CIBG
Ministerie van Volksgezondheid, Welzijn en Sport

CA model, Pasmodel, Certificaat- en CRL-profielen

Zorg CSP (productieomgeving)

Versie : 10.0

Datum : 25 maart 2020
Status : Definitief
Bestandsnaam : 20200325 CA model pasmodel certificaatprofielen v10_0.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*. 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 programma van eisen (PvE) van PKI voor de Overheid is het normatieve kader voor de certificaat- en CRL-profielen. In het PvE zijn de referenties opgenomen naar standaardisatiedocumenten vanuit ISO/ITU (bijv. X.509), IETF in de vorm van RFC’s en ETSI (met name voor het Qualified Certificate Profile).

1.4 Versie historie

Versie	Datum	Status	Omschrijving
7.1	5 juli 2016	Definitief	Aanpassingen vanwege PvE wijzigingen: - PvE delen (tabel 5) - PvE 331 KeyAgreement servercertificaten verwijderd - PvE 332 UserNotice UTF8String ipv Printable String - PvE 333 QcStatement + link PKI Disclosure Statement - PvE 341 BasicContstraints (opmerking correcte codering) - PvE 342 Extended KeyUsages - Emailadres is niet meer in gebruik bij servercertificaten en is verwijderd.
8.0	10 oktober 2016	Intern	Uitfasering G2: - Passen naar PKIoverheid public Root G3 - Servercertificaten naar PKIoverheid private Root G1 - CPS URI G3/G1 gewijzigd naar https://www.zorgcsp.nl/ - Wijzigingen organisatienaam in CIBG - authorityInfoAccess.CAissuer ook toegevoegd in eindcertificaten
9.0	18 januari 2017	Definitief	Aanpassingen: - door afwijzing wijzigingsverzoek voor PathLenConstraint = 1 is het CA model aangepast naar een model met 3 lagen CA's. - subject.organizationalIdentifier encoded als UTF-8 - alle URL's van CA certificaten verwijzen naar https://cert.pkioverheid.nl/ - update Extended KeyUsages conform PvE versie v4.3 - Toevoeging Subject.Surname en Subject.givenName (PvE change 347)
9.1	21 februari 2017	Definitief	Aanpassingen: - PvE spoedchange 356: Emailprotection EKU toegevoegd in alle authenticiteit- en handtekeningcertificaten (passen). Tabel 22, 23, 25, 26 en 28.
9.2	24 februari 2017	Definitief	Aanpassingen: - Redactionele wijzigingen: URL's en OID's zoveel mogelijk ingevuld in de tabellen met profielen ter verbetering leesbaarheid. - Verwijderd subject.organizationIdentifier in OCSP signer certificate profile (tabel 34)
9.3	16 maart 2017	Review	Aanpassingen: - PvE wijziging 358, subject.organisationIdentifier + QcStatement Medewerkerpas niet op naam (alleen voor G3) - PolicyIdentifier waarden uitgeschreven in OCSP profiel (tabel 34) inclusief aanpassing Policy OID voor G3 CA's in domein organisatie persoon.
9.5	16 aug. 2017	Definitief	Aanpassing: - PolicyIdentifier waarde in OCSP profiel (tabel 34) voor G3/G1 aangepast op basis van PvE versie 4.5 d.d. 1 juli 2017. - Expliciete vermelding dat UPN niet is opgenomen in handtekening- en vertrouwelijkheidcertificaten (par. 6.2). - In tabel 28 opmerking over stop uitgifte Medewerkerpas niet op naam vanaf 1 juli 2017 tot implementatie van PvE wijziging 358.
9.5a	5 sep. 2018	Definitief	Aanpassing: - Verwijderd in tabel 28 opmerking over stop uitgifte Medewerkerpas niet op naam vanaf 1 juli 2017. - Typo tabel 23 en 26: ... EU Verordening 910/2015 -> 910/2014
9.6	26 april 2019	Definitief	Aanpassing: - De lengte van certificate serialnumbers in eindgebruikercertificaten is expliciet opgenomen: 160 bits in productie per 10 mei 2019. - update calssuer URL i.v.m. resigning CA's voor passen. Change in productie per 1 juni 2019 (Tabel 19) - Fingerprints toegevoegd van de G1 CA certificaten (Tabel 21)
10.0	25 maart 2020	Definitief	Aanpassing: - Verwijdering SHA-2/G21 generatie; - Toegevoegd ExpiredCertsOnCRL

Tabel 1 Versie historie

2 CA model

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

2.1 CA model Public G3/Private G1 generatie

2.1.1 Algemene ontwerpkeuzes

Bij uitfasering van de SHA-2 (G21) hiërarchie is besloten om:

1. passen uit te gaan geven onder de publiek vertrouwde G3 Root van PKIoverheid (Public G3);
2. servercertificaten uit te geven onder de private Root CA G1 van PKIoverheid (Private G1). Onder deze private Root is het mogelijk om de zogenaamde subjectAltName.otherName te blijven gebruiken[1].

PKIoverheid heeft een nieuwe Staat der Nederlanden Root CA G3 en bijbehorende domein CA's gecreëerd. Bij invoering van deze G3 omgeving heeft Logius besloten om een apart domein voor services certificaten in te richten. Services certificaten zijn onder de Root CA G2 nog onderdeel van het domein Organisatie waaronder ook persoonsgebonden certificaten worden uitgegeven. Onder G3 zijn er aparte domein CA's gecreëerd voor persoonsgebonden en services certificaten.

Daarnaast heeft Logius een Private Root CA gecreëerd. Deze heeft als volgnummer G1 aangezien het de eerste private omgeving is.

In de G3 omgeving is de term 'CSP' vervangen door 'TSP' (Trust Service Provider) in lijn met de eIDAS verordening. De term 'TSP' komt niet in het CA certificaat voor in overleg met -en na goedkeuring van- de PA PKIoverheid om de herkenbaarheid van de producten zo duidelijk mogelijk te houden. In dit document is verder nog de term 'CSP' gebruikt.

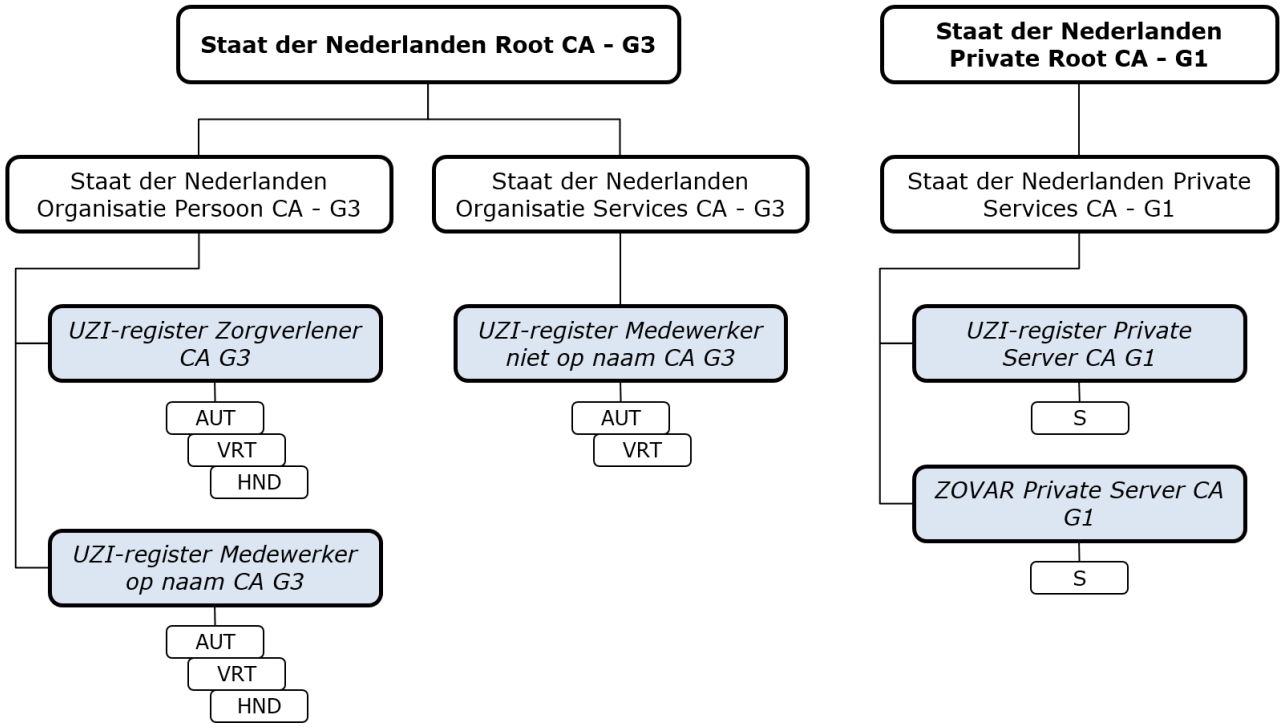
Met de invoering van G3 heeft Logius besloten om een PathLenConstraint van 0 te hanteren in alle CSP certificaten. Dit betekent dat de Zorg CSP scheiding tussen de verschillende producten moet realiseren door 5 CSP CA certificaten aan te vragen onder de domein CA's van PKIOverheid.

Door het besluit om passen en servercertificaten onder verschillende nieuwe Root CA certificaten uit te gaan geven, zijn er twee volledig nieuwe CA hiërarchieën die los van elkaar staan.

De volgende figuur geeft het CA model weer voor de productieomgeving van de Zorg CSP waarin de bovenstaande ontwerpkeuzes zijn verwerkt. De naamgeving (subject.CommonName in de betreffende CA certificaten) van de CA's is conform Figuur 2. De naamgeving is Case Sensitive. Cursief en lichtgrijs zijn de CA's weergegeven die de eindgebruikercertificaten ondertekenen.

Voor de volledigheid zijn ook de verschillende typen eindgebruikercertificaten opgenomen:
- AUT: Authenticiteitcertificaat;
- VRT: Vertrouwelijkheidcertificaat;
- HND: Handtekeningcertificaat;
- S: Servercertificaat.

[1] Die bevat noodzakelijke informatie voor toepassingen in het zorgveld (o.a. LSP en SBV-Z). Aangezien dit nagenoeg altijd systeem-systeem koppelingen zijn, is het mogelijk om de private Root CA G1 te gaan gebruiken.



Figuur 1: CA model productieomgeving Zorg CSP generatie Public G3/Private G1

2.1.2 Cryptografische algoritmen en sleutellengten

De Public G3/Private G1 hiërarchie gebruikt de volgende algoritmen:

'SHA256 with RSA Encryption' als het signing algorithm voor alle certificaten en CRL's.

Het algoritme is als volgt gespecificeerd:

```
OBJECT IDENTIFIER '1 2 840 113549 1 1 11'
{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)
sha256WithRSAEncryption(11)}
```

In het certificaat staat deze OID twee keer:

```
Certificate.signatureAlgorithm          1.2.840.113549.1.1.11
tbsCertificate.signature                1.2.840.113549.1.1.11
```

LET OP: het SHA-1 algoritme wordt nog wel gebruikt voor berekening van de zogenaamde key-identifiers in de certificaten. Dit zijn hashes van bijvoorbeeld de public key in het certificaat.

De Public G3/Private G1 hiërarchie gebruikt de volgende **RSA sleutellengten**:

Certificaat	RSA sleutellengte (bits)
Stamcertificaat	4096
Domeincertificaat	4096
CSP certificaat	4096
sub-CA certificaat	4096
Eindgebruikercertificaat	2048

Tabel 2 RSA sleutellengtes in Public G3/Private G1 generatie

2.1.3 Geldigheidsduur

De volgende tabel geeft een overzicht van de geldigheidsduur van de Public G3/Private G1 hiërarchie.

Certificaat	Geldig tot
Stamcertificaat	14 november 2028
Domeincertificaat	13 november 2028
CSP certificaten	12 november 2028
Eindgebruikercertificaat	Ongewijzigd: 3 jaar (Of uiterlijk tot einde geldigheid ondertekenend CSP CA certificaat.)

Tabel 3 Levensduur certificaten Public G3/Private G1 hiërarchie

Met de overgang naar de Public G3/Private G1 hiërarchie is de organisatienaam gewijzigd in 'CIBG'. Zie verder par. 5.3.

2.2 Domein PKI-overheid

Bij de invoering van de Public G3/Private G1 hiërarchie zijn de domeinen als volgt aangepast:
- Domein Organisatie Persoon: Zorgverlener en Medewerker op naam passen;
- Domein Organisatie Services: Medewerker niet op Naam passen;
- Domein Private Services: UZI-register en ZOVAR servercertificaten.

Dit komt in de gebruikerscertificaten tot uitdrukking in:
- Nieuwe waarden voor de OID Policyldentifier in de servercertificaten van de Private G1 generatie. Zie par. 4.6.1.

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. 4.8):

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	**Zorgverlener-pas**	**Medewerkerpas op naam**	**Medewerkerpas niet op naam**	**UZI-register Servercertificaat**	**ZOVAR Servercertificaat**
Certificaten	A,H,V	A,H,V	A,V	Gecombineerd A,V	Gecombineerd A,V
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 (CSP) CA (G3/G1)	UZI-register Zorgverlener CA G3	UZI-register Medewerker op naam CA G3	UZI-register Medewerker niet op naam CA G3	UZI-register Private Server CA G1	ZOVAR Private Server CA G1
Certificate Policy (Public G3/Private G1)	PvE deel 3a: Certificate Policy - Domein Organisatie Persoon (g3)		PvE deel 3b: CP auth.- en vertr. certificaten - Organisatie Services (g3)	PvE deel 3h: Certificate Policy Server Certificaten – Domein Private Services	

Tabel 5 Overzicht kenmerken producten Zorg CSP

Toelichting op de tabel:

Certificaten — Alle passen bevatten sleutelparen en certificaten voor authenticiteit (A) en vertrouwelijkheid (V). Een deel van de passen bevat sleutelparen en certificaten voor de handtekening (H).
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 hier naar 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.

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. 4.8.

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 E-mail adres

In het certificaatprofiel voor het UZI-register is geen E-mail adres opgenomen. Dit maakt het mogelijk de UZI-pas voor secure e-mail te gebruiken in combinatie met meerdere emailadressen én voorkomt 'spam' door het indirect bekend maken van emailadressen via de openbare directory met certificaten.

Er is getest of Microsoft Outlook het juiste certificaat selecteert gelet op de functie van het certificaat en de geadresseerde of afzender waarbij de instellingen worden gedaan zoals beschreven in Microsoft Knowledge Base Article – 276597 (How to Turn Off E-mail Matching for Certificates). Conclusie is dat het met de juiste registry settings mogelijk is om de UZI-pas te gebruiken met Outlook zonder E-mail adres in het certificaat. Voor de (Windows/Outlook) gebruikers van de UZI-pas vereist dit wel de juiste configuratie van de registry.

4.5 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. 4.8) 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.

4.6 Waarden van certificatePolicies extensie

De volgende waarden voor certificatePolicies extensie zullen worden geconfigureerd.

4.6.1 certificatePolicies.policyIdentifier

CSP en CA-certificaten generatie Public G3/Private G1

In alle CA certificaten (m.u.v. de Root CA certificaten) zijn de policyIdentifiers opgenomen zoals die zijn gespecificeerd in het Programma van Eisen.

Gebruikercertificaten

Tabel 7 geeft een overzicht PolicyIdentifiers (OID's). Deze zijn per beveiligingsfunctie voor alle persoonsgebonden pastypen gelijk. Uitzonderingen zijn de Servercertificaten die een gecombineerd authenticiteit- en vertrouwelijkheidcertificaat heeft en de Medewerkerpas niet op naam die onder het CP Services valt.

Naam UZI-pastype	OID (PolicyIdentifier)	Omschrijving
Authenticiteitcertificaten: • Zorgverlenerpas • Medewerkerpas op naam	2.16.528.1.1003.1.2.5.1	OID van de PKI-overheid Certificate Policy voor authenticiteitscertificaten in het domein organisatie.
Onweerlegbaarheidcertificaten • Zorgverlenerpas • Medewerkerpas op naam	2.16.528.1.1003.1.2.5.2	OID van het CP voor onweerlegbaarheid in domein organisatie.
Vertrouwelijkheidcertificaten • Zorgverlenerpas • Medewerkerpas op naam	2.16.528.1.1003.1.2.5.3	OID van het CP voor vertrouwelijkheid in domein organisatie.
Authenticiteitcertificaten • Medewerkerpas niet op naam	2.16.528.1.1003.1.2.5.4	Domein organisatie CP Services Authenticiteit
Vertrouwelijkheidcertificaten • Medewerkerpas niet op naam	2.16.528.1.1003.1.2.5.5	Domein organisatie CP Services Vertrouwelijkheid
UZI-register Servercertificaat	2.16.528.1.1003.1.2.8.6	Domein Private services (g1): Server
ZOVAR Servercertificaat	2.16.528.1.1003.1.2.8.6	Domein Private services (g1): Server

Tabel 7 Waarden PolicyIdentifier voor gebruikercertificaten Public G3/Private G1

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

CSP en CA-certificaten

Voor het CSP certificaat en alle CA certificaten: **géén User Notice**.

Gebruikercertificaten

Vanaf 1 januari 2011 is de volgende User Notice opgenomen:
Het toepassingsgebied van dit certificaat is beperkt tot communicatie binnen het domein Organisatie zoals aangegeven in het Programma van Eisen van de PKI voor de Overheid. Zie www.logius.nl

Aanpassing n.a.v. PvE wijziging 332: De userNotice.explicitText moet als UTF8String worden encoded. (Voordat deze wijziging is doorgevoerd, was de userNotice.explicitText als BMPString encoded.)

4.6.3 certificatePolicies.PolicyQualifier.cPS.uri

CA certificaten

In de CA Certificaten van de Public G3/Private G1 generatie is de link naar het PKIoverheid CPS opgenomen aangezien deze CA certificaten zijn uitgegeven door Logius:
https://cps.pkioverheid.nl

Gebruikercertificaten UZI-register generatie Public G3/Private G1

In de gebruikercertificaten is bij de generatie Public G3/Private G1 de volgende certificatePolicies.PolicyQualifier.cPS.uri opgenomen:
https://www.zorgcsp.nl/cps/uzi-register.html

Gebruikercertificaat ZOVAR generatie Private G1

In de ZOVAR Servercertificaten is bij generatie Public G3/Private G1 de volgende certificatePolicies.PolicyQualifier.cPS.uri opgenomen:
https://www.zorgcsp.nl/cps/zovar.html

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

Naar aanleiding van PvE wijziging 333 is de QcStatement extensie uitgebreid met onder andere 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 V1.1.1 (2016-02), 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/pds/pds.html

4.7 Waarden cRLDistributionPoints.distributionPoint.fullName

4.7.1 CA certificaten Zorg CSP

Door het gebruik van meerdere domein CA certificaten zijn er bij de CA certificaten van de Public G3/Private G1 generatie verschillende CRL's in gebruik. De volgende tabel geeft een overzicht van de CDP's van de Public G3/Private G1 generatie CA certificaten.

CA	CRL Distribution Point
UZI-register Zorgverlener CA G3	http://crl.pkioverheid.nl/DomOrganisatiePersoonLatestCRL-G3.crl
UZI-register Medewerker op naam CA G3	http://crl.pkioverheid.nl/DomOrganisatiePersoonLatestCRL-G3.crl
UZI-register Medewerker niet op naam CA G3	http://crl.pkioverheid.nl/DomOrganisatieServicesLatestCRL-G3.crl
UZI-register Private Server CA G1	http://crl.pkioverheid.nl/DomPrivateServicesLatestCRL-G1.crl
ZOVAR Private Server CA G1	http://crl.pkioverheid.nl/DomPrivateServicesLatestCRL-G1.crl

Tabel 8 CRL Distribution points in CA certificaten Zorg CSP generatie Public G3/Private G1

4.7.2 Gebruikercertificaten Productieomgeving

De volgende tabel geeft het overzicht van de CDP's per pastype in de Productieomgeving van de Public G3/Private G1 generatie.

Naam pastype	CRL Distribution Point
Zorgverlenerpas	http://www.csp.uzi-register.nl/cdp/uzi-register_zorgverlener_ca_g3.crl
Medewerkerpas op naam	http://www.csp.uzi-register.nl/cdp/uzi-register_medewerker_op_naam_ca_g3.crl
Medewerkerpas niet op naam	http://www.csp.uzi-register.nl/cdp/uzi-register_medewerker_niet_op_naam_ca_g3.crl
UZI-register Servercertificaat	http://www.csp.uzi-register.nl/cdp/uzi-register_private_server_ca_g1.crl
ZOVAR Servercertificaat	http://www.csp.zovar.nl/cdp/zovar_private_server_ca_g1.crl

Tabel 9 CRL Distribution points in gebruikercertificaten Zorg CSP generatie Public G3/Private G1

4.8 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. 4.8.1) en vervolgens de samenstelling van de waarde (par. 4.8.3 voor het UZI-register en 4.8.4 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. 4.8.1.

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. 4.8.3 voor het UZI-register en in par. 4.8.4 voor ZOVAR.

4.8.1 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}).

4.8.2 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 binnen het domein organisatie.

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 10 <OID CA> in gebruikerscertificaten Zorg CSP

4.8.3 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**	De Vektis AGB-Code. Zie par. 4.5.

Veld	Type	Waarde	Toelichting
		AGB-code van de abonnee voor Medewerkerpas op naam, Medewerkerpas niet op naam, UZI-register Servercertificaat: **OF** '00000000' indien niet opgegeven in aanvraag.	

Tabel 11 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 G3)
- <versie-nr> = 1
- <UZI-nummer> = 123456789
- <pastype> = Z (Zorgverlenerpas)
- <Abonnee-nr> = 12345678 (kan zowel een abonnee type organisatie als een abonnee type zorgverlener identificeren)
- <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 G3)
- <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 G3)
- <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 Private Server CA G1)
- <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

4.8.4 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 12 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 Private Server CA G1)
- <versie-nr> = 1
- <subject-nr> = 8643123456789
- <pastype> = V
- <UZOVI-nr> = 8643 (uniek identificerend nummer van de zorgverzekeraar.)
- <Erkenning> = ZV

4.9 Smartcard logon

Binnen PKI voor de Overheid is het mogelijk om het certificaatprofiel voor het authenticatiecertificaat aan te passen zodat het bruikbaar is voor smartcard logon in Windows omgevingen. Van deze mogelijkheid zal gebruikt gemaakt gaan worden in de UZI-passen waarvan de certificaten uitgegeven worden door de CA's vanaf de tweede generatie. Dit vereist de volgende wijzigingen van het certificaatprofiel:

1. Toevoegen Entended Key Usage attribuut
   Dit is een standaard attribuut dat voor ieder authenticatiecertificaat identiek zal zijn.
2. Uitbreiding subject.AltName attribuut
   Hierin dient in een extra otherName de Microsoft UPN (User Principal Name) toegevoegd te worden in het formaat 'gebruiker@domein'. Het UZI-register zal dit ondersteunen door het opnemen van
   <UZI-nummer>@<abonneenummer>

Deze invulling van de UPN is mogelijk omdat bij de Microsoft implementatie noch het gebruikerdeel, noch het abonneedeel enige relatie hoeft te hebben met een daadwerkelijke gebruikersnaam, respectievelijk domeinnaam. Beide delen zijn vrij in te vullen karakterreeksen. Microsoft's enige voorwaarde is dat elke UPN uniek is binnen een Domain Forest. Aan deze voorwaarde wordt voldaan: het UZI-nummer is uniek voor een persoon of medewerker niet op naam pas. Het abonneenummer is uniek voor de abonnee.

Uiteraard moet in de lokale Active Directory infrastructuur de relatie gelegd worden van de nummers naar een specifiek gebruikersaccount. In een Proof of Concept is aangetoond dat het beschikbaar maken van een abonnee nummer als domain een standaard actie is binnen active directory: het toevoegen van een user principal name suffix. Zie Microsoft technet artikel:
Add user principal name suffixes: http://technet2.microsoft.com/windowsserver/en/library/c61f2430-fcc3-41fd-b722-20cb11e1bf021033.mspx?mfr=true
Ook het aanpassen van de gebruikersnaam in <UZI-nummer> is standaard account beheer in Active Directory.
Voordelen van deze invulling van de UPN zijn:

- De nummers zijn nu al opgenomen in het certificaat en dus beschikbaar zonder wijziging in de interfaces tussen de systemen;
- 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.

5 Profiel CA certificaten

5.1 CA certificaatprofiel CSP CA

Deze paragraaf beschrijft de inhoud van de CSP 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/. Het certificaatprofiel is dus bepaald door Logius. 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. In de generatie Public G3/Private G1 zijn de CSP CA certificaten ook direct de issuing CA's van de eindgebruikercertificaten.

PROFIEL CA certificaat CSP CA/CA's				
Certificaatveld / attribuut	OID	Critical	Waarde	Omschrijving / Toelichting
tbsCertificate				
subject.countryName (C)			NL	PrintableString
subject.commonName (CN)			*Public G3/Private G1 generatie afhankelijk van domein:* • UZI-register Zorgverlener CA G3 • UZI-register Medewerker op naam CA G3 • UZI-register Medewerker niet op naam CA G3 • UZI-register Private Server CA G1 • ZOVAR Private Server CA G1	UTF8String
subject.organizationIdentifier			*Public G3/Private G1 generatie:* NTRNL-50000535	Encoded als UTF-8 string. Zie par. 5.3.
subject.organizationName (O)			*Public G3/Private G1 generatie:* CIBG	UTF8String
Standard Extension				
certificatePolicies.PolicyQualifier.cPS.uri			*Public G3/Private G1 generatie:* https://cps.pkioverheid.nl	Dit attribuut bevat de URL voor het Certificate Practice Statement van PKIoverheid (Public G3/Private G1). Zie. Par. 4.6.

Tabel 13 Profiel CSP CA certificaat

De sleutellengte is RSA 4096 bits. De geldigheidsduur is gespecificeerd in par. 2.1.

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. Vanaf de Public G3/Private G1 hiërarchie is er een verwijzing opgenomen vanuit de certificaten naar de Issuing CA die het (CA) certificaat heeft ondertekend.

Naam CA	URL's naar CA certificaat
Staat der Nederlanden Root CA - G3	http://cert.pkioverheid.nl/RootCA-G3.cer
Staat der Nederlanden Organisatie Persoon CA - G3	http://cert.pkioverheid.nl/DomOrganisatiePersoonCA-G3.cer
UZI-register Zorgverlener CA G3	tot en met 31 mei 2019: http://cert.pkioverheid.nl/UZI-register_Zorgverlener_CA_G3.cer na resigning, in productie per 1 juni 2019: http://cert.pkioverheid.nl/20190418_UZI-register_Zorgverlener_CA_G3.cer
UZI-register Medewerker op naam CA G3	tot en met 31 mei 2019: http://cert.pkioverheid.nl/UZI-register_Medewerker_op_naam_CA_G3.cer na resigning, in productie per 1 juni 2019: http://cert.pkioverheid.nl/20190418_UZI-register_Medewerker_op_naam_CA_G3.cer
Staat der Nederlanden Organisatie Services CA - G3	http://cert.pkioverheid.nl/DomOrganisatieServicesCA-G3.cer
UZI-register Medewerker niet op naam CA G3	tot en met 31 mei 2019: http://cert.pkioverheid.nl/UZI-register_Medewerker_niet_op_naam_CA_G3.cer na resigning, in productie per 1 juni 2019: http://cert.pkioverheid.nl/20190418_UZI-register_Medewerker_niet_op_naam_CA_G3.cer

Tabel 14 URL's van CA certificaten generatie Public G3

Naam CA	URL's naar CA certificaat
Staat der Nederlanden Private Root CA - G1	http://cert.pkioverheid.nl/PrivateRootCA-G1.cer
Staat der Nederlanden Private Services CA - G1	http://cert.pkioverheid.nl/DomPrivateServicesCA-G1.cer
UZI-register Private Server CA G1	http://cert.pkioverheid.nl/UZI-register_Private_Server_CA_G1.cer
ZOVAR Private Server CA G1	http://cert.pkioverheid.nl/ZOVAR_Private_Server_CA_G1.cer

Tabel 15 URL's van CA certificaten generatie Private G1

De Private G1 omgeving is niet standaard opgenomen in de Operating Systemen of certificate stores van applicaties. De juistheid van deze private CA certificaten is met behulp van volgende tabel vast te stellen op basis van de zogenaamde 'thumbprint'. Dit is de SHA-1 hash-waarde van het certificaat en deze is met de standaard Microsoft certificate viewer als volgt te verifiëren:

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

De officiële gegevens van de Private Root CA G1 zijn gepubliceerd in Staatscourant Nr. 6676 d.d. 12 maart 2015.

Naam CA	SHA-1 thumbprint CA certificaat
Staat der Nederlanden Private Root CA - G1	c6 c1 bb c7 1d 4f 30 c7 6d 4d b3 af b5 d0 66 de 49 9e 9a 2d
Staat der Nederlanden Private Services CA - G1	03 67 7b 4e c0 ff ca 9d 3c ad 6c 04 4a 73 3b 3e 7a 75 d1 fd
UZI-register Private Server CA G1	87 0c a5 9f 98 4d cd f0 eb c1 43 b7 3f 7c 88 9a ad 4a 0f b5
ZOVAR Private Server CA G1	79 21 e6 3a 45 64 26 08 b5 72 2f 1e fe 0e ea 7d 4b 80 ac 7f

Tabel 16 Thumbprints van CA certificaten van generatie Private G1

5.3 OrganizationIdentifier en naamgeving CSP organisatie

Met de invoering van de Public G3/ Private G1 hiërarchie is in de CA certificaten een nieuw attribuut toegevoegd n.a.v. PvE wijziging 340 die samenhangt met ETSI EN 319 412. Dit is de organizationIdentifier waarvan de syntax gespecificeerd is in paragraaf 5.1.4 van ETSI EN 319 412-1. Deze identifier komt op de volgende plaatsen terug in de certificaten:

- als subject.organizationIdentifier in het CSP CA certificaat;
- als issuer.organizationIdentifier en subject.organizationIdentifier in de sub CA certificaten;
- als issuer.organizationIdentifier in de eindgebruikercertificaten.

In de certificaten van de ZorgCSP is vanaf de Public G3/Private G1 hiërarchie de volgende organiszationIdentifier opgenomen: **NTRNL-50000535**

Waarbij:

- **NTR** aangeeft dat het een National Trade Register identifier betreft;
- **NL** het land aangeeft;
- En na de minus het KvK nummer van CIBG is opgenomen: **50000535**.

Met de overgang naar de Public G3/Private G1 hiërarchie is de officiële organisatienaam die is opgenomen in de certificaten gewijzigd in **CIBG**.

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.
signature			1.2.840.113549.1.1.11	VAST	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: sha256WithRSAEncryption
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		*Public G3/Private G1 generatie:* CIBG	VAST	Dit attribuut bevat de officiële organisatienaam van de uitgevende CSP.
issuer.organizationIdentifier			*Public G3/Private G1 generatie:* NTRNL-50000535		Encoded als UTF-8 string. Zie par. 5.3.
issuer.commonName	CN		*Generatie Public G3:* UZI-register Zorgverlener CA G3	VAST	Dit attribuut bevat de volledige naam van de uitgevende CA.
validity.notBefore			UTCTime waarop het certificaat is ondertekend.	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).
Subject					Deze attributen vormen samen de *distinguished name* van certificaathouder.

PROFIEL AUTHENTICITEITCERTIFICAAT Zorgverlenerpas					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
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 vanaf CIBG3 omgeving medio 2013.
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.
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.
subjectPublicKeyInfo.algorithm			rsaEncryption	VAST	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden.
subjectPublicKeyInfo. subjectPublicKey			RSA sleutel van certificaathouder:2048 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			2.16.528.1.1003.1.2.5.1	VAST	Dit attribuut identificeert de CP van de PKI overheid voor het relevante certificaat profiel (beveiligingsfunctie en domein). Zie. Par. 4.6.
certificatePolicies.PolicyQualifier. cPS.uri			*Public G3/Private G1 generatie:* https://www.zorgcsp.nl/cps/uzi-register.html	VAST	Dit attribuut bevat de URL voor het Certificate Practice Statement van het UZI-register. Zie. Par. 4.6.
certificatePolicies.PolicyQualifier. userNotice.explicitText			Het toepassingsgebied van dit certificaat is beperkt tot communicatie binnen het domein Organisatie zoals aangegeven in het Programma	VAST	In de user notice worden (een samenvatting van) de gebruikersvoorwaarden geplaatst c.q. waar die te vinden zijn. Zie. Par. 4.6. Encoded als UTF8String.

PROFIEL AUTHENTICITEITCERTIFICAAT Zorgverlenerpas					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
			van Eisen van de PKI voor de Overheid. Zie www.logius.nl		
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		Extensie aanwezig vanaf Public G3 hiërarchie.
.uniformResourceIndicator			*Public G3/Private G1 generatie:* http://cert.pkioverheid.nl/UZI-register_Zorgverlener_CA_G3.cer vanaf 1 juni 2019: http://cert.pkioverheid.nl/20190418_UZI-register_Zorgverlener_CA_G3.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 subject	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) document Signing (OID 1.3.6.1.4.1.311.10.3.12) EmailProtection (OID 1.3.6.1.5.5.7.3.4)	VAST	- clientAuth: certificaat bruikbaar voor client authenticatie - documentSigning: bruikbaar voor ondertekening documenten - EmailProtection: bruikbaar voor ondertekening van e-mail berichten
CRLDistributionPoints. distributionPoint.fullName	{id-ce 31}		*Public G3/Private G1 generatie:* http://www.csp.uzi-register.nl/cdp/uzi-register_zorgverlener_ca_g3.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. 4.7.
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. 4.8.	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			1.2.840.113549.1.1.11	VAST	Dit attribuut specificeert het algoritme waarmee de handtekening onder het certificaat is gezet: sha256WithRSAEncryption
signatureValue			Handtekening van CA over het tbsCertificate.	Variabel	

Tabel 17 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;
- tbsCertificate.extensions.certificatePolicies: PKIoverheid heeft een aparte OID en CP 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 is uitgebreid door PvE wijziging 333 die samenhangt met EU Verordening 910/2014. Het 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 V2.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.*
- Vanaf invoering van PvE wijziging 342 is er een Extended KeyUsage opgenomen in het handtekeningcertificaat.
- Handtekeningcertificaten (en vertrouwelijkheidcertificaten) bevatten geen UPN in subjectAltName.otherName.

PROFIEL HANDTEKENINGCERTIFICAAT ZORGVERLENERPAS				
Certificaatveld / attribuut	OID	Critical	Waarde	Omschrijving / toelichting
Certificate				
tbsCertificate				
subjectPublicKeyInfo. subjectPublicKey			RSA sleutel van certificaathouder: • 2048 bits	
Standard Extension				
certificatePolicies	{id-ce 32}			
certificatePolicies.PolicyIdentifier			2.16.528.1.1003.1.2.5.2	Dit attribuut identificeert de CP van de PKI overheid voor het relevante certificaat profiel (beveiligingsfunctie en domein). Zie. Par. 4.6.
keyUsage	{id-ce 15}	TRUE	NonRepudiation	
extKeyUsage	{id-ce 37}		document Signing (OID 1.3.6.1.4.1.311.10.3.12) EmailProtection (OID 1.3.6.1.5.5.7.3.4)	
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 uitgifte van gekwalificeerd certificatat overeenstemt met annex I van EU Verordening 910/2014.

PROFIEL HANDTEKENINGCERTIFICAAT ZORGVERLENERPAS				
Certificaatveld / attribuut	OID	Critical	Waarde	Omschrijving / toelichting
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) overeenstemmend met annex II van EU Verordening 910/2014.
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. 4.6.4.
.language			'en'. Encoded als PrintableString	Codering van taal van PDS.

Tabel 18 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. Deze verschillen zijn gelijk aan de lijst genoemd in par. 6.2. Daarnaast geldt dat vertrouwelijkheidcertificaten geen QcStatement bevatten.

PROFIEL VERTROUWELIJKHEIDCERTIFICAAT ZORGVERLENERPAS				
Certificaatveld / attribuut	OID	Critical	Waarde	Omschrijving / toelichting
Certificate				
tbsCertificate				
subjectPublicKeyInfo. subjectPublicKey			RSA sleutel van certificaathouder: • 2048 bits	
Standard Extension				
CertificatePolicies	{id-ce 32}			
certificatePolicies.PolicyIdentifier			2.16.528.1.1003.1.2.5.3	Dit attribuut identificeert de CP van de PKI overheid voor het relevante certificaat profiel (beveiligingsfunctie en domein). Zie. Par. 4.6.
keyUsage	{id-ce 15}	TRUE	keyEncipherment, dataEncipherment	
extKeyUsage	{id-ce 37}		emailProtection (OID 1.3.6.1.5.5.7.3.4) Encrypting File System (OID 1.3.6.1.4.1.311.10.3.4)	

Tabel 19 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.
signature			1.2.840.113549.1.1.11	VAST	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: sha256WithRSAEncryption
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		*Public G3/Private G1 generatie:* CIBG	VAST	Dit attribuut bevat de officiële organisatienaam van de uitgevende CA.
issuer.organizationIdentifier			*Public G3/Private G1 generatie:* NTRNL-50000535		Encoded als UTF-8 string. Zie par. 5.3.
issuer.commonName	CN		*Generatie Public G3:* UZI-register Medewerker op naam CA G3	VAST	Dit attribuut bevat de volledige naam van de uitgevende CA.
validity.notBefore			UTCTime waarop het certificaat is ondertekend.	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).

PROFIEL AUTHENTICITEITCERTIFICAAT Medewerkerpas op naam					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
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. PKIO RfC 265 vanaf CIBG3 omgeving medio 2013.
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.
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.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.
subjectPublicKeyInfo.algorithm			rsaEncryption	VAST	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden.
subjectPublicKeyInfo. subjectPublicKey			RSA sleutel van certificaathouder: • 2048 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			2.16.528.1.1003.1.2.5.1	VAST	Dit attribuut identificeert de CP van de PKI overheid voor het relevante certificaat profiel (beveiligingsfunctie en domein). Zie. Par. 4.6.
certificatePolicies.PolicyQualifier. cPS.uri			*Public G3/Private G1 generatie:* https://www.zorgcsp.nl/cps/uzi-register.html	VAST	Dit attribuut bevat de URL voor het Certificate Practice Statement van het UZI-register. Zie. Par. 4.6.

PROFIEL AUTHENTICITEITCERTIFICAAT Medewerkerpas op naam					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
certificatePolicies.PolicyQualifier. userNotice.explicitText			Het toepassingsgebied van dit certificaat is beperkt tot communicatie binnen het domein Organisatie zoals aangegeven in het Programma van Eisen van de PKI voor de Overheid. Zie www.logius.nl	VAST	In de user notice worden (een samenvatting van) de gebruikersvoorwaarden geplaatst c.q. waar die te vinden zijn. Zie. Par. 4.6. 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		Extensie aanwezig vanaf Public G3 hiërarchie.
.uniformResourceIndicator			Public G3/Private G1 generatie: http://cert.pkioverheid.nl/UZI-register_Medewerker_op_naam_CA_G3.cer vanaf 1 juni 2019: http://cert.pkioverheid.nl/20190418_UZI-register_Medewerker_op_naam_CA_G3.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 subject	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) document Signing (OID 1.3.6.1.4.1.311.10.3.12) EmailProtection (OID 1.3.6.1.5.5.7.3.4)	VAST	- clientAuth: het certificaat kan gebruikt worden voor client authenticatie - documentSigning: bruikbaar voor ondertekening documenten - EmailProtection: bruikbaar voor ondertekening van e-mail berichten
CRLDistributionPoints. distributionPoint.fullName	{id-ce 31}		*Public G3/Private G1 generatie:* http://www.csp.uzi-register.nl/cdp/uzi-register_medewerker_op_naam_ca_g3.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. 4.7.

PROFIEL AUTHENTICITEITCERTIFICAAT Medewerkerpas op naam					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
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. 4.8.	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			1.2.840.113549.1.1.11	VAST	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: sha256WithRSAEncryption
signatureValue			Handtekening van CA over het tbsCertificate.	Variabel	

Tabel 20 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				
subjectPublicKeyInfo. subjectPublicKey			RSA sleutel van certificaathouder: • 2048 bits	
Standard Extension				
certificatePolicies	{id-ce 32}			
certificatePolicies.PolicyIdentifier			2.16.528.1.1003.1.2.5.2	Dit attribuut identificeert de CP van de PKI overheid voor het relevante certificaat profiel (beveiligingsfunctie en domein). Zie. Par. 4.6.
keyUsage	{id-ce 15}	TRUE	NonRepudiation	
extKeyUsage	{id-ce 37}		document Signing (OID 1.3.6.1.4.1.311.10.3.12) EmailProtection (OID 1.3.6.1.5.5.7.3.4)	
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 uitgifte van gekwalificeerd certificatat overeenstemt met annex I van EU Verordening 910/2014.
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) overeenstemmend met annex II van EU Verordening 910/2014.
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. 4.6.4.
.language			'en'. Encoded als PrintableString	Codering van taal van PDS.

Tabel 21 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: • 2048 bits	
Standard Extension				
CertificatePolicies	{id-ce 32}			
certificatePolicies.PolicyIdentifier			2.16.528.1.1003.1.2.5.3	OID van CP van de PKI overheid voor het certificaat profiel (beveiligingsfunctie en domein). Zie. Par. 4.6.
keyUsage	{id-ce 15}	TRUE	keyEncipherment, dataEncipherment	
extKeyUsage	{id-ce 37}		emailProtection (1.3.6.1.5.5.7.3.4) Encrypting File System (1.3.6.1.4.1.311.10.3.4)	

Tabel 22 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.
signature			1.2.840.113549.1.1.11	VAST	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: sha256WithRSAEncryption
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		*Public G3/Private G1 generatie:* CIBG	VAST	Dit attribuut bevat de officiële organisatienaam van de uitgevende CSP.
issuer.organizationIdentifier			*Public G3/Private G1 generatie:* NTRNL-50000535		Encoded als UTF-8 string. Zie par. 5.3.
issuer.commonName	CN		*Generatie Public G3:* UZI-register Medewerker niet op naam CA G3	VAST	Dit attribuut bevat de volledige naam van de uitgevende CA.
validity.notBefore			UTCTime waarop het certificaat is ondertekend.	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. PKIO RfC 265 vanaf CIBG3 omgeving medio 2013.
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
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.organizationalUnitName	OU		Afdeling	Variabel	Dit **optionele** attribuut bevat een aanduiding van een afdeling waarmee de pashouder verbonden is.
subject.serialNumber			UZI-nummer	Variabel	Uniek nummer zie par. 4.2.
subject.organizationIdentifier			*Public G3/Private G1 generatie:* NTRNL-<kvk-nummer abonnee>		
subjectPublicKeyInfo.algorithm			rsaEncryption	VAST	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden.
subjectPublicKeyInfo. subjectPublic.Key			RSA sleutel van certificaathouder: • 2048 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			2.16.528.1.1003.1.2.5.4	VAST	Dit attribuut identificeert de CP van de PKI overheid voor het relevante certificaat profiel (beveiligingsfunctie en domein). Zie. Par. 4.6.
certificatePolicies.PolicyQualifier. cPS.uri			*Public G3/Private G1 generatie:* https://www.zorgcsp.nl/cps/uzi-register.html	VAST	Dit attribuut bevat de URL voor het Certificate Practice Statement van het UZI-register. Zie. Par. 4.6.
certificatePolicies.PolicyQualifier. userNotice.explicitText			Het toepassingsgebied van dit certificaat is beperkt tot communicatie binnen het domein Organisatie zoals aangegeven in het Programma van Eisen van de PKI voor de Overheid. Zie www.logius.nl	VAST	In de user notice worden (een samenvatting van) de gebruikersvoorwaarden geplaatst c.q. waar die te vinden zijn. Zie. Par. 4.6. 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		Extensie aanwezig vanaf Public G3 hiërarchie.
.uniformResourceIndicator			*Public G3/Private G1 generatie:* http://cert.pkioverheid.nl/UZI-register_Medewerker_niet_op_naam_CA_G3.cer		HTTP URI naar DER encoded issuing CA certificaat. Zie par. 5.2.

PROFIEL AUTHENTICITEITCERTIFICAAT Medewerkerpas niet op naam					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
			vanaf 1 juni 2019: http://cert.pkioverheid.nl/20190418_UZI-register_Medewerker_niet_op_naam_CA_G3.cer		
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 subject	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) document Signing (OID 1.3.6.1.4.1.311.10.3.12) EmailProtection (OID 1.3.6.1.5.5.7.3.4)	VAST	- clientAuth: het certificaat kan gebruikt worden voor client authenticatie - documentSigning: bruikbaar voor ondertekening documenten - EmailProtection: bruikbaar voor ondertekening van e-mail berichten
CRLDistributionPoints. distributionPoint.fullName	{id-ce 31}		*Public G3/Private G1 generatie:* http://www.csp.uzi-register.nl/cdp/uzi-register_medewerker_niet_op_naam_ca_g3.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. 4.7.
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.4.8.	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**		Toegevoegd in G3.
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			1.2.840.113549.1.1.11	VAST	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: sha256WithRSAEncryption

PROFIEL AUTHENTICITEITCERTIFICAAT Medewerkerpas niet op naam					
Certificaatveld / attribuut	OID	Critical	Waarde	Typering	Omschrijving / toelichting
signatureValue			Handtekening van CA over het tbsCertificate.	Variabel	

Tabel 23 Profiel authenticiteitcertificaat Medewerkerpas niet op naam

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: • 2048 bits	
Standard Extension				
CertificatePolicies	{id-ce 32}	FALSE		
certificatePolicies.PolicyIdentifier			2.16.528.1.1003.1.2.5.5	Dit attribuut identificeert de CP van de PKI overheid voor het relevante certificaat profiel (beveiligingsfunctie en domein). Zie. Par. 4.6.
keyUsage	{id-ce 15}	TRUE	keyEncipherment, dataEncipherment	
extKeyUsage	{id-ce 37}		emailProtection (OID 1.3.6.1.5.5.7.3.4) Encrypting File System (OID 1.3.6.1.4.1.311.10.3.4)	

Tabel 24 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.
Signature		1.2.840.113549.1.1.11	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: sha256WithRSAEncryption
Issuer			
Issuer.countryName (C)		NL	
Issuer.organisationName (O)		*Private G1 generatie:* CIBG	
Issuer.organization-Identifier		*Private G1 generatie:* NTRNL-50000535	Encoded als UTF-8 string. Zie par. 5.3.
Issuer.commonName (CN)		*Generatie Private G1:* UZI-register Private Server CA G1	
validity.notBefore		UTCTime van ondertekening certificaat	
validity.notAfter		UTCTime van einde geldigheid certificaat	3 jaar (= 1095 dagen)
Subject			
subject.commonName (CN)		Fully Qualified Domain Name (FQDN) van de service.	
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.Organizational UnitName (OU)		Afdeling	Dit **optionele** attribuut bevat een aanduiding van een onderdeel binnen de abonnee.
subject.serialNumber		UZI-nummer	Uniek nummer voor service. Zie par. 4.2.
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.StateOrProvinceName (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.
subjectPublicKeyInfo. Algorithm		rsaEncryption	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden.
subjectPublicKeyInfo. subjectPublicKey		RSA sleutel van server: • 2048 bits	Dit attribuut bevat de publieke sleutel, welke kan worden gebruikt voor de in dit certificaat gespecificeerde doeleinden.

PROFIEL UZI-register Servercertificaat			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / toelichting
Standard extensions			
certificatePolicies			
certificatePolicies. PolicyIdentifier		*Generatie Private G1:* 2.16.528.1.1003.1.2.8.6	De waarde is de OID van de PKI-overheid Certificate Policy voor servercertificaten in het betreffende domein. Zie. Par. 4.6.
certificatePolicies. PolicyQualifier.cPS.uri		*Private G1 generatie:* https://www.zorgcsp.nl/cps/uzi-register.html	Dit attribuut bevat de URL voor het Certificate Practice Statement van het UZI-register. Zie. Par. 4.6.
certificatePolicies. PolicyQualifier.userNotice. explicitText		Het toepassingsgebied van dit certificaat is beperkt tot communicatie binnen het domein Organisatie zoals aangegeven in het Programma van Eisen van de PKI voor de Overheid. Zie www.logius.nl	In de user notice worden (een samenvatting van) de gebruikersvoorwaarden geplaatst c.q. waar die te vinden zijn. Zie. Par. 4.6. 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	Extensie aanwezig vanaf Private G1 hiërarchie.
.uniformResourceIndicator		*Private G1 generatie:* http://cert.pkioverheid.nl/UZI-register_Private_Server_CA_G1.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 subject	Dit attribuut bevat het controle getal voor de publieke sleutel in dit certificaat.
CRLDistributionPoints. fullName		*Private G1 generatie:* http://www.csp.uzi-register.nl/cdp/uzi-register_private_server_ca_g1.crl	Zie. Par. 4.7.
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			
subjectAltName.dNSName		Fully Qualified Domain Name (FQDN) van de service.	Identieke inhoudt als de subject.commonName
subjectAltName.otherNam e		Samengesteld veld. zie par. 4.8.	
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		1.2.840.113549.1.1.11	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: • sha256WithRSAEncryption
signatureValue		Handtekening van CA over het tbsCertificate.	

Tabel 25 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.
signature		1.2.840.113549.1.1.11	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: sha256WithRSAEncryption
issuer			
Issuer.countryName (C)		NL	
Issuer.organisationName (O)		*Private G1 generatie:* CIBG	
Issuer.organization-Identifier		*Private G1 generatie:* NTRNL-50000535	Encoded als UTF-8 string. Zie par. 5.3.
Issuer.commonName (CN)		*Generatie Private G1:* ZOVAR Private Server CA G1	
validity.notBefore		UTCTime van ondertekening certificaat	
validity.notAfter		UTCTime van einde geldigheid certificaat	3 jaar geldig (= 1095 dagen)
subject			
subject.commonName (CN)		Fully Qualified Domain Name (FQDN) van de service.	
subject.organizationName (O)		Naam van de abonnee (type zorgverzekeraar) van het ZOVAR Servercertificaat.	
subject.organizational UnitName (OU)		Afdeling	Dit **optionele** attribuut bevat een aanduiding van een onderdeel binnen een abonnee.
subject.serialNumber		<UZOVI-nummer><ZOVAR-nummer>	Uniek nummer voor service. Zie par. 4.2.2.
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.
subjectPublicKeyInfo. algorithm		rsaEncryption	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden.
subjectPublicKeyInfo. subjectPublicKey		RSA sleutel van certificaathouder. Afhankelijk van hiërarchie:2048 bits	Dit attribuut bevat de publieke sleutel, welke kan worden gebruikt voor de in dit certificaat gespecificeerde doeleinden.

PROFIEL ZOVAR Servercertificaat			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / toelichting
Standard extensions			
certificatePolicies			
certificatePolicies. PolicyIdentifier		*Generatie Private G1:* 2.16.528.1.1003.1.2.8.6	De waarde is de OID van de PKI-overheid Certificate Policy voor servercertificaten in het betreffende domein. Zie. Par. 4.6.
certificatePolicies. PolicyQualifier.cPS.uri		*Private G1 generatie:* https://www.zorgcsp.nl/cps/zovar.html	Dit attribuut bevat de URL voor het Certificate Practice Statement van ZOVAR. Zie. Par. 4.6.
certificatePolicies. PolicyQualifier.userNotice. explicitText		Het toepassingsgebied van dit certificaat is beperkt tot communicatie binnen het domein Organisatie zoals aangegeven in het Programma van Eisen van de PKI voor de Overheid. Zie www.logius.nl	In de user notice worden (een samenvatting van) de gebruikersvoorwaarden geplaatst c.q. waar die te vinden zijn. Zie. Par. 4.6. 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	Extensie aanwezig vanaf Private G1 hiërarchie.
.uniformResourceIndicator		*Generatie Private G1:* http://cert.pkioverheid.nl/ZOVAR_Private_Server_CA_G1.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 subject	Dit attribuut bevat het controle getal voor de publieke sleutel in dit certificaat.
CRLDistributionPoints. fullName		*Generatie Private G1:* http://www.csp.zovar.nl/cdp/zovar_private_server_ca_g1.crl	Zie. Par. 4.7.
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			
subjectAltName.dNSName		Fully Qualified Domain Name (FQDN) van de service.	Identieke inhoudt als de subject.commonName
subjectAltName.otherName		Samengesteld veld. zie par. 4.8.	
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 ZOVAR Servercertificaat			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / toelichting
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: sha256WithRSAEncryption
signatureValue		Handtekening van CA over het tbsCertificate.	

Tabel 26 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
- Vanaf de Public G3/Private G1 certificaten blijven ingetrokken certificaten na het verlopen van de geldigheidsduur op de CRL staan.

11.2 CRL profiel van CSP CA

In de Public G3/Private G1 hiërarchie bevatten deze CRL's de serienummers van ingetrokken eindgebruiker certificaten.

CRL profiel van CSP CA			
CRL veld	**Critical**	**Waarde**	**Omschrijving / Toelichting**
TBSCertList			
Version		1	CRL version 2
Signature		1.2.840.113549.1.1.11	De waarde is de OID die het algoritme specificeert van de handtekening over de CRL: sha256WithRSAEncryption
Issuer.commonName (CN)		*Public G3/Private G1 generatie afhankelijk van pastype:* • UZI-register Zorgverlener CA G3 • UZI-register Medewerker op naam CA G3 • UZI-register Medewerker niet op naam CA G3 • UZI-register Private Server CA G1 • ZOVAR Private Server CA G1	
Issuer. organisationName (O)		*Public G3/Private G1 generatie:* CIBG	
issuer.organization Identifier		*Public G3/Private G1 generatie:* NTRNL-50000535	Encoded als UTF-8 string. Zie par. 5.3.
Issuer.country (C)		NL	
thisUpdate		Automatisch gegenereerd	Uitgiftetijdstip van de CRL.
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.

CRL profiel van CSP CA			
CRL veld	**Critical**	**Waarde**	**Omschrijving / Toelichting**
TBSCertList			
ExpiredCertsOnCRL	FALSE	OID 2 5 29 60	Zie *
date		mm/dd/jjjj	Zie **. Datum nog nader bepalen. Dit hangt mogelijk af van implementatie moment, maar het effect zal zijn dat alle ingetrokken Public G1/Private G3 certificaten op de CRL zullen blijven.
CertificateList			
signatureAlgorithm		1.2.840.113549.1.1.11	De waarde is de OID die het algoritme specificeert van de handtekening over de CRL: sha256WithRSAEncryption
signatureValue		Handtekening van CA over het tbsCertificateList.	

Tabel 27 CRL profiel van de CSP CA

* 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.*

** 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.

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 -PvE 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 4 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 op het hele uur ongeacht het feit of er sinds de voorafgaande publicatie UZI-passen zijn ingetrokken. Na een eventuele verstoring (systemen tijdelijk down of reboot) worden de CRL's altijd weer gegenereerd volgens dit vaste tijdschema.

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 enkele minuten na het hele uur. 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:

- 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;
- Alle OCSP communicatie voor producten van UZI-register verloopt via één URL: **http://ocsp.uzi-register.nl**.

12.3 Profiel OCSP responder certificaten

12.3.1 Toelichting specifieke attributen

Het OCSP responder certificaten volgen zoveel mogelijk het certificaatprofiel voor servercertificaten. Afwijkend is het feit dat de certificaten van de OCSP responders geen Subject.StateOrProvinceName Subject.LocalityName bevatten. Deze paragraaf geeft specifieke invulling gebaseerd op RFC 2560:

```
OCSP signing delegation SHALL be designated by the inclusion of unique value for
extendedKeyUsage=id-kp-OCSPSigning in the OCSP signer's certificate. (Non-
Critical extension)

   id-kp-OCSPSigning OBJECT IDENTIFIER ::= {id-kp 9}
                                       ::= { 1.3.6.1.5.5.7.3.9 }
```

De OCSP responder certificaten bevatten ook een CRL DistributionPoint. Reden is dat OCSP clients moeten weten hoe ze kunnen controleren dat een OCSP responder certificaat niet is ingetrokken.

12.3.2 Certificaatprofiel OCSP responders

Onderstaande tabel geeft het certificaatprofiel voor de OCSP responders. In termen van PKI voor de Overheid betreft het een zogenaamd service certificaat authenticiteit.

PROFIEL OCSP signers			
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).
signature		1.2.840.113549.1.1.11	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: sha256WithRSAEncryption
issuer			
Issuer.countryName (C)		NL	
Issuer.organisationName (O)		*Public G3/Private G1 generatie:* CIBG	
Issuer.organization Identifier		*Public G3/Private G1 generatie:* NTRNL-50000535	Encoded als UTF-8 string. Zie par. 5.3.
Issuer.commonName (CN)		[CN delegated CA]	Dus 'UZI-register Zorgverlener CA' voor de OCSP responder die status informatie geeft over zorgverlenerpassen (van de eerste generatie).
validity.notBefore		UTCTime van ondertekening	
validity.notAfter		UTCTime van einde geldigheid	3 jaar geldig
subject			
subject.countryName (C)		NL	
subject.commonName (CN)		OCSP responder [CN delegated CA]	Voor de 'UZI-register Zorgverlener CA' is de CN van de bijbehorende OCSP responder: **'OCSP responder UZI-register Zorgverlener CA'**
subject.organizationName (O)		*Public G3/Private G1 generatie:* CIBG	
subject.serialNumber		Uniek nummer	Indien aanwezig.
subjectPublicKeyInfo. algorithm		rsaEncryption	Dit attribuut specificeert het algoritme waarmee de publieke sleutel gebruikt dient te worden.
subjectPublicKeyInfo. subjectPublic.Key		RSA sleutel van certificaathouder: 2048 bits	Dit attribuut bevat de publieke sleutel, welke kan worden gebruikt voor de in dit certificaat gespecificeerde doeleinden.
standard extensions			
certificatePolicies			
certificatePolicies. PolicyIdentifier		*Public G3/ Private G1 generatie:* Domein Organisatie Persoon (UZI-register Zorgverlener CA G3 en UZI-register Medewerker op naam CA G3): **2.16.528.1.1003.1.2.5.1** DomeinOrganistatie Services (UZI-register	In Public G3/Private G1 zijn de OID's afhankelijk van de bovenliggende Domein en TSP CA's waarin een limitatieve lijst met OID's is opgenomen. Zie PvE wijziging 360 v0.5 zoals verwerkt in PvE basiseisen in tabel met OCSP Signing certificaat extensies.

PROFIEL OCSP signers			
Certificaatveld / attribuut	Critical	Waarde	Omschrijving / toelichting
		Medewerker niet op naam CA G3): **2.16.528.1.1003.1.2.5.4** Domein Private Services/server (UZI-register Private Server CA G1 en ZOVAR Private Server CA G1): **2.16.528.1.1003.1.2.8.4**	Zie. Par. 4.6.
certificatePolicies. PolicyQualifier.cPS.uri		Public G3/*Private G1 generatie:* https://www.zorgcsp.nl/cps/uzi-register.html https://www.zorgcsp.nl/cps/zovar.html	Zie. Par. 4.6. ZOVAR heeft eigen CPS URI.
certificatePolicies. PolicyQualifier.userNotice.explicitText		Het toepassingsgebied van dit certificaat is beperkt tot communicatie binnen het domein Organisatie zoals aangegeven in het Programma van Eisen van de PKI voor de Overheid. Zie www.logius.nl	Identiek aan UserNotice voor servercertificaat. Zie. Par. 4.6.
keyUsage	TRUE	DigitalSignature	Services authenticatie, hoewel een OCSP responder een specifieke toepassing is. Dit komt tot uitdrukking in de extended keyUsage.
extKeyUsage	TRUE	1.3.6.1.5.5.7.3.9	Voor de OCSP responder dient conform RFC 2560 een extended keyUsage opgenomen te worden voor OCSP signing.
authorityKeyIdentifier. keyIdentifier		SHA-1 hash van publieke CA sleutel.	Dit attribuut bevat het controle getal voor de publieke sleutel van CA die het certificaat heeft getekend.
subjectKeyIdentifier. keyIdentifier		SHA-1 hash van publieke sleutel van subject	Dit attribuut bevat het controle getal voor de publieke sleutel in dit certificaat.
CRLDistributionPoints. fullName		Zie. Par. 4.7.	Iedere OSCP responder certificaat heeft een CDP dat verwijst naar de CA waardoor het is uitgegeven. Dus voor de OCSP responder UZI-register Zorgverlener CA is de CDP.FullName 'http://www.uzi-register.nl/cdp/uzi-register_zorgverlener_ca.crl'
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
Certificate			
signatureAlgorithm		1.2.840.113549.1.1.11	De waarde is de OID die het algoritme specificeert van de handtekening over het certificaat: sha256WithRSAEncryption
signatureValue		Handtekening van CA over het tbsCertificate.	

Tabel 28 Profiel OCSP signer certificaat

12.4 Authority Information Access attribuut in gebruikercertificaten

Voor de volledigheid is hieronder aangegeven met welke certificaat attributen een verwijzing naar de OCSP dienst is opgenomen in alle gebruikercertificaten van het UZI-register. Deze verwijzing dient NIET opgenomen te worden in de OCSP signer certificaten.

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

12.5 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.

12.6 Signature Algorithm in OCSP responses

De OCSP responses zijn ondertekend door de OCSP responder. Deze paragraaf beschrijft het algoritme dat daarvoor wordt gebruikt.

In RFC 2560 OCSP staat het volgende over de algoritmes:

```
4.3  Mandatory and Optional Cryptographic Algorithms

   Clients that request OCSP services SHALL be capable of processing
   responses signed used DSA keys identified by the DSA sig-alg-oid
   specified in section 7.2.2 of [RFC2459]. Clients SHOULD also be
   capable of processing RSA signatures as specified in section 7.2.1 of
   [RFC2459]. OCSP responders SHALL support the SHA1 hashing algorithm.
```

Het ligt voor de hand om bij ondertekening van de OCSP responses ook sha256WithRSAEncryption te gebruiken. Dit is nog niet gestandaardiseerd omdat dit algoritme ontbreekt in RFC 2560 OCSP. Daarom is ook bij de SHA-2 generatie het sha-1WithRSAEncryption algoritme toegepast voor ondertekening van de OCSP responses.