Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aan de voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA Den Haag

www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk

Kenmerk
2019-0000152324

Uw kenmerk

Datum	22 maart 2019
Betreft	Vervanging certificaten PKIoverheid

Op 11 maart jl. heeft Logius, onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, vastgesteld dat certificaten die voor digitale dienstverlening van de Nederlandse overheid worden gebruikt, vervangen moeten worden. Met deze brief informeer ik u over de aanleiding daarvan en de wijze waarop de vervanging georganiseerd wordt.

Aanleiding vervanging digitale certificaten
Overheidsdiensten maken voor hun digitale dienstverlening gebruik van certificaten die de veiligheid en betrouwbaarheid van een dienst waarborgen. Burgers kunnen bijvoorbeeld aan de hand van zo'n certificaat in hun internetbrowser zien dat zij met een authentieke website van de overheid te maken hebben; dit is te herkennen aan het slotje in de adresbalk.

Deze certificaten worden op drie niveaus uitgegeven binnen het zogenaamde stelsel "Public Key Infrastructure" (PKIoverheid): een stamcertificaat, tussenliggende certificaten en eindgebruikerscertificaten. Eindgebruikerscertificaten zijn onderverdeeld in servercertificaten en persoonsgebonden certificaten. De uitgifte van certificaten binnen het stelsel vindt plaats onder de verantwoordelijkheid van de Nederlandse overheid. Logius geeft namens de Staat der Nederlanden het stamcertificaat uit, en als toezichthouder op het stelsel de tussenliggende certificaten. Zowel het stamcertificaat als de tussenliggende certificaten zijn bij Logius in beheer. Eindgebruikerscertificaten worden geleverd door publieke en private certificaatverstrekkers[1].

De minimale eisen die aan deze certificaten worden gesteld, worden in een internationale gemeenschap afgestemd en afgesproken. Deze gemeenschap bestaat uit internetbrowsers, verstrekkers van certificaten en toezichthouders. Met name de grote internetbrowsers (Mozilla, Apple, Microsoft en Google) hebben hier een krachtige stem, omdat zij veiligheid van hun browsers voor eindgebruikers willen garanderen. Zij laten daarom alleen maar diensten op hun browsers toe die voldoen aan de minimale eisen. Naast een veilig en betrouwbaar

[1] Zie https://www.logius.nl/diensten/pkioverheid voor meer informatie over het stelsel en www.pkioverheid.nl voor een overzicht van certificaten.

internet streven de internetbrowsers ook volledige transparantie na. Afspraken over eisen worden gemaakt en aangepast via het openbare internetforum van deze internationale gemeenschap.
Op 9 maart jl. is door de genoemde gemeenschap een strengere uitleg van één van de technische eisen gepubliceerd. Logius monitort als toezichthouder actief op aanpassingen in de gestelde eisen. Op 11 maart jl. heeft Logius op basis van de publicatie uitvraag gedaan onder verstrekkers van certificaten binnen het stelsel. Hierop is vastgesteld dat een deel van de tussen 30 september 2016 en 5 maart 2019 uitgegeven certificaten niet voldoet aan deze strengere uitleg. Logius heeft daarop onderzocht welke certificaten daadwerkelijk vervangen moeten worden. Het betreft tussenliggende en eindgebruikerscertificaten.

Het niet voldoen aan deze strengere uitleg betekent overigens niet dat het gebruik van bijvoorbeeld een website met zo'n certificaat onveilig is. Er is geen sprake van een beveiligingsprobleem. Om het vertrouwen in de Nederlandse certificaten internationaal te behouden, moeten deze wel aan die strenger uitgelegde eis gaan voldoen. Daartoe moeten deze vervangen worden.

Te nemen stappen
De verstrekkers van de te vervangen certificaten zijn door Logius als toezichthouder geïnformeerd over het niet voldoen aan de strenger uitgelegde eis. Op dit moment werkt Logius een plan voor deze vervanging uit. Logius heeft aangekondigd dat maximaal 14 tussenliggende certificaten en maximaal 22.000 daaronder vallende servercertificaten vervangen moeten worden. Belangrijke uitgangspunten bij de vervanging zijn het borgen van vertrouwen in de certificaten en continue beschikbaarheid van onze online diensten. De vervanging wordt gefaseerd uitgevoerd, waarmee de uitvoerbaarheid en zorgvuldigheid worden gewaarborgd.

Logius streeft ernaar binnen 14 maanden de certificaten te laten vervangen. Deze tijd is nodig vanwege het grote aantal nieuw uit te geven certificaten en de zorgvuldige procedure die voor de uitgifte van certificaten geldt. De certificaatverstrekkers informeren de organisaties waarvan de certificaten daadwerkelijk vervangen moeten worden.

Voor het vervangingsplan en de termijn wordt ook in internationaal verband draagvlak gezocht. Het kunnen uitvoeren van het beoogde vervangingsplan is namelijk afhankelijk van acceptatie door de internationale gemeenschap. Dit volgt uit de wijze waarop dit stelsel is georganiseerd, zoals ik eerder in deze brief heb toegelicht.

Datum
22 maart 2019

Kenmerk
2019-0000152324

Tot slot
Ik benadruk dat de veiligheid van de huidige certificaten niet in het geding is. Burgers kunnen veilig digitaal zaken met de overheid doen. Met het vervangen van de certificaten die niet aan de strenger uitgelegde eis voldoen, blijft het vertrouwen in de digitale diensten van de Nederlandse overheid ook in de toekomst gewaarborgd. Ik zal uw Kamer nader informeren over de uitvoering van het vervangingsplan.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

drs. R.W. Knops