



Certificaatwijziging Digipoort (koppelvlak FTP)

Geachte heer/mevrouw,

Volgens onze gegevens gebruikt u één of meerdere PKIoverheid-certificaten om veilig gebruik te maken van Digipoort (koppelvlak FTP) van Logius. Graag vragen wij uw aandacht voor een wijziging van het PKIoverheid-certificaat op Digipoort. Deze wijziging heeft mogelijk impact op uw systemen.

Wat verandert er?

De PKIoverheid-certificaten op Digipoort worden op 7 december 2011 voor de preproductie-omgeving en 21 december 2011 voor de productie-omgeving vervangen voor nieuwe certificaten op basis van SHA256. De nieuwe PKIoverheid-certificaten zijn gebaseerd op een verbeterde en meer toekomstvaste techniek, waardoor veilige dienstverlening ook in de toekomst optimaal blijft.

Om de dienstverlening van Digipoort te garanderen moet Logius dit certificaat vervangen. 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.

Woensdag 7 december 2011 - 10:00 uur

Logius vervangt het huidige certificaat door een nieuw SHA256-certificaat in de preproductie-omgeving. Dit betreft de volgende server:

- <ftp.pre.otpnet.nl>

Deze server kunt u gebruiken om uw eigen software te (laten) testen en te zien of uw systemen met SHA256 om kunnen gaan.

Woensdag 21 december 2011- 10:00 uur

Logius vervangt het huidige certificaat door een nieuw SHA256-certificaat in de productie-omgeving. Dit betreft de volgende server:

- <ftp.otpnet.nl>

Wat moet u doen?

Stap 1: Bepaal hoe uw systemen de identiteit van Digipoort verifiëren

Bepaal voor de preproductie- en productie-omgeving hoe uw systemen de identiteit van Digipoort verifiëren. Er zijn twee mogelijkheden:

1. Verificatie van de root 'Staat der Nederlanden Root CA – G2'
Wanneer u de identiteit van Digipoort verifieert aan de hand van alleen het rootcertificaat 'Staat der Nederlanden Root CA – G2', dan blijft uw verbinding met Digipoort werken.
2. Verificatie van het certificaat op het laagste niveau
Wanneer u de identiteit van Digipoort verifieert aan de hand van het certificaat op het laagste niveau van de keten, dan kunt u nadat wij het nieuwe certificaat hebben geïnstalleerd geen verbinding meer maken met Digipoort. Om uw verbinding te herstellen dient u het nieuwe certificaat op te nemen in uw trust-store. Dit doet u door het publieke deel van ons certificaat toe te voegen aan uw trust-store. Het [publieke deel van het certificaat](#) kunt u vinden op de website van Logius.

Stap 2: Vervang uw PKIoverheid-certificaten voor SHA256

Als u zelf gebruik maakt van een PKIoverheid-certificaat op basis van SHA1, adviseren wij u deze te vervangen door een PKIoverheid-certificaat op basis van SHA256. Nadat u het nieuwe certificaat geïnstalleerd heeft, moet u het publieke deel daarvan aan Logius sturen, zodat wij op onze beurt ook uw nieuwe certificaat kunnen opnemen in onze trust-store. U kunt het publieke deel sturen naar servicecentrum@logius.nl onder vermelding van 'Nieuw publieke deel Digipoort FTP', met een duidelijke opgave van organisatienaam en e-mailadres en telefoonnummer van een contactpersoon.

Stap 3: Nieuwe certificaat accepteren

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.

1. *Voor woensdag 7 december 2011*
Controleer en draag er zorg voor dat uw testapplicaties en -systemen SHA256-technologie ondersteunen en het nieuwe certificaat herkennen.
2. *Woensdag 7 december 2011 na 10:00 uur*
Test of uw systemen het nieuwe PKIoverheid-certificaat van Digipoort kunnen gebruiken.
3. *Voor woensdag 21 december 2011*
Zorg dat uw productieapplicaties en -systemen de metadata uit de nieuwe certificaten kunnen herkennen.
4. *Woensdag 21 december 2011 na 10:00 uur*
Controleer of uw systemen het nieuw PKIoverheid-certificaat van Digipoort kunnen gebruiken.

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

Achtergrond informatie

Wat is een PKIoverheid-certificaat?

Public Key Infrastructuur 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 niet langer de garantie biedt onkraakbaar te zijn. Reden om het zogenoemde SHA256 algoritme te gebruiken dat vele malen veiliger is. Zo kunt u ook in de toekomst veilig blijven werken met Digipoort.

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

Servicecentrum Logius

