

Van: Servicecentrum Logius
Verzonden: maandag 30 mei 2011 14:25
Onderwerp: Certificaatwijziging Digipoort



Logius
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Certificaatwijziging Digipoort

Geachte heer/mevrouw,

Volgens onze gegevens gebruikt u één of meerdere PKIoverheid-certificaten om veilig gebruik te maken van Digipoort (koppelvlak SOAP of WUS) van Logius. Bijvoorbeeld voor e-factureren, ziek- en herstelmeldingen, Standard Business Reporting of DigiInkoop. Graag vragen wij uw aandacht voor een wijziging van het PKIoverheid-certificaat op Digipoort. Deze wijziging heeft mogelijk impact op uw systemen.

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 PKIoverheid-certificaten is de informatie die personen en organisaties over het internet sturen op een hoog niveau van betrouwbaarheid beveiligd. Ook Digipoort is beveiligd door middel van een PKIoverheid-certificaat.

Veilige dienstverlening via internet

Uit recent internationaal onderzoek blijkt dat het algoritme onderliggend aan het SHA1-certificaat in de toekomst niet langer de garantie biedt onkraakbaar te zijn. Reden om het zogenoemde SHA256 algoritme te gebruiken dat vele malen veiliger is. Uw huidige PKIoverheid-certificaat kunt u gewoon blijven gebruiken. Om Digipoort ook in de toekomst veilig te kunnen blijven gebruiken vervangt Logius alvast het certificaat op de Digipoort.

Wat verandert er?

Het PKIoverheid-certificaat op Digipoort wordt op 11 augustus vervangen door een nieuw PKIoverheid-certificaat op basis van SHA256. Dit nieuwe certificaat bevat gewijzigde metadata (onder andere certificaathiërarchie, publieke sleutel en distinguished name).

Het nieuwe PKIoverheid-certificaat is gebaseerd op een verbeterde en meer toekomstvaste techniek, waardoor veilige dienstverlening ook in de toekomst gegarandeerd blijft.

Om de dienstverlening van Digipoort te garanderen moet Logius dit certificaat vervangen. Let wel: u hoeft uw eigen certificaat dus niet te vervangen. Het gaat hier slechts om de vervanging van het Digipoort-certificaat. Echter, om verstoringen in uw systemen te voorkomen, moet u wel een aantal acties ondernemen.

Logius heeft de meest recente informatie rondom SHA256 op [haar website](#) geplaatst.

Wat doet Logius?

Hieronder vindt u de precieze planning van de acties aan de zijde van Logius.

Donderdag 16 juni 2011 - 07:00 uur

Logius stelt op <https://preprod.procesinfrastructuur.nl> een preproductieserver beschikbaar waarop het nieuwe SHA256-certificaat is geïnstalleerd. Deze server kunt u gebruiken om uw eigen software te (laten) testen en te zien of uw systemen met SHA256 om kunnen gaan.

Donderdag 11 augustus 2011- 07:00 uur

Logius vervangt het huidige certificaat door een nieuw SHA256-certificaat in de productie-omgeving.

Wat moet u doen?

Neem contact op met uw intermediair, ICT-afdeling en/of PKIoverheid-leverancier om ervoor te zorgen dat uw applicaties en systemen voor Digipoort, die met PKIoverheid-certificaten werken, de SHA256-technologie ondersteunen.

Voor donderdag 16 juni 2011

Controleer en draag er zorg voor dat uw (test)applicaties en -systemen SHA256-technologie ondersteunen en de metadata uit de nieuwe certificaten herkennen.

Donderdag 16 juni 2011 na 07:00 uur

Configureer uw webservice met de preproductie-omgeving om de nieuwe metadata in te lezen. Hierna kunt u testen of uw systemen het nieuwe PKIoverheid-certificaat kunnen gebruiken.

Voor donderdag 11 augustus 2011

Zorg dat uw productieapplicaties en -systemen de metadata uit de nieuwe certificaten kunnen herkennen.

Donderdag 11 augustus 2011 na 07:00 uur

Configureer uw webservice met de productie-omgeving om de nieuwe metadata in te lezen. Wij kunnen u op verzoek al voorzien van de nieuwe metadata, door u het publiek deel van het nieuwe certificaat ter beschikking te stellen.

Voor de volledigheid wijzen wij er op dat de gehanteerde versleutel- en ondertekenalgoritmen in de koppelvlakken van Digipoort niet wijzigen.

Meer informatie

Als u na het lezen van deze brief vragen heeft, 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