Logius
Ministerie van Binnenlandse Zaken en Koninkriiksrelaties

Technisch Overleg Digikoppeling

Logius

Bezoekadres:
Wilhelmina v Pruisenweg 52
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

www.logius.nl
servicecentrum@logius.nl

Inlichtingen bij

Peter Haasnoot

digikoppeling@logius.nl

Datum
23 feb 2021

memo

Verplicht gebruik Private Root CA in Digikoppeling
Beveiligingsstandaarden en voorschriften

Toelichting

Hieronder worden de aanpassingen in de Digikoppeling Beveiligingsstandaarden en voorschriften toegelicht:

Private Root

Het TO Digikoppeling heeft eerder (05-03-2020) goedkeuring verleend om het toestaan van 'PKIO Private Root' certificaten (naast 'PKIO Public Root' certificaten) expliciet te benoemen in de Digikoppeling voorschriften.
Vanuit PKIOverheid is aangekondigd dat vanaf 1-1-2021 voor machine-to-machine verkeer de richtlijn is om alleen nog 'PKIO Private Root' certificaten te gebruiken. In het voorgaand TO is besproken dat het wenselijk was dat in de formulering in de Digikoppeling voorschriften wel rekening wordt gehouden met situaties waar het vanuit het oogpunt van certificaat beheer op 1 server voordelen heeft om 'PKIO Public Root' toe te staan in bepaalde situaties.

NCSC Beveiligingsrichtlijnen voor TLS

NCSC publiceerde in december 2020 versie 2.1 van de TLS richtlijnen:

- Afwaardering van TLS 1.2 van Goed naar Voldoende
- Vereiste volgorde algoritmeselecties is versimpeld. Alleen Goed > Voldoende > Uit te faseren nog voorgeschreven. Binnen de verschillende veiligheidsniveau is de volgorde hoofdzakelijk een prestatie-overweging en niet langer voorgeschreven.
- Alleen Goede algoritmeselecties? Dan hoeft de server niet langer de eigen volgorde af te dwingen.
- Client-initiated renegotation van Onvoldoende naar Voldoende

De nieuwe versie van de Digkoppeling beveiligingsvoorschriften verwijst naar deze nieuwe versie 2.1 van de NCSC Beveiligingsrichtlijnen voor TLS

Tekstuele aanpassingen n.a.v. ontwikkeling REST API profiel

De teksten zijn veralgemeniseerd t.b.v. opname REST API profiel, specifieke verwijzingen naar koppelvlak specificaties zijn verwijderd.

Zie voor een overzicht van de aanpassingen :

- *Release_Notes_Wijziging_Digikoppeling_Standaard_documentatie*
- *Overzicht van de tekstuele aanpassingen :* Aanpassingen Digikoppeling Beveiligingsstandaarden en voorschriften (link)

En de bijlagen voor de aangepaste documenten:

Gevraagd besluit aan het TO
Aan de leden van het TO wordt gevraagd in te stemmen met deze wijziging van de Digikoppeling Documentatie

Overzicht van de gewijzigde documenten

- Release_Notes_Wijziging_Digikoppeling_Standaard_documentatie.pdf
- Digikoppeling_Beveiligingsstandaarden_en_voorschriften_v1.4.pdf
- Digikoppeling_Gebruik_en_achtergrond_certificaten_v1.6.1.pdf
- Digikoppeling_Overzicht_Actuele_Documentatie_en_Compliance_v1.6.pdf