



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Intrekking van de DigiNotar PKIoverheid sub CA certificaten

Versie 1.0

Datum 23 september 2011
Status Definitief

Colofon

Projectnaam	Intrekken DigiNotar PKIoverheid sub CA certificaten
Versienummer	1.0
Contactpersoon	Policy Authority (PA) PKIoverheid
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl
Bijlage(n)	n.v.t.

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
23-9-2011	1.0	PA PKIoverheid	n.v.t.

Inhoud

Colofon	2
Inhoud	3
Inleiding	4
1 Intrekken DigiNotar sub CA certificaten en het effect	5
1.1 <i>Inleiding</i>	5
1.2 <i>Elk certificaat vermeldt zijn eigen geldigheidsperiode</i>	6
1.3 <i>Elk PKIoverheid certificaat bevat een verwijzing naar de CRL</i>	6
1.4 <i>Een PKI-toepassing moet zijn ingesteld voor CRL-opvraging.....</i>	6
1.5 <i>Een reëel risico op het gebruik van een verouderde CRL</i>	7
1.6 <i>Tot slot nog een taak voor de netwerkbeheerder</i>	8

Inleiding

Dit document gaat in op de intrekking op 28 september 2011 van de certificaten van DigiNotar PKIoverheid sub CA's door de Domein CA's van de Staat der Nederlanden.

Het onderwerp wat in dit document wordt behandeld is: wat betekent het intrekken van de DigiNotar PKIoverheid sub CA certificaten en wat is het effect.

1 Intrekken DigiNotar sub CA certificaten en het effect

1.1 Inleiding

De Staat der Nederlanden publiceert verscheidene lijsten met daarin de serienummers van de certificaten van ingetrokken PKIoverheid CA's. Een dergelijke lijst worden ook wel intrekingslijst of "Certificate Revocation List" (CRL) genoemd, beide termen worden in dit document gebruikt.

In het verleden heeft DigiNotar van de PKIoverheid Domein CA genaamd "Staat der Nederlanden Overheid CA" drie sub CA certificaten mogen ontvangen. Dat zijn:

- het certificaat van de "DigiNotar PKIoverheid CA Overheid" met serienummer 01314476 (= verlopen op 23 juni 2010);
- het certificaat van de "DigiNotar PKIoverheid CA Overheid en Bedrijven" met serienummer 013169b0;
- het certificaat van de "DigiNotar PKIoverheid CA Organisatie - G2" met serienummer 013134bf.

De PKIoverheid Domein sub CA's zullen op 28 september 2011 de intrekingslijst bijwerken en, in plaats van de huidige, die bijgewerkte versie publiceren. De voor de DigiNotar intrekking relevante intrekingslijsten zijn de volgende:

- Actuele lijst met ingetrokken CSP-certificaten onder Domein Overheid opvraagbaar op adres <http://crl.pkioverheid.nl/DomOvLatestCRL.crl>
- Actuele lijst met ingetrokken CSP-certificaten onder G2 Domein Organisatie opvraagbaar op adres <http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl>

Correct ingestelde PKI-toepassingen zullen de (bijgewerkte) intrekingslijsten weten te vinden en, op basis van die lijsten, kennisnemen van de ingetrokken status van de genoemde DigiNotar PKIoverheid sub CA's.

N.B. Bij "PKI-toepassingen" moet men denken aan alle hardware- en softwareproducten die met certificaten kunnen omgaan en de geldigheid van certificaten kunnen achterhalen. Dit omvat bekende programmatuur zoals webbrowsers, maar bijvoorbeeld ook de meeste besturingssystemen en standaard- en maatwerk communicatieprogrammatuur en -apparatuur.

Nu is het echter wel zo, dat de meeste PKI-toepassingen zelf het initiatief moeten nemen om intrekingslijsten al dan niet op te vragen en te controleren. Bepalend om van een certificaat de meest recente intrekingslijst al dan niet op te (kunnen) vragen zijn:

1. Of het tijdstip van einde geldigheid zoals vermeld in het te valideren certificaat zelf al aangeeft dat de geldigheidstermijn is verstreken;
2. Of een te valideren certificaat al dan niet verwijst naar het publicatiepunt van de voor hem geldende intrekingslijst;
3. Of de betreffende PKI-toepassing zodanig is ingesteld, dat hij notie neemt van die vermelding;
4. Of de betreffende PKI-toepassing al dan niet beschikt over een kopie van een oudere, maar volgens de toepassing nog steeds geldende,

intrekkingslijst;

5. Of de betreffende PKI-toepassing al dan niet in staat is om een netwerkverbinding met het betreffende publicatiepunt te realiseren.

Deze vijf situaties zijn in de vijf secties hieronder verder beschreven en uitgewerkt.

1.2 Elk certificaat vermeldt zijn eigen geldigheidsperiode

Elk certificaat vermeldt (tot op de seconde nauwkeurig) zijn eigen start- en einde geldigheid. Er van uitgaande dat de PKI-toepassing gebruik maakt van een zuivere systeemklok, zal de toepassing ieder certificaat waarvan de vermelde einde geldigheid is verstreken, als ongeldig beschouwen.

In zo'n geval is een (verdere) controle van een intrekkingslijst uiteraard overbodig.

Van een, op basis van de vermelde einde geldigheid, inmiddels verlopen certificaat zal diens uitgevende CA dan ook nooit het serienummer opnemen in een intrekkingslijst.

Het certificaat van één van de eerder genoemde DigiNotar PKIoverheid CA's is inmiddels verlopen. Dit betreft het certificaat van de "DigiNotar PKIoverheid CA Overheid" die een eindegeldigheid van "23 juni 2010 10:17:36" vermeldt. Dat certificaat zal dus niet (meer) worden ingetrokken.

1.3 Elk PKIoverheid certificaat bevat een verwijzing naar de CRL

Binnen de regelgeving van PKIoverheid is vereist dat, uitgezonderd de stamcertificaten, ieder certificaat een eenduidige verwijzing naar de voor hem geldende CRL bevat. Dit is niet anders voor de twee momenteel nog geldige certificaten van de inmiddels onbetrouwbare DigiNotar PKIoverheid CA's:

- Het certificaat van de "DigiNotar PKIoverheid CA Overheid en Bedrijven" verwijst naar de "Actuele lijst met ingetrokken CSP-certificaten Domein Overheid" opvraagbaar op adres <http://crl.pkioverheid.nl/DomOvLatestCRL.crl>
- Het certificaat van de "DigiNotar PKIoverheid CA Organisatie - G2" verwijst naar de "Actuele lijst met ingetrokken CSP-certificaten onder G2 Domein Organisatie" opvraagbaar op adres <http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl>

Elke PKI-toepassing die één van beide DigiNotar PKIoverheid sub CA-certificaten wil valideren, wordt hiermee gewezen op het bestaan en het publicatiepunt van de relevante intrekkingslijst.

1.4 Een PKI-toepassing moet zijn ingesteld voor CRL-opvraging

Er mag van worden uitgegaan dat de meeste systemen die gebruik maken van PKI certificaten in staat zijn om CRL controles uit te voeren. Echter, niet alle systemen zijn af-fabriek zodanig ingesteld, dat zij dit automatisch doen.

Een voorbeeld van dat laatste zijn de meeste, zo niet alle, versies van Microsoft Internet Explorer, waarin bijvoorbeeld de instelling "Check for server certificate revocation" expliciet moet worden geactiveerd door de gebruiker of beheerder. Wordt dat achterwege gelaten, zal Internet Explorer geen CRL-controles doen.

In het Programma van Eisen van PKIoverheid staat overigens expliciet vermeld, dat "vertrouwende partijen" geacht worden om certificaatstatus controles uit te voeren. Veel andere PKI-hiërarchieën stellen een vergelijkbare eis. Zonder die controle kan een "vertrouwende partij" geen enkele aanspraak doen op de betrouwbaarheid van een certificaat. Dit betekent dat PKI-toepassingen geacht worden de eerder genoemde intrekingslijsten op te vragen en te controleren.

1.5 Een reëel risico op het gebruik van een verouderde CRL

Elke CRL bevat, naast de lijst van serienummers van ingetrokken certificaten, een vermelding van het tijdstip waarop deze CRL werd gecreëerd ("thisUpdate") en van het tijdstip waarop uiterlijk een meer actuele versie van deze intrekingslijst gepubliceerd zal worden ("nextUpdate").

Veel PKI-toepassingen zijn af-fabriek zodanig ingesteld, dat zij de "nextUpdate" interpreteren als een soort houdbaarheidsdatum.

Met andere woorden, als zo'n PKI-toepassing een CRL-controle moet doen, maar hij beschikt nog over een lokaal opgeslagen exemplaar van de CRL waarvan de nextUpdate nog niet is verstreken, dan zal de PKI-toepassing gebruik maken van dat lokale exemplaar. Dit proces wordt "CRL-caching" genoemd.

Een CA kan echter op ieder moment, besluiten een CRL te actualiseren en te publiceren. Dit kan dus ook plaatsvinden ruim voor de nextUpdate, zoals die in een eerder gepubliceerde CRL-versie bestond.

PKI-toepassingen die CRL-caching gebruiken, lopen dan achter op de feiten en lopen het risico dat zij recent ingetrokken certificaten toch nog vertrouwen.

Voor de twee met de geplande intrekking van DigiNotar PKIoverheid sub CA's gemoeide CRL's wordt een publicatiefrequentie van 3 maanden gehanteerd.

De thisUpdate en nextUpdate van beide momenteel gepubliceerde CRL's zijn hieronder weergegeven:

Intrekingslijst (CRL)	thisUpdate	nextUpdate
Actuele lijst met ingetrokken CSP-certificaten domein Overheid	24-08-2011 11:41:05	22-11-2011 11:46:05
Actuele lijst met ingetrokken CSP-certificaten onder G2 domein Organisatie	11-08-2011 10:51:10	9-11-2011 10:56:10

Indien de certificaten van de DigiNotar PKIoverheid sub CA's nu (23-9-2011) zouden worden ingetrokken, duurt het CRL-caching effect ongeveer twee maanden.

Bovenstaande aanwijzing gaat er van uit dat aan de gebruikerszijde niets wordt gedaan aan de PKI-toepassingen. Aan die zijde kan de beheerder van een PKI-toepassing echter een eventuele CRL-cache geforceerd leeg maken, waarna de PKI-toepassing, bij gemis aan een lokaal exemplaar, vanzelf weer een actuele CRL zal ophalen.

Het beleid van PKIoverheid (Programma van Eisen) in acht nemend, is de laatstgenoemde procedure de enige correcte.

1.6 Tot slot nog een taak voor de netwerkbeheerder

Tot slot en wellicht een open deur: indien een PKI-toepassing een actuele CRL wenst op te vragen, is het noodzakelijk dat er een netwerkverbinding tussen de PKI-toepassing en de publicatieserver van PKIoverheid kan worden opgezet.

Of dit een directe dan wel indirecte verbinding betreft, maakt in principe niet uit. De desbetreffende netwerkbeheerder heeft hierbij de taak om deze verbinding te faciliteren.