

.....

In deze rubriek lichten we een product van Logius uit. Dit keer aandacht voor PKI-overheid certificaten.

Wat zijn PKI-overheid certificaten?

Public Key Infrastructure voor de overheid, oftewel PKI-overheid, 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. We gebruiken PKI-overheid certificaten bij het zetten van een rechtsgeldige elektronische handtekening en het betrouwbaar communiceren met websites. Maar ook voor het op afstand authenticeren van personen of services of het versleutelen van berichten. Logius houdt toezicht op een aantal organisaties dat namens PKI-overheid certificaten uitgeeft.

Wat verandert per 1 januari 2011?

Dan worden PKI-overheid certificaten alleen nog uitgegeven vanuit een nieuwe Root van de Staat der Nederlanden: de G2-root. Dit kan gevolgen hebben voor het gebruik van certificaten en dienstverlening. U gebruikt bijvoorbeeld elektronische certificaten voor het digitaal ondertekenen van documenten. Deze toepassing maakt gebruik van twee algoritmen. Eén om te bevestigen dat de informatie niet door derden is veranderd, de ander om de identiteit te bevestigen van degene die de informatie "ondertekent". Deze elektronische certificaten worden vanaf 1 januari 2011 met een verbeterde en meer toekomstvaste techniek uitgerust, de zogenoemde "SHA-256" in combinatie met

2048-bit sleutellengten. Dit gebeurt op aanbeveling van de Amerikaanse overheidsorganisatie NIST. Deze organisatie heeft aangegeven tot uiterlijk 31 december 2010 SHA-1-certificaten uit te geven en dan over te gaan op een algoritme van de sterkere SHA-2-familie. Daarom is het belangrijk om nu over te stappen naar de nieuwste veilige techniek.

Wat betekent dit voor u?

Check tijdig of uw applicatie of de software waarmee u werkt met de nieuwe SHA-256-technologie kan omgaan. In het ergste geval kan het namelijk voorkomen dat uw programma of applicatie hierdoor niet meer werkt.

Voor meer informatie:
www.logius.nl/pki-overheid.

