Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

PKIoverheid stopt met webcertificaten

Kies een andere leverancier

Factsheet 2021-03 | versie 1.0 | 30 september 2021

Logius heeft aangekondigd te stoppen met de uitgifte van publiek vertrouwde webservercertificaten onder PKIoverheid. Als uw organisatie op dit moment gebruikmaakt van zulke certificaten, dan zult u een alternatief moeten zoeken. Ga na welke van uw certificaten publiek vertrouwde webservercertificaten van PKIoverheid zijn. Bepaal voor elk van deze certificaten door welk type certificaat u het wilt vervangen. Kies vervolgens een of meerdere certificaatleveranciers die de benodigde certificaten kunnen leveren. De criteria in deze factsheet helpen u daarbij.

Achtergrond

Het PKIoverheid-stelsel is in beheer bij Logius. Binnen dit stelsel worden allerlei digitale certificaten uitgegeven, voor gebruik binnen en communicatie met de overheid. Eindcertificaten die binnen dit stelsel worden uitgegeven, heten ook wel PKIoverheid-certificaten. Logius heeft de daadwerkelijke uitgifte van PKIoverheid-certificaten uitbesteed, onder meer aan marktpartijen zoals Digidentity, KPN en QuoVadis.

Logius heeft op 2 augustus aangekondigd[1] te stoppen met de uitgifte van publiek vertrouwde webservercertificaten onder PKIoverheid. Deze certificaten zullen na 4 december 2022 niet meer geldig zijn. Ook zullen leveranciers enkele maanden daarvoor al stoppen met het uitgeven van nieuwe certificaten van dit type.

Webservercertificaten heten ook wel TLS-certificaten. Ze worden bijvoorbeeld gebruikt om bezoekers van een openbare website beveilgd te laten verbinden (https). Ook op intranetsites en zogenaamde machine-to-machine-koppelingen kunnen publiek vertrouwde webservercertificaten in gebruik zijn. Naast publiek vertrouwde webservercertificaten geeft PKIoverheid ook allerlei andere soorten certificaten uit.[2]

Wat is er aan de hand?

Als uw organisatie op dit moment gebruikmaakt van publiek vertrouwde webservercertificaten van PKIoverheid, dan zult u een alternatief moeten zoeken. De harde deadline voor het verlopen van de certificaten is 4 december 2022. Vanaf 4 december 2021, een jaar eerder, zullen publiek vertrouwde webservercertificaten van PKIoverheid nog enkele maanden worden uitgegeven met een verkorte levensduur, zodat ook deze verlopen op de harde deadline.

Doelgroep

Houders van publiek vertrouwde webservercertificaten van PKIoverheid

Aan deze factsheet hebben bijgedragen:

- AIVD/NBV
- Dienst Publiek en Communicatie
- Logius
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

[1] Zie https://logius.nl/actueel/pkioverheid-stopt-met-uitgeven-publiek-vertrouwde-webserver-ssltls-certificaten.

[2] Zie ook https://logius.nl/diensten/pkioverheid.

Wat adviseert het NCSC?

Het NCSC adviseert u na te gaan welke van uw certificaten publiek vertrouwde webservercertificaten van PKIoverheid zijn, en u voor te bereiden op de vervanging ervan.

Certificaten opzoeken in CT-logs

U kunt in zogenaamde Certificate Transparency-logs een overzicht opvragen van de publiek vertrouwde webservercertificaten die voor een domeinnaam zijn uitgegeven. In dit voorbeeld gebruiken we 'example.nl' in de plaats van uw domeinnaam.

1. Ga naar https://crt.sh en klik op 'Advanced...'.
2. Voer als zoekterm '%.example.nl' in en zet 'Exclude expired certificates' aan. Klik op 'Search'.
3. U krijgt een overzicht van alle nu geldige publiek vertrouwde webservercertificaten voor uw domeinnaam en subdomeinen.
4. Als bij een certificaat een van deze waardes in het Issuer Name-veld staat, gaat het om een PKIoverheid-certificaat:

- C=NL, O=Digidentity B.V., CN=Digidentity PKIoverheid Server CA 2020
- C=NL, O=KPN B.V., CN=KPN PKIoverheid Server CA 2020
- C=NL, O=QuoVadis Trustlink B.V., CN=QuoVadis PKIoverheid Server CA 2020

U kunt publiek vertrouwde webservercertificaten van PKIoverheid herkennen door te controleren of deze herleidbaar zijn naar het stamcertificaat "Staat der Nederlanden Domein Server CA 2020". Het NCSC adviseert een administratie bij te houden van uw certificaten en waar u deze gebruikt. Daar zou u deze informatie moeten kunnen terugvinden.[3] Voor een volledig overzicht kunt u ook de Certificate Transparency-logs raadplegen (zie kader "Certificaten opzoeken in CT-logs").

Bepaal voor elk van deze certificaten door welk type certificaat u het wilt vervangen. De paragraaf "Welk soort certificaat heb ik nodig?" helpt u hierbij.

Kies vervolgens een of meerdere certificaatleveranciers die de benodigde certificaten kunnen leveren. U vindt hierover informatie bij "Waar moet ik op letten als ik een certificaatleverancier kies?".

In het algemeen is het raadzaam om voor de selectie van beveiligingsproducten en leveranciers een risicoanalyse uit te voeren. Bij de aanschaf van een certificaat staan veel zaken al vast, of volgen ze uit eisen die men aan de clientzijde van de verbinding stelt. Soms moet u in de keuze voor een type certificaat of leverancier zelf een risicoanalyse maken. Dat staat dan in de tekst vermeld.

Welk soort certificaat heb ik nodig?

Webservercertificaten verschillen functioneel van elkaar in drie opzichten: de mate van controle bij uitgifte, de wijze waarop de domeinnaam vermeld staat, en het stamcertificaat waaronder het uitgegeven is. Bepaal op deze punten aan welke eisen uw certificaten in de toekomst moeten voldoen.

Merk op dat dit advies alleen betrekking heeft op het afnemen van webservercertificaten. PKIoverheid stopt alleen met de uitgifte van publiek vertrouwde webservercertificaten.

[3] Meer adviezen over certificaatbeheer vindt u in de NCSC-factsheet 'Veilig beheer van digitale certificaten': https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-veilig-beheer-van-digitale-certificaten.

Neemt u ook andere soorten certificaten van PKIoverheid af? Dat kunt u dan blijven doen. Voor deze andere certificaten hoeft u geen nieuwe leverancier te zoeken.

De controle: DV, OV, EV, QWAC

Voor openbare websites en de meeste andere toepassingen van webservercertificaten, voldoet een DV (Domain Validation)-certificaat. Bij DV-certificaten controleert de leverancier de vermelde domeinnaam, maar niet de identiteit van de aanvrager. Vraagt u bijvoorbeeld een DV-certificaat voor ncsc.nl aan, dan controleert de leverancier wel dat u de houder bent van de domeinnaam ncsc.nl, maar hij vraagt u niet de naam van uw organisatie, of verder bewijs dat u namens deze organisatie handelt.

Certificaten van het type Organisation Validation (OV), Extended Validation (EV) en Qualified Website Authentication Certificate (QWAC) kennen een oplopend niveau van controle op de identiteit van de aanvrager. Deze certificaten vermelden die identiteit ook, zodat het voor de bezoeker van een website mogelijk is om op te vragen wie de eigenaar van de website is. Vroeger leidde het gebruik van een EV-certificaat ook tot een zogenaamde 'groene balk' in de browser van bezoekers, maar geen van de populaire browsers doet dit nog. De meerwaarde van een OV-, EV- of QWAC-certificaat is daarmee beperkt voor toepassingen waar een lager niveau, zoals DV, ook geaccepteerd wordt.

In sommige sectoren is het gebruik van een certificaat met een zeker controleniveau voor bepaalde toepassingen verplicht. Deze verplichting volgt dan uit sectorale wet- en regelgeving. Het NCSC is op de hoogte van één geval waarin dit speelt. Bedrijven in de financiële sector zijn op basis van de PSD2-wetgeving verplicht om voor bepaalde machine-to-machine-koppelingen een QWAC-certificaat te gebruiken.

Sommige toepassingen vereisen een certificaat dat een OIN (Organisatie-Identificatienummer) bevat. Dit speelt een rol bij geautomatiseerde berichtenuitwisseling met de overheid. Digikoppeling is hiervan het belangrijkste voorbeeld.[4] Het OIN staat vermeld op OV-certificaten van PKIoverheid. U kunt na de deadline dergelijke OV-certificaten nog steeds bij PKIoverheid afnemen, onder het stamcertificaat "Staat der Nederlanden Private Root CA - G1". Meer informatie vindt u op de website van Logius.[5] Omdat certificaten onder dit stamcertificaat niet publiek vertrouwd zijn, kunt u deze niet gebruiken voor openbare websites.

De vermelding van de domeinnaam

Veel certificaten vermelden maar een of twee domeinnamen, maar het is mogelijk om een certificaat te maken dat voor veel meer domeinnamen tegelijk geldt. De domeinnamen waarvoor een certificaat geldt, staan vermeld in het Subject Alternative Name-veld.

Voor verschillende toepassingen kunt u het beste ook verschillende certificaten gebruiken. Als er dan iets misgaat met een certificaat, hoeft u het niet op allerlei andere plaatsen ook te vervangen. Maar als één toepassing meerdere domeinnamen betreft, kunt u deze wel samenvoegen op hetzelfde certificaat. Websites zijn hiervan een voorbeeld. Is één website onder meerdere domeinnamen te bereiken, dan is het logisch om een certificaat voor al die domeinnamen tegelijk aan te vragen. Gaat het om meerdere aparte websites? Gebruik dan aparte certificaten. Ook

[4] Zie https://www.logius.nl/diensten/digikoppeling.

[5] Zie https://www.logius.nl/diensten/oin.

als het om meerdere websites op één webserver gaat.

In sommige toepassingen is van tevoren niet bekend welke subdomeinen er precies zullen worden aangeroepen, of wilt u niet dat deze subdomeinen openbaar worden.[6] In zulke gevallen kunt u een *wildcardcertificaat* gebruiken. Dat is een certificaat dat voor alle subdomeinen van een domein tegelijk geldt. De vermelding is dan '*.example.nl'. Als u een wildcardcertificaat gebruikt, loopt u een iets groter risico dan bij een certificaat waar alle domeinnamen apart op staan. Een aanvaller die over de geheime sleutel beschikt, kan het immers ook gebruiken om andere toepassingen met een subdomein van die domeinnaam aan te vallen. Sommige certificaatleveranciers ondersteunen geen wildcardcertificaten. Overweegt u om een wildcardcertificaat te gebruiken, voer dan eerst een risicoanalyse uit.

Het stamcertificaat

Het stamcertificaat waaronder een webservercertificaat is uitgegeven, is bepalend voor het vertrouwen dat anderen in het certificaat stellen. Als clientsoftware een verbinding opzet, zal deze het certificaat van de server alleen accepteren als het is uitgegeven onder een voor hem vertrouwd stamcertificaat.

Als we spreken van *publiek vertrouwde* webservercertificaten, dan bedoelen we certificaten die zijn uitgegeven onder een stamcertificaat uit de web-PKI. De web-PKI is een verzameling van ruim honderd stamcertificaten die standaard vertrouwd worden door moderne browsers en veel andere TLS-clientsoftware. Gebruikt uw toepassing een certificaat dat onder een van deze stamcertificaten is uitgegeven, dan kunt u ervan uitgaan dat moderne TLS-clientsoftware zonder meer met uw server kan verbinden.

De samenstelling van de web-PKI kan enigszins variëren tussen browsers en andere TLS-clientsoftware. Het is dus mogelijk dat de ene browser of TLS-clientsoftware een certificaat accepteert, en de andere niet. De lijst van stamcertificaten die een browser of TLS-clientsoftware accepteert, heet de *trust store*. Is het voor u belangrijk dat een breed scala aan clientsoftware zonder problemen met uw server kan verbinden? Vraag uw certificaatleverancier dan in welke trust stores het gebruikte certificaat is opgenomen. Een overzicht van belangrijke trust stores vindt u op de website[7] van Logius.

Voor interne toepassingen is het niet nodig om een certificaat af te nemen dat is uitgegeven binnen de web-PKI. U kunt clientsoftware immers zo instellen dat hij een intern stamcertificaat ook accepteert. Voor zulke toepassingen kunt u bijvoorbeeld gebruikmaken van PKIoverheid-webservercertificaten onder het stamcertificaat 'Staat der Nederlanden Private Root CA - G1'. Dit heeft een aantal voordelen, zoals een langere geldigheidsduur van de uitgegeven certificaten. U kunt dergelijke certificaten afnemen bij de PKIoverheid-TSP's:[8] Digidentity, KPN en QuoVadis.

Waar moet ik op letten bij het kiezen van een leverancier?

Kies een certificaatleverancier die certificaten kan leveren die u nodig heeft, op basis van uw inventarisatie uit de vorige paragraaf. Waarschijnlijk zijn er dan alsnog honderden

[6] Publiek vertrouwde webservercertificaten worden opgenomen in openbare Certificate Transparency-logs. Alle domeinnamen waarvoor u een certificaat aanschaft, zijn daarmee ook voor derden in te zien.

[7] Zie https://www.logius.nl/diensten/pkioverheid/hoe-werkt-het/browserondersteuning.

[8] TSP staat voor Trust Service Provider, een partij die door de houder van een stamcertificaat is geautoriseerd om onderliggende certificaten uit te geven.

partijen die in aanmerking komen. Overweeg bij de verdere selectie daarom welke leverancier past bij de manier waarop uw organisatie certificaten gebruikt. U kunt de criteria eventueel prioriteren met behulp van een risicoanalyse.

Prijs

Certificaten variëren sterk in de aanschafprijs, van gratis bij sommige leveranciers van DV-certificaten, tot honderden euro's voor een QWAC-certificaat. Onderzoek daarom welk soort certificaat past bij uw toepassing, en koop geen certificaten met een strengere controle bij uitgifte dan voor uw toepassing noodzakelijk is. Ook kunt u leveranciers onderling op hun tarieven vergelijken.

Uitstraling

Een vertrouwde naam kan bijdragen aan de uitstraling van uw organisatie. Dat geldt ook voor uw certificaatleverancier. De meeste van uw bezoekers zullen weliswaar niet controleren wie uw webservercertificaat heeft uitgegeven, maar desondanks kan het voor u belangrijk zijn dat u hiervoor niet met zomaar een partij in zee gaat.

Een vergelijkbare overweging speelt bij het land van vestiging van de certificaatleverancier. Voor het feitelijke veiligheidsniveau maakt het weinig uit, maar het kan voor uw bezoekers desondanks een geruststelling zijn als u een certificaat gebruikt dat bijvoorbeeld door een Nederlandse of Europese partij geleverd is.

Ervaringen uit het verleden

Als u goede ervaringen heeft met de PKIoverheid-TSP (Digidentity, KPN, QuoVadis) die hiervoor uw publiek vertrouwde webservercertificaten voor PKIoverheid uitgaf, neemt u dan contact met hen op. Waarschijnlijk kunnen ze u onder een ander stamcertificaat alsnog van publiek vertrouwde webservercertificaten voorzien - ook nadat PKIoverheid daarmee stopt.

Levertijden voor certificaten

Veel certificaatleveranciers doen de controles voor nieuwe certificaten deels handmatig. Dit geldt in het bijzonder voor de strengere controles bij uitgifte, zoals voor EV- en QWAC-certificaten. Dit kan een belemmering vormen wanneer u snel of op ongebruikelijke momenten over nieuwe certificaten wilt beschikken. Zorg dat u een leverancier kiest die kan leveren in het tempo en op de momenten die bij uw organisatie passen.

Procedure voor domeinvalidatie

Verschillende certificaatleveranciers controleren het eigenaarschap van domeinen op verschillende manieren. Als u veel certificaten afneemt, dan kan dit een tijdrovende klus zijn. Kies daarom een leverancier die domeinnamen valideert op een manier die uw beheerders niet extra belast, bijvoorbeeld omdat ze ook eerder al zo werkten.

Automatisering: ACME

Steeds meer certificaatleveranciers automatiseren het proces van domeinvalidatie en certificaatuitgifte, in het bijzonder bij de uitgifte van DV-certificaten. De bekendste standaard hiervoor is ACME, die is ontwikkeld en gepopulariseerd door certificaatleverancier Let's Encrypt. Het aantal leveranciers dat ACME ondersteunt is nog beperkt, maar het valt te verwachten dat dit de komende jaren zal groeien. Neemt u veel certificaten af of heeft u interesse in het automatiseren van dit proces? Kies dan een leverancier die dit al ondersteunt, of die hier in elk geval plannen voor heeft.

Ondersteuning bij incidenten

Certificaten spelen een centrale rol in het creëren van vertrouwen in uw ICT. Bij incidenten in uw eigen organisatie of bij uw certificaatleverancier kan het daarom nodig zijn om intensief met uw leverancier samen te werken voor een effectieve respons. Zorg dat u een leverancier betrekt die minstens even

bereikbaar en professioneel is als uw eigen organisatie in het geval van een beveiligingsincident.

Een tweede leverancier?

Het NCSC adviseert om voor kritieke toepassingen een tweede certificaat bij een andere leverancier aan te schaffen. Als een leverancier ernstige beveiligingsproblemen heeft, kunnen beheerders van trust stores besluiten het vertrouwen in deze leverancier op te zeggen. Als uw primaire leverancier onverhoopt uit een belangrijke trust store verwijderd wordt, kan uw kritieke toepassing met een tweede certificaat nog steeds beschikbaar blijven. Kies voor dit tweede certificaat een leverancier die een ander stamcertificaat gebruikt dan uw primaire leverancier. Met een risicoanalyse kunt u bepalen of de aanschaf van een tweede certificaat voor uw toepassing van waarde is.

Tot slot

Voor de veiligheid van uw verbindingen maakt het in beginsel niet uit bij welke certificaatleverancier u uw publiek vertrouwde webservercertificaten afneemt. De web-PKI omvat honderden certificaatleveranciers. Elk van deze leveranciers heeft de technische mogelijkheid om publiek vertrouwde webservercertificaten voor uw domeinnamen uit te geven.

Als een van deze leveranciers zijn beveiliging niet op orde heeft, kan een aanvaller de systemen van deze leverancier misbruiken om een certificaat voor uw domeinnamen aan te vragen. Dat gebeurde bijvoorbeeld tijdens de Diginotar-crisis in 2011. Of u klant bent bij de aangevallen leverancier, doet voor dit risico niet ter zake.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

september 2021