CIBG
Ministerie van Volksgezondheid, Welzijn en Sport

CA model, Pasmodel, Certificaat- en CRL-profielen

Zorg CSP (productieomgeving G4)

Versie : 1.1

Datum : 6 december 2024
Status : Definitief
Bestandsnaam : 20241206 CA model pasmodel certificaatprofielen G4 v1_1 definitief.docx

Inhoudsopgave

Lijst met Tabellen

Lijst met Figuren

1 Inleiding

1.1 Doelstelling

Dit document specificeert de volgende zaken:
- CA model (H. 2);
- Pasmodel (H. 3);
- Algemene kenmerken certificaten (H. 4);
- Certificaatprofielen (H. 5 t/m 10);
- CRL profielen (H. 11);
- OCSP (H. 12).

Dit document specificeert de certificaatprofielen van de productieomgeving van de *Zorg CSP* onder de zogenaamde G4 generatie van PKIoverheid. De Zorg CSP omvat:
1. het UZI-register met als doelgroep zorgverleners en zorgaanbieders;
2. ZOVAR met als doelgroep zorgverzekeraars.

In deze specificaties is expliciet gemaakt wanneer bepaalde configuraties voor het UZI-register en ZOVAR van elkaar afwijken.

Voor de acceptatieomgeving -die de zogenaamde testpassen en test-servercertificaten uitgeeft voor ICT leveranciers- is een apart naamgevingdocument beschikbaar.

1.2 Toelichting bij notatiewijze certificaat- en CRL-profielen

In dit document zijn diverse tabellen opgenomen met certificaatprofielen. In deze tabellen zijn de volgende kolommen opgenomen:
- De kolom “Certificaatveld / attribuut” bevat de naam van de certificaatvelden en attributen;
- De kolom “OID” bevat de Object IDentifier of de standaard naamgeving of afkorting voor het veld of attribuut;
- De kolom “Critical” geeft met een “TRUE” aan dat voor een veld de markering critical aan moet staan;
- De kolom “Waarde” geeft aan welke waarde het veld dient te hebben. Indien van toepassing staat hier ook een referentie naar de velden in het Registratiesysteem. Daarbij zijn de definities gebruikt zoals beschreven in het *Gegevensmodel*;
- De kolom “Typering” geeft aan of een veld een vaste waarde of een variabele waarde kent. Met ‘variabel’ wordt aangegeven dat het veld per certificaat een andere inhoud kan krijgen;
- De kolom “Omschrijving / Toelichting” geeft toelichting bij de invulling van de velden.

De basisstructuur van een certificaat bestaat uit een to-be-signed gedeelte (tbsCertificate) en een handtekening van de uitgever. Het tbsCertificate bestaat uit een aantal verplichte basisvelden gevolgd door extensies. Deze structuur is in de tabellen weergegeven door aparte gekleurde rijen.

1.3 Uitgangspunten

Het Certificate Policy/Programme of Requirements PKIoverheid (PoR) is het normatieve kader voor de certificaat- en CRL-profielen. In het PoR zijn de referenties opgenomen naar standaardisatiedocumenten vanuit ISO/ITU (bijv. X.509), IETF in de vorm van RFC’s en ETSI (met name voor het Qualified Certificate Profile).

1.4 Versie historie

De wijziginghistorie van dit document is weergegeven in onderstaande tabel.

Dit document heeft als uitgangspunt *20240828 CA model pasmodel certificaatprofielen v10_5_2.pdf* maar herstart de versienummering. Er blijft een afzonderlijke specificatie voor certificaten onder de G3/G1 omdat de vele afwijkingen tussen G3/G1 en G4 niet goed in één document zijn te combineren.

Versie	Datum	Status	Omschrijving
0.1	25 oktober 2024	WIP (Work in Progress)	Gebaseerd op 20240828 CA model pasmodel certificaatprofielen v10_5_2.pdf De belangrijkste wijzigingen bij migratie naar de G4 PKIoverheid: - differentiatie Root CA's par 2.1 - update cryptografische algoritmen par. 2.1.2 naar RSASSA-PSS met SHA512 en MGF1 - verwijdering par. 4.4 toelichting e-mail adres - verwijdering par. 5.4 OrganizationIdentifier en naamgeving CSP organisatie - toevoeging fingerprints van alle CA's in par. 5.3 - toegevoegd in authenticiteitcertificaten en handtekeningcertificaten EKU id-kp-documentSigning 1.3.6.1.5.5.7.3.36 - G4 PKIoverheid certificate Policies - verwijdering subject.organizationIdentifier in TSP CA certificaten - verwijdering cspURI uit alle CA certificaten - certificaten UZI-passen en OCSP signing certificaten van 2048 --> 4096 bits RSA - ETSI NCP OID of 0.4.0.2042.1.1 toegevoegd in servercertificaten - verwijdering CRLDistributionPoints in OCSP signer certificaten (niet meer toegestaan onder G4) - short-lived OCSP signer certificaten - verwijdering subject.organizationalUnitName voor Medewerkerpassen niet op naam
0.2	31 oktober 2024	REVIEW	Toegevoegd CA issuers + fingerprints productie CA's. Eerste versie voor externe review.
1.0	14 november 2024	Definitief	Verwerking reviewcommentaar: - update figuur 1: weergave uzi-passen duidelijker - par. 2.1.3 toelichting verwijdering CDP in OCSP signer certificaten - Par. 4.1: opmerking verwerkt over volgorde DN attributen - par. 4.5.3 aanpassing cpsURI zodat er geen redirect meer nodig is - par. 4.5.4 aanpassing link naar PDS zodat er geen redirect meer nodig is - par. 4.6.2 geen aparte map voor de g4 crls - tabel 8 wijziging layout conform naamgevingsdocument acceptatie - par. 5.3 werkwijze berekenen fingerprints met openssl toegevoegd - par. 11.3.1 normatieve kader voor verwerken intrekking 4 --> 24 uur - par. 12.5.2 opmerking signature algoritme OCSP responses
1.1	6 december 2024	Definitief	Aanpassingen: - par. 5.3: toegevoegd referentie naar Staatscourant - alle linkjes naar CA certificaten van https gewijzigd naar http in tabellen 15, 16 en 17 en CA Issuers in tabellen met profielen

Tabel 1 Versie historie

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

2 CA model

Dit hoofdstuk specificeert het CA model van de Zorg CSP productieomgeving.

2.1 CA model Zorg CSP G4 generatie

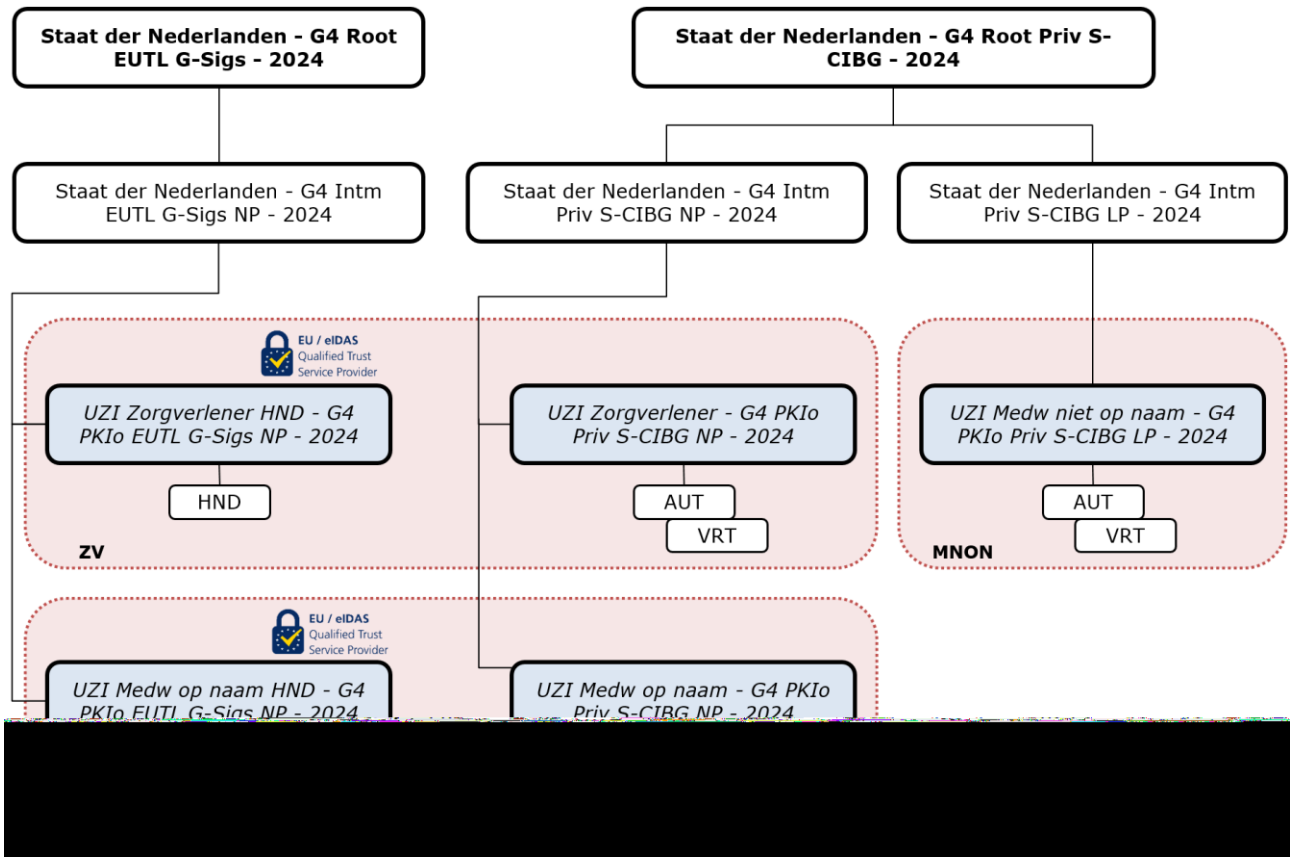
2.1.1 Algemene ontwerpkeuzes

Om overlappende normenkaders en bijbehorende compliance risico's zoveel mogelijk te voorkomen, is bij de PKIoverheid G4 omgeving een differentiatie in Root CA's doorgevoerd. Voor CIBG zijn relevant:

1. specifieke Private Root CA's voor uitgifte van niet gekwalificeerde certificaten binnen diverse branches zoals de zorgsector;
2. een generieke Private Root CA voor servercertificaten;
3. een generieke Private Root CA voor eIDAS gekwalificeerde certificaten.

De volgende figuur toont het CA model voor UZI-passen onder de G4 omgeving van PKIoverheid. De Zorgverlener- en Medewerkerpassen op naam zullen van twee volledig gescheiden Root CA's en CA hiërarchieën zijn voorzien:

- De *Staat der Nederlanden - G4 Root EUTL G-Sigs - 2024* waaronder alleen gekwalificeerde certificaten worden uitgegeven. Voor CIBG zijn dat de handtekening certificaten op de Zorgverlener- en Medewerkerpassen op naam.
  Deze eIDAS Root CA is generiek en ook in gebruik bij andere TSP's.
  Het vertrouwen is bepaald door opname van de TSP CA's (*UZI Zorgverlener HND - G4 PKIo EUTL G-Sigs NP - 2024* en *UZI Medw op naam HND - G4 PKIo EUTL G-Sigs NP - 2024*) op de eIDAS Trusted List (europa.eu).
- De *Staat der Nederlanden - G4 Root Priv S-CIBG - 2024* voor authenticiteit- en vertrouwelijkheidcertificaten. Deze Root CA is specifiek voor CIBG en de Zorgsector.



Figuur 1: CA model passen productieomgeving Zorg CSP generatie G4

SHA512, Secure Hash Algorithm dat resulteert in een 512 bit hash waarde. Zie Federal Information Processing Standard (FIPS) 180-4.

1.2.840.113549.1.1.8 {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) id-mgf1(8)}
Rivest, Shamir and Adleman (RSA) algorithm dat gebruikt maakt van de Mask Generator Function 1 (MGF1). Zie IETF RFC 3447 en RFC 8017.

De G4 hiërarchie gebruikt de volgende **RSA sleutellengten**:

Certificaat	RSA sleutellengte (bits)
Stamcertificaten	4096
Intermediate CA certificaten	4096
TSP CA certificaten	4096
Eindgebruikercertificaat UZI-passen	4096
Servercertificaten	4096
OCSP signer certificaten	4096

Tabel 2 RSA sleutellengtes in G4 generatie

2.1.3 Geldigheidsduur

De volgende tabel geeft een overzicht van de geldigheidsduur van de Public G4 hiërarchie.

Certificaat	Geldig tot
Stamcertificaten	20 mei 2039
Intermediate CA certificaten	19 mei 2039
TSP CA certificaten	18 mei 2039
Eindgebruikercertificaat	3 jaar (Of uiterlijk tot einde geldigheid ondertekenend TSP CA certificaat.)*
OCSP signer certificaten	7 dagen**

Tabel 3 Levensduur certificaten G4 hiërarchie

* bij vernieuwing van een Zorgverlenerpas of Medewerkerpas op naam wordt maximaal 1 maand extra geldigheid toegekend aan de nieuwe pas, om zo de gelegenheid te bieden een pas te vernieuwen zonder in te leveren op de effectieve gebruiksduur.

** onder de G4 is in navolging van de TLS Baseline Requirements van het CA Browser Forum geen CDP meer toegestaan in OCSP signer certificaten. Omdat deze certificaten daardoor niet meer zijn in te trekken, worden short-lived certificaten aanbevolen.

2.2 Toepassingsdomeinen PKI-overheid

Bij de invoering van de G4 zijn de toepassingsdomeinen verder opgesplitst en zijn hiervoor specifieke Root CA's zijn gemaakt. Door het aanmaken van een aparte root voor gekwalificeerde certificaten vallen de domeinen niet altijd samen met een bepaald pastype. De domeinen waarbinnen CIBG certificaten uitgeeft zijn:

- G4 EUTL Signatures Generic Natural Persons
- G4 Private TLS Generic Devices
- G4 Private CIBG Natural Persons
- G4 Private CIBG Legal Persons

Het domein komt in de gebruikerscertificaten tot uitdrukking in de root CA waaronder een certificaat is uitgegeven en de PolicyIdentifier(s) die in een certificaat is/zijn opgenomen. Zie par. 4.5.1.

3 Pasmodel

3.1 Portfolio Zorg CSP

Het portfolio van de Zorg CSP omvat 3 typen UZI-passen, een servercertificaat voor het UZI-register en een servercertificaat voor ZOVAR. De naam en codering van de diverse producttypen zijn hieronder weergegeven. De codering is in het certificaat opgenomen in het subjectAltName.OtherName (zie par. 4.7):

Naam producttypen Zorg CSP	**Codering producttype in subjectAltName.otherName**
Zorgverlenerpas	Z
Medewerkerpas op naam	N
Medewerkerpas niet op naam	M
UZI-register Servercertificaat	S
ZOVAR Servercertificaat	V

Tabel 4 Naamgeving en codering producttypen Zorg CSP

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

Producttype ---------- Eigenschappen	**Zorgverlenerpas**	**Medewerkerpas op naam**	**Medewerkerpas niet op naam**	**UZI-register Servercertificaat**	**ZOVAR Servercertificaat**
Certificaten	AUT, VRT, HND	AUT, VRT, HND	AUT, VRT	Gecombineerd AUT, VRT	Gecombineerd AUT, VRT
Persoonsgebonden	ja	ja	nee	nee	nee
Garantie zorgverlener	ja	nee	nee	nee	n.v.t.
Drager	smartcard	smartcard	smartcard	divers	divers
CA Common Name issuing CA	UZI Zorgverlener HND - G4 PKIo EUTL G-Sigs NP - 2024 UZI Zorgverlener - G4 PKIo Priv S-CIBG NP - 2024	UZI Medw op naam HND - G4 PKIo EUTL G-Sigs NP - 2024 UZI Medw op naam - G4 PKIo Priv S-CIBG NP - 2024	UZI Medw niet op naam - G4 PKIo Priv S-CIBG LP - 2024	UZI Server - G4 PKIo Priv G-TLS SYS - 2024	ZOVAR Server - G4 PKIo Priv G-TLS SYS - 2024
Certificate Policy G4	G4 EUTL Signatures Generic Natural Persons (H) G4 Private CIBG Natural Persons (A,V)		G4 Private CIBG Legal Persons	G4 Private TLS Generic Devices	

Tabel 5 Overzicht kenmerken producten Zorg CSP

Toelichting op de tabel:

Certificaten — Alle passen bevatten sleutelparen en certificaten voor authenticiteit (AUT) en vertrouwelijkheid (VRT). Een deel van de passen bevat sleutelparen en gekwalificeerde certificaten voor elektronische handtekening (HND).
Een Servercertificaat is een zogenaamd servicescertificaat waarin authenticiteit- en vertrouwelijkheid gecombineerd zijn in één certificaat.

Persoonsgebonden	Voor de persoonsgebonden passen wordt bij uitgifte een face-to-face controle en controle identiteitsbewijs uitgevoerd. Voor de niet-persoonsgebonden passen wordt een identiteitsvaststelling van de aanvrager uitgevoerd via een face-to-face controle en controle identiteitsbewijs.
Garantie Zorgverlener	Alleen voor de Zorgverlenerpassen geeft het UZI-register de zogenaamde garantie zorgverlener af. Het UZI-register heeft door toetsing in de door het ministerie van VWS erkende registers (o.a. BIG-register en Kwaliteitsregister Paramedici) vastgesteld dat de beoogde pashouder binnen het UZI-domein als zorgverlener kan worden aangemerkt. Uiteraard is dit n.v.t. voor ZOVAR. Over ZOVAR Servercertificaat geeft ZOVAR de garantie dat de abonnee een zorgverzekeraar is.
Drager	In eerste instantie zullen de passen een smartcard als drager hebben. Alleen Servercertificaten kunnen een andere drager hebben (o.a. Hardware Security Module).

4 Algemene keuzes certificaatprofielen

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

4.1 Codering X.520 attributen van het type DirectoryString

De X.520 attributen van het type DirectoryString (bijv. CN en O) zullen in het subjectDN en issuerDN van CA, en gebruikercertificaten evenals in de CRL's worden gecodeerd als **UTF8String**. Conform RFC5280 zal Country en subject.SerialNumber als PrintableString worden gecodeerd.

Vanaf de G4 dient de volgorde van de subject attributen (onder andere C, O, CN) gelijk te zijn aan de tabellen met de certificaatprofielen.

4.2 Uniek nummer in subject.serialNumber

In het certificaatprofiel van de Zorg CSP wordt het subject.serialNumber gevuld met een uniek nummer. Op die manier wordt gegarandeerd dat de zogenaamde subject Distinguished Name uniek is. De betekenis en de manier waarop dit unieke nummer wordt opgenomen verschilt echter per pas-/certificaattype en is in deze paragraaf gespecificeerd.

4.2.1 UZI-register

Bij het UZI-register wordt in de certificaten het zogenaamde UZI-nummer opgenomen in het subject.serialNumber van alle typen certificaten.

Voor de persoonsgebonden pastypen (i.e. de Zorgverlenerpas en de Medewerkerpas op naam) wordt een uniek nummer gekoppeld aan de natuurlijke persoon: het UZI-nummer. Als één zorgverlener bijvoorbeeld een Zorgverlenerpas aanvraagt voor meerdere abonnees, dan garandeert het UZI-register dat hetzelfde UZI-nummer wordt gebruikt voor alle passen. Bij de eerste registratie van een persoon wordt een nieuw uniek UZI-nummer gegenereerd. De volgende gegevens bepalen of een persoon uniek is: `<voornamen> + <voorvoegsels geboortenaam> + <geboortenaam> + <geboortedatum> + <geboorteplaats>`. Bij aanvragen van nieuwe passen voor dezelfde persoon wordt het reeds bestaande UZI-nummer overgenomen in de nieuwe aanvraag.

Bij de Medewerkerpas niet op naam wordt bij iedere aanvraag/pasuitgifte het Registratiesysteem een nieuw uniek UZI-nummer genereerd. Het UZI-nummer op dit pastype biedt vertrouwende partijen de mogelijkheid om bij de betreffende abonnee na te gaan om welke persoon het gaat. Bij iedere pasaanvraag zal een nieuw UZI-nummer worden gegenereerd omdat het UZI-register geen garantie kan afgeven dat het om dezelfde medewerker gaat. Dit wordt namelijk door de abonnee bijgehouden.

Bij een UZI-register Servercertificaat wordt bij iedere aanvraag / certificaat uitgifte een nieuw UZI-nummer gegenereerd omdat het UZI-register geen garantie af kan geven dat het om hetzelfde systeem gaat.

4.2.2 ZOVAR Servercertificaat

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

Het UZOVI-nummer is een door Vektis toegekend nummer dat een bepaalde zorgverzekeraar uniek identificeert. Het formaat van het UZOVI-nummer is 4NUM.
Aan ZOVAR Servercertificaten wordt -binnen het registratiesysteem van ZOVAR- een uniek nummer gekoppeld op dezelfde wijze zoals een UZI-nummer gekoppeld wordt aan servercertificaten van het UZI-register.

Het unieke ZOVAR-nummer heeft hetzelfde formaat (9NUM) én komt uit dezelfde nummerreeks als het UZI-nummer.

4.2.3 Gescheiden nummerreeks voor productie- en testdoeleinden

Het Registratiesysteem zal voor alle pastypen het unieke nummer genereren uit dezelfde 9 cijferige nummerreeks, startend bij 000010001 en eindigend bij 899999999. De volgende reeksen zijn gereserveerd voor testdoeleinden:

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

4.3 Abonneenummer

4.3.1 Toewijzing en uniciteit

Bij registratie van een abonnee koppelt het registratiesysteem van de Zorg CSP een uniek nummer aan de abonnee. Met uitzondering van de ZOVAR certificaten is dit nummer in de certificaten opgenomen in de subjectAltName.othername. Zie voor details par. 4.7.

Abonneenummers voor UZI-register en ZOVAR komen uit dezelfde nummerreeks.

4.3.2 Formaat en nummerreeks

Het Registratiesysteem genereert voor alle abonnees van de Zorg CSP een abonneenummer uit dezelfde 8 cijferige nummerreeks, startend bij 00010001 en eindigend bij 89999999.

De volgende reeksen zijn gereserveerd voor testdoeleinden:

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

4.4 AGB-code

Vanuit het zorgveld is er behoefte aan het opnemen van de AGB-code in het certificaatprofiel van de UZI-passen. De AGB-code zit in het subjectaltname.otherName (zie par. 4.7) als onderdeel van het <Subject ID>. Er zijn echter diverse AGB-codes in gebruik: gerelateerd aan instellingen, praktijken en zorgverleners. Bij de registratie van een abonnee wordt de opgegeven AGB-code van de abonnee vastgelegd in het Registratiesysteem. Vanuit Vektis is in Tabel 6 aangegeven welke AGB-code in welk pastype opgenomen moet worden.

Naam UZI-pastype	Soort AGB-code
Zorgverlenerpas	Zorgverlener (pashouder)
Medewerkerpas op naam	Abonnee
Medewerkerpas niet op naam	Abonnee
UZI-register Servercertificaat	Abonnee

Tabel 6 Overzicht AGB-code per pastype

OPMERKINGEN:

- De AGB-code is een optioneel veld. Als de aanvrager geen AGB-code opgeeft worden er als default waarde nullen ingevuld;
- De AGB-code van de abonnee kan zowel van een zorgverlener zijn als van een organisatie afhankelijk van het type abonnee;
- ZOVAR Servercertificaten bevatten geen AGB-code;
- Bij een pasaanvraag via de Digitale Aanvraag Faciliteit (DAF) wordt geen AGB-code opgenomen.

4.5 Waarden van certificatePolicies extensie

De volgende waarden voor certificatePolicies extensie zullen worden geconfigureerd.

4.5.1 certificatePolicies.policyIdentifier

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

Intermediate CA certificaten
Zie het PoR 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.

CommonName TSP CA	Certificate Policies
UZI Zorgverlener HND - G4 PKIo EUTL G-Sigs NP - 2024 UZI Medw op naam HND - G4 PKIo EUTL G-Sigs NP - 2024	ETSI NCP+ (0.4.0.2042.1.2) ETSI QCP-n-qscd (0.4.0.194112.1.2) PKIo G4 EUTL Sigs Gen TSP CA NP OCSP (2.16.528.1.1003.1.2.44.14.19.10) PKIo G4 EUTL Sigs Gen NP Individual Validated eSig (2.16.528.1.1003.1.2.44.14.11.5) PKIo G4 EUTL Sigs Gen NP Reg. Prof. Validated eSig (2.16.528.1.1003.1.2.44.14.12.5) PKIo G4 EUTL Sigs Gen NP Sponsor Validated eSig (2.16.528.1.1003.1.2.44.14.13.5) PKIo G4 EUTL Sigs Gen NP Reg. Prof. w/Sponsor Val. eSig (2.16.528.1.1003.1.2.44.14.14.5)
UZI Zorgverlener - G4 PKIo Priv S-CIBG NP - 2024 UZI Medw op naam - G4 PKIo Priv S-CIBG NP - 2024	ETSI NCP (0.4.0.2042.1.1) ETSI NCP+ (0.4.0.2042.1.2) PKIo G4 Priv CIBG NP Individual Validated Authenticity (2.16.528.1.1003.1.2.44.46.11.4) PKIo G4 Priv CIBG NP Individual Validated Confidentiality (2.16.528.1.1003.1.2.44.46.11.7) PKIo G4 Priv CIBG NP Individual Validated Authentication (2.16.528.1.1003.1.2.44.46.11.8) PKIo G4 Priv CIBG NP Reg. Prof. Validated Authenticity (2.16.528.1.1003.1.2.44.46.12.4) PKIo G4 Priv CIBG NP Reg. Prof. Validated Confidentiality (2.16.528.1.1003.1.2.44.46.12.7) PKIo G4 Priv CIBG NP Reg. Prof. Validated Authentication (2.16.528.1.1003.1.2.44.46.12.8) PKIo G4 Priv CIBG NP Sponsor Validated Authenticity (2.16.528.1.1003.1.2.44.46.13.4) PKIo G4 Priv CIBG NP Sponsor Validated Confidentiality (2.16.528.1.1003.1.2.44.46.13.7) PKIo G4 Priv CIBG NP Sponsor Validated Authentication (2.16.528.1.1003.1.2.44.46.13.8) PKIo G4 Priv CIBG NP Reg. Prof. w/Sponsor Val. Authenticity (2.16.528.1.1003.1.2.44.46.14.4) PKIo G4 Priv CIBG NP Reg. Prof. w/Sponsor Val. Confidentiality (2.16.528.1.1003.1.2.44.46.14.7) PKIo G4 Priv CIBG NP Reg. Prof. w/Sponsor Val. Authentication (2.16.528.1.1003.1.2.44.46.14.8) PKIo G4 Priv CIBG TSP CA NP OCSP (2.16.528.1.1003.1.2.44.46.19.10)
UZI Medw niet op naam - G4 PKIo Priv S-CIBG LP - 2024	ETSI NCP (0.4.0.2042.1.1) ETSI NCP+ (0.4.0.2042.1.2) PKIo G4 Priv CIBG TSP CA LP OCSP (2.16.528.1.1003.1.2.44.46.29.10) PKIo G4 Priv CIBG LP Org. Validated Authenticity (2.16.528.1.1003.1.2.44.46.25.4) PKIo G4 Priv CIBG LP Org. Validated Confidentiality (2.16.528.1.1003.1.2.44.46.25.7) PKIo G4 Priv CIBG LP Org. Validated Authentication (2.16.528.1.1003.1.2.44.46.25.8)
UZI Server - G4 PKIo Priv G-TLS SYS - 2024 ZOVAR Server - G4 PKIo Priv G-TLS SYS - 2024	ETSI NCP (0.4.0.2042.1.1) ETSI NCP+ (0.4.0.2042.1.2) PKIo G4 Priv TLS Gen TSP CA Sys OCSP (2.16.528.1.1003.1.2.44.15.39.10) PKIo G4 Priv TLS Gen Sys Organization Validated Server (2.16.528.1.1003.1.2.44.15.35.11)

Tabel 7 Waarden PolicyIdentifier in TSP CA certificaten G4

Gebruikercertificaten
De volgende tabel geeft een overzicht van de PolicyIdentifiers (OID's) die in gebruikercertificaten zijn opgenomen. 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). Voor de beschrijving van de toepassingsgebieden van de diverse Policies wordt verwezen naar het PoR.

Naam product	PolicyIdentifiers per certificaat type
Zorgverlenerpas	*AUT certificaat in ZV (PKIo G4 Priv CIBG NP)* ETSI EN 319 411-1, NCP+ (0.4.0.2042.1.2) Reg. Prof. Validated Authenticity (2.16.528.1.1003.1.2.44.46.12.4) Reg. Prof. Validated Authentication (2.16.528.1.1003.1.2.44.46.12.8) Reg. Prof. w/Sponsor Val. Authenticity (2.16.528.1.1003.1.2.44.46.14.4) Reg. Prof. w/Sponsor Val. Authentication (2.16.528.1.1003.1.2.44.46.14.8) *HND certificaat in ZV (PKIo G4 EUTL Sigs Gen NP)* ETSI EN 319 411-1, NCP+ (0.4.0.2042.1.2) Regulated Profession Validated eSig. (2.16.528.1.1003.1.2.44.14.12.5) Regulated Prof. w/Sponsor Val. eSig. (2.16.528.1.1003.1.2.44.14.14.5) ETSI EN 319 411-2, QCP-n-qscd (0.4.0.194112.1.2) *VRT certificaat in ZV (PKIo G4 Priv CIBG NP)* ETSI EN 319 411-1, NCP+ (0.4.0.2042.1.2) Reg. Prof. Validated Confidentiality (2.16.528.1.1003.1.2.44.46.12.7) Reg. Prof. w/Sponsor Val. Confidentiality (2.16.528.1.1003.1.2.44.46.14.7)
Medewerkerpas op naam	*AUT certificaat in MON (PKIo G4 Priv CIBG NP)* ETSI EN 319 411-1, NCP+ (0.4.0.2042.1.2) Individual Validated Authenticity (2.16.528.1.1003.1.2.44.46.11.4) Individual Validated Authentication (2.16.528.1.1003.1.2.44.46.11.8) Sponsor Validated Authenticity (2.16.528.1.1003.1.2.44.46.13.4) Sponsor Validated Authentication (2.16.528.1.1003.1.2.44.46.13.8) *HND certificaat in MON (PKIo G4 EUTL Sigs Gen NP)* ETSI EN 319 411-1, NCP+ (0.4.0.2042.1.2) Individual Validated eSignature (2.16.528.1.1003.1.2.44.14.11.5) Sponsor Validated eSignature (2.16.528.1.1003.1.2.44.14.13.5) ETSI EN 319 411-2, QCP-n-qscd (0.4.0.194112.1.2) *VRT certificaat in MON (PKIo G4 Priv CIBG NP)* ETSI EN 319 411-1, NCP+ (0.4.0.2042.1.2) Individual Validated Confidentiality (2.16.528.1.1003.1.2.44.46.11.7) Sponsor Validated Confidentiality (2.16.528.1.1003.1.2.44.46.13.7)
Medewerkerpas niet op naam	*AUT in MNON (PKIo G4 Priv CIBG LP)* ETSI EN 319 411-1 NCP+ (0.4.0.2042.1.2) Organization Validated Authenticity (2.16.528.1.1003.1.2.44.46.25.4) Organization Validated Authentication (2.16.528.1.1003.1.2.44.46.25.8) *VRT in MNON (PKIo G4 Priv CIBG NP)* ETSI EN 319 411-1 NCP+ (0.4.0.2042.1.2) Organization Validated Confidentiality: (OID: 2.16.528.1.1003.1.2.44.46.25.7)
UZI-register Servercertificaat **ZOVAR Servercertificaat**	ETSI TS EN 319 411-1 NCP (0.4.0.2042.1.1) PKIo G4 Priv TLS Gen Sys Organization Validated Server (2.16.528.1.1003.1.2.44.15.35.11)

Tabel 8 Waarden PolicyIdentifier voor gebruikercertificaten G4

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

CA-certificaten

Voor alle CA certificaten geldt dat er géén User Notice is opgenomen.

Gebruikercertificaten

In de G4 gebruikercertificaten is de volgende User Notice opgenomen:
Gebruik van dit certificaat dient te voldoen aan de beschrijving in par. 1.4 van het Programme of Requirements van PKIoverheid. Zie cp.pkioverheid.nl

4.5.3 certificatePolicies.PolicyQualifier.cPS.uri

CA certificaten

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

Gebruikercertificaten UZI-register en ZOVAR generatie G4

In de gebruikercertificaten is de volgende certificatePolicies.PolicyQualifier.cPS.uri opgenomen:
https://www.zorgcsp.nl/certification-practice-statement-cps

4.5.4 id-etsi-qcs-QcPDS (alleen in handtekeningcertificaten)

In de handtekeningcertificaten bevat de QcStatement extensie een link naar een PKI Disclosure Statement (PDS). Dit is een document dat een samenvatting geeft van de belangrijkste punten uit het CPS. Zie voor een toelichting op het doel en de structuur van een PDS *ETSI EN 319 411-1 V1.4.1 (2023-10), Annex A (informative): Model PKI disclosure statement*.

In de handtekeningcertificaten van Zorgverlenerpassen en Medewerkerpassen op naam is de volgende link naar het PKI Disclosure Statement opgenomen:
https://www.zorgcsp.nl/actueelpds

4.6 Waarden cRLDistributionPoints.distributionPoint.fullName

4.6.1 CDP's in CA certificaten Zorg CSP

De volgende tabel geeft een overzicht van de CDP's van de G4 generatie TSP CA certificaten, waarmee de status van het betreffende CA certificaat is te controleren.

CA	CRL Distribution Point
UZI Zorgverlener - G4 PKIo Priv S-CIBG NP - 2024 UZI Medw op naam - G4 PKIo Priv S-CIBG NP - 2024	http://crl.pkioverheid.nl/StaatderNederlandenG4IntmPrivSCIBGNP2024.crl
UZI Zorgverlener HND - G4 PKIo EUTL G-Sigs NP - 2024 UZI Medw op naam HND - G4 PKIo EUTL G-Sigs NP - 2024	http://crl.pkioverheid.nl/StaatderNederlandenG4IntmEUTLGSigsNP2024.crl
UZI Medw niet op naam - G4 PKIo Priv S-CIBG LP - 2024	http://crl.pkioverheid.nl/StaatderNederlandenG4IntmPrivSCIBGLP2024.crl
UZI Server - G4 PKIo Priv G-TLS SYS - 2024 ZOVAR Server - G4 PKIo Priv G-TLS SYS - 2024	http://crl.pkioverheid.nl/StaatderNederlandenG4IntmPrivGTLSSYS2024.crl

Tabel 9 CRL Distribution points in CA certificaten Zorg CSP generatie G4

4.6.2 CDP's in Gebruikercertificaten Productieomgeving

De volgende tabel geeft het overzicht van de CDP's per pastype in de Productieomgeving van de G4 generatie.

Naam pastype (certificaat)	CRL Distribution Point
Zorgverlenerpas (AUT, VRT)	http://www.csp.uzi-register.nl/cdp/uzi_zorgverlener-g4_pkio_priv_s-cibg_np-2024.crl
Zorgverlenerpas (HND)	http://www.csp.uzi-register.nl/cdp/uzi_zorgverlener_hnd-g4_pkio_eutl_g-sigs_np-2024.crl
Medewerkerpas op naam (AUT, VRT)	http://www.csp.uzi-register.nl/cdp/uzi_medw_op_naam-g4_pkio_priv_s-cibg_np-2024.crl
Medewerkerpas op naam (HND)	http://www.csp.uzi-register.nl/cdp/uzi_medw_op_naam_hnd-g4_pkio_eutl_g-sigs_np-2024.crl
Medewerkerpas niet op naam (AUT, VRT)	http://www.csp.uzi-register.nl/cdp/uzi_medw_niet_op_naam-g4_pkio_priv_s-cibg_lp-2024.crl
UZI-register Servercertificaat	http://www.csp.uzi-register.nl/cdp/uzi_server-g4_pkio_priv_g-tls_sys-2024.crl
ZOVAR Servercertificaat	http://www.csp.zovar.nl/cdp/zovar_server-g4_pkio_priv_g-tls_sys-2024.crl

Tabel 10 CRL Distribution points in gebruikercertificaten Zorg CSP generatie G4

4.7 SubjectAltName.otherName

Deze paragraaf beschrijft hoe de subjectAltName.othername in de certificaten van de Zorg CSP wordt opgenomen. Allereerst komt het type aan de orde (par. 4.7.1) en vervolgens de samenstelling van de waarde (par. 4.7.3 voor het UZI-register en 4.7.4 voor ZOVAR).

PKIoverheid specificeert een subjectAltName.othername met een OID-achtige structuur, als volgt: "**<OID CA>-<Subject ID>**". De <OID CA> en het <Subject ID> zijn gescheiden door een '-'.

Hierbij staat <OID CA> voor de OID van de uitgevende CA, die een weergave is van **<PKIoverheid>.<Domein>.<CSP>.<CA>**. Dit deel is bij toetreding van de Zorg CSP tot de PKI voor de overheid vastgelegd en is beschreven in par. 4.7.1.

Het <Subject ID> is een specifieke identificatie binnen het domein van de CSP. Hierin is door het UZI-register een keuze gemaakt om diverse nummers op te nemen die binnen de zorgsector betekenis kunnen hebben en het subject als zorgverlener binnen een bepaalde abonnee uniek identificeren. Dit is beschreven in par. 4.7.3 voor het UZI-register en in par. 4.7.4 voor ZOVAR.

4.7.1 SubjectAltName.otherName.type-id

Het subjectAltName.OtherName.Type-id is een **IA5 string** (OID 2.5.5.5 {joint-iso-itu-t(2) ds(5) attributeSyntax(5) 5}).

4.7.2 SubjectAltName.otherName waarden: <OID CA>

De waarde <OID CA>-<Subject ID> wordt vervolgens in de identifierValue gezet. Hoe deze waarde tot stand komt is nader toegelicht in het vervolg van deze paragraaf. De volgende tabel geeft de waarden van de <OID CA> in de productieomgeving zoals deze door Logius zijn toegekend. CIBG gebruikt deze OID's als een identifier van de CA ongeacht de specifieke generatie of variant (EUTL of S-CIBG).

CA type	OID
UZI-register Zorgverlener CA	2.16.528.1.1003.1.3.5.5.2
UZI-register Medewerker op naam CA	2.16.528.1.1003.1.3.5.5.3
UZI-register Medewerker niet op naam CA	2.16.528.1.1003.1.3.5.5.4
UZI-register Server CA	2.16.528.1.1003.1.3.5.5.5
ZOVAR Server CA	2.16.528.1.1003.1.3.5.5.6

Tabel 11 <OID CA> in gebruikerscertificaten Zorg CSP

4.7.3 SubjectAltName.otherName waarden: <Subject ID> voor certificaten UZI-register

Het <Subject ID> voor certificaten van het UZI-register is een samengesteld veld, bestaande uit door een '-' gescheiden velden:

<Subject ID> = <versie-nr>-<UZI-nr>-<pastype>-<Abonnee-nr>-<rol>-<AGB-code>
De volgende tabel geeft een toelichting bij de velden:

Veld	Type	Waarde	Toelichting
<versie-nr>	1NUM	1 voor alle producten.	Versienummer van de <Subject ID> specificatie t.b.v. mogelijke toekomstige ontwikkelingen.
<UZI-nr>	9NUM	UZI-nummer dat de persoon uniek identificeert voor Zorgverlenerpas en Medewerkerpas op naam **OF** UZI-nummer dat de pas uniek identificeert voor Medewerkerpas niet op naam **OF** UZI-nummer dat het UZI-register servercertificaat uniek identificeert	Een uniek persoonsgebonden nummer voor certificaathouders. Zie par. 4.2.
<pastype>	1 CHAR	Code voor het UZI-pastype. De volgende codering wordt toegepast: Z : Zorgverlenerpas N : Medewerkerpas op naam M : Medewerkerpas niet op naam S : UZI-register Servercertificaat	
<Abonnee-nr>	8NUM	Abonneenummer	UZI-register abonneenummer van organisatie of zorgverlener.
<rol>	6CHAR	Bevat de codering van de beroepstitel en indien aanwezig het specialisme voor Zorgverlenerpas **OF** 00.000 Voor Medewerkerpas op naam, Medewerkerpas niet op naam en UZI-register Servercertificaat	Codering is als volgt: `<code beroepstitel>.<code specialisme>` De <code beroepstitel>=2NUM De <code specialisme>=3NUM
<AGB-code>	8NUM	AGB-code van de zorgverlener (pashouder) voor de Zorgverlenerpas: **OF** AGB-code van de abonnee voor Medewerkerpas op naam, Medewerkerpas niet op naam, UZI-register Servercertificaat: **OF** '00000000' indien niet opgegeven in aanvraag.	De Vektis AGB-Code. Zie par. 4.4.

Tabel 12 Velden <Subject ID> in SubjectAltName.otherName van UZI-register certificaten

OPMERKING:
- In het Certificate Practice Statement is een volledige lijst opgenomen van de codering van beroepstitels en specialismen.

VOORBEELDEN SUBJECTALTNAME.OTHERNAME UZI-REGISTER

Zorgverlenerpas van een cardioloog (Hoofdpas)
<OID CA>-<versie-nr>-<UZI-nr>-<pastype>-<Abonnee-nr>-<rol>-<AGB-code>
2.16.528.1.1003.1.3.5.5.2-1-123456789-Z-12345678-01.010-12345678

In bovenstaand voorbeeld is:
- <OID CA> = 2.16.528.1.1003.1.3.5.5.2 (OID van de UZI-register Zorgverlener CA)
- <versie-nr> = 1
- <UZI-nummer> = 123456789
- <pastype> = Z (Zorgverlenerpas)
- <Abonnee-nr> = 12345678 (abonnee type organisatie of abonnee type zorgverlener)
- <rol> = 01.010 (beroepstitel 01=arts en specialisme 010=cardiologie)
- <AGB-code> = 12345678 AGB-code van de betreffende zorgverlener (pashouder)

Medewerkerpas op naam
<OID CA>-<versie-nr>-<UZI-nr>-<pastype>-<Abonnee-nr>-<rol>-<AGB-code>
2.16.528.1.1003.1.3.5.5.3-1-123456789-N-12349678-00.000-12345678

In bovenstaand voorbeeld is:
- <OID CA> = 2.16.528.1.1003.1.3.5.5.3 (OID UZI-register Medewerker op naam CA)
- <versie-nr> = 1
- <UZI-nummer> = 123456789
- <pastype> = N (Medewerkerpas op naam)
- <Abonnee-nr> = 12349678
- <rol> = 00.000 (00=geen beroepstitel en 000=geen specialisme)
- <AGB-code> = 12345678 AGB-code van de abonnee

Medewerkerpas niet op naam
<OID CA>.<versie-nr>-<UZI-nr>-<pastype>-<Abonnee-nr>-<rol>-<AGB-code>
2.16.528.1.1003.1.3.5.5.4-1-123456777-M-12345888-00.000-12555678

In bovenstaand voorbeeld is:
- <OID CA> = 2.16.528.1.1003.1.3.5.5.4 (OID van de UZI-register Medewerker niet op naam CA)
- <versie-nr> = 1
- <UZI-nummer> = 123456777
- <pastype> = M (Medewerkerpas niet op naam)
- <Abonnee-nr> = 12345888
- <rol> = 00.000 (00=geen beroepstitel en 000=geen specialisme)
- <AGB-code> = 12555678 AGB-code van de abonnee

UZI-register Private Servercertificaat
<OID CA>-<versie-nr>-<UZI-nr>-<pastype>-<Abonnee-nr>-<rol>-<AGB-code>
2.16.528.1.1003.1.3.5.5.5-1-010101019-S-02345678-00.000-12345678

In voorgaande voorbeeld is:
- <OID CA> = 2.16.528.1.1003.1.3.5.5.5 (OID van de UZI-register Server CA)
- <versie-nr> = 1

- <UZI-nummer> = 010101019
- <pastype> = S (Servercertificaat)
- <Abonnee-nr> = 02345678
- <rol> = 00.000 (00=geen beroepstitel en 000=geen specialisme)
- <AGB-code> = 12345678 AGB-code van de abonnee

4.7.4 SubjectAltName.otherName waarden: <Subject ID> voor ZOVAR Servercertificaat

Het <Subject ID> in het ZOVAR Servercertificaat is een samengesteld veld, bestaande uit door een '-' gescheiden velden:

<Subject ID> = <versie-nr>-<subject-nr>-<pastype>-<UZOVI-nr>-<Erkenning>

Veld	Type	Waarde	Toelichting
<versie-nr>	1NUM	1	Versienummer van de <Subject ID> specificatie t.b.v. mogelijke toekomstige ontwikkelingen.
<subject-nr>	13NUM	<UZOVI-nummer><ZOVAR-nummer>	Uniek nummer voor ZOVAR Servercertificaat.
<pastype>	1 CHAR	Codering van pastype: V : ZOVAR Servercertificaat	Uniek Pastype binnen Zorg CSP.
<UZOVI-nr>	4NUM	UZOVI-nummer	Het Vektis UZOVI-nummer.
<Erkenning>	2CHAR	Type erkenning: ZV : Zorgverzekeraar	Type erkenning. De Erkenning zal in eerste instantie altijd gevuld zal zijn met 'ZV' omdat alleen zorgverzekeraars abonnee van ZOVAR kunnen worden.

Tabel 13 Velden <Subject ID> in SubjectAltName.otherName ZOVAR Servercertificaat

VOORBEELD:
2.16.528.1.1003.1.3.5.5.6-1-8643123456789-V-8643-ZV
<OID CA>-<versie-nr>-<subject-nr>-<pastype>-<UZOVI-nr>-<Erkenning>

In bovenstaande voorbeeld is:
- <OID CA> = 2.16.528.1.1003.1.3.5.5.6 (OID van de Zovar Server CA)
- <versie-nr> = 1
- <subject-nr> = 8643123456789
- <pastype> = V
- <UZOVI-nr> = 8643 (uniek identificerend nummer van de zorgverzekeraar.)
- <Erkenning> = ZV

4.8 Microsoft User Principal Name (UPN)

Ten behoeve van authenticatie in Microsoft omgevingen is in de subject.AltName van authenticatiecertificaten van UZI-passen een extra otherName met de Microsoft UPN (User Principal Name) toegevoegd in het formaat 'gebruiker@domein'. Het UZI-register zal dit als volgt vullen:

<UZI-nummer>@<abonneenummer>

Voordelen van deze invulling van de UPN zijn:
- De UPN is uniek voor een persoon of medewerkerpas niet op naam binnen een organisatie;
- De nummers zijn onveranderlijk bij vernieuwing van een pas (m.u.v. Medewerkerpas niet op naam);

- Er ontstaat geen directe relatie met de lokale infrastructuur van zorginstellingen. Dat zou namelijk kunnen leiden tot vernieuwing van alle UZI-passen bij wijziging van de lokale infrastructuur (fusie, migratie domeinstructuur);
- De wijziging heeft geen invloed op de gegevens die het UZI-register in het registratieproces vast moeten leggen. De aanvrager zou anders UPN's van toekomstige pashouders moeten opgeven.

4.9 Kwaliteitscontrole publieke sleutel in servercertificaten

De aanvrager van een UZI-register of ZOVAR servercertificaat is verantwoordelijk voor het (laten) genereren van het sleutelpaar waarvan het publieke deel in het servercertificaat wordt opgenomen. Het aanleveren van de publieke sleutel ter certificering vindt plaats door het uploaden van een zogenaamd PKCS#10 bestand, ook wel bekend als Certificate Signing Request (CSR).

Bij het uploaden van het PKCS#10 bestand voert CIBG twee controles uit:
- dat het een RSA sleutelpaar betreft van 4096 bits;
- dat de ondertekening van het PKCS#10 bestand gebaseerd is op het SHA-256 hash algoritme (sha256WithRSAEncryption).

De CA software voert vanaf 28 augustus 2024 aanvullende kwaliteitscontroles uit op de aangeleverde publieke sleutel alvorens een servercertificaat uit te geven. De kwaliteitscontroles zijn gebaseerd op de volgende standaarden die naar elkaar verwijzen:
- CA/B Forum Baseline requirements for TLS certificates section 6.1.6;
- FIPS 186-4;
- NIST SP 800-89 sectie 5.3.3;
- NIST SP 56A: Revision 2.

Concreet betekent dit de volgende controles op de waarden van de RSA exponent en modulus:
- De public exponent is een oneven getal en ligt tussen 2^16+1 en 2^256-1;
- De modulus is
    - een oneven getal;
    - niet de macht van een priemgetal;
    - heeft geen factoren kleiner dan 752;
- De public key is geen ROCA weak key (CVE-2017-15361).

Wanneer validatie op één van deze element bij een aanvraag niet succesvol is, zal de aanvraag worden afgewezen.

***Disclaimer**: De bovenstaande kwaliteitscontroles staan bekend als 'plausibiliteitstesten' en bepalen of de publieke modulus en exponent 'aannemelijk' zijn, niet noodzakelijkerwijs of ze volledig veilig zijn. Dat wil zeggen dat ze voldoen aan alle vereisten voor het genereren van RSA-sleutels zoals gespecificeerd in genoemde standaarden. Plausibiliteitstesten kunnen onbedoelde fouten met een redelijke waarschijnlijkheid detecteren.*

5 Profiel CA certificaten

5.1 CA certificaatprofiel TSP CA

Deze paragraaf beschrijft de inhoud van de TSP CA certificaten. Deze certificaat zijn uitgegeven door Logius/PKIoverheid en het normatieve certificaatprofiel is gespecificeerd in het CPS van PKIoverheid, zie https://cps.pkioverheid.nl/. In de onderstaande tabel zijn daarom uitsluitend de attributen opgenomen waarvan de Zorg CSP de waarde zelf mag bepalen en door middel van een PKCS#10 certificatieverzoek aanlevert aan de PA voor certificering. De TSP CA certificaten zijn de issuing CA's van de eindgebruikercertificaten.

PROFIEL CA certificaat TSP CA/CA's				
Certificaatveld / attribuut	OID	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate				
subject.countryName (C)			NL	PrintableString
subject.organizationName (O)			CIBG	UTF8String
subject.commonName (CN)			*Afhankelijk van pas-/certificaattype:* • UZI Zorgverlener HND - G4 PKIo EUTL G-Sigs NP - 2024 • UZI Medw op naam HND - G4 PKIo EUTL G-Sigs NP - 2024 • UZI Zorgverlener - G4 PKIo Priv S-CIBG NP - 2024 • UZI Medw op naam - G4 PKIo Priv S-CIBG NP - 2024 • UZI Medw niet op naam - G4 PKIo Priv S-CIBG LP - 2024 • UZI Server - G4 PKIo Priv G-TLS SYS - 2024 • ZOVAR Server - G4 PKIo Priv G-TLS SYS - 2024	UTF8String
Standard Extension				

Tabel 14 Profiel TSP CA certificaat

De sleutellengte is RSA 4096 bits.
De geldigheidsduur is gespecificeerd in par. 2.1.
De certificatePolicies die opgenomen zijn in de TSP CA certificaten zijn gespecificeerd in par. 4.5.

5.2 URL's van CA certificaten

De **DER encoded** CA certificaten van de diverse generaties zijn te vinden via de URL's in de volgende tabellen. Deze URL's zijn als een verwijzing naar de Issuing CA die het (CA) opgenomen in de eind certificaten.

Naam CA	URL naar CA certificaat
Staat der Nederlanden - G4 Root EUTL G-Sigs - 2024	http://cert.pkioverheid.nl/StaatderNederlandenG4RootEUTLGSigs2024.cer
Staat der Nederlanden - G4 Intm EUTL G-Sigs NP - 2024	http://cert.pkioverheid.nl/StaatderNederlandenG4IntmEUTLGSigsNP2024.cer
UZI Zorgverlener HND - G4 PKIo EUTL G-Sigs NP - 2024	http://cert.pkioverheid.nl/UZIZorgverlenerHNDG4PKIoEUTLGSigsNP2024.cer
UZI Medw op naam HND - G4 PKIo EUTL G-Sigs NP - 2024	http://cert.pkioverheid.nl/UZIMedwopnaamHNDG4PKIoEUTLGSigsNP2024.cer

Tabel 15 URL's van CA certificaten G4 G-EUTL

Naam CA	URL naar CA certificaat
Staat der Nederlanden - G4 Root Priv S-CIBG - 2024	http://cert.pkioverheid.nl/StaatderNederlandenG4RootPrivSCIBG2024.cer
Staat der Nederlanden - G4 Intm Priv S-CIBG NP - 2024	http://cert.pkioverheid.nl/StaatderNederlandenG4IntmPrivSCIBGNP2024.cer
UZI Zorgverlener - G4 PKIo Priv S-CIBG NP - 2024	http://cert.pkioverheid.nl/UZIZorgverlenerG4PKIoPrivSCIBGNP2024.cer
UZI Medw op naam - G4 PKIo Priv S-CIBG NP - 2024	http://cert.pkioverheid.nl/UZIMedwopnaamG4PKIoPrivSCIBGNP2024.cer
Staat der Nederlanden - G4 Intm Priv S-CIBG LP - 2024	http://cert.pkioverheid.nl/StaatderNederlandenG4IntmPrivSCIBGLP2024.cer
UZI Medw niet op naam - G4 PKIo Priv S-CIBG LP - 2024	http://cert.pkioverheid.nl/UZIMedwnietopnaamG4PKIoPrivSCIBGLP2024.cer

Tabel 16 URL's van CA certificaten G4 S-CIBG

Naam CA	URL naar CA certificaat
Staat der Nederlanden - G4 Root Priv G-TLS - 2024	http://cert.pkioverheid.nl/StaatderNederlandenG4RootPrivGTLS2024.cer
Staat der Nederlanden - G4 Intm Priv G-TLS SYS - 2024	http://cert.pkioverheid.nl/StaatderNederlandenG4IntmPrivGTLSSYS2024.cer
UZI Server - G4 PKIo Priv G-TLS SYS - 2024	http://cert.pkioverheid.nl/UZIServerG4PKIoPrivGTLSSYS2024.cer
ZOVAR Server - G4 PKIo Priv G-TLS SYS - 2024	http://cert.pkioverheid.nl/ZOVARServerG4PKIoPrivGTLSSYS2024.cer

Tabel 17 URL's van CA certificaten G4 G-TLS

5.3 Fingerprints van CA certificaten

De G4 CA's zijn gepubliceerd op Overview of PKIoverheid certificates (cert.pkioverheid.nl). De officiële gegevens van de G4 CA's zijn gepubliceerd in Staatscourant 2024, 37801.

De G4 CA certificaten zijn niet standaard opgenomen in de Operating Systemen of certificate stores van applicaties. De juistheid van de CA certificaten is met behulp van volgende tabellen vast te stellen op basis van de zogenaamde 'fingerprint'. 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	Fingerprints CA certificaat
Staat der Nederlanden - G4 Root EUTL G-Sigs - 2024	6855279332EED73286B086425CF8C349DB508C53 5C8CAE4CDBC0DE389310DE0FE5A9A52133B74C2D20A806689417AE6682979474
Staat der Nederlanden - G4 Intm EUTL G-Sigs NP - 2024	32DD2AF0A8BD59CB081C8CA5AB5336A9F9DCBEB5 76A62072D1DE085F5007C8C15B51D2F34BD279ED57F84CC26142C03E0B95F75C
UZI Zorgverlener HND - G4 PKIo EUTL G-Sigs NP - 2024	5B49999F7BA36CA745BDF07B9C9A8D3558AE8104 83C53A8ED29F1ACF9460D55FB20B494AC718496312B5D093BDBA62F10F0A14DA
UZI Medw op naam HND - G4 PKIo EUTL G-Sigs NP - 2024	E6DC1FC65757DD38D74E083B36756D10941274EF 82E9C80FA0A848FC502C4AE9590DE98874A51C4526D06566FF5C934D3B7A485F

Tabel 18 Fingerprints van CA certificaten van generatie G4 G-EUTL

Naam CA	Fingerprints CA certificaat
Staat der Nederlanden - G4 Root Priv S-CIBG - 2024	4DEDDB47EB3A1628085A00643D288985AB937AE1 CA54D3B8B32A8A1ECE9E0BB5DEC603F982A8FB8D693F9B2EBC22297FE7059BFD
Staat der Nederlanden - G4 Intm Priv S-CIBG NP - 2024	DD59F85824E5B3922BE9E3E387FDAC4F265A8377 4BDE8352F73C9EBB5AB1ECD368AF96C7FF733B4CB727FA819C02BA2A5D5357A7
UZI Zorgverlener - G4 PKIo Priv S-CIBG NP - 2024	69C551B14951A8E0749C3C38E27A1E4BFEEBF570 72F7B29ECCAF60EA107EA4543438AE3C7B50D299076B6B4396578A53FC10DF12
UZI Medw op naam - G4 PKIo Priv S-CIBG NP - 2024	E5463FED696E6DFC256E4A6F15CA784335CFA820 FE1280D4E3382D602DCF40E01F1B9C40BA4B1AA17E4D9A0364442C26B7BF4E34
Staat der Nederlanden - G4 Intm Priv S-CIBG LP - 2024	67423758F036BB63911C046897CF79A89A7259B0 94548E125D3F94B32A734B81E416E703C52C3DBBF2405FCED9DDC1F0806B0423
UZI Medw niet op naam - G4 PKIo Priv S-CIBG LP - 2024	0165392584546D706FF9736028562CA2F8B0F5F0 3649459B7C63367D5BC3E9DA15AB4E530DF530D6E16D76DE1C5BDD217009D583

Tabel 19 Fingerprints van CA certificaten van generatie G4 S-CIBG

Naam CA	Fingerprints CA certificaat
Staat der Nederlanden - G4 Root Priv G-TLS - 2024	78F350B231F38C7FE905403313779B08FA2A27CB 4411F67D3D7F4F49D34FF8862249DE0D6692ADC92DF0855FB1DD67A169800484
Staat der Nederlanden - G4 Intm Priv G-TLS SYS - 2024	3315A3150F01EAB266B24A73F6078B466CDED6D0 A24F6F2FA192DD96CEEAF8D4C380D8663426F95858956A5ADFF5CFD36B30554F
UZI Server - G4 PKIo Priv G-TLS SYS - 2024	0CFC031467F03B7202135ABCF9E54E46FAB80DCA BF32F3D0243818CA608DBA0323669A10303D9AB2A81068AFFE373500D694687A
ZOVAR Server - G4 PKIo Priv G-TLS SYS - 2024	D2373E553C698D2612B016EEB971CF8BACAD68A5 593061DB2C1D5C4828DA07A9CE4D481400A20DEEDFEE4D84BC690E8BC0F86325

Tabel 20 Fingerprints van CA certificaten van generatie G4 G-TLS

6 Profiel gebruikercertificaten Zorgverlenerpas

Dit hoofdstuk specificeert het de certificaatprofielen van de Zorgverlenerpas.

6.1 Profiel authenticiteitcertificaat Zorgverlenerpas

PROFIEL AUTHENTICITEITCERTIFICAAT Zorgverlenerpas					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
tbsCertificate					
version			2	VAST	De waarde ‘2 ‘ betekent versie 3 van X.509
serialNumber			Uniek nummer binnen de CA	Variabel	Een door de UZI-register Zorgverlener CA random gegenereerd certificaatnummer (160 bits, positief integer). Dit nummer is voor ieder UZI Zorgverlener certificaat (binnen de uitgevende CA) uniek. Dit nummer wordt gebruikt in de Certificate Revocation List (CRL), waarin dit nummer komt te staan als een certificaat is ingetrokken.
signatureAlgorithm			1.2.840.113549.1.1.10	VAST	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: 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					De issuer attributen vormen samen de Distinguished Name van de CA: de UZI-register Zorgverlener CA.
issuer.countryName	C		NL	VAST	
issuer.organisationName	O		CIBG	VAST	Dit attribuut bevat de officiële organisatienaam van de uitgevende CSP.
issuer.commonName	CN		UZI Zorgverlener - G4 PKIo Priv S-CIBG NP - 2024	VAST	Dit attribuut bevat de volledige naam van de uitgevende CA.
validity.notBefore			UTCTime vanaf wanneer het certificaat geldig is.	Variabel	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is.
validity.notAfter			UTCTime tot wanneer het certificaat geldig is.	Variabel	De geldigheidsperiode (notAfter - notBefore) is 3 jaar (= 1095 dagen). Bij vernieuwing is dit maximaal 31 dagen extra, waarbij de nieuwe einddatum gebaseerd is op de einddatum van de oude pas + 1095 dagen.

PROFIEL AUTHENTICITEITCERTIFICAAT Zorgverlenerpas					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
Subject					Deze attributen vormen samen de *distinguished name* van certificaathouder.
subject.countryName	C		Twee-letter codering van land, volgens ISO 3166.	Variabel	In overeenstemming met het adres van de abonnee volgens geaccepteerd document of registratie.
subject.organizationName	O		Volledige naam van de abonnee	Variabel	Naam van de abonnee van de zorgverlener. Dit kan zowel abonnee type organisatie zijn als abonnee type zorgverlener.
subject.title	{ id-at 12 }		Aanspreektitel van de zorgverlener	Variabel	Dit attribuut bevat de aanspreektitel (rol) van de zorgverlener. Indien alleen de beroepstitel is ingevuld is het de aanspreektitel die hoort bij de beroepstitel (bijv. arts). Indien ook een specialisme is opgegeven dan is het de aanspreektitel die hoort bij het specialisme (bijv. cardioloog).
subject.serialNumber			UZI-nummer	Variabel	Dit attribuut bevat het UZI-nummer en maakt daarmee de subject DN uniek maakt binnen de CA. Zie par. 4.2.
subject.givenName			<voornamen>	Variabel	Dit attribuut bevat de volledige voorna(a)m(en) van de zorgverlener, zoals vermeld in het identiteitsbewijs.
subject.surname			<indien gevuld: voorvoegsels geboortenaam+ spatie><geboortenaam>	Variabel	Dit attribuut bevat de achternaam van de zorgverlener, zoals vermeld in het identiteitsbewijs.
subject.commonName	CN		<voornamen><spatie><indien gevuld: voorvoegsels geboortenaam+ spatie><geboortenaam>	Variabel	Dit attribuut bevat de volledige naam van de zorgverlener, zoals vermeld in het identiteitsbewijs.
subjectPublicKeyInfo.algorithm			rsaEncryption	VAST	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden.
subjectPublicKeyInfo. subjectPublicKey			RSA sleutel van certificaathouder: 4096 bits RSA	Variabel	Dit attribuut bevat de publieke sleutel, welke kan worden gebruikt voor de in dit certificaat gespecificeerde doeleinden.
Extentions	OID	Critical	Waarde		
certificatePolicies	{id-ce 32}				
certificatePolicies.PolicyIdentifier			Reg. Prof. Validated Authenticity (2.16.528.1.1003.1.2.44.46.12.4) Reg. Prof. Validated Authentication (2.16.528.1.1003.1.2.44.46.12.8) Reg. Prof. w/Sponsor Val. Authenticity (2.16.528.1.1003.1.2.44.46.14.4) Reg. Prof. w/Sponsor Val. Authentication (2.16.528.1.1003.1.2.44.46.14.8)	VAST	Dit attribuut identificeert de CP van de PKIoverheid voor het relevante certificaat profiel (beveiligingsfunctie en domein). Zie par. 4.5.

PROFIEL AUTHENTICITEITCERTIFICAAT Zorgverlenerpas					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
certificatePolicies.PolicyIdentifier			0.4.0.2042.1.2	VAST	ETSI EN 319 411-1 policy OID NCP+. Zie par. 4.5.
certificatePolicies.PolicyQualifier.cPS.uri			**https://www.zorgcsp.nl/certification-practice-statement-cps**	VAST	Dit attribuut bevat de URL voor het Certificate Practice Statement van het UZI-register. Zie. Par. 4.5.
certificatePolicies.PolicyQualifier.userNotice.explicitText			Gebruik van dit certificaat dient te voldoen aan de beschrijving in par. 1.4 van het Programme of Requirements van PKIoverheid. Zie cp.pkioverheid.nl	VAST	In de user notice worden (een samenvatting van) de gebruikersvoorwaarden geplaatst c.q. waar die te vinden zijn. Zie. Par. 4.5. Encoded als UTF8String.
keyUsage	{id-ce 15}	TRUE	digitalSignature	VAST	Dit veld definieert voor welke toepassingen de private key gebruikt mag worden.
AuthorityInfoAccess					
.accessMethod (OCSP)			1.3.6.1.5.5.7.48.1		
.uniformResourceIndicator			**http://ocsp.uzi-register.nl**		Op deze URL is de OCSP dienstverlening beschikbaar.
.accessMethod (CA Issuers)			1.3.6.1.5.5.7.48.2		
.uniformResourceIndicator			**http://cert.pkioverheid.nl/UZIZorgverlenerG4PKIoPrivSCIBGNP2024.cer**		HTTP URI naar DER encoded issuing CA certificaat. Zie par. 5.2
authorityKeyIdentifier.keyIdentifier	{id-ce 35}		SHA-1 hash van publieke CA sleutel.	VAST	Dit attribuut bevat het controle getal voor de publieke sleutel van het UZI register en kan van belang zijn als de CA meerdere sleutelparen heeft.
subjectKeyIdentifier.keyIdentifier	{id-ce 14}		SHA-1 hash van publieke sleutel van certificaat	VAST	Dit attribuut bevat het controle getal voor de publieke sleutel in dit certificaat.
extKeyUsage	{id-ce 37}		clientAuth (OID 1.3.6.1.5.5.7.3.2) szOID_KP_DOCUMENT_SIGNING (OID 1.3.6.1.4.1.311.10.3.12) id-kp-documentSigning (OID 1.3.6.1.5.5.7.3.36)	VAST	- clientAuth: certificaat bruikbaar voor client authenticatie - documentSigning: bruikbaar voor ondertekening documenten. Zowel Microsoft OID als pkix OID zie RFC 9336.
CRLDistributionPoints.distributionPoint.fullName	{id-ce 31}		**http://www.csp.uzi-register.nl/cdp/uzi_zorgverlener-g4_pkio_priv_s-cibg_np-2024.crl**	VAST	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. 4.6.
subjectAltName	{id-ce 17}				
subjectAltName.otherName			OID: 1.3.6.1.4.1.311.20.2.3 (Microsoft User Principle Name (UPN)) gevuld met een UTF-8 string met de volgende waarde: <UZI-nummer>@<abonneenummer>	Variabel	De othername met de UPN moet als eerste 'otherName' opgenomen zijn binnen de subjectAltName en is noodzakelijk voor Microsoft Smartcard logon.
subjectAltName.otherName			Samengesteld veld. zie par. 4.7.	Variabel	subjectAltName.OtherName

PROFIEL AUTHENTICITEITCERTIFICAAT Zorgverlenerpas					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
basicConstraints	{id-ce 19}	TRUE			
basicConstraints.cA			Zie toelichting.	VAST	Door het CA attribuut weg te laten, geldt de default waarde: CA=FALSE. Dit geeft aan dat het een certificaat voor eindgebruikers is (dus geen CA).
basicConstraints.pathLenConstraint			Zie toelichting.	VAST	Door het attribuut weg te laten, geldt de default waarde: None
Certificate					
signatureAlgorithm			1.2.840.113549.1.1.10	VAST	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: 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 tbsCertificate.	Variabel	

Tabel 21 Profiel authenticiteitcertificaat Zorgverlenerpas

6.2 Profiel handtekeningcertificaat Zorgverlenerpas

Het volgende certificaatprofiel wordt gebruikt voor een handtekeningcertificaat op een Zorgverlenerpas. Hierbij zijn alleen de verschillen opgenomen t.o.v. het profiel voor authenticiteitcertificaten. Deze verschillen hebben betrekking op:

- tbsCertificate.subjectPublicKeyInfo.subjectPublicKey: er is uiteraard een andere public key omdat het 3 certificatenmodel bij de PKI voor de overheid ook 3 sleutelparen inhoudt;
- dit resulteert in een andere subjectKeyIdentifier per certificaat type;
- tbsCertificate.extensions.certificatePolicies: PKIoverheid heeft een aparte OID's voor authenticatie, vertrouwelijkheid en onweerlegbaarheid;
- tbsCertificate.extensions.keyUsage. Dit is het primaire verschil. Dit attribuut geeft aan voor welke toepassingen de publieke sleutel gebruikt mag worden. Het UZI-register onderkent de volgende mogelijkheden:
    - handtekeningcertificaten: non-repudiation
    - vertrouwelijkheidcertificaten: keyEncipherment, dataEncipherment
    - authenticiteitcertificaten: digitalSignature
    - servercertificaten: Digital Signature, keyEncipherment
- tbsCertificate.extensions.qcStatements. Alleen handtekeningcertificaten kunnen 'gekwalificeerd' zijn en het bijbehorende qcStatement hebben in het profiel. Het qcStatement bevat een statement dat stelt dat het een gekwalificeerd certificaat betreft, één statement dat de private sleutel is beschermd met een smartcard, één statement betreft het type certificaat en één statement bevat een verwijzing naar het PKI Disclosure Statement (PDS). Zie voor referentie *ETSI EN 319 412-5 V2.4.1 (2023-09), Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.*
- Handtekeningcertificaten (en vertrouwelijkheidcertificaten) bevatten geen UPN in subjectAltName.otherName.
- Handtekeningcertificaten hebben een aparte EUTL CA en daarom een afwijkende Issuer, CA Issuers URL, authorityKeyIdentifier en CRL Distribution Point.

PROFIEL HANDTEKENINGCERTIFICAAT ZORGVERLENERPAS				
Certificaatveld / attribuut	OID	Critical	Waarde	Omschrijving / toelichting
Certificate				
tbsCertificate				
Issuer				
issuer.countryName	C		NL	
issuer.organisationName	O		CIBG	
issuer.commonName	CN		UZI Zorgverlener HND - G4 PKIo EUTL G-Sigs NP - 2024	
subjectPublicKeyInfo. subjectPublicKey			RSA sleutel van certificaathouder: • 4096 bits	
Standard Extension				
certificatePolicies	{id-ce 32}			
certificatePolicies.PolicyIdentifier			Regulated Profession Validated eSig. (2.16.528.1.1003.1.2.44.14.12.5) Reg. Prof. w/Sponsor Val. eSig. (2.16.528.1.1003.1.2.44.14.14.5)	Dit attribuut identificeert de CP van de PKIoverheid voor het relevante certificaat profiel (beveiligingsfunctie en domein). Zie. Par. 4.5.
certificatePolicies.PolicyIdentifier			0.4.0.2042.1.2	ETSI EN 319 411-1 policy OID NCP+. Zie par. 4.5.
certificatePolicies.PolicyIdentifier			0.4.0.194112.1.2	ETSI EN 319 411-2, QCP-n-qscd policy OID. Zie par. 4.5.
keyUsage	{id-ce 15}	TRUE	NonRepudiation	
AuthorityInfoAccess				

PROFIEL HANDTEKENINGCERTIFICAAT ZORGVERLENERPAS				
Certificaatveld / attribuut	OID	Critical	Waarde	Omschrijving / toelichting
.accessMethod (OCSP)			1.3.6.1.5.5.7.48.1	Voor volledigheid opgenomen. Gelijk voor alle eindgebruikercertificaten
.uniformResourceIndicator			**http://ocsp.uzi-register.nl**	
.accessMethod (CA Issuers)			1.3.6.1.5.5.7.48.2	
.uniformResourceIndicator			**http://cert.pkioverheid.nl/UZIZorgverlenerHNDG4PKIoEUTLGSigsNP2024.cer**	
authorityKeyIdentifier.keyIdentifier			SHA-1 hash van publieke CA sleutel.	Van EUTL CA
subjectKeyIdentifier.keyIdentifier			SHA-1 hash van publieke sleutel van certificaat	
extKeyUsage	{id-ce 37}		id-kp-documentSigning (1.3.6.1.5.5.7.3.36) szOID_KP_DOCUMENT_SIGNING (OID 1.3.6.1.4.1.311.10.3.12)	
CRLDistributionPoints. distributionPoint.fullName	{id-ce 31}		**http://www.csp.uzi-register.nl/cdp/uzi_zorgverlener_hnd-g4_pkio_eutl_g-sigs_np-2024.crl**	
qcStatements	**{id-pe 3}**		**OID 1.3.6.1.5.5.7.1.3**	
qcStatements.etsiQcsCompliance	{ id-etsi-qcs 1 }		OID 0.4.0.1862.1.1	Geeft aan dat het een gekwalificeerd certificaat betreft. Gedefinieerd in ETSI TS 101 862.
qcStatements.etsiQcsQcSSCD	{ id-etsi-qcs 4 }		OID 0.4.0.1862.1.4	Geeft aan dat de private sleutel behorende bij de publieke sleutel in het certificaat is opgeslagen op een qualified signature-creation device (QSCD). Gedefinieerd in ETSI EN 319 412-5.
qcStatements.etsiQcsQcType	{ id-etsi-qcs-QcType }		OID 0.4.0.1862.1.6	Geeft type gekwalificeerd certificaat overeenstemmend met annex I van EU Verordening 910/2014.
.Type 1			OID 0.4.0.1862.1.6.1	Type 1. { id-etsi-qcs-QcType 1 }. Certificate for electronic signatures (esign) as defined in Regulation (EU) No 910/2014
qcStatements.etsiQcsQcPDS	{ id-etsi-qcs 5 }		OID 0.4.0.1862.1.5	Verwijzing naar PKI Dislosure Statement (PDS)
.url			Link naar PDS. Encoded als IA5String	Zie voor PDS URL par. 4.5.4.
.language			'en'. Encoded als PrintableString	Codering van taal van PDS.

Tabel 22 Profiel handtekeningcertificaat Zorgverlenerpas

6.3 Profiel vertrouwelijkheidcertificaat Zorgverlenerpas

Het volgende certificaatprofiel wordt gebruikt voor een vertrouwelijkheidcertificaat op een Zorgverlenerpas. Hierbij zijn alleen de verschillen opgenomen t.o.v. het profiel voor authenticiteitcertificaten.

PROFIEL VERTROUWELIJKHEIDCERTIFICAAT ZORGVERLENERPAS				
Certificaatveld / attribuut	OID	Critical	Waarde	Omschrijving / toelichting
Certificate				
tbsCertificate				
subjectPublicKeyInfo. subjectPublicKey			RSA sleutel van certificaathouder: • 4096 bits	
Standard Extension				
CertificatePolicies	{id-ce 32}			
certificatePolicies.PolicyIdentifier			Reg. Prof. Validated Confidentiality (2.16.528.1.1003.1.2.44.46.12.7) Reg. Prof. w/Sponsor Val. Confidentiality (2.16.528.1.1003.1.2.44.46.14.7)	Dit attribuut identificeert de CP van de PKIoverheid voor het relevante certificaat profiel (beveiligingsfunctie en domein). Zie. Par. 4.5.
certificatePolicies.PolicyIdentifier			0.4.0.2042.1.2	ETSI EN 319 411-1 policy OID NCP+. Zie par. 4.5.
keyUsage	{id-ce 15}	TRUE	keyEncipherment, dataEncipherment	
subjectKeyIdentifier.keyIdentifier			SHA-1 hash van publieke sleutel van certificaat	
extKeyUsage	{id-ce 37}		Encrypting File System (OID 1.3.6.1.4.1.311.10.3.4)	

Tabel 23 Profiel vertrouwelijkheidcertificaat Zorgverlenerpas

7 Profiel gebruikercertificaten Medewerkerpas op naam

7.1 Profiel authenticiteitcertificaat Medewerkerpas op naam

PROFIEL AUTHENTICITEITCERTIFICAAT Medewerkerpas op naam					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
tbsCertificate					
version			2	VAST	De waarde '2 ' betekent versie 3 van X.509
serialNumber			Uniek nummer binnen de CA	Variabel	Een door de UZI-register Medewerkerpas op naam CA random gegenereerd certificaatnummer (160 bits, positief integer). Dit nummer is voor ieder UZI Medewerker op naam certificaat uniek. Dit nummer wordt gebruikt in de Certificate Revocation List (CRL), waarin dit nummer komt te staan als een certificaat is ingetrokken.
signatureAlgorithm			1.2.840.113549.1.1.10	VAST	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: RSASSA-PSS
hashingAlgorithm			2.16.840.1.101.3.4.2.3	VAST	SHA-512
maskAlgorithm			1.2.840.113549.1.1.8	VAST	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
Issuer					De issuer attributen vormen samen de Distinguished Name van de CA: de UZI-register Medewerker op naam CA.
issuer.countryName	C		NL	VAST	
issuer.organisationName	O		CIBG	VAST	Dit attribuut bevat de officiële organisatienaam van de uitgevende CA.
issuer.commonName	CN		UZI Medw op naam - G4 PKIo Priv S-CIBG NP - 2024	VAST	Dit attribuut bevat de volledige naam van de uitgevende CA.
validity.notBefore			UTCTime vanaf wanneer het certificaat geldig is.	Variabel	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is.
validity.notAfter			UTCTime tot wanneer het certificaat geldig is.	Variabel	De geldigheidsperiode (notAfter - notBefore) is 3 jaar (= 1095 dagen). Bij vernieuwing is dit maximaal 31 dagen extra, waarbij de nieuwe einddatum gebaseerd is op de einddatum van de oude pas + 1095 dagen.
Subject					De subject attributen vormen samen de distinguished name van de certificaathouder.
subject.countryName	C		Twee-letter codering van land, volgens ISO 3166.	Variabel	In overeenstemming met het adres van de abonnee volgens geaccepteerd document of registratie.
subject.organizationName	O		Volledige naam van de abonnee	Variabel	Naam van de abonnee van de zorgverlener. Dit kan zowel abonnee type organisatie zijn als abonnee type zorgverlener.

PROFIEL AUTHENTICITEITCERTIFICAAT Medewerkerpas op naam					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
subject.serialNumber			UZI-nummer	Variabel	Dit attribuut bevat het UZI-nummer en maakt daarmee de subject DN uniek maakt binnen de CA. Zie par. 4.2.
subject.givenName			<voornamen>	Variabel	Dit attribuut bevat de volledige voorna(a)m(en) van de medewerker, zoals vermeld in het identiteitsbewijs.
subject.surname			<indien gevuld: voorvoegsels geboortenaam+ spatie><geboortenaam>	Variabel	Dit attribuut bevat de achternaam van de medewerker, zoals vermeld in het identiteitsbewijs.
subject.commonName	CN		<voornamen><spatie><indien gevuld: voorvoegsels geboortenaam+ spatie><geboortenaam>	Variabel	Dit attribuut bevat de volledige naam van de medewerker, zoals vermeld in het identiteitsbewijs.
subjectPublicKeyInfo.algorithm			rsaEncryption	VAST	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden.
subjectPublicKeyInfo. subjectPublicKey			RSA sleutel van certificaathouder: • 4096 bits	Variabel	Dit attribuut bevat de publieke sleutel, welke kan worden gebruikt voor de in dit certificaat gespecificeerde doeleinden.
Extentions	OID	Critical	Waarde		
certificatePolicies	{id-ce 32}				
certificatePolicies.PolicyIdentifier			Individual Validated Authenticity (2.16.528.1.1003.1.2.44.46.11.4) Individual Validated Authentication (2.16.528.1.1003.1.2.44.46.11.8) Sponsor Validated Authenticity (2.16.528.1.1003.1.2.44.46.13.4) Sponsor Validated Authentication (2.16.528.1.1003.1.2.44.46.13.8)	VAST	Dit attribuut identificeert de CP van de PKIoverheid voor het relevante certificaat profiel (beveiligingsfunctie en domein). Zie par. 4.5.
certificatePolicies.PolicyIdentifier			0.4.0.2042.1.2	VAST	ETSI EN 319 411-1 policy OID NCP+. Zie par. 4.5.
certificatePolicies.PolicyQualifier. cPS.uri			**https://www.zorgcsp.nl/certification-practice-statement-cps**	VAST	Dit attribuut bevat de URL voor het Certificate Practice Statement van het UZI-register. Zie. Par. 4.5.
certificatePolicies.PolicyQualifier. userNotice.explicitText			Gebruik van dit certificaat dient te voldoen aan de beschrijving in par. 1.4 van het Programme of Requirements van PKIoverheid. Zie cp.pkioverheid.nl	VAST	In de user notice worden (een samenvatting van) de gebruikersvoorwaarden geplaatst c.q. waar die te vinden zijn. Zie. Par. 4.5. Encoded als UTF8String.
keyUsage	{id-ce 15}	TRUE	digitalSignature	VAST	Dit veld definieert voor welke toepassingen de private key gebruikt mag worden.

PROFIEL AUTHENTICITEITCERTIFICAAT Medewerkerpas op naam					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
AuthorityInfoAccess					
.accessMethod (OCSP)			1.3.6.1.5.5.7.48.1		
.uniformResourceIndicator			**http://ocsp.uzi-register.nl**		Op deze URL is de OCSP dienstverlening beschikbaar.
.accessMethod (CA Issuers)			1.3.6.1.5.5.7.48.2		
.uniformResourceIndicator			**http://cert.pkioverheid.nl/UZIMedwopnaamG4PKIoPrivSCIBGNP2024.cer**		HTTP URI naar DER encoded issuing CA certificaat. Zie par. 5.2.
authorityKeyIdentifier. keyIdentifier	{id-ce 35}		SHA-1 hash van publieke CA sleutel.	VAST	Dit attribuut bevat het controle getal voor de publieke sleutel van het UZI register en kan van belang zijn als de CA meerdere sleutelparen heeft.
subjectKeyIdentifier.keyIdentifier	{id-ce 14}		SHA-1 hash van publieke sleutel van certificaat	VAST	Dit attribuut bevat het controle getal voor de publieke sleutel in dit certificaat.
extKeyUsage	{id-ce 37}		clientAuth (OID 1.3.6.1.5.5.7.3.2) szOID_KP_DOCUMENT_SIGNING (OID 1.3.6.1.4.1.311.10.3.12) id-kp-documentSigning (OID 1.3.6.1.5.5.7.3.36)	VAST	- clientAuth: het certificaat kan gebruikt worden voor client authenticatie - documentSigning: bruikbaar voor ondertekening documenten Zowel Microsoft OID als pkix OID zie RFC 9336.
CRLDistributionPoints. distributionPoint.fullName	{id-ce 31}		**http://www.csp.uzi-register.nl/cdp/uzi_medw_op_naam-g4_pkio_priv_s-cibg_np-2024.crl**	VAST	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. 4.6.
subjectAltName	{id-ce 17}				
subjectAltName.otherName			OID: 1.3.6.1.4.1.311.20.2.3 (Microsoft User Principle Name (UPN)) gevuld met een UTF-8 string met de volgende waarde: <UZI-nummer>@<abonneenummer>	Variabel	De othername met de UPN moet als eerste 'otherName' opgenomen zijn binnen de subjectAltName en is noodzakelijk voor Microsoft Smartcard logon.
subjectAltName.otherName			Samengesteld veld. zie par. 4.7.	Variabel	
basicConstraints	{id-ce 19}	TRUE			
basicConstraints.cA			Zie toelichting.	VAST	Door het CA attribuut weg te laten, geldt de default waarde: CA=FALSE. Dit geeft aan dat het een certificaat voor eindgebruikers is (dus geen CA).
basicConstraints. pathLenConstraint			Zie toelichting.		Door het attribuut weg te laten, geldt de default waarde: None
Certificate					
signatureAlgorithm			1.2.840.113549.1.1.10	VAST	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: RSASSA-PSS
hashingAlgorithm			2.16.840.1.101.3.4.2.3	VAST	SHA-512

PROFIEL AUTHENTICITEITCERTIFICAAT Medewerkerpas op naam					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
maskAlgorithm			1.2.840.113549.1.1.8	VAST	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue			Handtekening van CA over het tbsCertificate.	Variabel	

Tabel 24 Profiel authenticiteitcertificaat Medewerkerpas op naam

7.2 Profiel handtekeningcertificaat Medewerkerpas op naam

Het volgende certificaatprofiel wordt gebruikt voor een handtekeningcertificaat bij een Medewerkerpas op naam. Hierbij zijn alleen de verschillen opgenomen t.o.v. het profiel voor authenticiteitcertificaten. Zie voor meer details par. 6.2.

PROFIEL HANDTEKENINGCERTIFICAAT Medewerkerpas op naam				
Certificaatveld / attribuut	OID	Critical	Waarde	Omschrijving / toelichting
Certificate				
tbsCertificate				
issuer.countryName	C		NL	
issuer.organisationName	O		CIBG	
issuer.commonName	CN		UZI Medw op naam HND - G4 PKIo EUTL G-Sigs NP - 2024	
subjectPublicKeyInfo. subjectPublicKey			RSA sleutel van certificaathouder: • 4096 bits	
Standard Extension				
certificatePolicies	{id-ce 32}			
certificatePolicies.PolicyIdentifier			Individual Validated eSignature (2.16.528.1.1003.1.2.44.14.11.5) Sponsor Validated eSignature (2.16.528.1.1003.1.2.44.14.13.5)	Dit attribuut identificeert de CP van de PKIoverheid voor het relevante certificaat profiel (beveiligingsfunctie en domein). Zie par. 4.5.
certificatePolicies.PolicyIdentifier			0.4.0.2042.1.2	ETSI EN 319 411-1 policy OID NCP+. Zie par. 4.5.
certificatePolicies.PolicyIdentifier			0.4.0.194112.1.2	ETSI EN 319 411-2, QCP-n-qscd policy OID. Zie par. 4.5. Zie par. 4.5.
keyUsage	{id-ce 15}	TRUE	NonRepudiation	
AuthorityInfoAccess				
.accessMethod (OCSP)			1.3.6.1.5.5.7.48.1	Voor volledigheid opgenomen. Gelijk voor alle eindgebruikercertificaten
.uniformResourceIndicator			**http://ocsp.uzi-register.nl**	
.accessMethod (CA Issuers)			1.3.6.1.5.5.7.48.2	
.uniformResourceIndicator			**http://cert.pkioverheid.nl/UZIMedwopnaamHNDG4PKIoEUTLGSigsNP2024.cer**	
authorityKeyIdentifier.keyIdentifier			SHA-1 hash van publieke CA sleutel.	Van EUTL CA
subjectKeyIdentifier.keyIdentifier			SHA-1 hash van publieke sleutel van certificaat	
extKeyUsage	{id-ce 37}		id-kp-documentSigning (1.3.6.1.5.5.7.3.36) szOID_KP_DOCUMENT_SIGNING (OID 1.3.6.1.4.1.311.10.3.12)	document Signing
CRLDistributionPoints. distributionPoint.fullName	{id-ce 31}		**http://www.csp.uzi-register.nl/cdp/uzi_medw_op_naam_hnd-g4_pkio_eutl_g-sigs_np-2024.crl**	
qcStatements	**{id-pe 3}**		**OID 1.3.6.1.5.5.7.1.3**	
qcStatements.etsiQcsCompliance	{ id-etsi-qcs 1 }		OID 0.4.0.1862.1.1	Geeft aan dat het een gekwalificeerd certificaat betreft. Gedefinieerd in ETSI TS 101 862.

qcStatements.etsiQcsQcSSCD	{ id-etsi-qcs 4 }		OID 0.4.0.1862.1.4	Geeft aan dat de private sleutel behorende bij de publieke sleutel in het certificaat is opgeslagen op een qualified signature-creation device (QSCD). Gedefinieerd in ETSI EN 319 412-5.
qcStatements.etsiQcsQcType	{ id-etsi-qcs-QcType }		OID 0.4.0.1862.1.6	Geeft type gekwalificeerd certificaat overeenstemmend met annex I van EU Verordening 910/2014.
.Type 1			OID 0.4.0.1862.1.6.1	Type 1. { id-etsi-qcs-QcType 1 }. Certificate for electronic signatures (esign) as defined in Regulation (EU) No 910/2014
qcStatements.etsiQcsQcPDS	{ id-etsi-qcs 5 }		OID 0.4.0.1862.1.5	Verwijzing naar PKI Dislosure Statement (PDS)
.url			Link naar PDS. Encoded als IA5String	Zie voor PDS URL par. 4.5.4.
.language			'en'. Encoded als PrintableString	Codering van taal van PDS.

Tabel 25 Profiel handtekeningcertificaat Medewerkerpas op naam

7.3 Profiel vertrouwelijkheidcertificaat Medewerkerpas op naam

Het volgende certificaatprofiel wordt gebruikt voor een vertrouwelijkheidcertificaat bij een Medewerkerpas op naam. Hierbij zijn alleen de verschillen opgenomen t.o.v. het profiel voor authenticiteitcertificaten. Zie voor meer details par. 6.3.

PROFIEL VERTROUWELIJKHEIDCERTIFICAAT Medewerkerpas op naam				
Certificaatveld / attribuut	OID	Critical	Waarde	Omschrijving / toelichting
Certificate				
tbsCertificate				
subjectPublicKeyInfo. subjectPublicKey			RSA sleutel van certificaathouder: • 4096 bits	
Standard Extension				
CertificatePolicies	{id-ce 32}			
certificatePolicies.PolicyIdentifier			Individual Validated Confidentiality (2.16.528.1.1003.1.2.44.46.11.7) Sponsor Validated Confidentiality (2.16.528.1.1003.1.2.44.46.13.7)	OID van CP van de PKIoverheid voor het certificaat profiel (beveiligingsfunctie en domein). Zie. Par. 4.5.
certificatePolicies.PolicyIdentifier			0.4.0.2042.1.2	ETSI EN 319 411-1 policy OID NCP+. Zie par. 4.5.
keyUsage	{id-ce 15}	TRUE	keyEncipherment, dataEncipherment	
subjectKeyIdentifier.keyIdentifier			SHA-1 hash van publieke sleutel van certificaat	
extKeyUsage	{id-ce 37}		Encrypting File System (1.3.6.1.4.1.311.10.3.4)	

Tabel 26 Profiel vertrouwelijkheidcertificaat Medewerkerpas op naam

8 Profiel gebruikercertificaten Medewerkerpas niet op naam

8.1 Profiel authenticiteitcertificaat Medewerkerpas niet op naam

PROFIEL AUTHENTICITEITCERTIFICAAT Medewerkerpas niet op naam					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
tbsCertificate					
version			2	VAST	De waarde '2 ' betekent versie 3 van X.509
serialNumber			Uniek nummer binnen de CA	Variabel	Een door de UZI-register Medewerkerpas niet op naam CA random gegenereerd certificaatnummer (160 bits, positief integer). Dit nummer is voor iedere Medewerkerpas niet op naam certificaat uniek.
signatureAlgorithm			1.2.840.113549.1.1.10	VAST	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: RSASSA-PSS
hashingAlgorithm			2.16.840.1.101.3.4.2.3	VAST	SHA-512
maskAlgorithm			1.2.840.113549.1.1.8	VAST	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
Issuer					De issuer attributen vormen samen de Distinguished Name van de CA: de UZI-register Medewerker niet op naam CA.
issuer.countryName	C		NL	VAST	
issuer.organisationName	O		CIBG	VAST	Dit attribuut bevat de officiële organisatienaam van de uitgevende CSP.
issuer.commonName	CN		UZI Medw niet op naam - G4 PKIo Priv S-CIBG LP - 2024	VAST	Dit attribuut bevat de volledige naam van de uitgevende CA.
validity.notBefore			UTCTime vanaf wanneer het certificaat geldig is.	Variabel	Dit attribuut specificeert het tijdstip vanaf wanneer het certificaat geldig is.
validity.notAfter			UTCTime tot wanneer het certificaat geldig is.	Variabel	Dit attribuut specificeert het tijdstip tot wanneer het certificaat geldig is. De geldigheidsperiode (notAfter - notBefore) is 3 jaar (= 1095 dagen).
Subject					Deze attributen vormen samen de distinguished name van certificaathouder.
subject.countryName	C		Twee-letter codering van land, volgens ISO 3166.	Variabel	In overeenstemming met het adres van de abonnee volgens geaccepteerd document of registratie.
subject.organizationName	O		Volledige naam van de abonnee	Variabel	Naam van de abonnee van de medewerker niet op naam. Dit kan zowel abonnee type organisatie zijn als abonnee type zorgverlener.
subject.organizationIdentifier			NTRNL-<kvk-nummer abonnee>		
subject.serialNumber			UZI-nummer	Variabel	Uniek nummer zie par. 4.2.
subject.commonName	CN		Functienaam	Variabel	Dit attribuut bevat de functienaam van de pashouder

PROFIEL AUTHENTICITEITCERTIFICAAT Medewerkerpas niet op naam					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
subjectPublicKeyInfo.algorithm			rsaEncryption	VAST	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden.
subjectPublicKeyInfo. subjectPublic.Key			RSA sleutel van certificaathouder: • 4096 bits	Variabel	Dit attribuut bevat de publieke sleutel, welke kan worden gebruikt voor de in dit certificaat gespecificeerde doeleinden.
Extentions	OID	Critical	Waarde		
certificatePolicies	{id-ce 32}				
certificatePolicies.PolicyIdentifier			Organization Validated Authenticity (2.16.528.1.1003.1.2.44. 46.25.4) Organization Validated Authentication (2.16.528.1.1003.1.2.44. 46.25.8)	VAST	Dit attribuut identificeert de CP van de PKIoverheid voor het relevante certificaat profiel (beveiligingsfunctie en domein). Zie. Par. 4.5.
certificatePolicies.PolicyIdentifier			0.4.0.2042.1.2	VAST	ETSI EN 319 411-1 policy OID NCP+. Zie par. 4.5.
certificatePolicies.PolicyQualifier. cPS.uri			**https://www.zorgcsp.nl/certification-practice-statement-cps**	VAST	Dit attribuut bevat de URL voor het Certificate Practice Statement van het UZI-register. Zie. Par. 4.5.
certificatePolicies.PolicyQualifier. userNotice.explicitText			Gebruik van dit certificaat dient te voldoen aan de beschrijving in par. 1.4 van het Programme of Requirements van PKIoverheid. Zie cp.pkioverheid.nl	VAST	In de user notice worden (een samenvatting van) de gebruikersvoorwaarden geplaatst c.q. waar die te vinden zijn. Zie. Par. 4.5. Encoded als UTF8String.
keyUsage	{id-ce 15}	TRUE	digitalSignature	VAST	Dit veld definieert voor welke toepassingen de private key gebruikt mag worden.
AuthorityInfoAccess					
.accessMethod (OCSP)			1.3.6.1.5.5.7.48.1		
.uniformResourceIndicator			**http://ocsp.uzi-register.nl**		
.accessMethod (CA Issuers)			1.3.6.1.5.5.7.48.2		
.uniformResourceIndicator			**http://cert.pkioverheid.nl/UZIMedwnietopnaamG4PKIoPrivSCIBGLP2024.cer**		HTTP URI naar DER encoded issuing CA certificaat. Zie par. 5.2.
authorityKeyIdentifier. keyIdentifier	{id-ce 35}		SHA-1 hash van publieke CA sleutel.	VAST	Dit attribuut bevat het controle getal voor de publieke sleutel van het UZI register en kan van belang zijn als de CA meerdere sleutelparen heeft.
subjectKeyIdentifier.keyIdentifier	{id-ce 14}		SHA-1 hash van publieke sleutel van certificaat	VAST	Controle getal voor de publieke sleutel in dit certificaat.
extKeyUsage	{id-ce 37}		clientAuth (OID 1.3.6.1.5.5.7.3.2) szOID_KP_DOCUMENT_SIGNING (OID 1.3.6.1.4.1.311.10.3.12) id-kp-documentSigning (OID 1.3.6.1.5.5.7.3.36)	VAST	- clientAuth: het certificaat kan gebruikt worden voor client authenticatie - documentSigning: bruikbaar voor ondertekening documenten Zowel Microsoft OID als pkix OID zie RFC 9336.

PROFIEL AUTHENTICITEITCERTIFICAAT Medewerkerpas niet op naam					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
CRLDistributionPoints. distributionPoint.fullName	{id-ce 31}		**http://www.csp.uzi-register.nl/cdp/uzi_medw_niet_op_naam-g4_pkio_priv_s-cibg_lp-2024.crl**	VAST	Dit attribuut bevat de URL van de Certificate Revocation List voor dit certificaat. Als het certificaat is ingetrokken (revoked) dan komt het serienummer van dit certificaat op deze lijst te staan. Zie. Par. 4.6.
subjectAltName	{id-ce 17}				
subjectAltName.otherName			OID: 1.3.6.1.4.1.311.20.2.3 (Microsoft User Principle Name (UPN)) gevuld met een UTF-8 string met de volgende waarde: <UZI-nummer>@<abonneenummer>	Variabel	De othername met de UPN moet als eerste 'otherName' opgenomen zijn binnen de subjectAltName en is noodzakelijk voor Microsoft Smartcard logon.
subjectAltName.OtherName			Samengesteld veld. zie par.4.7.	Variabel	
basicConstraints	{id-ce 19}	TRUE			
basicConstraints.cA			Zie toelichting.	VAST	Door het CA attribuut weg te laten, geldt de default waarde: CA=FALSE. Dit geeft aan dat het een certificaat voor eindgebruikers is (dus geen CA).
basicConstraints. pathLenConstraint			Zie toelichting.		Door het attribuut weg te laten, geldt de default waarde: None
QcStatements	**{id-pe 3}**		**OID 1.3.6.1.5.5.7.1.3**		
QcStatement2			OID 1.3.6.1.5.5.7.11.2		id-qcs-pkixQCSyntax-v2
SemanticsId-Legal			OID 0.4.0.194121.1.2		id-etsi-qcs-SemanticsId-Legal. This semantics identifier indicates that the organizationalIdentifier in the subject adheres to the prescribed layout.
Certificate					
signatureAlgorithm			1.2.840.113549.1.1.10	VAST	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: RSASSA-PSS
hashingAlgorithm			2.16.840.1.101.3.4.2.3	VAST	SHA-512
maskAlgorithm			1.2.840.113549.1.1.8	VAST	Mask Generator Function 1 (MGF1) Trailer field 1, salt length 0x40
signatureValue			Handtekening van CA over het tbsCertificate.	Variabel	

Tabel 27 Profiel authenticiteitcertificaat Medewerkerpas niet op naam

De Medewerkerpas niet op naam heeft geen handtekeningcertificaat.

8.2 Profiel vertrouwelijkheidcertificaat Medewerkerpas niet op naam

Het volgende certificaatprofiel wordt gebruikt voor een vertrouwelijkheidcertificaat bij een Medewerkerpas niet op naam. Hierbij zijn alleen de verschillen opgenomen t.o.v. het profiel voor authenticiteitcertificaten.

PROFIEL VERTROUWELIJKHEIDCERTIFICAAT Medewerkerpas niet op naam				
Certificaatveld / attribuut	OID	Critical	Waarde	Omschrijving / toelichting
Certificate				
tbsCertificate				
subjectPublicKeyInfo. subjectPublicKey			RSA sleutel van certificaathouder: • 4096 bits	
Standard Extension				
CertificatePolicies	{id-ce 32}	FALSE		
certificatePolicies.PolicyIdentifier			Organization Validated Confidentiality: (OID: 2.16.528.1.1003.1.2.44. 46.25.7)	Dit attribuut identificeert de CP van de PKIoverheid voor het relevante certificaat profiel (beveiligingsfunctie en domein). Zie. Par. 4.5.
certificatePolicies.PolicyIdentifier			0.4.0.2042.1.2	ETSI EN 319 411-1 policy OID NCP+. Zie par. 4.5.
keyUsage	{id-ce 15}	TRUE	keyEncipherment, dataEncipherment	
subjectKeyIdentifier.keyIdentifier			SHA-1 hash van publieke sleutel van certificaat	
extKeyUsage	{id-ce 37}		Encrypting File System (OID 1.3.6.1.4.1.311.10.3.4)	

Tabel 28 Profiel vertrouwelijkheidcertificaat Medewerkerpas niet op naam

De Medewerkerpas niet op naam heeft geen handtekeningcertificaat.

9 Profiel UZI-register Servercertificaat

Onderstaande tabel geeft het certificaatprofiel voor de UZI-register Servercertificaat. Het betreft hier een certificaat waarin vertrouwelijkheid en authenticiteit zijn gecombineerd in één certificaat.

PROFIEL UZI-register Servercertificaat			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / toelichting
tbsCertificate			
Version		2	(X.509v3)
serialNumber		Uniek nummer binnen de CA	Een door de UZI-register Services CA random gegenereerd certificaatnummer (160 bits, positief integer). Dit nummer is voor ieder UZI-register Servercertificaat uniek.
signatureAlgorithm		1.2.840.113549.1.1.10	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: 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			
Issuer.countryName (C)		NL	
Issuer.organisationName (O)		CIBG	
Issuer.commonName (CN)		UZI Server - G4 PKIo Priv G-TLS SYS - 2024	
validity.notBefore		UTCTime vanaf wanneer het certificaat geldig is.	
validity.notAfter		UTCTime van einde geldigheid certificaat	3 jaar (= 1095 dagen)
Subject			
subject.countryName (C)		Twee-letter codering van land, volgens ISO 3166.	Variabel. In overeenstemming met het adres van de abonnee volgens geaccepteerd document of registratie.
Subject.StateOrProvinceName (ST)		Provincie van vestigingsplaats abonnee.	Variabel. In overeenstemming met het adres van de abonnee.
Subject.LocalityName (L)		Vestigingsplaats abonnee	Variabel. In overeenstemming met het adres van de abonnee.
subject.organizationName (O)		Volledige abonneenaam van de abonnee van het UZI-register Server certificaat	Dit kan zowel abonnee type organisatie zijn als abonnee type zorgverlener.
subject.serialNumber		UZI-nummer	Uniek nummer voor service. Zie par. 4.2.
subject.commonName (CN)		Fully Qualified Domain Name (FQDN) van de service.	
subjectPublicKeyInfo. Algorithm		rsaEncryption	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden.
subjectPublicKeyInfo. subjectPublicKey		RSA sleutel van server: • 4096 bits	Dit attribuut bevat de publieke sleutel, welke kan worden gebruikt voor de in dit certificaat gespecificeerde doeleinden.
Standard extensions			
certificatePolicies			
certificatePolicies. PolicyIdentifier		Organization Validated Server (2.16.528.1.1003.1.2.44.15.35.11)	De waarde is de OID van de PKI-overheid Certificate Policy voor servercertificaten in het betreffende domein. Zie. Par. 4.5.

PROFIEL UZI-register Servercertificaat			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / toelichting
certificatePolicies. PolicyIdentifier		0.4.0.2042.1.1	ETSI EN 319 411-1 policy OID NCP. Zie par. 4.5.
certificatePolicies. PolicyQualifier.cPS.uri		**https://www.zorgcsp.nl/certification-practice-statement-cps**	Dit attribuut bevat de URL voor het Certificate Practice Statement van het UZI-register. Zie. Par. 4.5.
certificatePolicies. PolicyQualifier.userNotice. explicitText		Gebruik van dit certificaat dient te voldoen aan de beschrijving in par. 1.4 van het Programme of Requirements van PKIoverheid. Zie cp.pkioverheid.nl	In de user notice worden (een samenvatting van) de gebruikersvoorwaarden geplaatst c.q. waar die te vinden zijn. Zie. Par. 4.5. Encoded als UTF8String.
keyUsage	TRUE	DigitalSignature, KeyEncipherment	Servercertificaat, SSL certificaat met gecombineerde authenticatie en vertrouwelijkheid.
AuthorityInfoAccess			
.accessMethod (OCSP)		1.3.6.1.5.5.7.48.1	
.uniformResourceIndicator		**http://ocsp.uzi-register.nl**	Op deze URL is de OCSP dienstverlening beschikbaar.
.accessMethod(CA Issuers)		1.3.6.1.5.5.7.48.2	
.uniformResourceIndicator		**http://cert.pkioverheid.nl/UZIServerG4PKIoPrivGTLSSYS2024.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 5.2.
authorityKeyIdentifier. keyIdentifier		SHA-1 hash van publieke CA sleutel.	Dit attribuut bevat het controle getal voor de publieke sleutel van het UZI register.
subjectKeyIdentifier. keyIdentifier		SHA-1 hash van publieke sleutel van certificaat	Dit attribuut bevat het controle getal voor de publieke sleutel in dit certificaat.
CRLDistributionPoints. fullName		**http://www.csp.uzi-register.nl/cdp/uzi_server-g4_pkio_priv_g-tls_sys-2024.crl**	Zie. Par. 4.6.
extKeyUsage		ServerAuthenticatie (1.3.6.1.5.5.7.3.1) ClientAuthenticatie (1.3.6.1.5.5.7.3.2)	KeyPurposeId's id-kp-serverAuth en id-kp-clientAuth
subjectAltName			
.dNSName		Fully Qualified Domain Name (FQDN) van de service.	Identieke inhoud als de subject.commonName
.otherName		type-id: IA5 string (2.5.5.5) value: samengesteld veld. zie par. 4.7.	Samenstelling: <OID CA>-<versie-nr>-<UZI-nr>-<pastype>-<Abonnee-nr>-<rol>-<AGB-code>
.otherName			Toegevoegd vanaf 8 november 2023
.permanentIdentifier		1.3.6.1.5.5.7.8.3	
identifierValue		<UZI-register abonneenummer>	UTF8 string, 8NUM met UZI-register abonneenummer van zorgaanbieder (URA)
assigner		2.16.528.1.1007.3.3	OID van URA en assigner: {joint-iso-itu-t(2) country(16) nl(528) nederlandse-organisatie(1) **cibg(1007) uzi-identifiers(3) uzi-abonneenummer(3)**}
basicConstraints	TRUE		
basicConstraints.cA		Zie toelichting.	Door het CA attribuut weg te laten, geldt de default waarde: CA=FALSE. Dit geeft aan dat het een certificaat voor eindgebruikers is (dus geen CA).
basicConstraints. pathLenConstraint		Zie toelichting.	Door het attribuut weg te laten, geldt de default waarde: None

PROFIEL UZI-register Servercertificaat			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / toelichting
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: 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 tbsCertificate.	

Tabel 29 Profiel UZI-register Servercertificaat

10 Profiel ZOVAR Servercertificaat

Onderstaande tabel geeft het certificaatprofiel voor het ZOVAR Servercertificaat. Het betreft hier een certificaat waarin vertrouwelijkheid en authenticiteit zijn gecombineerd in één certificaat.

PROFIEL ZOVAR Servercertificaat			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / toelichting
tbsCertificate			
version		2	(X.509v3)
serialNumber		Uniek nummer binnen de CA	Een door de ZOVAR Server CA random gegenereerd certificaatnummer (160 bits, positief integer). Dit nummer is voor ieder ZOVAR Servercertificaat uniek.
signatureAlgorithm		1.2.840.113549.1.1.10	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: 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			
Issuer.countryName (C)		NL	
Issuer.organisationName (O)		CIBG	
Issuer.commonName (CN)		ZOVAR Server - G4 PKIo Priv G-TLS SYS - 2024	
validity.notBefore		UTCTime vanaf wanneer het certificaat geldig is.	
validity.notAfter		UTCTime van einde geldigheid certificaat	3 jaar geldig (= 1095 dagen)
subject			
subject.countryName (C)		Twee-letter codering van land, volgens ISO 3166.	Variabel. In overeenstemming met het adres van de abonnee volgens geaccepteerd document of registratie. PKIO RfC 265.
subject.StateOrProvince Name (ST)		Provincie van vestigingsplaats abonnee.	Variabel. In overeenstemming met het adres van de abonnee. PKIO RfC 247.
subject.LocalityName (L)		Vestigingsplaats abonnee	Variabel. In overeenstemming met het adres van de abonnee. PKIO RfC 247.
subject.organizationName (O)		Naam van de abonnee (type zorgverzekeraar) van het ZOVAR Servercertificaat.	
subject.serialNumber		<UZOVI-nummer><ZOVAR-nummer>	Uniek nummer voor service. Zie par. 4.2.2.
subject.commonName (CN)		Fully Qualified Domain Name (FQDN) van de service.	
subjectPublicKeyInfo. algorithm		rsaEncryption	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden.
subjectPublicKeyInfo. subjectPublicKey		RSA sleutel van server: • 4096 bits	Dit attribuut bevat de publieke sleutel, welke kan worden gebruikt voor de in dit certificaat gespecificeerde doeleinden.
Standard extensions			
certificatePolicies			
certificatePolicies. PolicyIdentifier		Organization Validated Server (2.16.528.1.1003.1.2.44.15.35.11)	De waarde is de OID van de PKI-overheid Certificate Policy voor servercertificaten in

PROFIEL ZOVAR Servercertificaat			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / toelichting
			het betreffende domein. Zie. Par. 4.5.
certificatePolicies. PolicyIdentifier		0.4.0.2042.1.1	ETSI EN 319 411-1 policy OID NCP. Zie par. 4.5.
certificatePolicies. PolicyQualifier.cPS.uri		**https://www.zorgcsp.nl/certification-practice-statement-cps**	Dit attribuut bevat de URL voor het Certificate Practice Statement van ZOVAR. Zie. Par. 4.5.
certificatePolicies. PolicyQualifier.userNotice. explicitText		Gebruik van dit certificaat dient te voldoen aan de beschrijving in par. 1.4 van het Programme of Requirements van PKIoverheid. Zie cp.pkioverheid.nl	In de user notice worden (een samenvatting van) de gebruikersvoorwaarden geplaatst c.q. waar die te vinden zijn. Zie. Par. 4.5. Encoded als UTF8String.
keyUsage	TRUE	DigitalSignature, KeyEncipherment	Servercertificaat, SSL certificaat met gecombineerde authenticatie + vertrouwelijkheid.
AuthorityInfoAccess			
.accessMethod (OCSP)		1.3.6.1.5.5.7.48.1	
.uniformResourceIndicator		**http://ocsp.zovar.nl**	Op deze URL is de OCSP dienstverlening beschikbaar.
.accessMethod(CA Issuers)		1.3.6.1.5.5.7.48.2	
.uniformResourceIndicator		**http://cert.pkioverheid.nl/ZOVARServerG4PKIoPrivGTLSSYS2024.cer**	HTTP URI naar DER encoded issuing CA certificaat. Zie par. 5.2.
authorityKeyIdentifier. keyIdentifier		SHA-1 hash van publieke CA sleutel.	
subjectKeyIdentifier. keyIdentifier		SHA-1 hash van publieke sleutel van subject	
CRLDistributionPoints. fullName		**http://www.csp.zovar.nl/cdp/zovar_server-g4_pkio_priv_g-tls_sys-2024.crl**	Zie. Par. 4.6.
extKeyUsage		ServerAuthenticatie (1.3.6.1.5.5.7.3.1) ClientAuthenticatie (1.3.6.1.5.5.7.3.2)	KeyPurposId's id-kp-serverAuth en id-kp-clientAuth
subjectAltName			
.dNSName		Fully Qualified Domain Name (FQDN) van de service.	Identieke inhoud als de subject.commonName
.otherName		type-id: IA5 string (2.5.5.5) value: samengesteld veld. zie par. 4.7.	Samenstelling: <OID CA>-<versie-nr>-<subject-nr>-<pastype>-<UZOVI-nr>-<Erkenning>
.otherName			Toegevoegd vanaf 28 november 2023
.permanentIdentifier		1.3.6.1.5.5.7.8.3	
identifierValue		<ZOVAR abonneenummer>	UTF8 string, 8NUM met het ZOVAR abonneenummer van zorgverzekeraar of zorgkantoor.
assigner		2.16.528.1.1007.15.2.1	OID van ZOVAR nummer en assigner: {joint-iso-itu-t(2) country(16) nederland(528) nederlandse-organisatie(1) **cibg(1007) zovar(15) zovar-identifiers(2) zovar-abonneenummer(1)**}
basicConstraints	TRUE		
basicConstraints.cA		Zie toelichting.	Door het CA attribuut weg te laten, geldt de default waarde: CA=FALSE. Dit geeft aan dat het een certificaat voor eindgebruikers is (dus geen CA).

PROFIEL ZOVAR Servercertificaat			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / toelichting
basicConstraints. pathLenConstraint		Zie toelichting.	Door het attribuut weg te laten, geldt de default waarde: None
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: 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 tbsCertificate.	

Tabel 30 Profiel ZOVAR Servercertificaat

11 CRL profielen

11.1 Ontwerpkeuzes

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

- Er is 1 CRL per CA, die certificate.serialNumbers van zowel CA- als gebruikercertificaten kan bevatten;
- Er wordt géén gebruik gemaakt van de zogenaamde 'Reason Code' waarmee de reden van intrekking weergegeven kan worden in de CRL;
- De CRL wordt ondertekend door dezelfde CA als de CA die de certificaten ondertekent met dezelfde sleutel;
- Het UZI-register geeft alleen volledige CRL's uit
- Ingetrokken certificaten na het verlopen van de geldigheidsduur op de CRL staan (ExpiredCertsOnCRL).

11.2 CRL profiel van TSP CA

Deze CRL's -die ondertekend zijn door de TSP CA certificaten- bevatten de serienummers van ingetrokken eindgebruiker certificaten.

CRL profiel van TSP CA			
CRL veld	**Critical**	**Waarde**	**Omschrijving / Toelichting**
TBSCertList			
Version		1	CRL version 2
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
Issuer.commonName (CN)		*Afhankelijk van pas-/certificaattype:* • UZI Zorgverlener HND - G4 PKIo EUTL G-Sigs NP - 2024 • UZI Medw op naam HND - G4 PKIo EUTL G-Sigs NP - 2024 • UZI Zorgverlener - G4 PKIo Priv S-CIBG NP - 2024 • UZI Medw op naam - G4 PKIo Priv S-CIBG NP - 2024 • UZI Medw niet op naam - G4 PKIo Priv S-CIBG LP - 2024 • UZI Server - G4 PKIo Priv G-TLS SYS - 2024 • ZOVAR Server - G4 PKIo Priv G-TLS SYS - 2024	
Issuer. organisationName (O)		CIBG	
Issuer.country (C)		NL	
thisUpdate		Automatisch gegenereerd	Uitgiftetijdstip van de CRL.

CRL profiel van TSP CA			
CRL veld	**Critical**	**Waarde**	**Omschrijving / Toelichting**
TBSCertList			
nextUpdate		Automatisch gegenereerd	Dit is de datum/tijdstip waarop de geldigheid van de CRL eindigt. **Uitgiftetijdstip + 48 uur**.
revokedCertificates			Lijst van ingetrokken certificaten bestaande uit het serienummer van het certificaat en de datum van revocatie.
crlExtensions			
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	Conform ETSI EN 319 411-2: CSS-6.3.10-05: *If CRLs are provided and the TSP does not remove from the CRL revoked certificates after they have expired, the CRL shall include the X.509 "ExpiredCertsOnCRL" extension as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509.*
date		<implementatiedatum>	De ExpiredCertsOnCRL extensie bevat de datum waarop de CRL begint met het bijhouden van informatie over de intrekkingsstatus voor verlopen certificaten. D.w.z. intrekkingsvermeldingen worden niet verwijderd van de CRL voor certificaten die verlopen op of na de datum opgenomen in de ExpiredCertsOnCRL extensie.
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 31 CRL profiel van de TSP CA

11.3 CRL publicatie frequentie

Deze paragraaf geeft toelichting op de publicatiefrequentie van de CRL's en specificeert de tijdstippen van publicatie. Deze informatie is vooral van belang voor applicatieontwikkelaars omdat op servers vaak de CRL's tijdelijk worden opgeslagen (caching). Caching vindt plaats om te voorkomen dat voor iedere UZI-pashouder die wil inloggen de betreffende CRL moet worden opgehaald om het certificaat te valideren.

11.3.1 Normatief kader en Publicatieschema CRL's

Het normatieve kader van het UZI-register - PoR van de PKI voor de overheid- vereist dat de maximale vertraging tussen een verzoek tot intrekking van een UZI-pas en de publicatie van de aangepaste statusinformatie 24 uur is. Om ruime marge te hebben én snel status updates te verspreiden, genereert het UZI-register ieder uur een nieuwe CRL.

Het UZI-register genereert en publiceert iedere uur automatisch een CRL ongeacht het feit of er sinds de voorafgaande publicatie UZI-passen zijn ingetrokken.

11.3.2 Geldigheidsduur CRL's en CRL overlap

In het 'nextUpdate' attribuut van de CRL staat dat een CRL 48 uur geldig is. Zie par. 11.2.
Het 'nextUpdate' tijdstip uur is de uiterste grens waarop een CRL nog vertrouwd kan worden. In de praktijk zal ieder uur een nieuwe CRL gepubliceerd worden. Daarmee realiseert het UZI-register een zogenaamde 'CRL overlap'. CRL overlap periode is de tijd tussen de publicatie van een nieuwe CRL en het verlopen van de voorafgaande CRL. Dus in het geval van het UZI-register is er een 'CRL overlap' van 47 uur. Alleen de laatst gegenereerde CRL staat op de website.

De CRL overlap periode is noodzakelijk om voldoende tijd te hebben om bij een calamiteit over te schakelen naar de uitwijkomgeving van het UZI-register. Het ontbreken van een geldige CRL kan problemen opleveren voor vertrouwende partijen omdat men certificaten niet meer kan valideren. Door de CRL overlap heeft het UZI-register voldoende tijd om in uitwijk te gaan zonder verstoringen voor vertrouwende partijen. De 48 uur is echter de uiterste grens waarop een CRL nog gebruikt kan worden.

Vertrouwende partijen zijn conform het Certificate Practice Statement verplicht om altijd de actuele CRL te gebruiken. Dit houdt in dat men ieder uur een nieuwe CRL op moet halen als de CRL in de cache ouder is dan 1 uur en enkele minuten, d.w.z. na het 'thisUpdate' tijdstip opgenomen in het CRL bestand. De extra geldigheidsperiode van een CRL (overlap) is uitsluitend bedoeld om verstoring te kunnen overbruggen.

12 OCSP (Online Certificate Status Protocol)

12.1 Inleiding

Naast de publicatie van CRL's biedt de Zorg CSP certificaat statusinformatie via OCSP (Online Certificate Status Protocol).

OCSP validatie is een online validatie methode waarbij de Zorg CSP aan de vertrouwende partij een elektronisch ondertekend bericht (OCSP response) verstuurt nadat de vertrouwende partij een specifiek verzoek heeft verstuurd (OCSP request) naar de OCSP dienst (OCSP responder) van de Zorg CSP. In dit bericht staat de opgevraagde status van het betreffende certificaat. Deze status kan de volgende waarden aannemen: `goed`, `ingetrokken` of `onbekend`. Als een OCSP response om enigerlei reden uitblijft dan kan daaruit geen conclusie getrokken worden met betrekking tot de status van het certificaat.

De URL van de OCSP Responder waarmee de intrekkingstatus van een certificaat gevalideerd kan worden, staat in het `AuthorityInfoAccess.uniformResourceIndicator` attribuut van het certificaat.

Een OCSP respons is altijd door de OCSP responder verzonden en ondertekend. Een vertrouwende partij dient de handtekening onder de OCSP respons verifiëren met het servercertificaat dat meegestuurd wordt in de OCSP respons. Dit servercertificaat is uitgegeven door dezelfde CA als de CA die het certificaat heeft uitgegeven waarvan de intrekkingstatus wordt opgevraagd.

De informatie die via OCSP wordt verstrekt kan actueler zijn dan de informatie die via de CRL wordt gecommuniceerd. Dit is alleen het geval als er een intrekking heeft plaatsgevonden en de reguliere CRL update nog niet heeft plaatsgevonden.

12.2 Ontwerpkeuzes

Voor OCSP zijn de volgende ontwerpkeuzes gemaakt:

- De OCSP dienst voldoet aan RFC 6960, PKIX OCSP;
- De OCSP dienst maakt geen gebruik van pre-computed responses.
- Iedere CA van het UZI-register die gebruikercertificaten uitgeeft, heeft een eigen OCSP responder die de OCSP responses ondertekent met een eigen private key. In totaal zijn er dus 5 OCSP-signers per generatie: voor iedere CA/producttype één;
- Iedere OCSP responder heeft een servercertificaat, waarmee een vertrouwende partij de respons kan valideren. Dit certificaat is uitgegeven door de CA waarvan de OCSP responder de status informatie geeft, zie ook de toelichting in par. 12.4;
- Alle OCSP communicatie voor producten van UZI-register verloopt via **`http://ocsp.uzi-register.nl`**
- Alle OCSP communicatie voor ZOVAR verloopt via **`http://ocsp.zovar.nl`**

12.3 Profiel OCSP responder certificaten

De OCSP responder certificaten volgen zoveel mogelijk het certificaatprofiel voor servercertificaten maar zijn op enkele punten afwijkend o.a. vanwege eisen uit de Baseline Requirements van het CA/Browser Forum. De belangrijkste verschillen zijn:

- de Subject.StateOrProvinceName en Subject.LocalityName ontbreken;
- de Extended Key Usage OCSP signing is gebruikt;
- het ocsp-nocheck attribuut is opgenomen. Desondanks bevatten de OCSP responder certificaten wel een CRL DistributionPoint. Dit biedt OCSP clients de mogelijkheid om te controleren of een OCSP responder certificaat is ingetrokken.

Onderstaande tabel bevat het certificaatprofiel voor de OCSP responders.

PROFIEL OCSP signer certificaten			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / toelichting
tbsCertificate			
version		2	(X.509v3)
serialNumber		Uniek nummer binnen de CA	Een door de uitgevende CA random gegenereerd uniek certificaatnummer (160 bits, positief integer).
signatureAlgorithm		1.2.840.113549.1.1.10	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: 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			
Issuer.countryName (C)		NL	
Issuer.organisationName (O)		CIBG	
Issuer.commonName (CN)		[CN delegated CA]	Bijvoorbeeld 'UZI Zorgverlener G4 PKIo Priv S CIBG NP 2024' voor de OCSP responder die status informatie geeft over authenticiteit- en vertrouwelijkheidcertificaten van zorgverlener-passen.
validity.notBefore		UTCTime van ondertekening	
validity.notAfter		UTCTime van einde geldigheid	7 dagen geldig
subject			
subject.countryName (C)		NL	
subject.organizationName (O)		CIBG	
subject.organization Identifier		NTRNL-50000535	Encoded als UTF-8 string.
subject.commonName (CN)		OCSPsigner [CN delegated CA]	Bijvoorbeeld voor de 'UZI Medw niet op naam - G4 PKIo Priv S-CIBG LP - 2024' is de CN van de bijbehorende OCSP responder: 'OCSPsigner UZI Medw niet op naam - G4 PKIo Priv S-CIBG LP - 2024'. Zie voor volledigheid tabel 33.
subjectPublicKeyInfo. algorithm		rsaEncryption	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden.
subjectPublicKeyInfo. subjectPublic.Key		RSA sleutel voor OCSP signing: • 4096 bits	Dit attribuut bevat de publieke sleutel, welke kan worden gebruikt voor de in dit certificaat gespecificeerde doeleinden.
standard extensions			
certificatePolicies			
certificatePolicies. PolicyIdentifier		*Alle OCPS signer certificaten* ETSI NCP+ (0.4.0.2042.1.2) *ZV HND, MON HND* PKIo G4 EUTL Sigs Gen TSP CA NP OCSP (2.16.528.1.1003.1.2.44.14.19.10)	Afhankelijk van de CA is hier een andere waarde opgenomen. Zie voor volledigheid tabel 33.

PROFIEL OCSP signer certificaten			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / toelichting
		ZV AUT/VRT, MON AUT/VRT PKIo G4 Priv CIBG TSP CA NP OCSP (2.16.528.1.1003.1.2.44.46.19.10) *MON AUT/VRT* PKIo G4 Priv CIBG TSP CA LP OCSP (2.16.528.1.1003.1.2.44.46.29.10) *UZI Server / ZOVAR* PKIo G4 Priv TLS Gen TSP CA Sys OCSP (2.16.528.1.1003.1.2.44.15.39.10)	
certificatePolicies.PolicyIdentifier		0.4.0.2042.1.2	ETSI EN 319 411-1 policy OID NCP+.
certificatePolicies.PolicyQualifier.cPS.uri		**https://www.zorgcsp.nl/certification-practice-statement-cps**	Zie. Par. 4.5. ZOVAR heeft eigen CPS URI.
certificatePolicies.PolicyQualifier.userNotice.explicitText		Gebruik van dit certificaat dient te voldoen aan de beschrijving in par. 1.4 van het Programme of Requirements van PKIoverheid. Zie cp.pkioverheid.nl	Identiek aan UserNotice voor servercertificaat. Zie. Par. 4.5.
keyUsage	TRUE	DigitalSignature	Services authenticatie, hoewel een OCSP responder een specifieke toepassing is. Dit komt tot uitdrukking in de Extended Key Usage.
extKeyUsage	TRUE	1.3.6.1.5.5.7.3.9	Voor de OCSP responder dient conform RFC 6960 een Extended Key Usage opgenomen te worden voor OCSP signing (id-kp-OCSPSigning).
authorityKeyIdentifier.keyIdentifier		SHA-1 hash van publieke CA sleutel.	Dit attribuut bevat het controle getal voor de publieke sleutel van de betreffende CA
subjectKeyIdentifier.keyIdentifier		SHA-1 hash van publieke sleutel van subject	Dit attribuut bevat het controle getal voor de publieke sleutel in dit certificaat.
ocsp-nocheck		iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) ocsp(1) no-check(5)}	N.a.v. PKIO change 241
basicConstraints	TRUE		
basicConstraints.cA		FALSE	Geeft aan dat het een certificaat voor eindgebruikers is (dus geen CA).
basicConstraints.pathLenConstraint			None. Geen beperking
QcStatements		**OID 1.3.6.1.5.5.7.1.3**	
QcStatement2		OID 1.3.6.1.5.5.7.11.2	id-qcs-pkixQCSyntax-v2
SemanticsId-Legal		OID 0.4.0.194121.1.2	id-etsi-qcs-SemanticsId-Legal
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.10	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: 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 tbsCertificate.	

Tabel 32 Profiel OCSP signer certificaat

De volgende tabel specificeert de policyIdentifiers die zijn opgenomen in de OCSP signer certificaten.

CommonName OCSP signer CA	Certificate Policies
OCSPsigner UZI Zorgverlener HND - G4 PKIo EUTL G-Sigs NP - 2024 OCSPsigner UZI Medw op naam HND - G4 PKIo EUTL G-Sigs NP - 2024	ETSI NCP+ (0.4.0.2042.1.2) PKIo G4 EUTL Sigs Gen TSP CA NP OCSP (2.16.528.1.1003.1.2.44.14.19.10)
OCSPsigner UZI Zorgverlener - G4 PKIo Priv S-CIBG NP - 2024 OCSPsigner UZI Medw op naam - G4 PKIo Priv S-CIBG NP - 2024	ETSI NCP+ (0.4.0.2042.1.2) PKIo G4 Priv CIBG TSP CA NP OCSP (2.16.528.1.1003.1.2.44.46.19.10)
OCSPsigner UZI Medw niet op naam - G4 PKIo Priv S-CIBG LP - 2024	ETSI NCP+ (0.4.0.2042.1.2) PKIo G4 Priv CIBG TSP CA LP OCSP (2.16.528.1.1003.1.2.44.46.29.10)
OCSPsigner UZI Server - G4 PKIo Priv G-TLS SYS - 2024 OCSPsigner ZOVAR Server - G4 PKIo Priv G-TLS SYS - 2024	ETSI NCP+ (0.4.0.2042.1.2) PKIo G4 Priv TLS Gen TSP CA Sys OCSP (2.16.528.1.1003.1.2.44.15.39.10)

Tabel 33 Waarden PolicyIdentifiers in OCSP signer certificaten

12.4 Hiërarchie OCSP responder certificaten

De Zorg CSP maakt gebruik van een zogenaamde 'delegated' OCSP responder. Dit houdt in dat de handtekeningen onder de OCSP responses geverifieerd kunnen worden met een specifiek servercertificaat dat is getekend door dezelfde CA als de CA die het gebruikercertificaat heeft uitgegeven dat gevalideerd wordt. Op die manier wordt aangegeven dat de responder geautoriseerd is om request over de status van certificaten van een bepaalde CA te beantwoorden. Dit certificaat wordt met iedere response meegestuurd, zodat de vertrouwende partij de response kan controleren. Per pastype en per generatie is er dus een uniek OCSP responder certificaat.

12.5 Voorbeeld OCSP request en response

Deze paragraaf bevat ter illustratie een voorbeeld van een OCSP request en response in een tekst weergave.

12.5.1 OCSP request

De OCSP request bevat de volgende informatie:

- de SHA1 Hash van de CommonName en de Key van de uitgevende CA;
- het serienummer (of een lijst van serienummers) van de certificaten waarvan de status wordt opgevraagd;
- Optioneel kan men een zogenaamde nonce toevoegen. Deze zal ook in de reponse opgenomen worden zodat de OCPS client zekerheid heeft dat het een actueel gegenereerd antwoord is.

Hieronder is de logging van een OCSP request opgenomen.

To do: vervangen door request na implementatie productieomgeving

```
OCSP Request Version: 1
OCSP Request Requester Name: null
    Cert Id:
```

```
        Hash Algorithm: SHA (1.3.14.3.2.26)
        Issuer Name Hash: A0:D2:4D:07:E7:34:A6:4A:5A:4B:09:AB:D4:58:1B:ED:49:1B:81:D4
        Issuer Key Hash: A0:D2:4D:07:E7:34:A6:4A:5A:4B:09:AB:D4:58:1B:ED:49:1B:81:D4
        Serial No: 6541508541959342484 (5ac81b5c4aab8994)
Full Request Extensions:
        Nonce: 04:13:30:2E:30:34:32:35:38:33:37:37:33:39:34:34:34:38:30:32:31
```

12.5.2 OCSP respons

De OCSP responses bevatten de volgende informatie:

- De informatie uit het request waarmee het certificaat is gespecificeerd;
- De status: `good`, `revoked` of `unknown`;
- Drie tijdstippen:
    - Moment van aanmaken OCPS response (produced at)
    - Moment waarop de status is vastgesteld (this update)
    - Moment tot waarop de client op deze informatie kan steunen (nextupdate)
- ondertekening van de response op basis van hetzelfde ~~sha256WithRSAEncryption~~ algoritme als gebruikt wordt voor ondertekening van certificaten;
- De nonce zoals opgenomen in het request.
- Drie certificaten van de OCPS responder, het betreffende TSP CA certificaat en het PKIoverheid domein CA certificaat.

Hieronder is de logging van een OCSP response beknopt opgenomen.

To do: vervangen door response na implementatie productieomgeving

```
OCSP Response Status: successful 0
OCSP Response Bytes Response Type: OBJECT ID = id-pkix-ocsp-basic
Basic Response Data Version: 1
Basic Response Data Responder Id: byKey:
17:94:F4:66:5C:2F:FF:F6:2F:B7:EC:33:7F:86:9B:56:B4:30:83:55
Basic Response Data Produced At: Tue Dec 01 15:04:42 GMT 2020
Basic Response Data Responses:
    Cert Id:
        Hash Algorithm: SHA (1.3.14.3.2.26)
        Issuer Name Hash: A0:D2:4D:07:E7:34:A6:4A:5A:4B:09:AB:D4:58:1B:ED:49:1B:81:D4
        Issuer Key Hash: A0:D2:4D:07:E7:34:A6:4A:5A:4B:09:AB:D4:58:1B:ED:49:1B:81:D4
        Serial No: 6541508541959342484 (5ac81b5c4aab8994)
    Cert Status: good
    This Update: Tue Dec 01 15:04:42 GMT 2020
    Next Update: Thu Dec 03 15:04:42 GMT 2020
Basic Response Signature Algorithm: sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Basic Response Signature:
9D:1E:48:39:AB:93:80:CC:40:A1:0C:86:9B:69:E9:D4:3A:91:06:02:B3:40:D1:F0:15:08:96:CD:1C:91
:B5:DE:7C:E2:9D:D6:5F:26:C0:BC:0A:CA:05:E0:E8:3A:44:01:5C:1B:3D:EC:82:2C:0A:00:21:04:4E:C
1:8B:39:D5:3E:F6:EB:AA:97:5A:EB:B0:65:B2:CE:12:17:61:9C:21:8A:4F:FA:97:74:EE:D1:30:EF:20:
58:04:2A:77:6F:42:A8:0E:F8:ED:CD:F2:30:F2:3B:06:64:94:2E:7A:4E:D2:BD:80:59:C0:88:54:61:A6
:CD:7A:EB:26:03:51:78:F7:23:4D:C2:1D:86:E6:4B:78:F1:65:F5:A8:FC:C5:2D:16:A5:97:4B:A3:63:1
9:F0:39:EA:87:9E:94:A2:08:01:DD:9C:E9:35:3C:C9:3F:01:64:CF:B6:8B:8E:DA:59:56:35:B0:92:08:
22:C9:E1:28:EF:34:2E:69:7F:68:6F:87:80:83:0F:26:81:A8:BE:09:52:69:5F:3F:E3:6B:67:D5:A2:CE
:B0:40:12:E7:39:D9:D6:FD:AF:F5:8D:6D:26:E8:86:09:99:20:02:50:5C:C1:95:13:53:D1:D8:D8:02:7
C:98:B3:15:F8:89:DF:BE:4B:C0:45:6B:73:80:E7:52:92:C0:6F
Basic Response Extensions:
    Nonce: 30:2E:30:34:32:35:38:33:37:37:33:39:34:34:34:38:30:32:31
```

```
Certificate:
Version: 3
Serial number: 418292658575116243012668419046288185857809369287
Signature algorithm: sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer: CN=UZI-register Medewerker op naam CA G3,2.5.4.97=NTRNL-50000535,O=CIBG,C=NL
Valid not before: Thu Jul 16 10:30:16 GMT 2020
      not after: Fri Jul 16 10:30:16 GMT 2021
Subject: CN=OCSP responder UZI-register Medewerker op naam CA G3,O=CIBG,C=NL
```

```
Certificate:
Version: 3
Serial number: 210856240016418662923104299514615549886949161115
Signature algorithm: sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer: CN=Staat der Nederlanden Organisatie Persoon CA - G3,O=Staat der Nederlanden,C=NL
Valid not before: Thu Apr 18 08:15:14 GMT 2019
      not after: Sun Nov 12 00:00:00 GMT 2028
Subject: CN=UZI-register Medewerker op naam CA G3,2.5.4.97=NTRNL-50000535,O=CIBG,C=NL
```

```
Certificate:
Version: 3
Serial number: 10003014
Signature algorithm: sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer: CN=Staat der Nederlanden Root CA - G3,O=Staat der Nederlanden,C=NL
Valid not before: Thu Nov 14 15:09:37 GMT 2013
      not after: Sun Nov 12 23:00:00 GMT 2028
Subject: CN=Staat der Nederlanden Organisatie Persoon CA - G3,O=Staat der
Nederlanden,C=NL
```