Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Guidance gebruik PKIoverheid-certificaten bij routeringsdienst

Guidance gebruik PKIoverheid-certificaten bij routeringsdienst

Met deze guidance wordt inzichtelijk gemaakt welke PKIOverheid certificat(en) er voor welk toepassingsgebied nodig zijn met betrekking tot aansluiting op een routeringsdienst. Hierbij worden de nieuwe uitgangspunten van PKIoverheid gevolgd.

Versiegegevens

Publicatiedatum: 16 september 2020
Versie: 1.0

Meer informatie over nieuwe uitgangspunten van PKIoverheid:

- NCSC-factsheet 'PKIoverheid verandert: Coördineer de benodigde veranderingen in uw ICT-processen'
- Bekijk ook algemene vragen en antwoorden over de aanpassingen in PKIoverheid

Toelichting op aanpassing in werking PKIoverheid certificaten

Onderstaand een samenvatting van de aanpassing die in de bovengenoemde factsheet beschreven staat:

PKIoverheid-certificaten die zijn uitgegeven onder de ‘Staat der Nederlanden Root CA G3’ (Public G3 root) worden gebruikt voor zowel Webauthenticatie als Machine-to-machine interacties. Deze Public G3 root wordt beëindigd: er kunnen géén nieuwe certificaten meer op worden uitgegeven en bestaande certificaten zullen naar verwachting in februari 2021 niet meer functioneren.

Na beëindiging van Public G3 root certificaten wordt de te kiezen ‘Root’ bij aanschaf en uitgifte van het certificaat bepaald door het beoogde toepassingsgebied:

- Voor *Webauthenticatie* (authenticatie van webdienst naar eindgebruiker via een webbrowser) moeten certificaten worden gebruikt uitgegeven onder de EV-Root. Deze certificaten hebben een geldigheidsduur van 1 jaar en 1 maand.
- Voor *Machine-to-machine* toepassingen moeten certificaten worden gebruikt die zijn uitgegeven onder de G1 ‘Private root’. Deze certificaten hebben een geldigheidsduur van 3 jaar en bevatten een identificerend nummer waarmee machine-tomachine interacties veilig kunnen worden uitgevoerd.

Relatie PKI-Overheid-certificaten en routeringsdienst

Wat is de relatie tussen PKI-Overheid-certificaten en een routeringsdienst?

Om aan te kunnen aansluiten op een routeringsdienst is het gebruik van PKI-Overheid-certificaten vereist. Deze certificaten moeten het OIN van de aangesloten partij bevatten, daarmee kunnen controles in het aansluitproces efficiënt en betrouwbaar worden uitgevoerd.

Er kunnen 2 typen partijen worden aangesloten:

- Dienstverlener (DV)
- SaaS-partij in de rol van Leverancier Clusteraansluiting (LC)(alleen via koppelvlak eID SAML 4.4)

Het aansluiten op de routeringsdienst is vanuit PKIoverheid-perspectief een *Machine-to-machine* toepassing.

In koppelvlak eID SAML 4.4 wordt een PKIoverheid-certificaat gebruikt om het BSN te versleutelen voor de ontvangende DV. Ook dit is binnen het toepassingsgebied Machine-to-Machine.

De aangesloten partij moet de website (webdienst) die hij presenteert aan de gebruiker (via een webbrowser) authentiseren door middel van een PKIoverheid-certificaat. Dit valt binnen het toepassingsgebied ‘Webauthenticatie’.

Welke certificaten heeft u nodig?

Onderstaand een overzicht van het geadviseerde gebruik van PKIoverheid-certificaten bij aansluiten op een routeringsdienst, per toepassingsgebied.

Koppelen via eID SAML 4.4

Van toepassing op: Routeringsdienst TVS

			Toepassingsgebied certificaat	
	Machine-to-machine	***Machine-to-machine***	***Machine-to-machine***	***Webauthenticatie***
Functie * > Wijze van aansluiten	**TLS**	**Signing**	**Encryptie**	**Webdienst***
1. DV Rechtstreeks	G1 DV	G1 DV	G1 DV	EV-Root DV
2. DV via LC (domein LC)	G1 LC	G1 LC	G1 Per DV	EV-Root LC
3. DV via LC (eigen domein DV)	G1 LC	G1 LC	G1 Per DV	EV-Root Per DV

* De eis voor het gebruik van PKI-Overheid certificaten voor de *webdienst* is afkomstig van de DigiD Checklist testen die ook van toepassing is op partijen die op DigiD aangesloten zijn via een routeringsdienst. Binnen de eID SAML koppelvlakspecificaties 4.4 zijn de certificaten voor TLS, Signing en Encryptie gedefinieerd.

Toelichting op ‘Wijze van aansluiten’

1. DV Rechtstreeks. DV heeft een eigen website (‘dienstverlenerwebsite.nl’) en levert via de betreffende website een dienst waarvoor authenticatie via een routeringsdienst nodig is.
2. DV via LC (Domein LC): DV levert via de website van de (SaaS-)softwareleverancier de betreffende dienst (‘softwareleverancierwebsite.nl’) waarvoor authenticatie via een routeringsdienst nodig is.
3. DV via LC (Eigen domein): DV levert via de applicatie van de (SaaS)softwareleverancier de betreffende dienst, maar wel op zijn eigen domein (‘dienstverlenerwebsite.nl’) waarvoor authenticatie via een routeringsdienst nodig is.

Overgangssituatie EV-Root voor machine-to-machine toepassing

De onder ‘EV-Root’ (intermediate root ‘Staat der Nederlanden Domein Server 2020 CA’) uitgegeven certificaten kunnen nog worden gebruikt voor Machine-to-machine toepassingen indien er een OIN in het certificaat is opgenomen. Een toekomstvaste oplossing voor machine-to-machine toepassingen is het gebruik van G1 certificaten. (zoals opgenomen in bovenstaande tabel)