



PKIoverheid en SHA256

ZORG DAT UW DIGITALE DIENSTVERLENING VOLDOET AAN DE NIEUWSTE VEILIGHEIDSSTANDAARD

Per 1 januari 2011 zijn alle nieuwe PKIoverheid-certificaten standaard voorzien van de SHA256-technologie en een 2048 bits sleutellengte. In de meeste toepassingen is ondersteuning hiervoor al geïmplementeerd. Verouderde software kan hier echter niet mee omgaan en dit kan impact hebben op uw diensten. Wij willen u attenderen op de stappen die u moet nemen om gebruik te kunnen maken van deze nieuwe generatie van veiligheidscertificaten.

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.

Veilige dienstverlening via internet

Uit recent internationaal onderzoek blijkt dat het algoritme onderliggend aan het huidige certificaat niet langer de garantie biedt onkraakbaar te zijn. Reden om een nieuw algoritme te ontwikkelen dat

vele malen veiliger is. Om te waarborgen dat uw en onze digitale dienstverlening veilig blijft, heeft Logius besloten dat er vanaf januari 2011 alleen nog PKIoverheid-certificaten worden uitgegeven die voldoen aan de nieuwste veiligheidstandaard. Deze zijn gebaseerd op het zogenoemde SHA256 algoritme. Zo kunnen uw gebruikers ook in de toekomst veilig blijven inloggen met DigiD en veilig gegevens uitwisselen via Digipoort en Digikoppeling. Mocht u geïnteresseerd zijn in meer informatie over PKIoverheid en de SHA256-technologie dan kunt u die vinden op de website van Logius: www.logius.nl/pkioverheid.

Wat doet Logius

De invoering van de verbeterde certificaten gaat niet vanzelf. Hieronder kunt u lezen wat Logius heeft gedaan en gaat doen om de wijziging soepel te laten verlopen.

1. Logius heeft ervoor gezorgd dat leveranciers van de PKIoverheid-certificaten vanaf januari 2011 alleen nog verbeterde certificaten uitgeven.
2. Logius vervangt vanaf dit jaar de certificaten op haar producten en beveiligde websites door het verbeterde SHA256-certificaat.
3. Logius heeft de meest recente informatie rondom deze ontwikkeling op haar website geplaatst.

Wat moet u doen

Ook uw organisatie moet enkele voorzorgsmaatregelen nemen om er voor te zorgen dat uw elektronische dienstverlening goed beveiligd is. En u moet er voor zorgen dat uw applicaties en systemen voorbereid zijn op het verwerken van de nieuwe generatie PKIoverheid-certificaten die onderdeel vormen van producten zoals DigiD, Digipoort en Digikoppeling. Hieronder vindt u een overzicht van de acties die u vanaf nu dient te nemen.

1. Neem contact op met uw ICT-afdeling en/of leverancier om ervoor te zorgen dat uw applicaties en systemen, die met PKIoverheid-certificaten werken, de SHA256-technologie ondersteunen. Dit is van belang zodra Logius een certificaat vervangt door een SHA256-certificaat.

2. Neem contact op met uw PKIoverheid-leverancier om in kaart te brengen wanneer uw huidige PKIoverheid-certificaten verlopen. Zodra een van uw certificaten verloopt, kunt u alleen nog maar SHA256-certificaten kopen. Zorg er vervolgens samen met uw ICT-afdeling en/of leverancier tijdig voor dat u de nieuwe certificaten op uw applicaties en systemen kunt installeren.
3. Zorg dat de besturingssystemen en internetbrowsers binnen uw organisatie voldoen aan de minimale eisen die de SHA256-technologie vraagt. Hiermee maakt u uw organisatie klaar voor de nieuwste generatie van beveiligingscertificaten. Een overzicht van de minimale eisen staat op de website van Logius: www.logius.nl/pkioverheid.
4. Informeer de gebruikers van uw digitale diensten. Webapplicaties die gebruik maken van het beter beveiligde SHA256-certificaat vragen om recente besturingssystemen en internetbrowsers. Voorkom dat bezoekers van uw webapplicatie problemen ondervinden en bijvoorbeeld niet meer kunnen inloggen met DigiD of gebruik kunnen maken van Digipoort.

Conclusie

Wacht niet langer en kom nu in actie om uw digitale dienstverlening te laten voldoen aan de nieuwste veiligheidstandaard.

Contactgegevens

Heeft u vragen of wilt u meer informatie? Neem dan contact op met Servicecentrum Logius.

Telefoon: 0900 555 4555 (10 ct p/m)

E-mail: servicecentrum@logius.nl

www.logius.nl/pkioverheid

Oplage: 250

© juni 2011. Logius

Deze factsheet is gedrukt op FSC papier.