Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

PKIoverheid verandert

Coördineer de benodigde veranderingen in uw ICT-processen

Factsheet FS-2020-05 | versie 1.0 | 4 september 2020

De komende maanden zullen er wijzigingen in het PKIoverheid-stelsel plaatsvinden om een in juli ontdekt probleem op te lossen. De certificaat-verstrekkers zijn inmiddels gestart met het vervangen van PKIoverheid-eindcertificaten. Als uw proces steunt op PKIoverheid-eindcertificaten die worden vervangen, dan kan uw proces stilvallen of verstoord raken. Het NCSC adviseert u om te onderzoeken of er wijzigingen in uw ICT-proces nodig zijn, en centrale coördinatie te voeren op deze wijzigingen. De benodigde wijzigingen zullen zitten in de manier waarop software in uw ICT-proces eindcertificaten controleert.

Achtergrond

Digitale certificaten worden gebruikt in allerlei toepassingen als basis voor het verkrijgen van vertrouwen. Voorbeelden van zulke toepassingen zijn beveiligde verbindingen, digitale handtekeningen en versleuteld berichtenverkeer. De authenticiteit van het gebruikte certificaat is cruciaal voor de veiligheid van de toepassing waarin het gebruikt wordt.

Digitale certificaten worden in de praktijk vaak georganiseerd in een Public Key Infrastructure (PKI). Met behulp van een PKI kan een partij de authenticiteit van een aangeboden eindcertificaat controleren. Een PKI bestaat uit een aantal stamcertificaten en afspraken over de manier waarop vertrouwen in uitgegeven eindcertificaten wordt toegekend. PKI's vormen de basis van toepassingen als HTTPS, S/MIME en persoonsauthenticatie.

Elke toepassing van eindcertificaten op basis van een PKI kent globaal dezelfde opzet. De houders van stamcertificaten in de PKI stellen geautoriseerde certificaatverstrekkers[1] aan, en voorzien hen van een tussencertificaat. De certificaatverstrekkers leveren eindcertificaten aan certificaathouders. Deze eindcertificaten maken ze met behulp van hun tussencertificaat. Een certificaathouder kan zijn identiteit bewijzen door zijn eindcertificaat te tonen aan een controlerende partij. De controlerende partij gaat na of het eindcertificaat van de certificaathouder te herleiden is tot een stamcertificaat uit de PKI. Zo ja, dan accepteert hij het certificaat.

PKIoverheid is een Nederlandse overheids-PKI die wordt beheerd door Logius. PKIoverheid bevat drie stamcertificaten:[2]

- Staat der Nederlanden EV Root CA ('EV-root')
- Staat der Nederlanden Root CA G3 ('public root')
- Staat der Nederlanden Private Root CA G1 ('private root')

Doelgroep

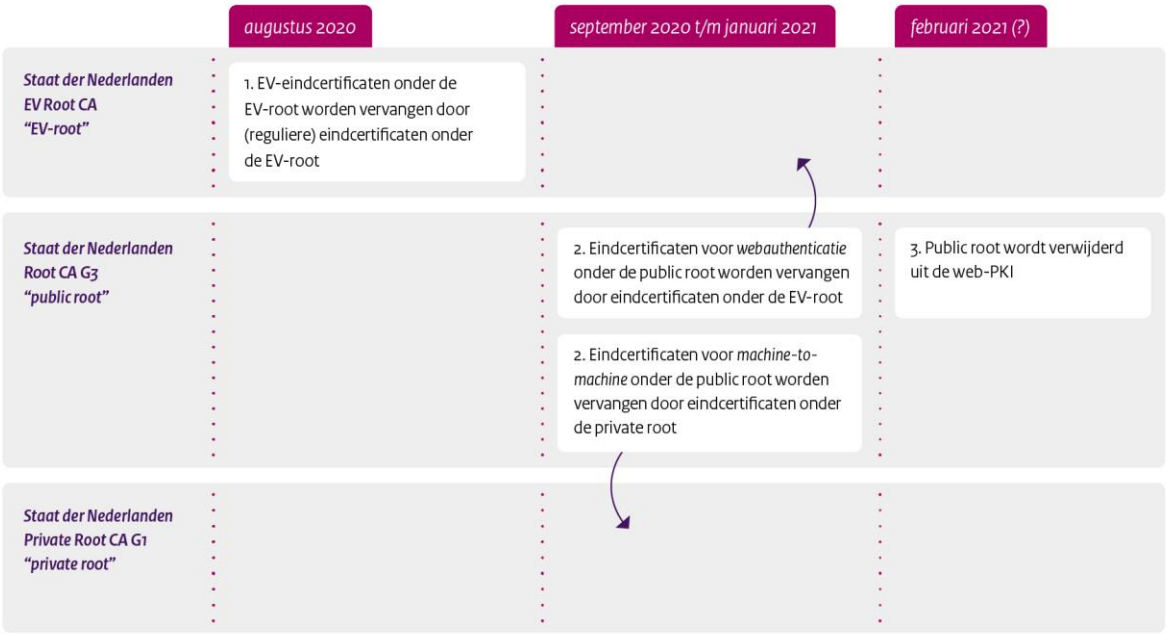
Beleidsmedewerkers ICT die verantwoordelijk zijn voor processen die PKIoverheid-eindcertificaten gebruiken

Aan deze factsheet hebben bijgedragen:

- Informatiebeveiligingsdienst gemeenten
- Logius
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

[1] Deze partijen worden ook wel trust service providers (TSP's) genoemd.

[2] Zie voor meer informatie over de stamcertificaten van PKIoverheid https://pkioverheid.nl/.

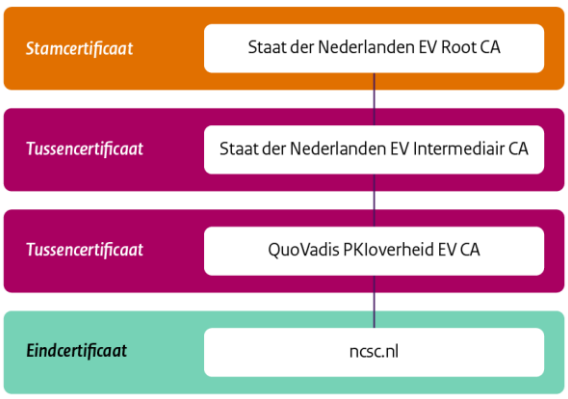


Figuur 1: Het actieplan van Logius

Logius heeft voor PKIoverheid verschillende certificaatverstrekkers aangewezen, zowel overheidspartijen als commerciële aanbieders van certificaten. Afhankelijk van de toepassing kunnen certificaathouders bij een van deze verstrekkers terecht om een PKIoverheid-eindcertificaat te verkrijgen.

Elke toepassing van eindcertificaten kent eigen regels over de te gebruiken PKI. Zo kan een toepassing direct PKIoverheid gebruiken. Elk eindcertificaat binnen deze toepassing moet dan herleidbaar zijn naar een PKIoverheid-stamcertificaat. In andere gevallen worden de PKIoverheid-stamcertificaten samen met andere stamcertificaten in een grotere PKI gebruikt. Certificaathouders hebben dan meer keuze bij welke certificaatverstrekker ze hun eindcertificaten verkrijgen.

Webbrowsers maken gebruik van een speciale PKI, de web-PKI. Deze PKI bestaat uit meer dan honderd stamcertificaten die door webbrowsers vertrouwd worden. Elk van de houders van zo'n stamcertificaat kan eindcertificaten uitgeven die in elke browser vertrouwd worden voor het opzetten van een HTTPS-verbinding. Twee van de PKIoverheid-stamcertificaten, de public root en de EV-root, zijn onderdeel van de web-PKI. Eindcertificaten die uitgegeven zijn onder deze stamcertificaten worden dus in alle webbrowsers vertrouwd.



Figuur 2: Een voorbeeld van de samenhang tussen stam-, tussen- en eindcertificaten

De web-PKI wordt ook regelmatig gebruikt in andere toepassingen. Zo kan boekhoudsoftware bijvoorbeeld de verbinding met een overheidsdienst beveiligen door het controleren van een eindcertificaat, dat hij weet te herleiden naar een stamcertificaat uit de web-PKI. In feite gaat het hierbij om oneigenlijk gebruik van de web-PKI. Browsermakers, de partijen die de

Het actieplan van Logius in het kort[5]

1. Logius en de certificaatverstrekkers vervangen alle extended validation (EV-) eindcertificaten onder de EV-root door reguliere (OV-) eindcertificaten onder hetzelfde stamcertificaat. Dit gebeurt voor 4 september 2020.
2. Logius en de certificaatverstrekkers vervangen alle eindcertificaten onder de public root die geschikt zijn voor TLS-verkeer door eindcertificaten onder de EV-root of de private root. Dit geldt zowel voor eindcertificaten die gebruikt worden voor het beveiligen van webverkeer (HTTPS) als voor machine-to-machine-verkeer. Eindcertificaten die dienen voor het beveiligen van webverkeer worden overgezet naar de EV-root, eindcertificaten die alleen dienen voor machine-to-machine-verkeer worden overgezet naar de private root. Voor deze vervanging heeft Logius een tijdpad tot en met januari 2021 vastgesteld, waarbij voor eindcertificaten voor het beveiligen van webverkeer kortere deadlines gelden.
3. Logius verzoekt de browsermakers om de public root uit de web-PKI te verwijderen. Alle resterende eindcertificaten onder de public root zijn vanaf dan niet langer vertrouwd in webbrowsers en andere toepassingen die de web-PKI gebruiken. Deze stap is voorzien voor februari 2021.

samenstelling van de web-PKI bepalen, nemen het belang van zulke andere toepassingen namelijk niet mee in hun besluiten over de regels en de samenstelling van de web-PKI. Verandert de samenstelling van de web-PKI plotseling, dan kan dat tot verstoringen in zulke toepassingen leiden.

Wat is er aan de hand?

Begin juli is er een probleem ontdekt in 29 tussencertificaten van PKIoverheid.[3] Dit probleem was wereldwijd aanwezig in bijna driehonderd tussencertificaten uit de web-PKI. De fout stelde houders van PKIoverheid-tussencertificaten in staat om mededelingen te doen over de geldigheid van elkaars tussencertificaten. Binnen het PKIoverheid-stelsel levert deze fout slechts een beperkt risico op.[4] Wel vormde deze fout een overtreding van de baseline requirements. De baseline requirements zijn de eisen die browsermakers stellen aan houders van stamcertificaten uit de web-PKI. De ultieme sanctie wanneer de houder van een stamcertificaat een overtreding van de baseline requirements niet verhelpt, is dat de browsermakers het stamcertificaat verwijderen uit de web-PKI. Gebeurt dat bijvoorbeeld bij PKIoverheid, dan zouden bezoekers van websites die PKIoverheid-eindcertificaten gebruiken een foutmelding te zien krijgen. Ook bij andere toepassingen die de web-PKI gebruiken, zou het controleren van PKIoverheid-eindcertificaten tot verstoringen leiden.

Logius heeft besloten om het PKIoverheid-stelsel te herstructureren, om op deze manier het probleem met de PKIoverheid-tussencertificaten op te lossen. Met deze wijzigingen zorgt Logius dat webbrowsers PKIoverheid-eindcertificaten blijven vertrouwen. Ook richt Logius op deze manier

[3] Zie ook https://logius.nl/actueel/logius-onderzoekt-certificaten-die-niet-voldoen-aan-de-afgesproken-richtlijnen.

[4] Zie ook https://www.ncsc.nl/actueel/nieuws/2020/juli/8/aantal-certificaten-voldoen-niet-aan-de-afgesproken-richtlijnen.

[5] Zie ook https://logius.nl/actueel/logius-onderzoekt-certificaten-die-niet-voldoen-aan-de-afgesproken-richtlijnen.

het PKIoverheid-stelsel toekomstvaster in, zodat toekomstige fouten minder grote gevolgen voor het stelsel hoeven te hebben.

De komende maanden zullen Logius en de onderliggende certificaatverstrekkers nieuwe tussencertificaten aanmaken, oude tussencertificaten intrekken en eindcertificaten vervangen. Bij het vervangen geeft Logius de voorrang aan certificaten die voor websites gebruikt worden. De certificaatverstrekkers nemen contact op met hun klanten, de certificaathouders, wanneer het nodig is om hun eindcertificaten te vervangen.

Wat kan er gebeuren?

Als Logius en de certificaatverstrekkers eindcertificaten intrekken of vervangen waar uw proces op steunt, dan kan uw proces stilvallen of verstoord raken. Dit hangt af van de wijze waarop controlerende partijen in uw proces eindcertificaten controleren. Als de wijze waarop partijen eindcertificaten controleren niet aansluit bij de wijzigingen, dan denken controlerende partijen dat alle eindcertificaten die ze na de wijzigingen controleren, ongeldig zijn. Dit kan zorgen dat deze partijen geen beveiligde verbindingen meer op kunnen zetten, niet langer gebruik kunnen maken van digitale handtekeningen, of geen persoonsauthenticatie meer uit kunnen voeren. Afhankelijk van de aard van uw proces kan zo'n verstoring grote organisatorische of maatschappelijke gevolgen hebben.

Een dergelijke verstoring kan op twee manieren ontstaan.

Controleren partijen in uw proces eindcertificaten aan de hand van de web-PKI, dan kan verstoring optreden wanneer eindcertificaten vervangen worden door eindcertificaten buiten de web-PKI, of als het bovenliggende stamcertificaat niet langer in de web-PKI zit. In het actieplan van Logius geldt dit voor twee typen certificaten. Ten eerste worden eindcertificaten voor machine-to-machine-verkeer onder de public root overgezet naar de private root (stap 2). Ten tweede blijven eindcertificaten die niet geschikt zijn voor TLS-verkeer achter onder de public root, terwijl de public root uit de web-PKI verwijderd wordt (stap 3).

Controleren partijen in uw proces eindcertificaten aan de hand van het bovenliggende stamcertificaat, dan kan verstoring optreden wanneer eindcertificaten vervangen worden door eindcertificaten onder een ander stamcertificaat. In het actieplan van Logius geldt dit voor twee typen certificaten. Ten eerste worden eindcertificaten voor het beveiligen van webverkeer onder de public root overgezet naar de EV-root (stap 2). Ten tweede worden eindcertificaten voor machine-to-machine-verkeer onder de public root overgezet naar de private root (stap 2).

Het actieplan van Logius bevat waarborgen om certificaathouders via hun certificaat-verstrekker te informeren over de aanstaande veranderingen. In overleg met de certificaat-houders zorgen de certificaatverstrekkers dat hun eindcertificaten tijdig vervangen worden. Afhankelijk van de aard van uw proces, kunnen certificaathouders de controlerende partijen of de overheidsorganisatie die voor het ICT-proces beleidsverantwoordelijk is, op de hoogte stellen van de aanstaande veranderingen.

Logius informeert niet zelfstandig de controlerende partijen of de overheids-organisaties die voor deze ICT-processen beleidsverantwoordelijk zijn, ook niet via de certificaatverstrekkers. Dat is ook niet mogelijk, omdat er geen totaallijst van dergelijke partijen bestaat. Zo'n lijst is ook niet op basis van technische criteria op te stellen.

Wat adviseert het NCSC?

Het NCSC adviseert u om te onderzoeken of er wijzigingen in uw ICT-proces nodig zijn naar aanleiding van de veranderingen in het PKIoverheid-stelsel, en centrale coördinatie te voeren op deze wijzigingen. De benodigde wijzigingen zullen zitten in de manier waarop

software in uw ICT-proces eindcertificaten controleert.

Inventariseer welke van uw ICT-processen steunen op PKIoverheid-eindcertificaten. Vraag dit bijvoorbeeld na bij de architecten van uw ICT-processen. Geef hierbij prioriteit aan processen die andere software dan een webbrowser gebruiken voor het controleren van eindcertificaten. Het beveiligen van webverkeer is waarschijnlijk de bekendste toepassing van PKIoverheid, maar slechts een klein deel van de PKIoverheid-eindcertificaten wordt daarvoor gebruikt. Bij het beveiligen van webverkeer zijn de benodigde aanpassingen klein, en Logius en de certificaatverstrekkers voeren hier regie op.

Bepaal bij elk van deze ICT-processen wie de certificaathouders zijn, en wie de partijen zijn die eindcertificaten controleren. Betrek hen bij het uitvoeren van de benodigde onderzoeken en wijzigingen, bijvoorbeeld door hen te wijzen op het handelingsperspectief achterin deze factsheet.

Maak een lijst van de software die controlerende partijen gebruiken om eindcertificaten te controleren. In sommige processen gebruiken alle controlerende partijen dezelfde software, in andere zijn er veel verschillende mogelijkheden. Zijn er verschillende versies van de software in gebruik, noteer dit dan ook op de lijst.

Ga na of er wijzigingen te verwachten zijn in de aard van de eindcertificaten die certificaathouders in uw proces gebruiken. Er zijn vier mogelijkheden:

- Uw proces gebruikt EV-eindcertificaten. Deze worden opnieuw uitgegeven als reguliere eindcertificaten. Dit is stap 1 van het actieplan van Logius.
- Uw proces gebruikt eindcertificaten onder de public root die opnieuw worden uitgegeven onder een ander stamcertificaat, de EV-root of de private root. Dit is stap 2 van het actieplan van Logius.
- Uw proces gebruikt eindcertificaten onder de public root die *niet* opnieuw worden uitgegeven onder een ander stamcertificaat. Uiteindelijk wordt de public root uit de web-PKI verwijderd. Dit is stap 3 van het actieplan van Logius.
- Uw proces gebruikt eindcertificaten onder de private root. Voor deze eindcertificaten verandert er niets.

Onderzoek op welke manier de software van controlerende partijen eindcertificaten controleert. Overweeg of deze controle ook zou slagen na de wijzigingen van Logius. Controleert de software bijvoorbeeld tot welk stamcertificaat het eindcertificaat te herleiden is, dan zal de controle niet meer slagen als de eindcertificaten onder een ander stamcertificaat worden uitgegeven.

Valt te verwachten dat het actieplan van Logius gevolgen heeft voor uw ICT-proces omdat u de manier waarop software eindcertificaten controleert moet laten aanpassen? Stel dan zelf een plan van aanpak op om deze aanpassingen uit te voeren en informeer Logius en het NCSC over de te verwachten gevolgen voor uw ICT-proces. Zo kunnen deze partijen overzicht houden over de te verwachten gevolgen. Ook kunnen ze tijdig optreden wanneer er verstoringen te voorzien zijn.

Verdere adviezen over het gebruiken en beheren van digitale certificaten vindt u in de NCSC-factsheet 'Veilig beheer van digitale certificaten'.[6]

[6] Zie https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-veilig-beheer-van-digitale-certificaten.

Handelingsperspectief voor certificaathouders

1. Wacht op bericht van uw certificaatverstrekker. Als er wijzigingen noodzakelijk zijn in de eindcertificaten die u gebruikt, dan stelt uw certificaatverstrekker u daarvan op de hoogte.
2. Wilt u zelf bepalen of er wijzigingen te verwachten zijn? Ga dan na welk geval bij u van toepassing is.

- Gebruikt u eindcertificaten onder de private root? Deze veranderen niet door het actieplan van Logius.
- Gebruikt u EV-eindcertificaten? Deze worden vervangen door reguliere eindcertificaten onder hetzelfde stamcertificaat, de EV-root.
- Gebruikt u eindcertificaten onder de public root, en verkrijgt u deze van een commerciële certificaatverstrekker? Uw certificaatverstrekker zal contact met u opnemen om te overleggen over vervanging. Eindcertificaten die u gebruikt voor het beveiligen van webverkeer worden vervangen door eindcertificaten onder de EV-root. Eindcertificaten die u gebruikt voor machine-to-machineverkeer worden vervangen door eindcertificaten onder de private root.
- Gebruikt u eindcertificaten onder de public root, en verkrijgt u deze van een overheidsorganisatie?[7] Uw eindcertificaten worden niet vervangen. Op termijn zal het bijbehorende stamcertificaat worden verwijderd uit de web-PKI.

Handelingsperspectief voor partijen die eindcertificaten controleren

Ga na op welke manier uw software en systemen PKIoverheid-eindcertificaten controleren, en zorg dat deze manier om kan gaan met de wijzigingen uit het actieplan van Logius.

Uw software steunt op de web-PKI. U laat externe partijen bepalen wat voor u vertrouwde eindcertificaten zijn. Dat is in sommige gevallen acceptabel, bijvoorbeeld voor webbrowsers. Het actieplan verwijdert één van de PKIoverheid-stamcertificaten, de public root, uit de web-PKI. Als certificaathouders die u controleert gebruik blijven maken van eindcertificaten onder dit stamcertificaat, dan zal uw controle vanaf dat moment niet meer slagen.

Uw software bevat een instelbare lijst van vertrouwde stamcertificaten. Dit is een flexibele manier om de controle van eindcertificaten in te richten. Controleer of u de juiste vertrouwde stamcertificaten heeft ingesteld om om te gaan met de veranderingen uit het actieplan van Logius. Sommige eindcertificaten worden in de toekomst uitgegeven onder een ander stamcertificaat.

Uw software bevat ingebakken ('hard-coded') certificaatinformatie. Deze manier om de controle van eindcertificaten in te richten is niet toekomstvast.[8] Elk digitaal certificaat heeft een levensduur, ook stamcertificaten en tussencertificaten. Richt uw software of systeem zo in dat de beheerder vertrouwde stamcertificaten in kan stellen.

[7] De overheidsorganisaties die PKIoverheid-eindcertificaten verstrekken, zijn het ministerie van Defensie, het ministerie van Infrastructuur en Waterstaat en het CIBG.

[8] Er zijn specifieke gevallen, zoals mobiele apps, waarin deze aanpak wel acceptabel is. Het risico op uitval of verstoring wordt dan beheerst door te zorgen dat nieuwe softwareversies binnen zeer korte tijd bij alle gebruikers geïnstalleerd worden.

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 2020