Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

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
Pieter Hering
M 06 11597802
pieter.hering@logius.nl

Datum
9 september 2018

Kenmerk

Uw kenmerk

notitie

Gebruik Private Root Certificaat voor Digikoppeling Verkeer

Aanleiding

Op de website van Logius verscheen op 26 maart 2018 vanuit PKIoverheid (PKIo) een artikel[1] over het feit dat Public PKIo services servercertificaten minder lang geldig zijn. De geldigheidsduur van PKIo services servercertificaten met een Public Root is per 2018 verkort naar maximaal *2* jaar.

Logius wijst er in het artikel op dat afnemers ook zogenaamde *Private Root* services servercertificaten kunnen afnemen. Deze certificaten hebben een geldigheidsduur van *3* jaar. Naast de geldigheidsduur verschillen de services servercertificaten van elkaar doordat een Private Root certificaat minder geschikt is voor publiek verkeer over het internet aangezien browsers en operating systemen het certificaat niet automatisch zullen vertrouwen. De eisen die PKIo *Policy Authority* stelt aan de uitgevers van Private Root servercertificaten zijn gelijk aan de eisen die gesteld worden aan de Public Root certificaten.

Het document Digikoppeling Beveiligingsstandaarden en voorschriften schrijft het gebruik van PKIoverheidcertificaten voor, maar vermeldt nergens de begrippen *Public* of *Private Root* PKIO server-certificaten.

Vraag aan het Technisch Overleg

Logius wil in het kader van transparantie over het gebruik van PKIoverheid certificaten het gebruik van zowel Public als Private Root certificaten expliciet toestaan en dus benoemen, vandaar stellen we de volgende vragen aan het TO:

1. **Bent u het eens dat Digikoppeling het gebruik van zowel Public als Private Root moet toestaan?**
   Dit betekent dat Digikoppeling Providers de Private Root PKIo services server-certificaten moeten accepteren. Dit betekent ook dat Providers zelf ook kunnen kiezen voor een Private Root PKIO-services servercertificaat, zodat afnemers ook de Private Root zullen moeten vertrouwen.
2. **Bent u het eens dat Digikoppeling het gebruik van zowel Public als Private Root expliciet moet benoemen in het document Digikoppeling Beveiligingsstandaarden en voorschriften?**

[1] https://www.logius.nl/over-logius/actueel/item/titel/pkioverheid-certificaten-minder-lang-geldig/

Achtergrondinformatie en huidige situatie

PKIoverheid-services servercertificaten worden binnen de digitale overheid veel gebruikt voor het beveiligen van websites en verbindingen tussen systemen, zoals bijvoorbeeld Digipoort. Tot op heden werden daar voornamelijk *publiek vertrouwde* PKIoverheid-server certificaten voor gebruikt. "Publiek vertrouwd" betekent dat het bovenliggende vertrouwensanker (de Root CA) bij operatingsystemen en softwareleveranciers als Microsoft en Google is aangemeld. Dit betekent dat bezoekers van websites die beveiligd zijn met een PKIoverheid-certificaat, het certificaat automatisch vertrouwen. In ruil daarvoor dient Logius te voldoen aan de regelgeving en certificeringen die deze partijen hebben opgesteld.

Omdat softwareleveranciers vele verschillende PKI-infrastructuren ondersteunen met verschillende betrouwbaarheidsniveaus, wordt het eisenpakket van softwareleveranciers de afgelopen jaren uitgebreid en zwaarder. Dit is vanuit de betrouwbaarheidsoptiek van PKIoverheid die al het hoogste niveau ondersteunt, geen enkel probleem. Men stelt echter ook steeds meer eisen aan de levensduur van services servercertificaten. Dit vormt wel een probleem, omdat het daar kan conflicteren met het gebruiksgemak en de eisen vanuit PKIoverheid. Logius heeft daarom Private Root certificaten gecreëerd. Een Private Root certificaat is niet aangemeld bij de leveranciers van browsers en operating systemen en hoeft dus niet te voldoen aan de door hun gestelde eisen. Uiteraard voldoen de certificaten wel aan de reguliere eisen die er ook aan Public Root PKIoverheid-certificaten worden gesteld. Dit betekent dat ze veilig beheerd worden en getoetst zijn door een derde, onafhankelijke (externe) partij.

Per 1 maart 2018 is de maximum geldigheidsduur van services servercertificaten, mits zij publiekelijk worden vertrouwd, gemaximaliseerd op 2 jaar. Dit geldt alleen voor services servercertificaten. Alle andere typen PKIoverheid certificaten onder Public Root blijven dezelfde geldigheid houden.

Overheden en afnemers moeten een afweging maken of ze de voorkeur geven aan een Public dan wel Private Root services servercertificaat. Een Private Root certificaat is langer geldig maar kan eigenlijk niet gebruikt worden voor browserverkeer over het internet aangezien browsers het certificaat niet automatisch vertrouwen. Het is dus belangrijk dat klanten en afnemers een helder beeld hebben van waarvoor ze het certificaat willen gebruiken zodat ze een goede afweging kunnen maken.