Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# Veilig beheer van digitale certificaten

Factsheet FS-2012-02 | versie 1.1 | 14 december 2017

**Sinds het DigiNotar-incident in 2011 zijn er vele ontwikkelingen geweest rond het versterken van het digitale certificatenstelsel. Verschillende stappen zijn gezet om de robuustheid en weerbaarheid van het certificatenstelsel te vergroten, zoals bijvoorbeeld strengere richtlijnen vanuit het CA/Browser Forum en recente technische ontwikkelingen zoals Certificate Transparency (CT) en Certificate Authority Authorization (CAA). Het DigiNotar-incident heeft geleid tot inzichten die beheerders en gebruikers van certificaten kunnen helpen om hun stelsel van maatregelen te toetsen en aan te scherpen. Deze factsheet beschrijft maatregelen om de kans op incidenten met certificaten zo klein mogelijk te maken en, in het geval van een incident, de schade zo snel mogelijk te herstellen.**

## Achtergrond

Digitale certificaten zijn bedoeld om de vertrouwelijkheid, authenticiteit en integriteit van informatie te garanderen. Een digitaal certificaat speelt een sleutelrol om de authenticiteit van een website te garanderen, dit type certificaat wordt toegepast door het TLS-protocol binnen de Public Key Infrastructure (PKI). Een digitaal certificaat kan ook de integriteit van documenten garanderen door een digitale handtekening te genereren. Daarnaast kan een digitaal certificaat de vertrouwelijkheid van (e-mail)-berichten garanderen door deze te versleutelen met de publieke sleutel van de ontvanger. Alleen de ontvanger kan dit bericht dan ontcijferen met zijn privésleutel.

## Doelgroep

Deze factsheet is bedoeld voor IT-managers, certificaateigenaars, security officers en informatiebeveiligingsadviseurs.

## Aan deze factsheet hebben bijgedragen

KPN, Logius, Belastingdienst en Rabobank

PKI is een samenstel van architectuur, techniek, organisatie, en procedures waarmee publiekesleutelcertificaten worden uitgegeven en beheerd. Er zijn verschillende soorten PKI's. Websites op internet gebruiken bijvoorbeeld certificaten uit de web-PKI. Organisaties kunnen ook zelf een interne PKI hebben.

## *Web-PKI*

Door het DigiNotar-incident in 2011 zijn de kwetsbaarheden van de web-PKI zichtbaar geworden. De web-PKI is de PKI van root-CA's die in moderne browsers vertrouwd worden. Websites die https op internet aanbieden, hebben een certificaat dat uitgegeven is door een van deze root-CA's of een onderliggende CA. Kwaadwillenden konden misbruik van dit vertrouwen maken omdat er onvoldoende controle op het certificaatuitgifteproces was. De DigiNotar-crisis zorgde ervoor dat de digitalecertificatenbranche de zaken beter op orde wilde krijgen. Men was zich ervan bewust geworden dat digitale certificaten op verschillende manieren gecompromitteerd en misbruikt kunnen worden. Tussen 2011 en nu zijn door de branche veel stappen ondernomen om de robuustheid en weerbaarheid van het digitalecertificatensysteem te verbeteren. Een van de grootste verbeteringen voor het digitalecertificatenstelsel is de omarming van Certificate Authority Authorization (CAA) en Certificate Transparency (CT ) (zie voor uitleg van deze termen het blauwe kader: 'advies voor certificaateigenaren'). Een voorbeeld van een succesverhaal is dat Google snel in staat was incorrect uitgegeven certificaten van de certificaatautoriteit (CA) Symantec te vinden.[1] Symantec was als CA verantwoordelijk voor het uitgeven van legitieme digitale certificaten. Omdat de incorrecte uitgifte werd opgemerkt, kon de digitalecertificatengemeenschap Symantec hierop aanspreken. Symantec kreeg hierdoor de kans om tijdig gepaste maatregelen te treffen.

## *Wat kan er gebeuren?*

Aanvallers hanteren verschillende werkwijzen, die ook verschillende gevolgen hebben voor uw organisatie. In deze factsheet bespreken we een aantal scenario's hoe bedrijfsprocessen die steunen op digitale certificaten gecompromitteerd kunnen worden.

In het eerste scenario dringt een kwaadwillende binnen in een systeem van een certificaatautoriteit. Eenmaal in het systeem van de CA kan de kwaadwillende de CA overtuigen om frauduleuze certificaten te verstrekken. Zo kan de kwaadwillende zich voordoen als de eigenaar van een van uw domeinnamen. Het DigiNotar-incident in 2011 is een voorbeeld van dit scenario. In 2011 werd bekend dat DigiNotar meerdere incorrecte certificaat had uitgegeven als gevolg van een systeeminbraak. Toen de incorrecte certificaten uiteindelijk worden ontdekt, trokken browsers als consequentie het vertrouwen in in de certificaatautoriteit Diginotar. Als dit gebeurt bij de certificaatautoriteit die uw certificaten uitgeeft, worden uw certificaten niet meer als geldig herkend, wat uw bedrijfsprocessen ernstig kan verstoren.

Het kan ook voorkomen dat een CA zijn bedrijfsprocessen niet goed op orde heeft en een fout maakt. Er is in dit scenario geen sprake van kwade bedoelingen. In oktober 2016 maakte de CA Comodo een fout bij de uitgifte, waardoor er onterecht certificaten op naam van een Oostenrijkse internetprovider werden uitgegeven. Comodo ontdekte de fout en kon zijn bedrijfsproces aanscherpen. Tot dat moment was het immers voor een aanvaller mogelijk zich voor te doen als deze internetprovider, bijvoorbeeld tegenover de klanten van deze provider.[2]

Een ander mogelijk scenario is een aanval waarbij de privésleutel van een uitgegeven certificaat in de verkeerde handen valt. Een certificaat heeft een publieke en een privésleutel. Het is essentieel dat de privésleutel geheim blijft. Deze aanval kan bijvoorbeeld worden uitgevoerd door een inbraak in het systeem, hierdoor kan het digitale certificaat gecompromitteerd worden.

## Handelingsperspectief

Het NCSC raadt de volgende stappen aan:

- Onderzoek welke personen, afdelingen, leveranciers en partners er betrokken zijn bij het beleid voor beheer van digitale certificaten.
- Beschrijf het beheerproces rond certificaten (inclusief lifecyclemanagement, back-upsystemen en monitoring). Organiseer hiervoor trainingen, risicoanalyses en evaluatiemomenten.
- Inventariseer en leg vast welke certificaten waar (op welke systemen) er in gebruik zijn.
- Schrijf een plan waarin staat hoe u zo snel mogelijk eventueel gecompromitteerde certificaten in kunt trekken en vervangen. Beschrijf hierbij ook de escalatieprocedures en een communicatieplan. Bespreek het plan met betrokken technische medewerkers.

## *Wat kunt u doen?*

Incidenten hebben duidelijk gemaakt dat het omgaan met certificaten een prominente plek verdient in de informatiebeveiliging. Maatregelen moeten niet alleen de kans op incidenten verkleinen, maar moeten bij een incident ook

[1] https://www.security.nl/posting/508375/Google+gaat+vertrouwen+in+Symantec-certificaten+opzeggen

[2] https://www.security.nl/posting/489975/Comodo+verstrekte+onterecht+ssl-certificaat+door+ocr-fout

zorgen dat de schade beperkt blijft en zo snel mogelijk hersteld wordt.

Maatregelen kunnen ingedeeld worden in de categorieën mens, organisatie en techniek.

Daarnaast geeft deze factsheet aan of de maatregel een preventieve (P), detectieve (D) of responsieve (R) werking heeft. Het NCSC adviseert om een integraal stelsel van preventie-, detectie- en responsmaatregelen in te voeren.

### Mens

- Zorg voor bewustwording en training. (P)
  Beheerders dienen op de hoogte te zijn van procedures en verantwoordelijkheden. Gebruikers dienen gewezen te worden op verantwoord gebruik van de privésleutel van de certificaten. Extra technische training over certificaten kan hierbij helpen.

- Evalueer, oefen of simuleer procedures. (P)
  Onderwerp procedures aan onderzoek om te kijken of ze werken. Trek lessen uit de oefening van de procedures zodat gevonden problemen eruit kunnen worden gehaald. Door te oefenen werkt u ook aan het opbouwen van relaties en weet u uw collega's en belangrijke derden te vinden tijdens een incident.

### Organisatie

- Beschrijf het proces voor beheer van digitale certificaten. (P)
  Wie is verantwoordelijk voor het aanvragen, installeren en intrekken van certificaten?

- Leg vast welke certificaten waar (in de organisatie en in systemen) in gebruik zijn. (P)
  Leg bij alle nieuwe certificatenaanvragen de volgende informatie vast:

1. Wie is verantwoordelijk voor het aanvragen en intrekken van het certificaat?
2. Wat is de verloopdatum van het certificaat? Het is nodig om dit te weten voor het tijdig verlengen van het certificaat.
3. Waarvoor wordt dit systeem of deze applicatie gebruikt?
4. Wat is de contactinformatie van de systeem- of applicatie-eigenaar?
5. Betreft het een certificaat in bezit van een derde partij, maar wel cruciaal voor uw bedrijfsvoering?
6. Welke CA heeft het certificaat uitgegeven, en wat is het CA-pad dat wordt gebruikt (inclusief het certificaat van de root CA en alle tussenliggende CA's)?
7. Biedt het systeem of de applicatie de mogelijkheid de certificaten te vervangen?
8. Met welke techniek is het certificaat uitgegeven? Denk aan gebruikte algoritmen en sleutellengte. Als later bekend wordt dat een bepaalde soort versleuteling of algoritme niet veilig genoeg is, weet u precies welke certificaten vervangen moeten worden. Steun bij de keuze van algoritmen en sleutellengtes op de adviezen en normen van bijvoorbeeld het NIST of ETSI. Voor meer informatie leest u de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS).[3]

Onderzoek ook of u al deze informatie beschikbaar heeft van de certificaten die uw organisatie reeds in gebruik heeft. Is dat niet het geval, leg deze informatie dan alsnog vast.

## Advies voor certificaateigenaren: gebruik CAA en CT

Een certificaatautoriteit (CA) is een entiteit die certificaten kan uitgeven voor elk domein. Er is een risico dat iemand anders op ongeoorloofde wijze een certificaat ontvangt voor een domein dat u toebehoort, zonder dat u dit in de gaten heeft. Een dergelijk misbruik kan kwalijke gevolgen hebben voor u en voor de instantie die de betreffende CA beheert. Om dit misbruik te voorkomen is Certificate Authority Authorization (CAA) ontwikkeld.

Met CAA kan een eigenaar van een domein opgeven welke CA certificaten mag uitgeven voor zijn of haar domein. Dit kan een eigenaar doen door het opnemen van een extra DNS-record voor zijn of haar domein. Elke CA is sinds september 2017 verplicht op dit DNS-record te controleren bij het uitgeven van een certificaat.[4] CAA kan dus voorkomen dat een certificaat wordt uitgegeven door een CA waarvoor de eigenaar van het domein geen toestemming heeft gegeven. Uw certificaatleverancier kan u hierover meer informatie geven.

Als onverhoopt toch een certificaat voor uw domein zonder uw medeweten is uitgegeven, dan kunt u met Certificate Transparency achteraf detecteren dat dit gebeurd is. Per maart 2018 is het voor CA's verplicht om publieke certificaten te loggen in zogenaamde Certificate Transparency (CT) logs.[5] Een eigenaar kan CT gebruiken om te controleren of er onterechte certificaten voor zijn of haar domein zijn uitgegeven.[6] Er zijn mogelijkheden om dit te monitoren en automatisch een notificatie te ontvangen zodra dit gebeurt.

[3] https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html
[4] https://www.sslcertificaten.nl/support/Terminologie/CAA_DNS_Records
[5] CA/Browser Forum, https://cabforum.org/2017/03/08/ballot-187-make-caa-checking-mandatory/
[6] https://www.certificate-transparency.org/what-is-ct

- Weet wat de potentiële gevolgen zijn van incidenten. (risicoanalyses) (P)
  Maak een risico-en impactanalyse en breng in kaart welke diensten getroffen kunnen worden (zowel intern als extern). Houd ook rekening met de invloed van certificaten van derden op de bedrijfsvoering en de invloed van het gebruik van uw certificaten op derden.

- Zorg dat u een plan heeft om zo snel mogelijk gecompromitteerde certificaten te vervangen en in te trekken. (R)
  Maak dit onderdeel van een incidentresponse- of calamiteitenplan, en zorg dat uw medewerkers op de hoogte zijn van dit plan. Mocht uw primaire certificatenleverancier gecompromitteerd worden, dan heeft u een snelle uitwijkmogelijkheid. Mocht uw systeem dusdanig bedrijfskritisch zijn dat snelle vervanging niet afdoende is, dan kunt u tegelijkertijd met de aanschaf van een primair certificaat een extra backupexemplaar bestellen bij een andere CA.

- Zorg voor escalatieprocedures en een communicatieplan. (R)
  Dit plan kan in het geval van een belangrijk incident gevolgd worden. Bedenk vooraf wie welke taken en verantwoordelijkheden heeft, met wie u moet samenwerken, wie u moet informeren en van wie u informatie nodig heeft. Meld incidenten aan gebruikers van certificaten.

- Besteed aandacht aan onderzoek en ontwikkeling. (P)
  Het is essentieel dat uw organisatie op de hoogte blijft van nieuwe technische ontwikkelingen rond PKI. Controleer of uw certificaten nog voldoen aan de standaarden. Zijn bijvoorbeeld de algoritmen en sleutellengtes nog sterk genoeg?

### Techniek

- Tref technische beveiligingsmaatregelingen om privésleutels te beschermen. (P)
  Zorg dat het systeem waar de privésleutel op staat goed beveiligd is. Denk daarnaast ook aan het inrichten van autorisatiebeheer. Overweeg het gebruik een Hardware Security Module voor opslag van de privésleutel.

- Besluit voor elke toepassing welk type certificaten gekozen moet worden. (P)
  Leveranciers bieden vaak verschillende niveaus aan (DV, OV en EV). Zie voor uitleg van deze termen het blauwe kader: 'Kies een passend certificaat bij elke toepassing'. Bekijk nauwkeurig wat de waarborgen zijn die elk van de niveaus bieden en zorg dat deze aansluiten op beveiligingseisen van de organisatie.

- Maak een afgewogen keuze voor een CA. (P)
  Let op land van vestiging, naamsbekendheid, financiële toestand, incidenten in het verleden, veiligheidsmaatregelen, certificeringen en audits, etc. Onderzoek ook welke apparaten en software de root CA vertrouwen. Daarnaast is het belangrijk dat u aanvullende vragen stelt. Heeft de CA een positieve reputatie qua securityincidenten?

## Kies een passend certificaat bij elke toepassing

CA's bieden vaak certificaten aan met verschillende vormen van verificatie. Voor website (server) certificaten is er sprake van de volgende vormen van verificatie:

Controle van domeinnaam: Domain Validation (DV)-certificaten worden uitgegeven na verificatie dat de aanvrager controle heeft over het genoemde domein. De aanvrager hoeft dus geen eigenaar van het domein te zijn en kan dus ook een leverancier zijn die de daadwerkelijke server beheert waarop een website draait of de DNS-operator. De enige zekerheid die hiermee verkregen wordt is dat een gebruiker contact heeft met een specifiek domein (bijv. www.rijksoverheid.nl). Over de identiteit van de eigenaar worden geen uitspraken gedaan. Dit type certificaat is geschikt als de domeinnaam bij alle bezoekers bekend is, bijvoorbeeld bij een heel bekende domeinnaam of bij machine-to-machinecommunicatie.

Controle van domeinnaam en van identiteit: Bij uitgifte van OV- en EV-certificaten controleert de certificaatautoriteit de identiteit van de aanvrager. Daarnaast controleert hij of de aanvrager controle heeft over het genoemde domein, net als bij DV-certificaten. Bij EV-certificaten gaat de controle van de identiteit veel verder dan bij OV-certificaten. EV-certificaten leveren een zogenaamde 'groene balk' op in de browser van bezoekers. De identiteit van de houder is voor de bezoeker goed zichtbaar.

- Maak gebruik van CAA. (P)
  CAA is een nieuwe technische standaard die het CA/Browser Forum in september 2017 als eis heeft gesteld aan de CA's. Het is belangrijk dat uw organisatie hier ook van gebruikmaakt. Geef minimaal twee CA's op via CAA die gemachtigd zijn om certificaten uit te geven voor uw organisatie. Zo kunt u ook als uw primaire certificaatautoriteit gecompromitteerd is, nog steeds certificaten aanvragen. Onderzoek voordat u CAA toepast, welke CA's uw organisatie momenteel gebruikt teneinde

het bedrijfsvoeringproces niet te verstoren. U kunt bijvoorbeeld CT-logs gebruiken om te onderzoeken welke CA's uw organisatie al in gebruik heeft.

- Controleer periodiek de CT-logs op certificaten die aan uw organisatie lijken toe te behoren. (D)
  CT-logging geeft u inzicht in welke certificaten er zijn uitgegeven voor uw domeinnamen. Door periodiek deze logs te controleren kunt u snel fraude opsporen en ingrijpen. Er zijn tools die u hiermee handmatig en geautomatiseerd kunnen helpen.[7]

- Monitor uw netwerk. (D)
  Heeft u aanwijzingen dat kwaadwillenden uw systeem zijn binnengedrongen, denk dan ook aan mogelijke ongeoorloofde toegang tot (de privésleutels van) uw certificaten. Houd als vuistregel aan dat een binnengedrongen systeem altijd een nieuw certificaat nodig heeft. Houd de bronnen in de gaten waarop mogelijke incidenten met certificaten gemeld worden (bijvoorbeeld de NCSC-website, de website van softwareleveranciers, etc.). Lees voor meer informatie de factsheet 'SOC inrichten, begin klein' [8].

- Bescherm uw webbrowser tegen onveilige CA's. (P)
  Elke browser gebruikt een lijst van vertrouwde CA's, ook wel Certificate Trust List genoemd. Fabrikanten van bekende webbrowsers en besturingssystemen zorgen er continu voor dat alleen CA's die aan de regels voldoen in deze lijst zitten. Deze lijsten kunnen echter met voldoende beheerrechten op uw systemen worden aangepast. Controleer daarom regelmatig dat deze lijst goed is afgeschermd en er geen ongeautoriseerde CA's in staan. Raadpleeg de website van uw browser voor meer informatie.[9]

## Tot slot

Maak beheer van digitale certificaten een belangrijk onderdeel van uw organisatie. Kijk kritisch naar uw eigen beheerbeleid en controleer periodiek of de maatregelen goed zijn geïmplementeerd.

***Het is noodzakelijk om voor een veilig beleid voor beheer van digitale certificaten een integraal stelsel van preventie-, detectie- en respons maatregelen op te zetten en te handhaven.***

[7] Zie bijvoorbeeld https://crt.sh/ om CT-logs te raadplegen.
[8] https://www.ncsc.nl/actueel/factsheets/factsheet-soc-inrichten-begin-klein.html
[9] Microsoft: https://social.technet.microsoft.com/wiki/contents/articles/40296.microsoft-trusted-root-certificate-program-participants-as-of-september-26-2017.aspx
Apple: https://support.apple.com/en-us/HT204132
Mozilla: https://wiki.mozilla.org/CA/Included_Certificates
Google: Chrome Heeft geen eigen lijst maar gebruikt die van onderliggende systeem: https://www.chromium.org/Home/chromium-security/root-ca-policy

**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

FS-2012-02 | versie 1.1 | 14 december 2017