Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

# Hoofdlijnen PKIoverheid veranderingen

## 1 Let op: PKIoverheid verandert

Met behulp van deze infographic kunt u inzicht krijgen in de veranderingen die er binnen de PKIoverheid infrastructuur plaatsvinden. Onderzoek zelf (met uw technische collega's of leverancier) hoe de situatie bij u is. Deze infographic is een vereenvoudigde weergave, niet alle technische aspecten en details komen aan bod. Aan deze infographic kunnen geen rechten worden ontleend.

## 2 Beknopt overzicht van veranderingen

Om alle certificaten weer aan de internationale richtlijnen te laten voldoen is een vervangingsplan opgesteld. Dat plan hebben we in deze infographic samengevat.

Datum: 5 oktober 2020
Versie 1.1 - NL

Controleer of u de nieuwste versie bekijkt

https://logius.nl/diensten/pkioverheid/infographic

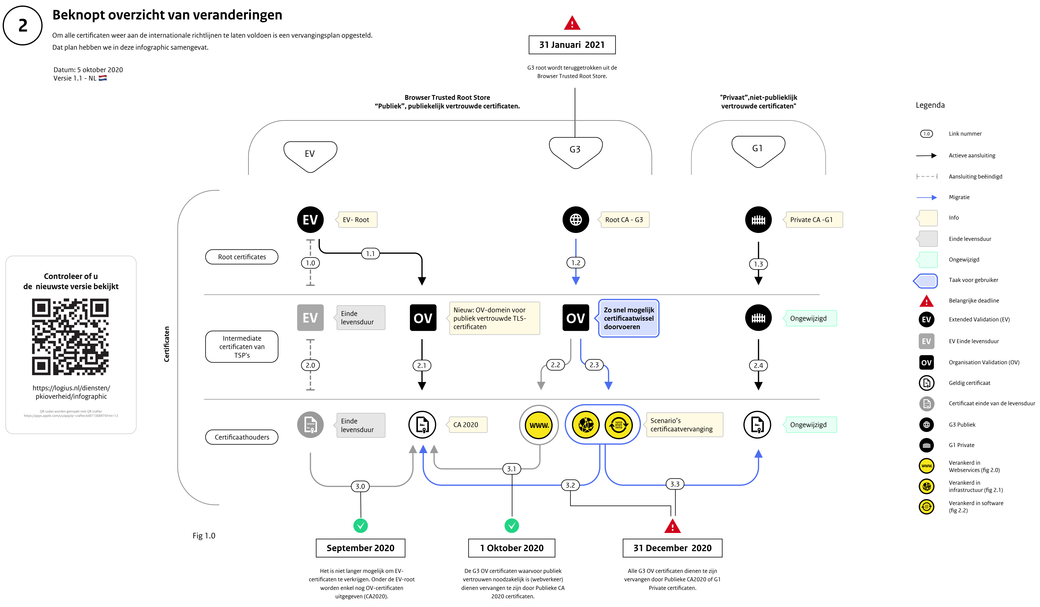


Fig 1.0

## 3 Scenario's certificaatvervanging

Onderstaand ziet u drie veelvoorkomende locaties in digitale dienstverlening waar certificaten gebruikt worden. Per locatie is omcirkeld waar mogelijk certificaten vervangen moeten worden. Onderzoek zelf (met uw technische collega's of leverancier) hoe de situatie werkelijk is.


Fig 2.0

### Verankerd in Webservices

Dit is een mixed use case. Certificaten die gebruikt worden voor machine-naar-machineverkeer (M2M) en Web-services moeten van elkaar gescheiden worden. Neem contact op met uw TSP trust service provider voor meer informatie. Voorbeelden: SAML, Apps, Websites, enz.


Fig 2.1

### Verankerd in infrastructuur

Dit is vooral een infrastructuurketen met veel plaatsen waar het certificaat door verschillende partijen wordt gebruikt, niet wendbaar genoeg als het gaat om het vervangen van certificaten. Voorbeelden: (omgekeerde) volmachten, load-balancers, certificaat pinning etc.


Fig 2.2

### Verankerd in software

Software-instellingen moeten worden aangepast om het certificaat te laten werken Voorbeelden: SBR, enz.

## 4 Veelgestelde vragen

Op onze website (logius.nl) verzamelen we antwoorden op vragen die vaak gesteld worden. Die pagina wordt regelmatig bijgewerkt. Staat uw vraag er niet tussen, dan kunt u in de meeste gevallen het beste contact opnemen met uw certificaatverstrekker (de partij waar u uw certificaat gekocht heeft). Zij kunnen u het beste helpen. Wijs ook uw technische collega's op de factsheet van het Nationaal Cybersecurity Centrum (NCSC).

### logius.nl

https://logius.nl/diensten/pkioverheid/pkioverheid-update/certificaat-vervangingsplan-veelgestelde-vragen

### ncsc.nl

https://www.ncsc.nl/documenten/factsheets/2020/september/4/factsheet-pkioverheid-verandert

## 5 Woordenlijst

In het onderstaande overzicht lichten we veelgebruikte termen toe. De toelichting kan helpen om het gesprek binnen uw organisatie te voeren over de noodzakelijke certificaatvervanging.

**Public Key Infrastructure (PKI)**
Een publieke sleutelinfrastructuur (PKI) is een reeks rollen, beleidslijnen, hardware, software en procedures die nodig zijn om digitale certificaten te creëren, te beheren, te distribueren, te gebruiken, op te slaan en te herroepen en om publieke-sleutel encryptie te beheren. Het doel van een PKI is het vergemakkelijken van de veilige elektronische overdracht van informatie voor een reeks netwerkactiviteiten zoals e-commerce, internetbankieren en vertrouwelijke e-mail.

**Certificate Authority (CA)**
In de cryptografie is een certificeringsautoriteit of een certificeringsinstantie (CA) een entiteit die digitale certificaten afgeeft. Een certificaat levert heel sterk bewijs dat een persoon of organisatie is wie hij zegt te zijn. Dit gebeurt door middel van sleutels. Dit maakt het mogelijk voor anderen (afhankelijke partijen) om te vertrouwen op handtekeningen of op beweringen over de private sleutel die overeenkomt met de gecertificeerde publieke sleutel. Een CA zorgt ervoor dat de eigenaar van het certificaat en bijvoorbeeld een aanvrager van een digitale dienst elkaar kunnen vertrouwen.

**Trust Service Provider (TSP)**
Een TSP is een een organisatie of rechtspersoon die een of meer vertrouwensdiensten verleent als gekwalificeerde of niet-gekwalificeerde aanbieder van vertrouwensdiensten. Zij (kunnen) optreden als een CA in het kader van de eIDAS-verordening zoals die door de Europese Commissie is uitgevaardigd.

**Certificaathouders**
Een certificaathouder sluit namens een of meer certificaathouders een overeenkomst met een aanbieder van telecommunicatiediensten.

**Transport Layer Security (TLS-verbindingen)**
en diens voorganger Secure Sockets Layer (SSL), zijn encryptie-protocollen die de communicatie tussen computers (bijvoorbeeld op het internet) beveiligen. TLS wordt voornamelijk gebruikt in situaties waarin het nodig is te verifiëren of men inderdaad verbonden is met de gewenste server. Met name in bancaire toepassingen (internetbankieren) of communicatie met de overheid is dit van groot belang, aangezien vaak financiële belangen in het spel zijn, of persoonlijke of anderszins vertrouwelijke informatie wordt uitgewisseld.

**Extended Validation (EV)**
Extended validatie certificaten zijn ontworpen om "een stap boven" de OV-certificaten te zijn (zie hieronder). Afgifte van EV-certificaten moet voldoen aan strenge internationale normen met betrekking tot de identiteitsvalidatie (bijv. de informatie in een EV-certificaat). Hoewel dit in theorie een betrouwbare partij meer informatie geeft over de identiteit van de website-exploitant, is het in de praktijk erg moeilijk om dit te doen. De speciale UI-behandeling van EV PKI-certificaten (de zogenaamde "groene balk") is dan ook in 2019 door grote browserleveranciers stopgezet. Voor het overige is een EV-certificaat, met uitzondering van identiteitsgegevens, identiek aan een OV-certificaat.

**Organizational Validation (OV)**
Vergelijkbaar met EV-certificaten zijn OV-certificaten bedoeld om een betrouwbare partij meer informatie te verschaffen over een website of server operator. Hoewel er een aantal basisvereisten van de industrie zijn, bestaat er een veel breder spectrum aan identiteitsinformatie in een certificaat en het niveau van validatie door een TSP/CA. Zo benadert het niveau van validatie dat vereist is voor PKIoverheid OV-certificaten in sommige opzichten de EV-normen.

**Browser Root Stores**
In een rootstore staat welke certificaten webbrowsers vertrouwen in het internetverkeer. Een bezoek aan bijvoorbeeld een website die geen geldig certificaat heeft, levert een foutmelding in het scherm op. Een root store kan worden onderhouden door een grote softwareleverancier (zoals een browser of OS-leverancier zoals Microsoft, Google of Apple) of zelf worden gedefinieerd door een beheerder van een server. In het eerste geval kan een CA een aanvraag indienen om opgenomen te worden in een root store (die meestal toelatingseisen heeft). In het kader van deze factsheet ligt de focus op de browser-gerelateerde variant.

**G1 Private (Staat der Nederlanden Private Root CA – G1)**
Een door Logius in 2014 gecreëerde Root CA / hiërarchie die, naar ontwerp, niet is opgenomen in een publieke root store. Dit is de eerste generatie certificaten van dit type (vandaar de G1 bijlage). Hoewel de PKIoverheid regelgeving en het toezicht volledig van kracht zijn, zijn niet alle eisen die aan de G3- of EV-certificaten worden gesteld van toepassing. Er is dus meer ruimte voor specifieke gevallen van overheidsgebruik die in strijd zijn met de eisen van de browser (bijvoorbeeld termijnen voor de vervanging van certificaten of de levensduur van certificaten).

**G3 (3rd generation)**
De derde iteratie van publiek vertrouwde PKIoverheidscertificaten. Geïntroduceerd in 2014, in actief gebruik sinds 2018. Als publieke vertrouwde hiërarchie was het de standaardkeuze van veel abonnees, ook al was het publieke vertrouwen niet noodzakelijkerwijs nodig (zie Private Root). Momenteel wordt de uitgifte van TLS (OV)-certificaten afgebouwd.