
Van: Servicecentrum Logius

Verzonden: dinsdag 9 november 2010 16:47

Onderwerp: Wijzigingen PKIoverheid certificaat vanaf 2011



Logius
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Geachte heer / mevrouw,

Volgens onze gegevens bent u een gebruiker van één of meerdere Logius producten. De producten van Logius zijn beveiligd middels een PKIoverheid certificaat. Aangezien er belangrijke wijzigingen op komst zijn voor het PKIoverheid certificaat ontvangt u deze brief.

Wat is een PKIoverheid certificaat?

Public Key Infrastructure voor de overheid, oftewel PKIoverheid, is de standaard voor het beveiligen van elektronische overheidsdiensten. Met behulp van PKI-certificaten is de informatie die personen en organisaties over het internet sturen op een hoog niveau van betrouwbaarheid beveiligd.

Wat verandert per 1 januari 2011?

Het PKIoverheid certificaat wordt vanaf 1 januari 2011 alleen nog uitgegeven vanuit de nieuwe Root van de Staat der Nederlanden. Dit is een verbeterde en meer toekomstvaste techniek, de zogenoemde "SHA-256" in combinatie met een 2048-bit sleutellengte. Deze wijziging kan gevolgen hebben voor uw dienstverlening.

Hoe kunt u problemen voorkomen?

Wij adviseren u om tijdig een impactanalyse uit te voeren, eventueel in samenwerking met uw leverancier, om te inventariseren of uw applicatie(s) en software met de nieuwe SHA-256 technologie kan omgaan. Applicaties die met de certificaten werken, moeten met deze vernieuwde technologie overweg kunnen. Deze applicaties gebruikt u onder meer om de producten van Logius aan te bieden aan uw klanten. Denk hierbij aan:

- uw webserver die SSL certificaten gebruikt (Windows server, Apache, etc.);
- uw mailclient waarmee u e-mails ondertekent (Outlook, etc.);
- uw operating system dat hiermee samenwerkt (Windows XP, Vista, etc.);
- uw ondertekeningprogrammatuur in uw Document Management System (PDF Sign&Seal, DMS, etc.);
- uw eigen maatwerk toepassing die met certificaten werkt.

Van bepaalde standaard software is een inventarisatie beschikbaar die aangeeft of deze software met SHA-256 overweg kan. De link naar deze inventarisatie treft u aan op de website van Logius:

<http://www.logius.nl/producten/toegang/pkioverheid/documentatie/certificaten-pkioverheid/staat-der-nederlanden-g2/toepasbaarheid/>

Wanneer kunt u het beste beginnen?

Uw huidige certificaten kunt u blijven gebruiken totdat deze niet meer geldig zijn. U hebt nog een aantal maanden de tijd om zekerheid te krijgen dat alles goed blijft werken na introductie van SHA-256. Om verrassingen te voorkomen is het van belang wel alvast te beginnen met uw inventarisatie. Op die manier heeft u voldoende tijd om eventuele upgrades van producten door te voeren of - in het ergste geval - enige software aan te passen.

En mijn oude certificaten?

Die blijven gewoon geldig totdat ze aflopen. U hoeft geen certificaten om te ruilen.

Heeft u vragen naar aanleiding van deze brief, dan kunt u op werkdagen van 8.00 tot 17.00 uur contact opnemen met Servicecentrum Logius op het telefoonnummer 0900 555 4555 (10 ct p/m) of per e-mail via servicecentrum@logius.nl.

Met vriendelijke groet

Gertie Dullens
Hoofd afdeling Markt