CIBG
Ministerie van Volksgezondheid, Welzijn en Sport

Veelgestelde vragen

Uitfasering G2-hiërarchie van de Zorg CSP

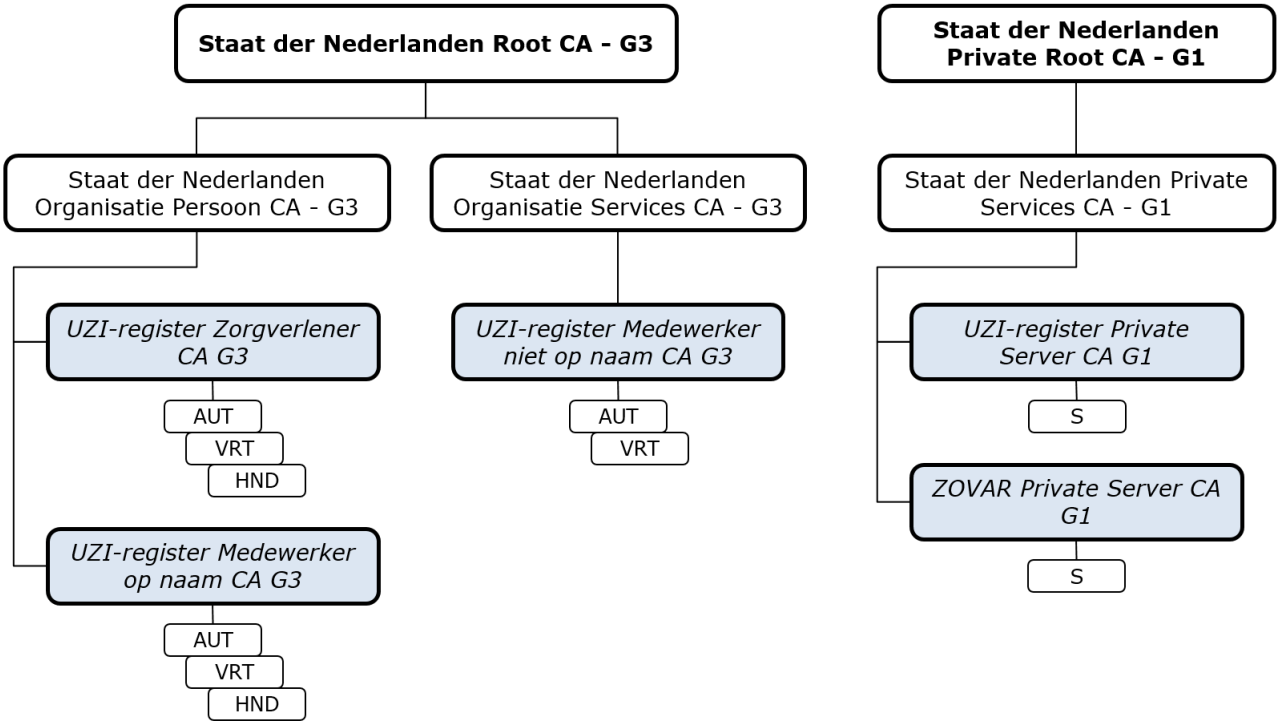
Met dit document beantwoorden wij veelgestelde vragen die te maken hebben met het uitfaseren van de zogenaamde G2-hiërarchie, voor passen en certificaten van de Zorg Certificate Service Provider (Zorg CSP). De G2-hiërarchie is de huidige generatie van CA-certificaten waaronder het CIBG certificaten uitgeeft. Dit document is voor ICT-leveranciers.

Waarom moet de huidige generatie CA-certificaten worden vervangen?

Wij geven nu UZI-passen uit onder de G2-hiërarchie van PKIOverheid. De einddatum van deze G2-hiërarchie is 22 maart 2020. Wij geven producten uit met een minimum van twee jaar. Dit betekent dat u uiterlijk 22 maart 2018 de benodigde aanpassingen gedaan moet hebben om de nieuwe CA-hiërarchie mogelijk te maken.

Hoe ziet het nieuwe CA-model eruit?

Figuur 1 toont het nieuwe CA-model voor de productieomgeving van de Zorg CSP. De naamgeving (subject.CommonName in de betreffende CA-certificaten) van de CA's komt overeen met figuur 1. De naamgeving is Case Sensitive. De CA's die de certificaten ondertekenen, zijn cursief en lichtgrijs weergegeven.



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

Toelichting:
Voor de volledigheid zijn in figuur 1 ook de verschillende typen certificaten opgenomen:

- AUT: Authenticiteitcertificaat;
- VRT: Vertrouwelijkheidcertificaat;
- HND: Handtekeningcertificaat;
- S: Servercertificaat.

Wat zijn de belangrijkste wijzigingen bij invoering van de Public G3/Private G1-hiërarchie?

Bij de invoering van de Public G3/Private G1-hiërarchie zijn de volgende zaken gewijzigd in het CA-model:

1. Uitgifte van certificaten voor passen vindt straks plaats onder de publiek vertrouwde G3 Root van PKIOverheid (Public G3). Uitgifte van servercertificaten valt straks onder de private Root CA G1 van PKIOverheid (Private G1).
2. 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 een apart domein voor services certificaten in te richten. Hierdoor hebben de 'medewerkerpassen niet op naam' andere intermediate CA's.
3. Met de invoering van G3 heeft Logius besloten om geen zogenaamde sub-CA's meer toe te staan. Daarom is er één niveau uit de CA-hiërarchie verwijderd (Zorg CSP CA) en worden alle CA-certificaten direct door Logius uitgegeven.

Gebruikt de Public G3/Private G1-hiërarchie andere cryptografische algoritmen of een andere sleutellengte?

Nee, er is geen enkele wijziging in de cryptografie. Wel zijn er kleine wijzigingen doorgevoerd in de certificaatprofielen om te voldoen aan het actuele normenkader. Deze zijn in detail beschreven in het 'CA model, Pasmodel, Certificaat- en CRL-profielen Zorg CSP'-document zoals gepubliceerd op onze website.

Tot wanneer zijn de CA-certificaten van Public G3/Private G1-hiërarchie geldig?

Inherent aan het gebruik van certificaten is een einddatum. Deze is in de certificaten opgenomen. De volgende tabel geeft een overzicht van de geldigheidsduur van de certificaten in de Public G3/Private G1-hiërarchie.

Certificaat	Geldig tot
Stamcertificaat	14 november 2028
Domeincertificaat	13 november 2028
CSP-certificaten	12 november 2028
Eindgebruikercertificaat	Ongewijzigd: drie jaar (of uiterlijk tot het einde van de geldigheid van het ondertekend CSP CA-certificaat)

Tabel 1: Levensduur certificaten Public G3/Private G1-hiërarchie

Waarom is gekozen voor de Private G1-hiërarchie voor servercertificaten?

Onder deze Private Root is het mogelijk om de zogenaamde subjectAltName.otherName te blijven gebruiken. Dit attribuut bevat noodzakelijke informatie voor toepassingen in het zorgveld (o.a. SBV-Z en LSP), maar is niet meer toegestaan binnen de regels van het CA/Browser Forum. Omdat de private Root niet valt onder de eisen die browserpartijen stellen, is het mogelijk om op sommige punten af te wijken. Bijvoorbeeld door het opnemen van UZI-nummers in de certificaten. Daarnaast zijn er ontwikkelingen die waarschijnlijk gaan leiden tot een veel kortere levensduur van SSL-certificaten die vallen onder de regels van het CA/Browser Forum (één jaar). Terwijl onder de Private Root driejarige servercertificaten mogelijk blijven.

Is de Private G1-hiërarchie wel betrouwbaar?

Ja, deze valt ook onder het toezicht van Logius en onafhankelijke certificering. Hij wordt technisch en procedureel op dezelfde manier beheerd als de publiek vertrouwde hiërarchie. Het enige verschil is dat de formele procedures niet zijn uitgevoerd voor opname van het stamcertificaat in operating systemen en in browsers. Dit kan omdat de Private omgeving specifiek is bedoeld voor certificaten die gebruikt worden voor koppelingen tussen systemen zoals het LSP.

Hoe kan ik de echtheid van het Private G1 stamcertificaat vaststellen?

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

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

Is een private servercertificaat bruikbaar voor beveiliging van een webserver?

Technisch is dat wel het geval, maar als clients het stamcertificaat niet hebben vertrouwd, leidt dit tot een foutmelding in de browser van de gebruiker. Natuurlijk is het in een gecontroleerde omgeving mogelijk om het Private stamcertificaat te distribueren naar clients. Maar het advies is om in die situaties over te stappen op een PKIOverheid servercertificaat zoals aangeboden door diverse commerciële certificatiedienstverleners.

Waar kan ik de CA-certificaten van de productieomgeving downloaden?

Alle CA-certificaten zijn gepubliceerd op https://cert.pkioverheid.nl/.

Verandert er functioneel iets door de invoering van de Public G3/Private G1?

Nee, functioneel verandert er niets aan de UZI-pas of servercertificaten door de Public G3/Private G1. Om te voldoen aan het aangescherpte normenkader zijn er zogenaamde Extended Key usages toegevoegd die het gebruik van de certificaten beperken. De verwachting is dat dit voor het gebruik in de zorg geen effect zal hebben, maar dit moet u wel testen.

Blijven huidige passen onder de G2-hiërarchie en servercertificaten gewoon bruikbaar?

Ja, deze blijven bruikbaar tot het einde van de geldigheidsduur waarvoor ze zijn uitgegeven.

Wat verandert er bij het aanvragen van UZI-passen en servercertificaten?

Bij het aanvragen van passen en servercertificaten verandert niets.

Wanneer worden er in productie passen en servercertificaten uitgegeven onder de Public G3/Private G1-hiërarchie?

Vanaf 4 januari 2018 zijn er UZI– en ZOVAR-servercertificaten uitgegeven onder de Private G1-hiërarchie. Vanaf 22 maart 2018 worden er UZI-passen uitgegeven onder de Public G3-hiërarchie.

Is een software-update noodzakelijk voor de transitie naar G3/G1?

Als het goed is zou alleen een configuratiewijziging noodzakelijk moeten zijn door de nieuwe CA-certificaten toe te voegen aan de zogenaamde 'certificate trust store' die uw systeem gebruikt. Cryptografisch zijn er geen wijzigingen in gebruikte algoritmen, sleutellengte of chip op de UZI-pas. Met testmiddelen moet u vaststellen of uw applicatie overweg kan met de nieuwe certificaatprofielen.

Meer informatie?

Als u nog andere vragen heeft, kijkt u dan op onze website. Kunt u iets niet vinden? Dan kunt u ons op werkdagen bereiken op 0900 – 232 43 42. U kunt ook een e-mail sturen naar info@uzi-register.nl.