datum expiredCertsOnCRL opgenomen
1.7	5 november 2026	Definitief	- Tabel 21 CommonName OCSP responder certificaten uniek per instance

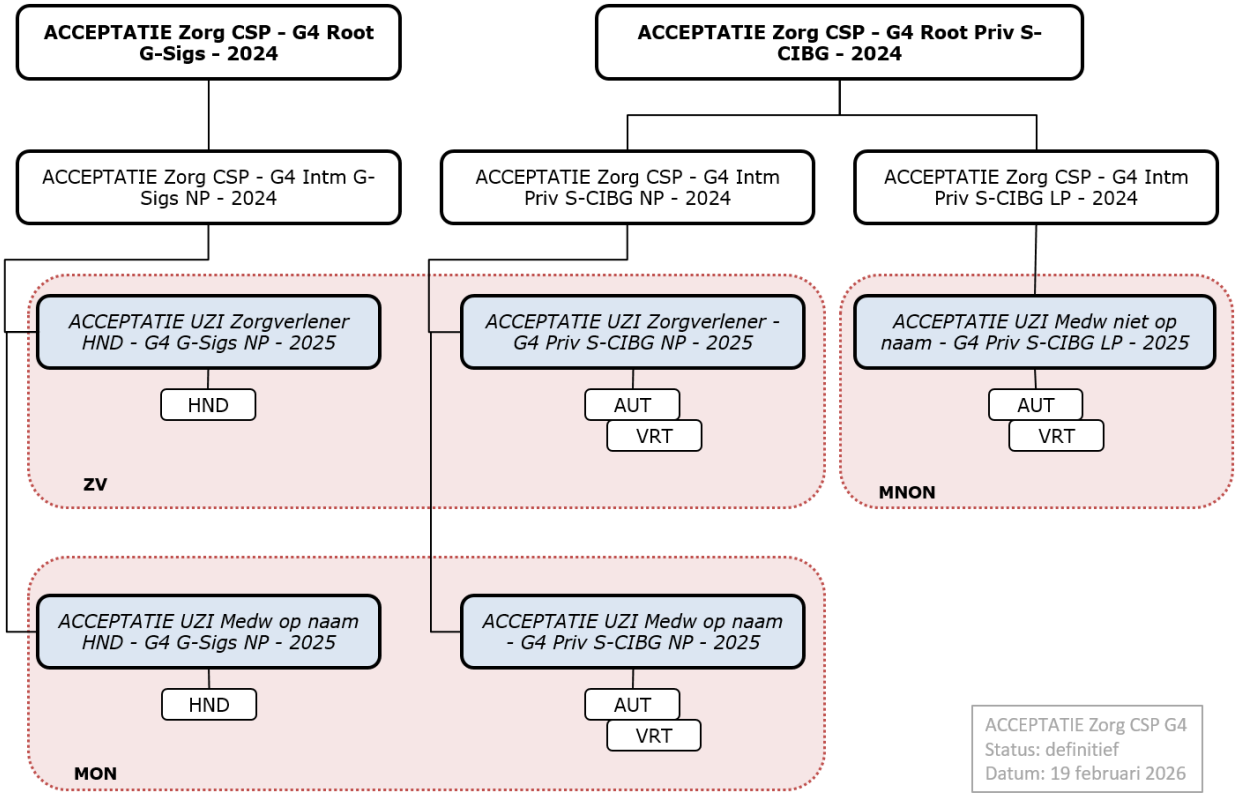
Tabel 1 Versie historie

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

2 CA model acceptatieomgeving Zorg CSP G4

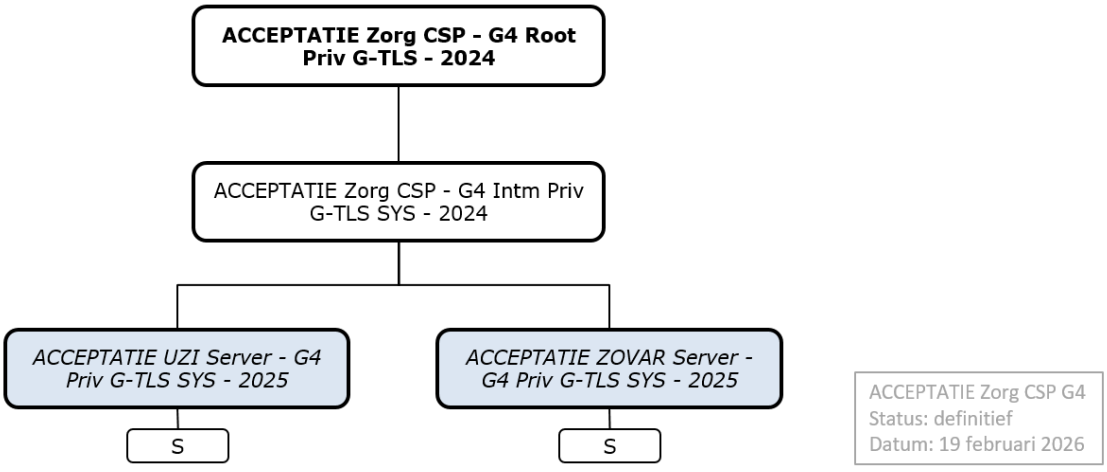
2.1 Naamgeving acceptatieomgeving

Onderstaande figuur geeft het CA model weer voor de G4 generatie van de acceptatieomgeving van de Zorg CSP voor UZI-testpassen. De naamgeving (subject.CommonName in de betreffende CA certificaten) van de CA's is opgenomen in de figuur. De naamgeving is Case Sensitive.



Figuur 1: CA model acceptatieomgeving generatie G4 UZI-testpassen

Onderstaande figuur geeft het CA model weer voor de G4 generatie van de acceptatieomgeving van de Zorg CSP voor servercertificaten van UZI-register en ZOVAR.



Figuur 2: CA model acceptatieomgeving generatie G4 test-servercertificaten

De naamgeving van de Acceptatie CA's is via de volgende systematiek afgeleid van de naamgeving van de G4 productieomgeving:

Voor Root en Intermediate CA's:
```
Staat der Nederlanden --> ACCEPTATIE Zorg CSP
EUTL verwijderd
```

Voor TSP (issuing) CA's:
```
EUTL verwijderd
PKIo verwijderd
UZI --> ACCEPTATIE UZI
ZOVAR --> ACCEPTATIE ZOVAR
```

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
ACCEPTATIE Zorg CSP - G4 Root G-Sigs - 2024	http://www.uzi-register-test.nl/cacerts/acceptatie_zorg_csp-g4_root_g-sigs-2024.cer
ACCEPTATIE Zorg CSP - G4 Intm G-Sigs NP - 2024	http://www.uzi-register-test.nl/cacerts/acceptatie_zorg_csp-g4_intm_g-sigs_np-2024.cer
ACCEPTATIE UZI Zorgverlener HND - G4 G-Sigs NP - 2025	http://www.uzi-register-test.nl/cacerts/acceptatie_uzi_zorgverlener_hnd-g4_g-sigs_np-2025.cer
ACCEPTATIE UZI Medw op naam HND - G4 G-Sigs NP - 2025	http://www.uzi-register-test.nl/cacerts/acceptatie_uzi_medw_op_naam_hnd-g4_g-sigs_np-2025.cer

Tabel 2 URL's van CA certificaten in acceptatieomgeving generatie G4 (G-Sigs)

Naam CA	URL van CA certificaat
ACCEPTATIE Zorg CSP - G4 Root Priv S-CIBG - 2024	http://www.uzi-register-test.nl/cacerts/acceptatie_zorg_csp-g4_root_priv_s-cibg-2024.cer
ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG NP - 2024	http://www.uzi-register-test.nl/cacerts/acceptatie_zorg_csp-g4_intm_priv_s-cibg_np-2024.cer
ACCEPTATIE UZI Zorgverlener - G4 Priv S-CIBG NP - 2025	http://www.uzi-register-test.nl/cacerts/acceptatie_uzi_zorgverlener-g4_priv_s-cibg_np-2025.cer
ACCEPTATIE UZI Medw op naam - G4 Priv S-CIBG NP - 2025	http://www.uzi-register-test.nl/cacerts/acceptatie_uzi_medw_op_naam-g4_priv_s-cibg_np-2025.cer
ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG LP - 2024	http://www.uzi-register-test.nl/cacerts/acceptatie_zorg_csp-g4_intm_priv_s-cibg_lp-2024.cer
ACCEPTATIE UZI Medw niet op naam - G4 Priv S-CIBG LP - 2025	http://www.uzi-register-test.nl/cacerts/acceptatie_uzi_medw_niet_op_naam-g4_priv_s-cibg_lp-2025.cer

Tabel 3 URL's van CA certificaten in acceptatieomgeving generatie G4 (S-CIBG)

Naam CA	URL van CA certificaat
ACCEPTATIE Zorg CSP - G4 Root Priv G-TLS - 2024	http://www.uzi-register-test.nl/cacerts/acceptatie_zorg_csp-g4_root_priv_g-tls-2024.cer
ACCEPTATIE Zorg CSP - G4 Intm Priv G-TLS SYS - 2024	http://www.uzi-register-test.nl/cacerts/acceptatie_zorg_csp-g4_intm_priv_g-tls_sys-2024.cer
ACCEPTATIE UZI Server - G4 Priv G-TLS SYS - 2025	http://www.uzi-register-test.nl/cacerts/acceptatie_uzi_server-g4_priv_g-tls_sys-2025.cer
ACCEPTATIE ZOVAR Server - G4 Priv G-TLS SYS - 2025	http://www.csp.zovar-test.nl/cacerts/acceptatie_zovar_server-g4_priv_g-tls_sys-2025.cer

Tabel 4 URL's van CA certificaten in acceptatieomgeving generatie G4 (G-TLS)

2.3 Controle juistheid van CA certificaten in acceptatieomgeving (fingerprints)

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'.

De fingerprints zijn ook met de volgende openssl commando's te berekenen:

```
openssl x509 -in cert.pem -fingerprint -sha1
openssl x509 -in cert.pem -fingerprint -sha256
```

In de volgende tabellen zijn zowel de SHA-1 als SHA256 fingerprints van de CA certificaten opgenomen

Naam CA	Fingerprint CA certificaat
ACCEPTATIE Zorg CSP - G4 Root G-Sigs - 2024	124C1363E1A2B9852DF8EFF638BFEA5DCC53F459 FCE09CCABFA2C9114C40B033125A4972D20441C44CEAD71032835A26A20E5270
ACCEPTATIE Zorg CSP - G4 Intm G-Sigs NP - 2024	D7BB747249F17DF34F01D8988174BE8DA7BDEB4D 90CE6191ADD9CD80B531F940DD75C99F4F485EAFF9A59B76FE5D5338F58B660A
ACCEPTATIE UZI Zorgverlener HND - G4 G-Sigs NP - 2025	AC7F6D96D6F4321C99E0306D0E24B3A393267272 1484678E99DA2751A24435797443EECB269F406E32BD81136EC83D1BAA3D0D7C
ACCEPTATIE UZI Medw op naam HND - G4 G-Sigs NP - 2025	6E3FF52656DFD7BED3AE6015230332EAA28C71B9 1CA0DEB36D73ADC2BB3B48F1C14B5BA476B8726B872DD8909A7D7151DABF1383

Tabel 5 Fingerprints van CA certificaten in acceptatieomgeving generatie G4 (G-Sigs)

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

Naam CA	Fingerprint CA certificaat
ACCEPTATIE Zorg CSP - G4 Root Priv S-CIBG - 2024	F39946B2ABAC0446E067C7461DFB2F700A17EE09 203F2E29478BA12D54EE8508402ABFDDAA4891C8A68C973398EC484C0F11E613
ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG NP - 2024	7205F6E330D2EB44559AAE7A58B3880F3378E9D7 CC05B908E8D4232DB5730CDA5335F50A0EB34E447F587F010938B5FA53DB4F31
ACCEPTATIE UZI Zorgverlener - G4 Priv S-CIBG NP - 2025	3487685744F8AEBA458B9CA05A847DECAC9CB8E9 95B858975C7CF2364DE146A90723110D61053E21ABFBF608679E3492CCBEE10D
ACCEPTATIE UZI Medw op naam - G4 Priv S-CIBG NP - 2025	826215644CDB43841FF9901A670E0F3E25C0A02C 4A17BEB854D813B3CE6E454D8DA4047B961BC4B876909425CEA0A3842C912AD8
ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG LP - 2024	BBD5AB5AC4FEB926BDB7BE0BA640424731EE5FDB C8CC0C66B8A2A917B2B3392E4A772A9EEC9741B8C0594FE6F7C7634F2FE44DEE
ACCEPTATIE UZI Medw niet op naam - G4 Priv S-CIBG LP - 2025	A1568CD74F1843BBD599613D44BC04BF05C43A1E 12BB78FAC834CBACBE6AE7D54152F24792F7963631F3D0B9B9586FE4A29EAB7D

Tabel 6 Fingerprints van CA certificaten in acceptatieomgeving generatie G4 (S-CIBG)

Naam CA	Fingerprint CA certificaat
ACCEPTATIE Zorg CSP - G4 Root Priv G-TLS - 2024	AFD2C2BE45115DE984FF581252EDA925F3FEB594 EB99A72624EC7D1B633F8A84E6E3C9093A3F01F5F5EB0D6F6C7F378975A860DC
ACCEPTATIE Zorg CSP - G4 Intm Priv G-TLS SYS - 2024	B1893B26365187C92C28361DA574E0EE97F6D277 D32599709F041A835912C89BEEFBA2C474EEB5769F14280B523C8579C4C54C75
ACCEPTATIE UZI Server - G4 Priv G-TLS SYS - 2025	9DA8FCC902210F0934382DD6D351D7F0F20C8775 B2F2B3371852D3B57574A91E91639957477A028EFFAAF8EA5DE816077D988D91
ACCEPTATIE ZOVAR Server - G4 Priv G-TLS SYS - 2025	ACAD9D6F0BEA16BC8EE3F27435A8E6A539985AAB 66E884141882FAA937A37CDFB6CAC5D881A9215F0A401558EE8E095EB98F8348

Tabel 7 Fingerprints van CA certificaten in acceptatieomgeving generatie G4 (G-TLS)

3 Pasmodel acceptatieomgeving Zorg CSP G4

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 8 Naamgeving en codering testpassen en -certificaten

De volgende tabel geeft een overzicht van de specifieke kenmerken van de verschillende testpastypen. In de beschrijving van de diverse processen wordt hiernaar verwezen.

Producttype ---------- Eigenschappen	Zorgverlener-testpas	Medewerker-testpas op naam	Medewerkertestpas niet op naam	UZI-register test Servercertificaat	ZOVAR test Servercertificaat
Certificaten	AUT,VRT,HND	AUT,VRT,HND	AUT,VRT	Gecombineerd AUT,VRT	Gecombineerd AUT,VRT
Drager	smartcard	smartcard	smartcard	divers	divers
CA Common Name issuing CA	ACCEPTATIE UZI Zorgverlener HND - G4 G-Sigs NP - 2025 ACCEPTATIE UZI Zorgverlener - G4 Priv S-CIBG NP - 2025	ACCEPTATIE UZI Medw op naam HND - G4 G-Sigs NP - 2025 ACCEPTATIE UZI Medw op naam - G4 Priv S-CIBG NP - 2025	ACCEPTATIE UZI Medw niet op naam - G4 Priv S-CIBG LP - 2025	ACCEPTATIE UZI Server - G4 Priv G-TLS SYS - 2025	ACCEPTATIE ZOVAR Server - G4 Priv G-TLS SYS - 2025

Tabel 9 Overzicht kenmerken testpassen en test-servercertificaten

4 Algemene keuzes certificaatprofielen acceptatieomgeving Zorg CSP G4

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

Root CA certificaten
In de Root CA certificaten zijn geen policyIdentifiers opgenomen.

Intermediate CA certificaten
Zie Hoofdstuk 8 voor de policyIdentifiers die zijn opgenomen in de Intermediate CA certificaten.

TSP CA certificaten generatie G4
De volgende tabel specificeert de policyIdentifiers die zijn opgenomen in de TSP CA certificaten in Acceptatie.

Deze policyIdentifiers zijn via de volgende systematiek gebaseerd op de productie omgeving:

PKIo certificatePolicies
Omschrijving: `PKIo G4 --> Uzi-test g4cp`
OID: `2.16.528.1.1003.1.2. --> 2.16.528.1.1007.99.`

ETSI certificatePolicies
Omschrijving: `ETSI --> Uzi-test`
OID direct onder uzi-test OID: `2.16.528.1.1007.99.`

CommonName TSP CA	policyIdentifiers
ACCEPTATIE UZI Zorgverlener HND - G4 G-Sigs NP - 2025 ACCEPTATIE UZI Medw op naam HND - G4 G-Sigs NP - 2025	Uzi-test ncpplus (2.16.528.1.1007.99.204212) Uzi-test qcp-n-qscd (2.16.528.1.1007.99.194112) Uzi-test g4cp Sigs Gen NP Individual Validated eSig (2.16.528.1.1007.99.44.14.11.5) Uzi-test g4cp Sigs Gen NP Reg. Prof. Validated eSig (2.16.528.1.1007.99.44.14.12.5) Uzi-test g4cp Sigs Gen NP Sponsor Validated eSig (2.16.528.1.1007.99.44.14.13.5) Uzi-test g4cp Sigs Gen NP Reg. Prof. w/Sponsor Val. eSig (2.16.528.1.1007.99.44.14.14.5)
ACCEPTATIE UZI Zorgverlener - G4 Priv S-CIBG NP - 2025 ACCEPTATIE UZI Medw op naam - G4 Priv S-CIBG NP - 2025	Uzi-test ncp (2.16.528.1.1007.99.204211) Uzi-test ncpplus (2.16.528.1.1007.99.204212) Uzi-test g4cp Priv CIBG NP Individual Validated Authenticity (2.16.528.1.1007.99.44.46.11.4) Uzi-test g4cp Priv CIBG NP Individual Validated Confidentiality (2.16.528.1.1007.99.44.46.11.7) Uzi-test g4cp Priv CIBG NP Individual Validated Authentication (2.16.528.1.1007.99.44.46.11.8) Uzi-test g4cp Priv CIBG NP Reg. Prof. Validated Authenticity (2.16.528.1.1007.99.44.46.12.4) Uzi-test g4cp Priv CIBG NP Reg. Prof. Validated Confidentiality (2.16.528.1.1007.99.44.46.12.7) Uzi-test g4cp Priv CIBG NP Reg. Prof. Validated Authentication (2.16.528.1.1007.99.44.46.12.8) Uzi-test g4cp Priv CIBG NP Sponsor Validated Authenticity (2.16.528.1.1007.99.44.46.13.4) Uzi-test g4cp Priv CIBG NP Sponsor Validated Confidentiality (2.16.528.1.1007.99.44.46.13.7) Uzi-test g4cp Priv CIBG NP Sponsor Validated Authentication (2.16.528.1.1007.99.44.46.13.8) Uzi-test g4cp Priv CIBG NP Reg. Prof. w/Sponsor Val. Authenticity (2.16.528.1.1007.99.44.46.14.4) Uzi-test g4cp Priv CIBG NP Reg. Prof. w/Sponsor Val. Confidentiality (2.16.528.1.1007.99.44.46.14.7) Uzi-test g4cp Priv CIBG NP Reg. Prof. w/Sponsor Val. Authentication (2.16.528.1.1007.99.44.46.14.8)
ACCEPTATIE UZI Medw niet op naam - G4 Priv S-CIBG LP - 2025	Uzi-test ncp (2.16.528.1.1007.99.204211) Uzi-test ncpplus (2.16.528.1.1007.99.204212) Uzi-test g4cp Priv CIBG LP Org. Validated Authenticity (2.16.528.1.1007.99.44.46.25.4) Uzi-test g4cp Priv CIBG LP Org. Validated Confidentiality (2.16.528.1.1007.99.44.46.25.7) Uzi-test g4cp Priv CIBG LP Org. Validated Authentication (2.16.528.1.1007.99.44.46.25.8)
ACCEPTATIE UZI Server - G4 Priv G-TLS SYS - 2025 ACCEPTATIE ZOVAR Server - G4 Priv G-TLS SYS - 2025	Uzi-test ncp (2.16.528.1.1007.99.204211) Uzi-test ncpplus (2.16.528.1.1007.99.204212) Uzi-test g4cp Priv TLS Gen Sys Organization Validated Server (2.16.528.1.1007.99.44.15.35.11)

Tabel 10 Waarden PolicyIdentifier in TSP CA certificaten acceptatieomgeving G4

Gebruikertestcertificaten

Tabel 11 geeft een overzicht PolicyIdentifiers (OID's) van de verschillende pas-/certificaattypen. Deze zijn onder de G4 verder gedifferentieerd en geven beveiligingsfunctie aan (authenticatie/authentication/vertrouwelijkheid/handtekening), type certificaathouder (natuurlijk persoon, organisatie), garantie erkend beroep (Regulated Profession) en Organisatie validatie (Sponsor validated).

Naam product	PolicyIdentifiers per certificaat type
Zorgverlenertestpas	*AUT certificaat in ZV (Uzi-test g4cp Priv CIBG NP)* Uzi-test ncpplus (2.16.528.1.1007.99.204212) Reg. Prof. Validated Authentication (2.16.528.1.1007.99.44.46.12.8) Reg. Prof. w/Sponsor Val. Authentication (2.16.528.1.1007.99.44.46.14.8) *HND certificaat in ZV (Uzi-test g4cp Sigs Gen NP)* Uzi-test ncpplus (2.16.528.1.1007.99.204212) Regulated Profession Validated eSig. (2.16.528.1.1007.99.44.14.12.5) Regulated Prof. w/Sponsor Val. eSig. (2.16.528.1.1007.99.44.14.14.5) Uzi-test qcp-n-qscd (2.16.528.1.1007.99.194112) *VRT certificaat in ZV (Uzi-test g4cp Priv CIBG NP)* Uzi-test ncpplus (2.16.528.1.1007.99.204212) Reg. Prof. Validated Confidentiality (2.16.528.1.1007.99.44.46.12.7) Reg. Prof. w/Sponsor Val. Confidentiality (2.16.528.1.1007.99.44.46.14.7)
Medewerkertestpas op naam	*AUT certificaat in MON (Uzi-test g4cp Priv CIBG NP)* Uzi-test ncpplus (2.16.528.1.1007.99.204212) Individual Validated Authentication (2.16.528.1.1007.99.44.46.11.8) Sponsor Validated Authentication (2.16.528.1.1007.99.44.46.13.8) *HND certificaat in MON (Uzi-test g4cp Sigs Gen NP)* Uzi-test ncpplus (2.16.528.1.1007.99.204212) Individual Validated eSignature (2.16.528.1.1007.99.44.14.11.5) Sponsor Validated eSignature (2.16.528.1.1007.99.44.14.13.5) Uzi-test qcp-n-qscd (2.16.528.1.1007.99.194112) *VRT certificaat in MON (Uzi-test g4cp Priv CIBG NP)* Uzi-test ncpplus (2.16.528.1.1007.99.204212) Individual Validated Confidentiality (2.16.528.1.1007.99.44.46.11.7) Sponsor Validated Confidentiality (2.16.528.1.1007.99.44.46.13.7)
Medewerkertest-pas niet op naam	*AUT in MNON (Uzi-test g4cp Priv CIBG LP)* Uzi-test ncpplus (2.16.528.1.1007.99.204212) Organization Validated Authentication (2.16.528.1.1007.99.44.46.25.8) *VRT in MNON (Uzi-test g4cp Priv CIBG NP)* Uzi-test ncpplus (2.16.528.1.1007.99.204212) Organization Validated Confidentiality: (OID: 2.16.528.1.1007.99.44.46.25.7)
UZI-register Server-testcertificaat **ZOVAR Server-testcertificaat**	Uzi-test ncp (2.16.528.1.1007.99.204211) Uzi-test g4cp Priv TLS Gen Sys Organization Validated Server (2.16.528.1.1007.99.44.15.35.11)

Tabel 11 Waarden PolicyIdentifier voor gebruikertestcertificaten in acceptatieomgeving G4

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

CA-certificaten acceptatieomgeving

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. CIBG 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. CIBG is in geen geval aansprakelijk voor eventuele schade.

4.3.3 certificatePolicies.PolicyQualifier.cPS.uri

CA-certificaten acceptatieomgeving
In de CA Certificaten van de G4 generatie is geen cPS.uri opgenomen.

Gebruikertestcertificaten UZI-register en ZOVAR generatie
In alle gebruikercertificaten is bij de generatie G4 de volgende certificatePolicies.PolicyQualifier.cPS.uri opgenomen in de acceptatieomgeving:
https://acceptatie.zorgcsp.nl/certification-practice-statement-cps

4.4 Waarden cRLDistributionPoints.distributionPoint.fullName

4.4.1 CDP in CA certificaten acceptatieomgeving Zorg CSP

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

Naam CA	Waarde CRL Distribution Point in certificaat
ACCEPTATIE Zorg CSP - G4 Root G-Sigs - 2024	GEEN ATTRIBUUT CRL DISTRIBUTION POINT
ACCEPTATIE Zorg CSP - G4 Intm G-Sigs NP - 2024	http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_root_g-sigs-2024.crl
ACCEPTATIE UZI Zorgverlener HND - G4 G-Sigs NP - 2025 ACCEPTATIE UZI Medw op naam HND - G4 G-Sigs NP - 2025	http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_intm_g-sigs_np-2024.crl

Tabel 12 CRL Distribution points in CA certificaten acceptatieomgeving generatie G4 (G-Sigs)

Naam CA	Waarde CRL Distribution Point in certificaat
ACCEPTATIE Zorg CSP - G4 Root Priv S-CIBG - 2024	GEEN ATTRIBUUT CRL DISTRIBUTION POINT
ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG NP - 2024	http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_root_priv_s-cibg-2024.crl
ACCEPTATIE UZI Zorgverlener - G4 Priv S-CIBG NP - 2025 ACCEPTATIE UZI Medw op naam - G4 Priv S-CIBG NP - 2025	http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_intm_priv_s-cibg_np-2024.crl
ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG LP - 2024	http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_root_priv_s-cibg-2024.crl
ACCEPTATIE UZI Medw niet op naam - G4 Priv S-CIBG LP - 2025	http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_intm_priv_s-cibg_lp-2024.crl

Tabel 13 CRL Distribution points in CA certificaten acceptatieomgeving generatie G4 (S-CIBG)

Naam CA	Waarde CRL Distribution Point in certificaat
ACCEPTATIE Zorg CSP - G4 Root Priv G-TLS - 2024	GEEN ATTRIBUUT CRL DISTRIBUTION POINT
ACCEPTATIE Zorg CSP - G4 Intm Priv G-TLS SYS - 2024	http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_root_priv_g-tls-2024.crl
ACCEPTATIE UZI Server - G4 Priv G-TLS SYS - 2025 ACCEPTATIE ZOVAR Server - G4 Priv G-TLS SYS - 2025	http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_intm_priv_g-tls_sys-2024.crl

Tabel 14 CRL Distribution points in CA certificaten acceptatieomgeving generatie G4 (G-TLS)

4.4.2 CDP in Gebruikertestcertificaten acceptatieomgeving

Bij de gebruikertestcertificaten verschilt het CDP per pas-/certificaattype afhankelijk van de CA die het certificaat uitgeeft. De volgende tabellen geven een overzicht van de CDP's per pas-/certificaattype in de acceptatieomgeving.

Naam UZI-pastype (certificaat)	CRL Distribution Point
Zorgverlenertestpas (AUT, VRT)	http://www.uzi-register-test.nl/cdp/acceptatie_uzi_zorgverlener-g4_priv_s-cibg_np-2025.crl
Zorgverlenertestpas (HND)	http://www.uzi-register-test.nl/cdp/acceptatie_uzi_zorgverlener_hnd-g4_g-sigs_np-2025.crl
Medewerkertestpas op naam (AUT, VRT)	http://www.uzi-register-test.nl/cdp/acceptatie_uzi_medw_op_naam-g4_priv_s-cibg_np-2025.crl
Medewerkertestpas op naam (HND)	http://www.uzi-register-test.nl/cdp/acceptatie_uzi_medw_op_naam_hnd-g4_g-sigs_np-2025.crl
Medewerkertestpas niet op naam (AUT, VRT)	http://www.uzi-register-test.nl/cdp/acceptatie_uzi_medw_niet_op_naam-g4_priv_s-cibg_lp-2025.crl
UZI-register Servertestcertificaat	http://www.uzi-register-test.nl/cdp/acceptatie_uzi_server-g4_priv_g-tls_sys-2025.crl
ZOVAR Servertestcertificaat	http://www.csp.zovar-test.nl/cdp/acceptatie_zovar_server-g4_priv_g-tls_sys-2025.crl

Tabel 15 CRL Distribution points in gebruikertestcertificaten generatie G4

5 Profiel gebruikertestcertificaten acceptatieomgeving Zorg CSP G4

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 Figuur 1 en 2.

5.2 ETSI QC statements

5.2.1 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.

5.2.2 TSP CA Certificaten en Medewerker niet op Naam certificaten

Het qcStatement dat aangeeft welke syntax en semantiek de subject.organizationidentifier heeft (0.4.0.194121.1.2, qcsSemanticsIdLegal) ontbreekt in alle TSP CA certificaten en Medewerker niet op Naam certificaten in de Acceptatie omgeving.

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 16 AuthorityInfoAccess in gebruikertestcertificaten acceptatieomgeving Zorg CSP G4

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. CIBG gebruikt deze OID's als een identifier van de CA ongeacht de specifieke generatie of variant (EUTL of S-CIBG).

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 17 <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 acceptatieomgeving Zorg CSP G4

6.1 CRL profiel van ACCEPTATIE Zorg CSP G4 Root CA's

Dit is een CRL die in de productieomgeving wordt uitgegeven door PKIoverheid 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 Intermediate CA certificaat is ingetrokken.

CRL profiel van ACCEPTATIE Zorg CSP G4 Root CA's			
CRL veld	**Critical**	**Waarde**	**Omschrijving / Toelichting**
TBSCertList			
version		1	CRL version 2
signature		1.2.840.113549.1.1.10	De waarde is de OID die het algoritme specificeert van de handtekening over de CRL: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
Issuer.country (C)		NL	
Issuer. organizationName (O)		CIBG	
Issuer. commonName (CN)		*Afhankelijk van domein G4 generatie:* • ACCEPTATIE Zorg CSP - G4 Root G-Sigs - 2024 • ACCEPTATIE Zorg CSP - G4 Root Priv S-CIBG - 2024 • ACCEPTATIE Zorg CSP - G4 Root Priv G-TLS - 2024	
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.
CertificateList			
signatureAlgorithm		1.2.840.113549.1.1.10	De waarde is de OID die het algoritme specificeert van de handtekening over de CRL: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue		Handtekening van CA over het tbsCertificateList.	

Tabel 18 CRL profiel van ACCEPTATIE Zorg CSP G4 Root CA's

6.2 CRL profiel van ACCEPTATIE Zorg CSP G4 Intermediate CA's

Dit is een CRL die in de productieomgeving wordt uitgegeven door PKIoverheid. Op deze CRL komen alleen entries voor als er een TSP CA certificaat is ingetrokken. In het onderstaande profiel zijn alleen de afwijkingen ten opzichte van het CRL profiel van de ACCEPTATIE Zorg CSP Root CA's weergegeven.

CRL profiel van ACCEPTATIE Zorg CSP G4 Intermediate CA's		
CRL veld	**Critical**	**Waarde**
Velden		
Issuer.commonName (CN)		*Afhankelijk van domein G4 generatie:* • ACCEPTATIE Zorg CSP - G4 Intm G-Sigs NP - 2024 • ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG NP - 2024 • ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG LP - 2024 • ACCEPTATIE Zorg CSP - G4 Intm Priv G-TLS SYS - 2024

Tabel 19 CRL profiel van ACCEPTATIE Zorg CSP G4 Intermediate CA's

6.3 CRL profiel van ACCEPTATIE G4 CA's voor eindgebruikercertificaten

In de onderstaande tabel zijn alleen de afwijkingen ten opzichte van het CRL profiel van de ACCEPTATIE Zorg CSP Root CA's weergegeven. Het betreft hier de TSP CA's die testcertificaten uitgeven voor eindgebruikers.

CRL profiel van ACCEPTATIE G4 CA's eindgebruikercertificaten		
CRL veld	**Waarde**	**Omschrijving / Toelichting**
Velden		
issuer.CN	ACCEPTATIE UZI Zorgverlener HND - G4 G-Sigs NP - 2025	CRL met ingetrokken Zorgverlener testcertificaten (HND).
issuer.CN	ACCEPTATIE UZI Zorgverlener - G4 Priv S-CIBG NP - 2025	CRL met ingetrokken Zorgverlener testcertificaten (AUT, VRT).
issuer.CN	ACCEPTATIE UZI Medw op naam HND - G4 G-Sigs NP - 2025	CRL met ingetrokken Medewerker op naam testcertificaten (HND).
issuer.CN	ACCEPTATIE UZI Medw op naam - G4 Priv S-CIBG NP - 2025	CRL met ingetrokken Medewerker op naam testcertificaten (AUT, VRT).
issuer.CN	ACCEPTATIE UZI Medw niet op naam - G4 Priv S-CIBG LP - 2025	CRL met ingetrokken Medewerker niet op naam testcertificaten.
issuer.CN	ACCEPTATIE UZI Server - G4 Priv G-TLS SYS - 2025	CRL met de ingetrokken UZI-register Servertestcertificaten.
issuer.CN	ACCEPTATIE ZOVAR Server - G4 Priv G-TLS SYS - 2025	CRL met de ingetrokken ZOVAR Servertestcertificaten.

Tabel 20 CRL profiel van ACCEPTATIE G4 CA's voor eindgebruikercertificaten

6.3.1 ExpiredCertsOnCRL

De CRL's van CA's voor eindgebruikertestcertificaten bevatten additoneel op het generieke CRL profiel de ExpiredCertsOnCRL extensie:

CRL veld	Critical	Waarde	Omschrijving / Toelichting
crlExtensies			
ExpiredCertsOnCRL	FALSE	OID 2 5 29 60	Ingetrokken certificaten blijven op CRL ook na verlopen geldigheidsduur.
date		2026-04-12 18:42:23 UTC	Datum van implementatie (kolom waarde is indicatief). Het effect zal zijn dat alle ingetrokken eindgebruiker-certificaten op de CRL zullen blijven staan.

6.4 CRL publicatieschema en publicatiefrequentie acceptatieomgeving

Het CRL publicatieschema en de publicatiefrequentie van de CRL's die de TSP CA's ondertekenen, zijn in de acceptatieomgeving identiek aan de productieomgeving.

Het CRL publicatieschema en de publicatiefrequentie van CRL's die de Root CA's en Intermediate CA's ondertekenen is gelijk aan de TSP CA's. Dit wijkt af van de PKIoverheid productieomgeving waar deze CRL's 1 jaar geldig zijn aangezien deze CA's in productieomgeving off-line zijn.

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

7 OCSP acceptatieomgeving Zorg CSP G4

OCSP is in de acceptatieomgeving identiek ingericht als in productie

- Alle OCSP communicatie voor gebruikertestcertificaten van UZI-register verloopt via **`http://ocsp.uzi-register-test.nl`**
- Alle OCSP communicatie voor gebruikertestcertificaten ZOVAR verloopt via **`http://ocsp.zovar-test.nl`**

De volgende tabel specificeert de CommonNames in de verschillende OCPS signer certificaten.

CommonName CA	CommonName delegated OCSP signer certificaat
ACCEPTATIE UZI Zorgverlener HND - G4 G-Sigs NP - 2025	ACCEPTATIE UZI Zorgverlener HND - G4 G-Sigs N-OCSP - 2025-n
ACCEPTATIE UZI Medw op naam HND - G4 G-Sigs NP - 2025	ACCEPTATIE UZI Medw op naam HND - G4 G-Sigs N-OCSP - 2025-n
ACCEPTATIE UZI Zorgverlener - G4 Priv S-CIBG NP - 2025	ACCEPTATIE UZI Zorgverlener - G4 Priv S-CIBG N-OCSP - 2025-n
ACCEPTATIE UZI Medw op naam - G4 Priv S-CIBG NP - 2025	ACCEPTATIE UZI Medw op naam - G4 Priv S-CIBG N-OCSP - 2025-n
ACCEPTATIE UZI Medw niet op naam - G4 Priv S-CIBG LP - 2025	ACCEPTATIE UZI Medw niet op naam - G4 Priv S-CIBG L-OCSP - 2025-n
ACCEPTATIE UZI Server - G4 Priv G-TLS SYS - 2025	ACCEPTATIE UZI Server - G4 Priv G-TLS S-OCSP - 2025-n
ACCEPTATIE ZOVAR Server - G4 Priv G-TLS SYS - 2025	ACCEPTATIE ZOVAR Server - G4 Priv G-TLS S-OCSP - 2025-n

Tabel 21 Waarden CommonName in delegated OCSP signer certificaten

Toelichting: de CommonNames zijn uniek per instance van de OCSP responder. De ‘n’ aan het einde van de CommonName bevat een nummer dat de instance aanduidt. Bijvoorbeeld: *ACCEPTATIE UZI Zorgverlener HND - G4 G-Sigs N-OCSP - 2025-1*

8 Profielen CA certificaten acceptatieomgeving Zorg CSP G4

Dit hoofdstuk bevat de profielen/naming documents voor alle CA certificaten in de acceptatieomgeving. Deze zijn volledig 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.

LET OP: de volgorde van de subject attributen dient gelijk te zijn aan de tabellen in dit hoofdstuk. Dus eerst Country, dan OrganizationName en vervolgens commonName.

8.1 Profielen ACCEPTATIE Zorg CSP CA's G4 G-Sigs

8.1.1 ACCEPTATIE Zorg CSP - G4 Root G-Sigs - 2024

ACCEPTATIE Zorg CSP - G4 Root G-Sigs - 2024			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd CA	Uniek certificaatnummer.
signature		1.2.840.113549.1.1.10	OID van het algoritme waarmee handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
issuer.countryName (C)		**NL**	PrintableString
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Root G-Sigs - 2024**	UTF8String
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**20 mei 2039** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Gelijk aan G4 productie Root CA's
subject.countryName (C)		**NL**	PrintableString
subject.organizationName (O)		**CIBG**	UTF8String
subject.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Root G-Sigs - 2024**	UTF8String
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			
authorityKeyIdentifier		SHA-1 hash van issuer public key	Bij Root CA gelijk aan subjectKeyIdentifier
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	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	Algoritme waarmee de handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512

ACCEPTATIE Zorg CSP - G4 Root G-Sigs - 2024			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue		Selfsigned handtekening (ASN.1 DER)	

Tabel 22 Profiel ACCEPTATIE Zorg CSP - G4 Root G-Sigs - 2024

8.1.2 ACCEPTATIE Zorg CSP - G4 Intm G-Sigs NP - 2024

ACCEPTATIE Zorg CSP - G4 Intm G-Sigs NP - 2024			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd CA	Uniek certificaatnummer.
signature		1.2.840.113549.1.1.10	OID van het algoritme waarmee handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
issuer.countryName (C)		**NL**	PrintableString
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Root G-Sigs - 2024**	UTF8String
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**19 mei 2039** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Geldigheid Root CA - 1 dag.
subject.countryName (C)		**NL**	PrintableString
subject.organizationName (O)		**CIBG**	UTF8String
subject.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Intm G-Sigs NP - 2024**	UTF8String
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			
authorityKeyIdentifier		SHA-1 hash van issuer public key	sha-1 hash publieke sleutel van de Root CA
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/acceptatie_zorg_csp-g4_root_g-sigs-2024.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 2.2

ACCEPTATIE Zorg CSP - G4 Intm G-Sigs NP - 2024			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
certificatePolicies			
.PolicyIdentifier		2.16.528.1.1007.99.204212 2.16.528.1.1007.99.194112 2.16.528.1.1007.99.44.14.18.10 2.16.528.1.1007.99.44.14.19.10 2.16.528.1.1007.99.44.14.11.5 2.16.528.1.1007.99.44.14.12.5 2.16.528.1.1007.99.44.14.13.5 2.16.528.1.1007.99.44.14.14.5	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3).
extKeyUsage		id-kp-documentSigning (OID 1.3.6.1.5.5.7.3.36) szOID_KP_DOCUMENT_SIGNING (OID 1.3.6.1.4.1.311.10.3.12)	documentSigning: bruikbaar voor ondertekening documenten. Zowel Microsoft OID als pkix OID zie RFC 9336.
CRLDistributionPoints. distributionPoint.fullName		**http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_root_g-sigs-2024.crl**	Dit attribuut bevat de URL van de Certificate Revocation List (CRL) voor dit certificaat. Als het certificaat is ingetrokken (revoked) dan staat het serienummer op deze CRL. Zie par. 4.4
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	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	Algoritme waarmee de handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue		Handtekening (ASN.1 DER)	

Tabel 23 Profiel ACCEPTATIE Zorg CSP - G4 Intm G-Sigs NP - 2024

8.1.3 ACCEPTATIE UZI Zorgverlener HND - G4 G-Sigs NP - 2025

ACCEPTATIE UZI Zorgverlener HND - G4 G-Sigs NP - 2025			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd CA	Uniek certificaatnummer.
signature		1.2.840.113549.1.1.10	OID van het algoritme waarmee handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
issuer.countryName (C)		**NL**	PrintableString
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Intm G-Sigs NP - 2024**	UTF8String
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**18 mei 2039** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is.

ACCEPTATIE UZI Zorgverlener HND - G4 G-Sigs NP - 2025			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
			Geldigheid Intermediate CA - 1 dag.
subject.countryName (C)		**NL**	PrintableString
subject.organizationName (O)		**CIBG**	UTF8String
subject.commonName (CN)		**ACCEPTATIE UZI Zorgverlener HND - G4 G-Sigs NP - 2025**	UTF8String
subject.organizationIdentifier		**NTRNL-50000535**	UTF8String
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			
authorityKeyIdentifier		SHA-1 hash van issuer public key	sha-1 hash publieke sleutel van de Root CA
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/acceptatie_zorg_csp-g4_intm_g-sigs_np-2024.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 2.2
certificatePolicies			
.PolicyIdentifier		2.16.528.1.1007.99.204212 2.16.528.1.1007.99.194112 2.16.528.1.1007.99.44.14.11.5 2.16.528.1.1007.99.44.14.12.5 2.16.528.1.1007.99.44.14.13.5 2.16.528.1.1007.99.44.14.14.5	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3).
extKeyUsage		id-kp-documentSigning (OID 1.3.6.1.5.5.7.3.36) szOID_KP_DOCUMENT_SIGNING (OID 1.3.6.1.4.1.311.10.3.12)	documentSigning: bruikbaar voor ondertekening documenten. Zowel Microsoft OID als pkix OID zie RFC 9336.
CRLDistributionPoints. distributionPoint.fullName		**http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_intm_g-sigs_np-2024.crl**	URL van de (CRL) voor dit certificaat. Als het certificaat is ingetrokken (revoked) dan staat het serienummer op deze CRL. Zie par. 4.4
subjectKeyIdentifier		SHA-1 hash van subject public key	
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint			0
keyUsage	TRUE	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	Algoritme waarmee de handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue		Handtekening (ASN.1 DER)	

Tabel 24 Profiel ACCEPTATIE UZI Zorgverlener HND - G4 G-Sigs NP - 2025

8.1.4 ACCEPTATIE UZI Medw op naam HND - G4 G-Sigs NP - 2025

ACCEPTATIE UZI Medw op naam HND - G4 G-Sigs NP - 2025			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd CA	Uniek certificaatnummer.
signature		1.2.840.113549.1.1.10	OID van het algoritme waarmee handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
issuer.countryName (C)		**NL**	PrintableString
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Intm G-Sigs NP - 2024**	UTF8String
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**18 mei 2039** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Geldigheid Intermediate CA - 1 dag.
subject.countryName (C)		**NL**	PrintableString
subject.organizationName (O)		**CIBG**	UTF8String
subject.commonName (CN)		**ACCEPTATIE UZI Medw op naam HND - G4 G-Sigs NP - 2025**	UTF8String
subject.organizationIdentifier		**NTRNL-50000535**	UTF8String
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			
authorityKeyIdentifier		SHA-1 hash van issuer public key	sha-1 hash publieke sleutel van de Root CA
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/acceptatie_zorg_csp-g4_intm_g-sigs_np-2024.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 2.2
certificatePolicies			
.PolicyIdentifier		2.16.528.1.1007.99.204212 2.16.528.1.1007.99.194112 2.16.528.1.1007.99.44.14.11.5 2.16.528.1.1007.99.44.14.12.5 2.16.528.1.1007.99.44.14.13.5 2.16.528.1.1007.99.44.14.14.5	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3).
extKeyUsage		id-kp-documentSigning (OID 1.3.6.1.5.5.7.3.36) szOID_KP_DOCUMENT_SIGNING (OID 1.3.6.1.4.1.311.10.3.12)	documentSigning: bruikbaar voor ondertekening documenten. Zowel Microsoft OID als pkix OID zie RFC 9336.
CRLDistributionPoints. distributionPoint.fullName		**http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_intm_g-sigs_np-2024.crl**	Dit attribuut bevat de URL van de Certificate Revocation List (CRL) voor dit certificaat. Als het certificaat is ingetrokken (revoked) dan staat het serienummer op deze CRL. Zie par. 4.4

ACCEPTATIE UZI Medw op naam HND - G4 G-Sigs NP - 2025			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
subjectKeyIdentifier		SHA-1 hash van subject public key	
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint			0
keyUsage	TRUE	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	Algoritme waarmee de handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue		Handtekening (ASN.1 DER)	

Tabel 25 Profiel ACCEPTATIE UZI Medw op naam HND - G4 G-Sigs NP - 2025

8.2 Profielen ACCEPTATIE Zorg CSP CA's G4 S-CIBG

8.2.1 ACCEPTATIE Zorg CSP - G4 Root Priv S-CIBG - 2024

ACCEPTATIE Zorg CSP - G4 Root Priv S-CIBG - 2024			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd CA	Uniek certificaatnummer.
signature		1.2.840.113549.1.1.10	OID van het algoritme waarmee handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
issuer.countryName (C)		**NL**	PrintableString
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Root Priv S-CIBG - 2024**	UTF8String
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**20 mei 2039** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Gelijk aan G4 productie Root CA's
subject.countryName (C)		**NL**	PrintableString
subject.organizationName (O)		**CIBG**	UTF8String
subject.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Root Priv S-CIBG - 2024**	UTF8String
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			
authorityKeyIdentifier		SHA-1 hash van issuer public key	Bij Root CA gelijk aan subjectKeyIdentifier
subjectKeyIdentifier		SHA-1 hash van subject public key	-

ACCEPTATIE Zorg CSP - G4 Root Priv S-CIBG - 2024			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint			Geen beperking (none)
keyUsage	TRUE	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	Algoritme waarmee de handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue		Selfsigned handtekening (ASN.1 DER)	

Tabel 26 Profiel ACCEPTATIE Zorg CSP - G4 Root Priv S-CIBG - 2024

8.2.2 ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG NP - 2024

ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG NP - 2024			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd CA	Uniek certificaatnummer.
signature		1.2.840.113549.1.1.10	OID van het algoritme waarmee handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
issuer.countryName (C)		**NL**	PrintableString
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Root Priv S-CIBG - 2024**	UTF8String
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**19 mei 2039** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Geldigheid Root CA - 1 dag.
subject.countryName (C)		**NL**	PrintableString
subject.organizationName (O)		**CIBG**	UTF8String
subject.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG NP - 2024**	UTF8String
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			
authorityKeyIdentifier		SHA-1 hash van issuer public key	sha-1 hash publieke sleutel van de Root CA
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.

ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG NP - 2024			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
.accessLocation		**http://www.uzi-register-test.nl/cacerts/acceptatie_zorg_csp-g4_root_priv_s-cibg-2024.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 2.2
certificatePolicies			
.PolicyIdentifier		2.16.528.1.1007.99.204211 2.16.528.1.1007.99.204212 2.16.528.1.1007.99.44.46.11.4 2.16.528.1.1007.99.44.46.11.7 2.16.528.1.1007.99.44.46.11.8 2.16.528.1.1007.99.44.46.18.10 2.16.528.1.1007.99.44.46.19.10 2.16.528.1.1007.99.44.46.12.4 2.16.528.1.1007.99.44.46.12.7 2.16.528.1.1007.99.44.46.12.8 2.16.528.1.1007.99.44.46.13.4 2.16.528.1.1007.99.44.46.13.7 2.16.528.1.1007.99.44.46.13.8 2.16.528.1.1007.99.44.46.14.4 2.16.528.1.1007.99.44.46.14.7 2.16.528.1.1007.99.44.46.14.8	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3).
extKeyUsage		id-kp-documentSigning (OID 1.3.6.1.5.5.7.3.36) Clientauthenticatie (1.3.6.1.5.5.7.3.2) szOID_KP_DOCUMENT_SIGNING (OID 1.3.6.1.4.1.311.10.3.12) Encrypting File System (1.3.6.1.4.1.311.10.3.4)	documentSigning: bruikbaar voor ondertekening documenten. Zowel Microsoft OID als pkix OID zie RFC 9336. clientAuthenticatie: certificaat bruikbaar voor client authenticatie Encrypting File System
CRLDistributionPoints. distributionPoint.fullName		**http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_root_priv_s-cibg-2024.crl**	Dit attribuut bevat de URL van de Certificate Revocation List (CRL) voor dit certificaat. Als het certificaat is ingetrokken (revoked) dan staat het serienummer op deze CRL. Zie par. 4.4
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	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	Algoritme waarmee de handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue		Handtekening (ASN.1 DER)	

Tabel 27 Profiel ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG NP - 2024

8.2.3 ACCEPTATIE UZI Zorgverlener - G4 Priv S-CIBG NP - 2025

ACCEPTATIE UZI Zorgverlener - G4 Priv S-CIBG NP - 2025			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd CA	Uniek certificaatnummer.
signature		1.2.840.113549.1.1.10	OID van het algoritme waarmee handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
issuer.countryName (C)		**NL**	PrintableString
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG NP - 2024**	UTF8String
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**18 mei 2039** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Geldigheid Intermediate CA - 1 dag.
subject.countryName (C)		**NL**	PrintableString
subject.organizationName (O)		**CIBG**	UTF8String
subject.commonName (CN)		**ACCEPTATIE UZI Zorgverlener - G4 Priv S-CIBG NP - 2025**	UTF8String
subject.organizationIdentifier		**NTRNL-50000535**	UTF8String
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			
authorityKeyIdentifier		SHA-1 hash van issuer public key	sha-1 hash publieke sleutel van de Root CA
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/acceptatie_zorg_csp-g4_intm_priv_s-cibg_np-2024.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 2.2
certificatePolicies			
.PolicyIdentifier		2.16.528.1.1007.99.204211 2.16.528.1.1007.99.204212 2.16.528.1.1007.99.44.46.11.4 2.16.528.1.1007.99.44.46.11.7 2.16.528.1.1007.99.44.46.11.8 2.16.528.1.1007.99.44.46.12.4 2.16.528.1.1007.99.44.46.12.7 2.16.528.1.1007.99.44.46.12.8 2.16.528.1.1007.99.44.46.13.4 2.16.528.1.1007.99.44.46.13.7 2.16.528.1.1007.99.44.46.13.8 2.16.528.1.1007.99.44.46.14.4 2.16.528.1.1007.99.44.46.14.7 2.16.528.1.1007.99.44.46.14.8	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3).

ACCEPTATIE UZI Zorgverlener - G4 Priv S-CIBG NP - 2025			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
extKeyUsage		id-kp-documentSigning (OID 1.3.6.1.5.5.7.3.36) szOID_KP_DOCUMENT_SIGNING (OID 1.3.6.1.4.1.311.10.3.12) Clientauthentication (1.3.6.1.5.5.7.3.2) Encrypting File System (1.3.6.1.4.1.311.10.3.4)	documentSigning: bruikbaar voor ondertekening documenten. Zowel Microsoft OID als pkix OID zie RFC 9336.
CRLDistributionPoints. distributionPoint.fullName		**http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_intm_priv_s-cibg_np-2024.crl**	Dit attribuut bevat de URL van de Certificate Revocation List (CRL) voor dit certificaat. Als het certificaat is ingetrokken (revoked) dan staat het serienummer op deze CRL. Zie par. 4.4
subjectKeyIdentifier		SHA-1 hash van subject public key	
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint			0
keyUsage	TRUE	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	Algoritme waarmee de handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue		Handtekening (ASN.1 DER)	

Tabel 28 Profiel ACCEPTATIE UZI Zorgverlener - G4 Priv S-CIBG NP - 2025

8.2.4 ACCEPTATIE UZI Medw op naam - G4 Priv S-CIBG NP - 2025

ACCEPTATIE UZI Medw op naam - G4 Priv S-CIBG NP - 2025			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd CA	Uniek certificaatnummer.
signature		1.2.840.113549.1.1.10	OID van het algoritme waarmee handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
issuer.countryName (C)		**NL**	PrintableString
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG NP - 2024**	UTF8String
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**18 mei 2039** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Geldigheid Intermediate CA - 1 dag.
subject.countryName (C)		**NL**	PrintableString
subject.organizationName (O)		**CIBG**	UTF8String

ACCEPTATIE UZI Medw op naam - G4 Priv S-CIBG NP - 2025			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
subject.commonName (CN)		**ACCEPTATIE UZI Medw op naam - G4 Priv S-CIBG NP - 2025**	UTF8String
subject.organizationIdentifier		**NTRNL-50000535**	UTF8String
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			
authorityKeyIdentifier		SHA-1 hash van issuer public key	sha-1 hash publieke sleutel van de Root CA
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/acceptatie_zorg_csp-g4_intm_priv_s-cibg_np-2024.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 2.2
certificatePolicies			
.PolicyIdentifier		2.16.528.1.1007.99.204211 2.16.528.1.1007.99.204212 2.16.528.1.1007.99.44.46.11.4 2.16.528.1.1007.99.44.46.11.7 2.16.528.1.1007.99.44.46.11.8 2.16.528.1.1007.99.44.46.12.4 2.16.528.1.1007.99.44.46.12.7 2.16.528.1.1007.99.44.46.12.8 2.16.528.1.1007.99.44.46.13.4 2.16.528.1.1007.99.44.46.13.7 2.16.528.1.1007.99.44.46.13.8 2.16.528.1.1007.99.44.46.14.4 2.16.528.1.1007.99.44.46.14.7 2.16.528.1.1007.99.44.46.14.8	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3).
extKeyUsage		id-kp-documentSigning (OID 1.3.6.1.5.5.7.3.36) szOID_KP_DOCUMENT_SIGNING (OID 1.3.6.1.4.1.311.10.3.12) Clientauthentication (1.3.6.1.5.5.7.3.2) Encrypting File System (1.3.6.1.4.1.311.10.3.4)	documentSigning: bruikbaar voor ondertekening documenten. Zowel Microsoft OID als pkix OID zie RFC 9336.
CRLDistributionPoints. distributionPoint.fullName		**http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_intm_priv_s-cibg_np-2024.crl**	Dit attribuut bevat de URL van de Certificate Revocation List (CRL) voor dit certificaat. Als het certificaat is ingetrokken (revoked) dan staat het serienummer op deze CRL. Zie par. 4.4
subjectKeyIdentifier		SHA-1 hash van subject public key	
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint			0
keyUsage	TRUE	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	Algoritme waarmee de handtekening onder het certificaat is gezet: RSASSA-PSS

ACCEPTATIE UZI Medw op naam - G4 Priv S-CIBG NP - 2025			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue		Handtekening (ASN.1 DER)	

Tabel 29 Profiel ACCEPTATIE UZI Medw op naam - G4 Priv S-CIBG NP - 2025

8.2.5 ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG LP - 2024

ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG LP - 2024			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd CA	Uniek certificaatnummer.
signature		1.2.840.113549.1.1.10	OID van het algoritme waarmee handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
issuer.countryName (C)		**NL**	PrintableString
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Root Priv S-CIBG - 2024**	UTF8String
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**19 mei 2039** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Geldigheid Root CA - 1 dag.
subject.countryName (C)		**NL**	PrintableString
subject.organizationName (O)		**CIBG**	UTF8String
subject.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG LP - 2024**	UTF8String
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			
authorityKeyIdentifier		SHA-1 hash van issuer public key	sha-1 hash publieke sleutel van de Root CA
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/acceptatie_zorg_csp-g4_root_priv_s-cibg-2024.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 2.2

ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG LP - 2024			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
certificatePolicies			
.PolicyIdentifier		2.16.528.1.1007.99.204211 2.16.528.1.1007.99.204212 2.16.528.1.1007.99.44.46.28.10 2.16.528.1.1007.99.44.46.29.10 2.16.528.1.1007.99.44.46.25.4 2.16.528.1.1007.99.44.46.25.7 2.16.528.1.1007.99.44.46.25.8	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3).
extKeyUsage		id-kp-documentSigning (OID 1.3.6.1.5.5.7.3.36) Clientauthenticatie (1.3.6.1.5.5.7.3.2) szOID_KP_DOCUMENT_SIGNING (OID 1.3.6.1.4.1.311.10.3.12) Encrypting File System (1.3.6.1.4.1.311.10.3.4)	documentSigning: bruikbaar voor ondertekening documenten. Zowel Microsoft OID als pkix OID zie RFC 9336. clientAuthenticatie: certificaat bruikbaar voor client authenticatie Encrypting File System
CRLDistributionPoints. distributionPoint.fullName		**http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_root_priv_s-cibg-2024.crl**	Dit attribuut bevat de URL van de Certificate Revocation List (CRL) voor dit certificaat. Als het certificaat is ingetrokken (revoked) dan staat het serienummer op deze CRL. Zie par. 4.4
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	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	Algoritme waarmee de handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue		Handtekening (ASN.1 DER)	

Tabel 30 Profiel ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG LP - 2024

8.2.6 ACCEPTATIE UZI Medw niet op naam - G4 Priv S-CIBG LP - 2025

ACCEPTATIE UZI Medw niet op naam - G4 Priv S-CIBG LP - 2025			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd CA	Uniek certificaatnummer.
signature		1.2.840.113549.1.1.10	OID van het algoritme waarmee handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
issuer.countryName (C)		**NL**	PrintableString
issuer.organizationName (O)		**CIBG**	UTF8String

ACCEPTATIE UZI Medw niet op naam - G4 Priv S-CIBG LP - 2025			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
issuer.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Intm Priv S-CIBG LP - 2024**	UTF8String
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**18 mei 2039** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Geldigheid Intermediate CA - 1 dag.
subject.countryName (C)		**NL**	PrintableString
subject.organizationName (O)		**CIBG**	UTF8String
subject.commonName (CN)		**ACCEPTATIE UZI Medw niet op naam - G4 Priv S-CIBG LP - 2025**	UTF8String
subject.organizationIdentifier		**NTRNL-50000535**	UTF8String
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			
authorityKeyIdentifier		SHA-1 hash van issuer public key	sha-1 hash publieke sleutel van de Root CA
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/acceptatie_zorg_csp-g4_intm_priv_s-cibg_lp-2024.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 2.2
certificatePolicies			
.PolicyIdentifier		2.16.528.1.1007.99.204211 2.16.528.1.1007.99.204212 2.16.528.1.1007.99.44.46.25.4 2.16.528.1.1007.99.44.46.25.7 2.16.528.1.1007.99.44.46.25.8	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3).
extKeyUsage		id-kp-documentSigning (OID 1.3.6.1.5.5.7.3.36) szOID_KP_DOCUMENT_SIGNING (OID 1.3.6.1.4.1.311.10.3.12) Clientauthentication (1.3.6.1.5.5.7.3.2) Encrypting File System (1.3.6.1.4.1.311.10.3.4)	documentSigning: bruikbaar voor ondertekening documenten. Zowel Microsoft OID als pkix OID zie RFC 9336.
CRLDistributionPoints. distributionPoint.fullName		**http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_intm_priv_s-cibg_lp-2024.crl**	Dit attribuut bevat de URL van de Certificate Revocation List (CRL) voor dit certificaat. Als het certificaat is ingetrokken (revoked) dan staat het serienummer op deze CRL. Zie par. 4.4
subjectKeyIdentifier		SHA-1 hash van subject public key	
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint			0
keyUsage	TRUE	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	Algoritme waarmee de handtekening onder het certificaat is gezet: RSASSA-PSS

ACCEPTATIE UZI Medw niet op naam - G4 Priv S-CIBG LP - 2025			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue		Handtekening (ASN.1 DER)	

Tabel 31 Profiel ACCEPTATIE UZI Medw niet op naam - G4 Priv S-CIBG LP - 2025

8.3 Profielen ACCEPTATIE Zorg CSP CA's G4 G-TLS

8.3.1 ACCEPTATIE Zorg CSP - G4 Root Priv G-TLS - 2024

ACCEPTATIE Zorg CSP - G4 Root Priv G-TLS - 2024			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd CA	Uniek certificaatnummer.
signature		1.2.840.113549.1.1.10	OID van het algoritme waarmee handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
issuer.countryName (C)		**NL**	PrintableString
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Root Priv G-TLS - 2024**	UTF8String
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**20 mei 2039** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Gelijk aan G4 productie Root CA's
subject.countryName (C)		**NL**	PrintableString
subject.organizationName (O)		**CIBG**	UTF8String
subject.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Root Priv G-TLS - 2024**	UTF8String
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			
authorityKeyIdentifier		SHA-1 hash van issuer public key	Bij Root CA gelijk aan subjectKeyIdentifier
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	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	Algoritme waarmee de handtekening onder het certificaat is gezet: RSASSA-PSS

ACCEPTATIE Zorg CSP - G4 Root Priv G-TLS - 2024			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue		Selfsigned handtekening (ASN.1 DER)	

Tabel 32 Profiel ACCEPTATIE Zorg CSP - G4 Root Priv G-TLS - 2024

8.3.2 ACCEPTATIE Zorg CSP - G4 Intm Priv G-TLS SYS - 2024

ACCEPTATIE Zorg CSP - G4 Intm Priv G-TLS SYS - 2024			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd CA	Uniek certificaatnummer.
signature		1.2.840.113549.1.1.10	OID van het algoritme waarmee handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
issuer.countryName (C)		**NL**	PrintableString
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Root Priv G-TLS - 2024**	UTF8String
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**19 mei 2039** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Geldigheid Root CA - 1 dag.
subject.countryName (C)		**NL**	PrintableString
subject.organizationName (O)		**CIBG**	UTF8String
subject.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Intm Priv G-TLS SYS - 2024**	UTF8String
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			
authorityKeyIdentifier		SHA-1 hash van issuer public key	sha-1 hash publieke sleutel van de Root CA
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/acceptatie_zorg_csp-g4_root_priv_g-tls-2024.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 2.2
certificatePolicies			
.PolicyIdentifier		2.16.528.1.1007.99.204211 2.16.528.1.1007.99.204212 2.16.528.1.1007.99.44.15.38.10 2.16.528.1.1007.99.44.15.39.10 2.16.528.1.1007.99.44.15.35.11	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3).

ACCEPTATIE Zorg CSP - G4 Intm Priv G-TLS SYS - 2024			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
extKeyUsage		ClientAuthenticatie (1.3.6.1.5.5.7.3.2) ServerAuthenticatie (1.3.6.1.5.5.7.3.1)	KeyPurposId's id-kp-clientAuth en id-kp-serverAuth
CRLDistributionPoints. distributionPoint.fullName		**http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_root_priv_g-tls-2024.crl**	Dit attribuut bevat de URL van de Certificate Revocation List (CRL) voor dit certificaat. Als het certificaat is ingetrokken (revoked) dan staat het serienummer op deze CRL. Zie par. 4.4
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	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	Algoritme waarmee de handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue		Handtekening (ASN.1 DER)	

Tabel 33 Profiel ACCEPTATIE Zorg CSP - G4 Intm Priv G-TLS SYS - 2024

8.3.3 ACCEPTATIE UZI Server - G4 Priv G-TLS SYS - 2025

ACCEPTATIE UZI Server - G4 Priv G-TLS SYS - 2025			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd CA	Uniek certificaatnummer.
signature		1.2.840.113549.1.1.10	OID van het algoritme waarmee handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
issuer.countryName (C)		**NL**	PrintableString
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Intm Priv G-TLS SYS - 2024**	UTF8String
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**18 mei 2039** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Geldigheid Intermediate CA - 1 dag.
subject.countryName (C)		**NL**	PrintableString
subject.organizationName (O)		**CIBG**	UTF8String
subject.commonName (CN)		**ACCEPTATIE UZI Server - G4 Priv G-TLS SYS - 2025**	UTF8String
subject.organizationIdentifier		**NTRNL-50000535**	UTF8String
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).

ACCEPTATIE UZI Server - G4 Priv G-TLS SYS - 2025			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
SubjectPublicKeyInfo. subjectPublic.Key		4096 bits publieke RSA sleutel	Dit attribuut bevat de publieke sleutel.
Standard Extension			
authorityKeyIdentifier		SHA-1 hash van issuer public key	sha-1 hash publieke sleutel van de Root CA
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/acceptatie_zorg_csp-g4_intm_priv_g-tls_sys-2024.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 2.2
certificatePolicies			
.PolicyIdentifier		2.16.528.1.1007.99.204211 2.16.528.1.1007.99.204212 2.16.528.1.1007.99.44.15.35.11	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3).
extKeyUsage		Clientauthentication (1.3.6.1.5.5.7.3.2) Serverauthenticatie (1.3.6.1.5.5.7.3.1)	
CRLDistributionPoints. distributionPoint.fullName		**http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_intm_priv_g-tls_sys-2024.crl**	Dit attribuut bevat de URL van de Certificate Revocation List (CRL) voor dit certificaat. Als het certificaat is ingetrokken (revoked) dan staat het serienummer op deze CRL. Zie par. 4.4
subjectKeyIdentifier		SHA-1 hash van subject public key	
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint			0
keyUsage	TRUE	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	Algoritme waarmee de handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue		Handtekening (ASN.1 DER)	

Tabel 34 Profiel ACCEPTATIE UZI Server - G4 Priv G-TLS SYS - 2025

8.3.4 ACCEPTATIE ZOVAR Server - G4 Priv G-TLS SYS - 2025

ACCEPTATIE ZOVAR Server - G4 Priv G-TLS SYS - 2025			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate			
version		2	X.509v3
serialNumber		Uniek nummer gegenereerd CA	Uniek certificaatnummer.
signature		1.2.840.113549.1.1.10	OID van het algoritme waarmee handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
issuer.countryName (C)		**NL**	PrintableString
issuer.organizationName (O)		**CIBG**	UTF8String
issuer.commonName (CN)		**ACCEPTATIE Zorg CSP - G4 Intm Priv G-TLS SYS - 2024**	UTF8String
validity.notBefore		UTCTime	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is (key ceremonie).
validity.notAfter		**18 mei 2039** (UTCTime)	Het tijdstip tot wanneer het certificaat geldig is. Geldigheid Intermediate CA - 1 dag.
subject.countryName (C)		**NL**	PrintableString
subject.organizationName (O)		**CIBG**	UTF8String
subject.commonName (CN)		**ACCEPTATIE ZOVAR Server - G4 Priv G-TLS SYS - 2025**	UTF8String
subject.organizationIdentifier		**NTRNL-50000535**	UTF8String
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			
authorityKeyIdentifier		SHA-1 hash van issuer public key	sha-1 hash publieke sleutel van de Root CA
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/acceptatie_zorg_csp-g4_intm_priv_g-tls_sys-2024.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 2.2
certificatePolicies			
.PolicyIdentifier		2.16.528.1.1007.99.204211 2.16.528.1.1007.99.204212 2.16.528.1.1007.99.44.15.35.11	Dit attribuut bevat de OID(s) van de Policy die van toepassing is (Zie par. 4.3).
extKeyUsage		Clientauthentication (1.3.6.1.5.5.7.3.2) Serverauthenticatie (1.3.6.1.5.5.7.3.1)	
CRLDistributionPoints. distributionPoint.fullName		**http://www.uzi-register-test.nl/cdp/acceptatie_zorg_csp-g4_intm_priv_g-tls_sys-2024.crl**	Dit attribuut bevat de URL van de Certificate Revocation List (CRL) voor dit certificaat. Als het certificaat is ingetrokken (revoked) dan staat het serienummer op deze CRL. Zie par. 4.4
subjectKeyIdentifier		SHA-1 hash van subject public key	
BasicConstraints	TRUE		
.CA		TRUE	Geeft aan dat het een CA certificaat betreft.
.pathLenConstraint			0

ACCEPTATIE ZOVAR Server - G4 Priv G-TLS SYS - 2025			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / Toelichting
keyUsage	TRUE	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	Algoritme waarmee de handtekening onder het certificaat is gezet: RSASSA-PSS
hashingAlgorithm		2.16.840.1.101.3.4.2.3	SHA-512
maskAlgorithm		1.2.840.113549.1.1.8	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue		Handtekening (ASN.1 DER)	

Tabel 35 Profiel ACCEPTATIE ZOVAR Server - G4 Priv G-TLS SYS - 2025