Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

CERTIFICATION PRACTICE STATEMENT (CPS)
Policy Authority PKIoverheid voor Extended Validation certificaten uit te geven door de Policy Authority van de PKI voor de overheid

Datum oktober 2016
Versie 1.5

Colofon

Versienummer 1.5
Contactpersoon Policy Authority PKIoverheid

Organisatie Logius

Bezoekadres
Wilhelmina van Pruisenweg 85

Postadres
Postbus 96810
2509 JE DEN HAAG

T 0900 - 555 4555
servicecentrum@logius.nl

Inhoud

Revisiegegevens

Versie	Datum goedkeuring	Datum Inwerkingtreding	Status	Auteur	Manager	Omschrijving
1.0	18-01-2011	25-01-2011	Vastgesteld door directeur Logius 18 januari 2011	Policy Authority	H. Verweij	Definitieve versie
1.1	24-06-2011	01-07-2011	Vastgesteld door directeur Logius 24-06-2011	Policy Authority	H. Verweij	Aanpassing i.v.m. nieuwe adresgegevens Logius. Daarnaast enkele redactionele wijzigingen.
1.2	04-02-2013	04-02-2013	Vastgesteld door BZK	Policy Authority	H. Verweij	Wijzigingsprocedure is opgenomen in Bijlage C.
1.3	Juni 2014	Juli 2014	Vastgesteld door Directeur Logius	Policy Authority	Mark Janssen	Paragraafindeling op basis van RFC 3647 verder aangescherpt. Diverse wijzigingen doorgevoerd naar aanleiding van de Webtrust audit.
1.4	februari 2015	februari 2015	Vastgesteld door Directeur Logius	Policy Authority	Mark Janssen	Redactionele wijzigingen + wijziging certificaatprofiel EKU + opm over controle CAA records
1.5	Oktober 2016	Oktober 2016	Vastgesteld door Directeur Logius	Policy Authority	Mark Janssen	Redactionele wijzigingen + wijziging ETSI normenkader TS 102 042 naar EN 319 411-1. Tevens diverse redactionele wijzigingen.

1 Inleiding

1.1 Overzicht

1.1.1 *Policy Authority voor de PKI voor de overheid*

De Policy Authority van de PKI voor de overheid (PA PKIoverheid) ondersteunt de Minister van Binnenlandse Zaken en Koninkrijksrelaties bij het beheer over de PKI voor de overheid.

De PKI voor de overheid is een afsprakenstelsel. Dit maakt generiek en grootschalig gebruik mogelijk van de elektronische handtekening, en faciliteert voorts identificatie op afstand en vertrouwelijke communicatie. De taken van de PA PKIoverheid zijn:

- het leveren van bijdragen voor de ontwikkeling en het beheer van het normenkader dat aan de PKI voor de overheid ten grondslag ligt, het zogeheten Programma van Eisen (PvE);
- het proces van toetreding door Certification Service Providers (CSP's) tot de PKI voor de overheid begeleiden en voorbereiden van de afhandeling;
- het toezicht houden op en controleren van de werkzaamheden van CSP's die onder de root van de PKI voor de overheid certificaten uitgeven.

De Policy Authority (PA) is verantwoordelijk voor het beheer van de gehele infrastructuur. De PKI voor de overheid is zo opgezet dat externe organisaties, de Certification Service Providers (CSP's), onder voorwaarden toe kunnen treden tot de PKI voor de overheid. Deelnemende CSP's zijn verantwoordelijk voor de dienstverlening binnen de PKI voor de overheid. De PA ziet toe op de betrouwbaarheid van de gehele PKI voor de overheid.

In algemene zin is de PA in het kader van PKIoverheid Extended Validation verantwoordelijk voor:

1. beheer van het normenstelsel van de PKI voor de overheid, het Programma van Eisen deel 3f;
2. beheer van Object Identifiers, de unieke nummers voor CSP's en hun CPS's;
3. creatie en beheer van sleutelpaar en het bijbehorende EV stamcertificaat;
4. intrekken van het EV stamcertificaat en ad hoc publicatie van de CRL;
5. periodieke publicatie van de EV CRL;
6. creatie en beheer van sleutelparen en het bijbehorende EV Intermediair certificaat;
7. intrekken van het EV Intermediair certificaat en ad hoc publicatie van de bijbehorende CRL;
8. voorbereiding inzake het toelaten van CSP's tot de PKIoverheid Extended Validation;
9. effectuering van de toelating van CSP's met inbegrip van creatie, uitgifte en beheer van EV CSP CA-certificaten;
10. voorbereiding inzake het intrekken van EV CSP CA-certificaten;
11. effectuering van het intrekken van EV CSP CA-certificaten;

12. houden van toezicht op toegelaten CSP's;
13. voorbereiding inzake het vernieuwen van EV CSP CA-certificaten;
14. effectuering van het vernieuwen van EV CSP CA-certificaten met inbegrip van creatie, uitgifte en beheer van nieuwe EV CSP CA-certifcaten;
15. registreren en beoordelen van meldingen omtrent aantasting van de PKIoverheid Extended Validation.

Het technisch beheer van de Staat der Nederlanden EV Root CA, de Staat der Nederlanden EV Intermediair CA plus de bijbehorende Certificate Revocation Lists (CRL's) en OCSP responders vindt plaats door KPN B.V.

Het beheer van het stamcertificaat is opgedragen aan de Policy Authority van de PKI voor de overheid. Deze organisatie is ondergebracht bij Logius (http://www.logius.nl), dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

De doelstelling van de Policy Authority is:
Het handhaven van een werkbaar en betrouwbaar normenkader voor PKI-diensten die voorziet in een vastgesteld beveiligingsniveau voor de communicatiebehoefte van de overheid en transparant is voor de gebruikers.

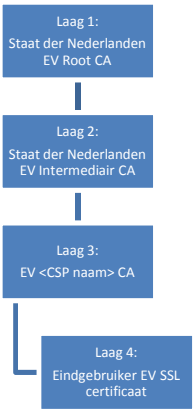
1.1.2 CA model PKIoverheid Extended Validation (geen RFC 3647)

De Public Key Infrastructuur (PKI) voor de overheid kent een structuur waarbij een centraal en een uitvoerend c.q. lokaal deel van PKIoverheid is gedefinieerd.

Voor de EV root bestaat het centrale deel uit een root- en intermediairniveau. Dit overkoepelende overheidsniveau en het intermediairniveau vormen de beleidsstructuur van de PKI. Binnen deze niveaus worden beleid en normen vastgesteld en wordt het toezicht georganiseerd.

Het CSP-niveau vormt het uitvoerend c.q. lokaal deel van het Public Key Infrastructuur (PKI) voor de overheid waar de directe interactie met de gebruikers plaatsvindt. Op het CSP-niveau heeft de CSP-organisatie de eindverantwoordelijkheid voor het uitgeven van certificaten.

Om duidelijk te maken dat het gaat om Extended Validation certificaten wordt bij de naamformatie de letters “EV” gebruikt. Dit geldt voor alle CA certificaten in de PKIoverheid Extended Validation hiërarchie. Binnen PKIoverheid Extended Validation is de naamformatie van de commonName (CN) als volgt:



Zie verder Bijlage A voor de certificaatprofielen van de Staat der Nederlanden EV Root CA en de Staat der Nederlanden EV Intermediair CA.

1.2 Documentnaam en identificatie

De Certification Practice Statement EV certificaten binnen de PKI voor de overheid (verder te noemen CPS) biedt informatie aan *CSP's, abonnees, vertrouwende partijen en certificaathouders*[1] over de procedures en getroffen maatregelen ten aanzien van de dienstverlening van de PA met betrekking tot EV certificaten. Het CPS beschrijft de processen, procedures en beheersingsmaatregelen voor het aanvragen, produceren, verstrekken, beheren en intrekken van EV certificaten, voor zover dat valt onder directe verantwoordelijkheid van de PA. Dit betekent dat dit CPS alleen betrekking heeft op PKIoverheid Extended Validation Laag 1 (Staat der Nederlanden EV Root CA) en Laag 2 (Staat der Nederlanden EV Intermediair CA).

Daarnaast beschrijft dit CPS de processen en procedures voor het aanvragen, produceren, verstrekken en intrekken van Laag 3 EV (<CSP naam> CA certificaten.

Voor een beschrijving van de processen, procedures en beheersings-maatregelen voor het aanvragen, produceren, verstrekken, beheren en intrekken van Laag 4 (EV SSL certificaten) wordt hierbij verwezen naar de betreffende diverse EV Certification Practice Statements van de PKIoverheid certificatiedienstverleners

De indeling van dit CPS is zoveel mogelijk conform de RFC3647[2] standaard (voluit: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework") van de Internet Engineering Task Force.

Formeel wordt het voorliggend document aangeduid als 'Certification Practice Statement EV certificaten binnen de PKI voor de overheid'.

1 Zie voor meer informatie omtrent afkortingen het Programma van Eisen PKIoverheid deel 4: definities en afkortingen (https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-csp/programma-van-eisen/)

2 http://www.ietf.org/rfc/rfc3647.txt?number=3647

CPS	Omschrijving
Naamgeving	CERTIFICATION PRACTICE STATEMENT (CPS) Policy Authority PKIoverheid voor Extended Validation certificaten uit te geven door de Policy Authority van de PKI voor de overheid
Link	https://cps.pkioverheid.nl
OID	n.v.t.

Openbare informatie over de PA of de PKI voor de overheid is te vinden op http://www.logius.nl/pkioverheid.

1.2.1 Doel CPS (geen RFC 3647)

Dit CPS biedt informatie aan *CSP's, abonnees, vertrouwende partijen en certificaathouders* over de procedures en getroffen maatregelen ten aanzien van de dienstverlening van de PA inzake PKIoverheid Extended Validation. De kwaliteit van de dienstverlening ligt ten grondslag aan het vertrouwen dat in PKIoverheid Extended Validation gesteld kan worden. Hierbij is ook de relatie tussen de PA en de Certification Service Providers (CSP's) van belang. Deze relatie en de voorwaarden waaronder CSP's kunnen deelnemen aan de PKIoverheid Extended Validation zijn op hoofdlijnen beschreven. CSP's die zijn geïnteresseerd in deelname aan PKIoverheid Extended Validation kunnen over dit onderwerp meer gedetailleerde informatie vinden in PKIoverheid Programma van Eisen deel 2.

1.2.2 Verhouding CPS en CP (geen RFC 3647)

Het CP PvE deel 3f beschrijft de minimumeisen die zijn gesteld aan de dienstverlening van een CSP binnen PKIoverheid Extended Validation naast de basiseisen die van toepassing zijn op alle CP's. Dit voorliggende CPS geeft aan op welke wijze invulling wordt gegeven aan de PKIoverheid Extended Validation dienstverlening, voor zover dit valt onder directe verantwoordelijkheid van de PA.

1.2.3 CA/Browser Forum Guidelines (geen RFC 3647)

De PA van PKIoverheid conformeert zich aan de huidige versie van de Guidelines zoals gepubliceerd op http://www.cabforum.org. Mocht er een inconsistentie aanwezig zijn tussen het PvE deel 3f, het voorliggende CPS en de betreffende Guidelines dan prevaleert het gestelde in de Guidelines.

1.2.4 ertificate Policies (CP's) (geen RFC 3647)

Dit deel (deel 3) heeft betrekking op de eisen die aan de dienstverlening van een Certification Service Provider (CSP) worden gesteld. Er zijn negen gebieden gedefinieerd die elk in een afzonderlijk deel worden behandeld, te weten:
Deel 3a – Certificate Policy voor Domein, Organisatie en Organisatie Persoon;
Deel 3b – Certificate Policy voor Domein Organisatie en Organisatie Services;
Deel 3c – Certificate Policy voor Domein Burger;
Deel 3d – Certificate Policy voor Domein Autonome Apparaten;
Deel 3e – Certificate Policy voor Server Certificaten.
Deel 3f – Certificate Policy voor Extended Validation
Deel 3g – Certificate Policy voor Private Services
Deel 3h – Certificate Policy voor Private server certificaten
Deel 3i – Certificate Policy voor Private personen
Dit CPS heeft alleen betrekking op deel 3f – Certificate Policy voor Extended Validation. Het "CPS Policy Authority PKIoverheid voor certificaten uit te geven door de Policy Authority van de PKI voor de overheid" heeft betrekking op de andere PvE delen (behalve delen g, h, en i).

1.2.4.1 *Positionering Programma van Eisen(geen RFC 3647)*
Het *Programma van Eisen* is het uitgangspunt voor de dienstverlening van de PA. In het Programma van Eisen zijn de eisen geformuleerd voor de PKI voor de overheid, deze eisen zijn ontleend aan internationale standaarden en de van toepassing zijnde wetgeving. Het Programma van Eisen omvat negen delen en in ieder deel is een bepaald aspect van de PKI voor de overheid nader uitgewerkt. Hieronder staat een korte introductie van de betreffende delen van het Programma van Eisen.

1.2.4.2 Introductie Programma van Eisen (geen RFC 3647)
Dit deel (deel 1) bevat een introductie op het Programma van Eisen en de PKI voor de overheid.

1.2.4.3 Toetreding tot en toezicht (geen RFC 3647)
In deel 2 wordt beschreven op welke wijze een CSP kan toetreden tot de PKI voor de overheid, conformiteit aan de eisen kan aantonen en aan welke formaliteiten moet worden voldaan. Tevens is beschreven op welke wijze de PA toezicht houdt op de toegetreden CSP's.

1.3 Betrokken partijen

Bij de PKI voor de overheid kennen wij de navolgende betrokken partijen:
- Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK);
- PA;
- CSP;
- Abonnee;
- Certificaathouder;
- Vertrouwende partij.

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is verantwoordelijk voor PKIoverheid Extended Validation. BZK neemt beslissingen met betrekking tot de inrichting van de infrastructuur en de deelname van CSP's aan PKIoverheid Extended Validation. De directeur van Logius vertegenwoordigt BZK in deze.

De *PA* is verantwoordelijk voor het beheer van het centrale deel[3] van de PKIoverheid EV infrastructuur en het toezicht houden op en controleren van de werkzaamheden van CSP's die onder de Staat der Nederlanden EV Root CA van de PKI voor de overheid, EV SSL certificaten uitgeven.

Een *CSP* heeft als functie het beheren van EV CSP CA certificaten en het verstrekken van PKIoverheid EV SSL certificaten en sleutelinformatie, met inbegrip van de hiervoor voorziene dragers (bijvoorbeeld een SUD). De CSP heeft tevens de eindverantwoordelijkheid voor het leveren van de certificatiediensten.

Een *abonnee* gaat een overeenkomst aan met een CSP namens één of meer certificaathouders. Hóe de levering van EV SSL certificaten door de CSP aan die certificaathouders plaatsvindt, regelen de abonnee en de CSP onderling.

3 Het centrale deel betreft de Staat der Nederlanden EV Root CA en Staat der Nederlanden EV Intermediair CA.

De *certificaathouder* is de houder van de private sleutel behorend bij de publieke sleutel die in het EV certificaat vermeld is. Op alle niveaus in de EV hiërarchie van de PKI voor de overheid bevinden zich certificaathouders. Eindgebruikers ontvangen de EV SSL certificaten van de CSP's. De PA geeft EV certificaten uit aan zichzelf (Staat der Nederlanden EV Root CA en Staat der Nederlanden EV Intermediair CA) en aan CSP's (EV CSP CA).

De *vertrouwende partij* is de ontvanger van een EV SSL certificaat dat is uitgegeven binnen PKIoverheid Extended Validation.

1.4 Certificaatgebruik

Binnen PKIoverheid Extended Validation worden EV SSL certificaten gebruikt voor het beveiligen van een verbinding tussen een bepaalde client en een server via het TLS/SSL protocol. De PKIoverheid EV certificaten zijn te herkennen aan de specifieke unieke PKIoverheid EV Policy Object Identifier (OID) **2.16.528.1.1003.1.2.7**. Deze OID verwijst naar de CP PvE deel 3f en staat vermeldt in het veld Certificaatbeleid (certificatePolicies) van het certificaat Staat der Nederlanden EV Intermediair CA, de EV CSP CA certificaten en de eindgebruiker EV SSL certificaten.

1.4.1 Primaire doeleinden

Het primaire doel van een PKIoverheid EV SSL certificaat is om:

1. de organisatie te identificeren die de controle heeft over de website: een PKIoverheid EV SSL certificaat zorgt voor een redelijke mate van zekerheid dat de website, die door de gebruiker van een internet browser c.q. een vertrouwende partij wordt bezocht, onder de controle staat van de organisatie, die staat vermeldt in het PKIoverheid EV SSL certificaat én;
2. het mogelijk te maken versleuteld te communiceren met een website: een PKIoverheid EV SSL certificaat maakt het mogelijk om sleutels uit te wisselen. Hiermee is het mogelijk dat, via het internet, de gebruiker van een internet browser versleutelde informatie uitwisselt met een website.

1.4.2 Secundaire doeleinden

Een PKIoverheid EV SSL certificaat:

1. maakt het moeilijker om phishing- en andere on-line identiteitsfraude aanvallen uit te voeren waarbij gebruik wordt gemaakt van certificaten;
2. helpt organisaties die het doelwit zijn van phishing- of andere on-line identiteitsfraude aanvallen, door hen een voorziening te geven waarmee zij zich beter kunnen identificeren ten opzichte van gebruikers én;
3. helpt Justitie bij een onderzoek naar phishing- en andere on-line identiteitsfraude. In voorkomende gevallen zal PKIoverheid hiertoe contact opnemen met Justitie, zelf nader onderzoek verrichten of juridische stappen nemen tegen de betreffende organisatie.

1.4.3 Uitgesloten doeleinden

Een PKIoverheid EV SSL certificaat geeft alleen meer zekerheid over de identiteit van de eigenaar van de website. Een PKIoverheid EV SSL

certificaat geeft geen uitsluitsel over de reputatie van een organisatie of de service die zij bieden. Als zodanig is een PKIoverheid EV SSL certificaat niet bedoeld om enige zekerheid te bieden, of anderszins te garanderen dat:

1. de organisatie vermeldt in het PKIoverheid EV SSL certificaat er een actieve bedrijfsvoering op nahoudt;
2. de organisatie vermeldt in het PKIoverheid EV SSL certificaat zich houdt aan de Nederlandse wetgeving;
3. de organisatie vermeldt in het PKIoverheid EV SSL certificaat betrouwbaar, eerlijk of een goede reputatie heeft op het gebied van zaken doen óf;
4. dat het "vertrouwd" is om zaken te doen met de organisatie zoals vermeldt in het PKIoverheid EV SSL certificaat.

1.5 Beheer CPS

1.5.1 Organisatie verantwoordelijk voor het beheer van het CPS

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor dit CPS. Het ministerie heeft deze taak gedelegeerd aan Logius. Dit omvat ook het goedkeuren van wijzigingen op dit CPS.

1.5.2 Contactinformatie

Voor klachten, vragen of meldingen kunnen CSP's binnen het PKIoverheid stelsel contact opnemen met medewerkers van de PA PKIoverheid via de gebruikelijke kanalen. De PA PKIoverheid is binnen kantooruren beschikbaar en zal zo spoedig mogelijk reageren. In het geval van meldingen van incidenten of calamiteiten buiten kantoren wordt verzocht contact op te nemen met het Servicecentrum van Logius dat 24 uur per dag beschikbaar is.

Abonnees die vragen hebben omtrent certificaatuitgifte worden verzocht in eerste instantie contact op te nemen met hun (potentiële) CSP.

Overige betrokken partijen kunnen contact opnemen met het servicecentrum van Logius. Het servicecentrum registreert de vraag en beantwoordt deze binnen de gestelde termijn. Indien noodzakelijk worden vragen via het servicecentrum doorgezet naar de PA PKIoverheid of in het geval van een incident, de dienstdoende incidentmanager.

Contactgegevens:
Policy Authority PKIoverheid
Wilhelmina van Pruisenweg 52
Postbus 96810
2509 JE DEN HAAG
http://www.logius.nl/pkioverheid
Algemeen telefoonnummer: 0900-555 4555
email: servicecentrum@logius.nl

1.5.3 *Persoon die geschiktheid beoordeelt van CPS voor het CP*
De PA PKIoverheid kent geen eigen Certificate Policy. Goedkeuring van het CPS wordt behandeld in 1.5.4.

1.5.4 *Wijzigingsprocedure CPS*
De PA van PKIoverheid heeft het recht dit CPS te wijzigen of aan te vullen. Wijzigingen gelden vanaf het moment dat het nieuwe CPS gepubliceerd is, conform het gestelde in paragraaf 9.10. Het management van het Logius is verantwoordelijk voor een juiste navolging van de procedure zoals beschreven in paragraaf 9.12 en voor de uiteindelijke goedkeuring van dit CPS conform deze procedure.

1.6 Definities en afkortingen

Voor een overzicht van de gebruikte definities en afkortingen wordt verwezen naar https://www.logius.nl/begrippenlijst.

In deel 4 zijn de in het Programma van Eisen gehanteerde definities en afkortingen toegelicht.

1.7 Waarborgen

Bij de uitgifte van een PKIoverheid EV-certificaat zijn onder meer de volgende partijen te onderkennen:

A. Abonnee;
B. Eindgebruiker;
C. Organisaties die internet browser software ontwikkelen;
D. Vertrouwende partijen.

Aan deze partijen wordt kenbaar gemaakt dat:
PKIoverheid Extended Validation en haar certificatiedienstverleners waarborgen dat zij, gedurende de tijd dat een PKIoverheid EV (SSL) certificaat geldig is, bij de uitgifte van een PKIoverheid EV (SSL) certificaat de eisen uit de CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates en het PvE deel 3f, hebben gevolgd en dat zij de gegevens, zoals opgenomen in het EV (SSL) certificaat, hebben gecontroleerd op juistheid en volledigheid.

Voor een beschrijving van de waarborgen wordt hierbij verwezen naar de betreffende diverse EV Certification Practice Statements van de PKIoverheid certificatiedienstverleners.

1.8 Programma van Eisen en stelseloverleg PKIoverheid

Het Programma van Eisen geldt als het formele normenkader ten aanzien van de betrouwbaarheid en kwaliteit van dienstverlening binnen de PKI voor de overheid. Bij het door de PA onderhouden van dit normenstelsel is het van belang dat ook de praktijkervaringen en ideeën vanuit gebruikers worden meegewogen. Om dit draagvlak voor de toepassing van het Programma van Eisen te kunnen realiseren is een stelseloverleg PKIoverheid ingesteld die wordt geconsulteerd bij de besluitvorming over wijzigingsvoorstellen op het Programma van Eisen. Daarnaast komen in dit overleg ook onderwerpen aan de orde die in het algemeen relevant zijn voor de PKI –ontwikkelingen.

De volledige procedures voor het wijzigingenbeheer van het Programma van Eisen van PKIoverheid zijn opgenomen in Annex C.

2 Publicatie en verantwoordelijkheid voor elektronische opslagplaats

2.1 Elektronische Opslagplaats

Op https://cert.pkioverheid.nl, zullen de volgende zaken worden gepubliceerd:

- de Staat der Nederlanden EV Root CA en Staat der Nederlanden EV Intermediair CA certificaten;
- de EV CSP CA certificaten;

De Certificate Revocation Lists (CRL's) van de Staat der Nederlanden EV Root CA en Staat der Nederlanden EV Intermediair CA zijn te vinden op https://crl.pkioverheid.nl/

Op de websites van de verschillende CSP's zijn de CRL's ten behoeve van de eindgebruiker EV SSL certificaten te vinden.

2.2 Publicatie certificaat informatie

De volgende EV certificaten worden gepubliceerd:

- Staat der Nederlanden EV Root CA;
- Staat der Nederlanden EV Intermediair CA;
- EV <Naam CSP> CA.

Dit CPS is te vinden op de volgende url:
https://cps.pkioverheid.nl

De volgende CRL's worden gepubliceerd:

- Ten behoeve van het ingetrokken Staat der Nederlanden EV Intermediair CA certificaat:
  http://crl.pkioverheid.nl/EVRootLatestCRL.crl
- Ten behoeve van ingetrokken EV CSP CA certificaten:
  http://crl.pkioverheid.nl/EVIntermediairLatestCRL.crl

2.2.1 Officiële elektronische bekendmaking (geen RFC 3647)

De identificerende gegevens van het Staat der Nederlanden EV Root CA stamcertificaat zijn in de Staatscourant jaargang 2011, nr. 527 gepubliceerd en te raadplegen sinds donderdag 13 januari 2011 om 9:01. Tot de identificerende gegevens behoren de naam van de houder van het certificaat (common name, organisation en country), de datum waarop de geldigheid van het certificaat verloopt, het serienummer en de vingerafdruk op basis van het SHA-1 algoritme. (Bijlage B bevat de tekst van de publicatie in de Staatscourant met betrekking tot het Staat der Nederlanden EV Root CA stamcertificaat)

2.2.2 Distributie publieke sleutel (geen RFC 3647)

De publieke sleutel van het Staat der Nederlanden EV Root CA stamcertificaat wordt onder meer gedistribueerd via de trusted root certificate programma's van verschillende software leveranciers. Op https://www.logius.nl/ondersteuning/pkioverheid/browserondersteuning-pkioverheid/staat een actuele lijst van de softwareproducten die het Staat der Nederlanden EV Root CA stamcertificaat bevatten.

Daarnaast wordt het Staat der Nederlanden EV Root CA stamcertificaat op https://cert.pkiovehreid.nl op een betrouwbare wijze aangeboden.

2.3 Frequentie van publicatie

De PA publiceert de lijsten met ingetrokken certificaten, de CRL's. Er is een CRL gegenereerd ten behoeve van het Staat der Nederlanden EV Intermediair CA certificaat. Deze CRL wordt jaarlijks opnieuw gepubliceerd. Ad hoc publicatie van deze CRL vindt plaats na intrekking van het Staat der Nederlanden EV Intermediair CA certificaat.

De CRL met ingetrokken EV CSP CA certificaten wordt standaard elke 12 uur opnieuw gepubliceerd en heeft een geldigheid van 7 dagen. Ad hoc publicatie van deze CRL vindt plaats na intrekking van een EV CSP CA certificaat. Elke CRL bevat het tijdstip van de volgende geplande CRL-uitgifte.

Op de websites van de verschillende CSP's zijn de CRL locaties ten behoeve van de eindgebruiker EV SSL certificaten te vinden. De CRL met ingetrokken eindgebruiker EV SSL certificaten wordt standaard elke 48 uur opnieuw gepubliceerd. Ad hoc publicatie van de CRL met ingetrokken eindgebruiker EV SSL certificaten vindt plaats na intrekking van een eindgebruiker EV SSL certificaat. Daarnaast maakt elke CSP gebruik van een Online Certificate Status Protocol (OCSP) om de certificaatstatus informatie van eindgebruiker EV-certificaten beschikbaar te stellen. Ondersteuning met het OCSP vindt plaats in overeenstemming met RFC2560[4].

2.4 Toegang tot publicatie

Gepubliceerde informatie is publiek van aard en vrij toegankelijk. De Elektronische Opslagplaats kan vierentwintig uur per dag en zeven dagen per week worden geraadpleegd. De Elektronische Opslagplaats is beschermd tegen het aanbrengen van ongeautoriseerde wijzigingen.

Voor het geval van het optreden van systeemdefecten of andere factoren die de beschikbaarheid van de Elektronische Opslagplaats negatief beïnvloeden is er een passende set van continuïteitsmaatregelen gerealiseerd om ervoor te zorgen dat de CRL binnen 4 uur en de overige onderdelen van de Elektronische Opslagplaats binnen 24 uur weer bereikbaar zijn. Een voorbeeld van een dergelijke maatregel is het hebben gerealiseerd van een uitwijklocatie en –scenario. Daarnaast ondergaat de Elektronische Opslagplaats jaarlijks een penetratietest. Deze wordt uitgevoerd door een extern IT security bedrijf.

4 http://www.ietf.org/rfc/rfc2560.txt

3 Identificatie en authenticatie

3.1 Naamgeving

3.1.1 Soorten naamformaten

Alle EV certificaten die door de PA van PKIOverheid worden uitgegeven, bezitten een 'subject'-veld (DistinguishedName) waarin de benaming van de houder is opgenomen. De in EV certificaten gebruikte namen voldoen aan de X.501 naam standaard. De namen bestaan uit de volgende onderdelen:

Attribuut	Staat der Nederlanden EV Root CA	Staat der Nederlanden EV Intermediair CA	<CSP naam> PKIoverheid EV CA
Country (C)	NL	NL	NL
Organization (O)	Staat der Nederlanden	Staat der Nederlanden	<CSP Organisatienaam>
CommonName (CN)	Staat der Nederlanden EV Root CA	Staat der Nederlanden EV Intermediair CA	<CSP Organisatienaam> PKIoverheid EV CA

Zie verder Bijlage A voor de volledige certificaatprofielen van de Staat der Nederlanden EV Root CA en Staat der Nederlanden EV Intermediair CA.

Voor overige bepalingen betreffende de wijze waarop identificatie en authenticatie plaatsvindt binnen PKIoverheid Extended Validation wordt hierbij verwezen naar de betreffende diverse EV Certification Practice Statements van de PKIoverheid certificatiedienstverleners.

3.1.2 Noodzaak gebruik betekenisvolle namen

Er zijn geen nadere bepalingen op dit gebied voor de certificaatdienstverlening door de PA.

3.1.3 Pseudoniemen

Het gebruik van pseudoniemen of anonieme certificaten wordt niet toegestaan.

3.1.4 Regels voor het interpreteren van verschillende naamvormen

De naam van de CSP CA wordt overgenomen van het uittreksel uit het Nederlands Handelsregister.

3.1.5 Uniciteit van namen

Alle certificaten die onder dit CPS worden uitgegeven, bezitten een uniek subjectveld (*DistinguishedName*).

3.1.6 Erkenning, authenticatie en de rol van handelsmerken

De PA gaat uit van de correctheid van de naamgeving van organisaties zoals opgenomen in het Nederlands Handelsregister van de Kamer van Koophandel.

3.2 Initiële identiteitsvalidatie

3.2.1 Initieel Registratieproces

Zie voor de eisen die worden gesteld aan een initieel registratieproces het Programma van Eisen, deel 2 van PKIoverheid.

3.2.2 Authenticatie van organisatorische entiteit

Op basis van het aanvraagformulier en de aangeleverde bewijsmiddelen verifieert de PA,

- dat de CSP een bestaande organisatie is die is opgenomen in het NHR of een organisatorische entiteit behorend bij een bestaande organisatie die is opgenomen in het NHR. In het geval van een overheidsorganisatie die niet is ingeschreven in het NHR zal de Staatsalmanak worden geraadpleegd;
- dat de door de CSP aangemelde organisatienaam en landnaam die in het certificaat wordt opgenomen juist en volledig is en dat de aanvrager bevoegd is de organisatie te vertegenwoordigen;
- de aanwezigheid van de relevante registratie-informatie van de aspirant CSP met het daarbij behorende bewijsmateriaal (uittreksel KvK etc.). Er moet sprake zijn van een origineel uittreksel dat niet ouder mag zijn dan 13 maanden;

Nota bene: Indien de toetredende partij minder dan drie jaar bestaat en niet voorkomt in de meest recente versie van genoemde registratiebronnen kan de identiteit en validiteit van de aspirant CSP eventueel worden vastgesteld aan de hand van een moedermaatschappij of kerndepartement, die wel geregistreerd zijn in de KVK of de Staatsalmanak.

3.2.3 Authenticatie van persoonlijke identiteit

Bij initiële toetreding tot het PKIoverheid stelsel verifieert de PA de opgegeven persoonsgegevens van de bevoegd vertegenwoordiger van de CSP aan de hand van een in art. 1 van de Wet op de Identificatieplicht genoemd identiteitsdocument:

- een geldig reisdocument als bedoeld in de Paspoortwet;
- een geldig rijbewijs dat is afgegeven op basis van de Wegenverkeerswet, als bedoeld in artikel 107 van de Wegenverkeerswet 1994

3.3 Identificatie en authenticatie bij vernieuwing van een certificaat.

Dikwijls zal een CSP al toegetreden zijn tot het PKIoverheid stelsel wanneer een nieuwe CSP CA aangemaakt dient te worden onder een nieuwe generatie van de reguliere root. Ook is het mogelijk dat een reeds toegetreden CSP certificaten wil uitgeven onder een nieuw domein of een andere root. In dat geval kan een verkorte procedure gehanteerd worden voor de identificatievalidatie omdat de CSP CA reeds bekend is bij de PA en is toegetreden tot het PKIoverheid stelsel.

Het is dan voldoende als de PA controleert of de organisatienaam en naam van het land opgegeven in het Naming document / CSR nog steeds correct is. Dit kan op de volgende manieren worden gecontroleerd:

1. Door het online raadplegen van het NHR om te controleren of de CSP CA een bestaande organisatie is;
2. Door het online raadplegen van een database zoals Dunn & Bradstreet die up-to-date wordt gehouden en wordt beschouwd als een betrouwbare bron.

Daarnaast dient de PA te controleren dat de aanvraag daadwerkelijk van de CSP CA afkomstig is. Een aanvraag kan op twee manieren worden ingediend:

1. De bevoegd vertegenwoordiger kan een aanvraagformulier versturen via e-mail en ondertekenen met een PKIoverheid certificaat;
2. De bevoegd vertegenwoordiger kan een aanvraagformulier ondertekenen en per post te versturen.

In het tweede geval dient tevens contact te worden opgenomen met de bij de PA PKIoverheid geregistreerde bevoegd vertegenwoordiger van de CSP CA om de aanvraag te verifieren. Ter controle kunnen identificerende gegevens van de contactpersoon of organisatie worden opgevraagd.

Deze identificatiecontrole door de PA wordt vastgelegd en gearchiveerd in het dossier van de CSP CA.

3.4 Identificatie en authenticatie bij intrekking van een certificaat

Een verzoek tot intrekking van een certificaat kan worden ingediend door de CSP CA. Bij een verzoek tot intrekking zal altijd een opgave van redenen moeten worden gegeven. In overleg met betrokken partijen zal worden gekeken in hoeverre aan het verzoek voldaan zou kunnen worden aangezien intrekking van een CSP CA betekent dat onderliggende certificaat niet meer geldig zullen zijn.

Identificatie en authenticatie van de indiener van het verzoek tot intrekking van de CSP CA kan op één van onderstaande wijzen geschieden:

- Een verzoek per e-mail aan de PA, waarbij het verzoek digitaal wordt ondertekend met een gekwalificeerde elektronische handtekening;
- Een verzoek per ondertekende brief;

In alle drie de gevallen zal de PA telefonisch contact opnemen met de bevoegd vertegenwoordiger van de CSP CA om vast te stellen dat de aanvraag tot intrekking authenthiek is. Ter controle kunnen identificerende gegevens van de contactpersoon of organisatie worden opgevraagd.

4 Operationele eisen certificaatcyclus

4.1 Toepassingsgebied

Binnen PKIoverheid Extended Validation zijn op vier niveaus verschillende typen certificaten gedefinieerd, te weten:

- Staat der Nederlanden EV Root CA;
- Staat der Nederlanden EV Intermediair CA;
- EV CSP CA;
- Eindgebruiker EV SSL certificaten.

Dit CPS heeft betrekking op de betrouwbaarheid van de dienstverlening van de PA. Dit betekent dat dit CPS alleen betrekking heeft op PKIoverheid Extended Validation Laag 1 (Staat der Nederlanden EV Root CA) en Laag 2 (Staat der Nederlanden EV Intermediair CA).

Daarnaast beschrijft dit CPS de processen en procedures voor het aanvragen, produceren, verstrekken en intrekken van Laag 3 EV (<CSP naam> CA certificaten.

4.2 Aanvraag van certificaten

Het Staat der Nederlanden EV Root CA, Staat der Nederlanden EV Intermediair CA en de EV CSP CA certificaten worden in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties aangemaakt door de PA van de PKI voor de overheid.

Opdracht tot het maken van EV CSP CA certificaten vindt plaats naar aanleiding van een aanvraag hiertoe door een CSP. Uitsluitend een CSP die is toegetreden tot de PKI voor de overheid (zie hiervoor PvE deel 2) kan en mag een aanvraag indienen voor het aanmaken van een EV CSP CA certifcaat.

De PA PKIoverheid controleert geen CAA records bij het tekenen van CSP CA's.

4.2.1 Werkwijze met betrekking tot creatie van certificaten

Het creëren van het Staat der Nederlanden EV Root CA, Staat der Nederlanden EV Intermediair CA en de EV CSP CA certificaten vindt plaats tijdens speciale creatieceremonies. Een gecertificeerde externe IT-auditor fungeert als getuige tijdens de creatieceremonies van de Staat der Nederlanden EV Root CA en de Staat der Nederlanden EV Intermediair CA. Voor iedere creatieceremonie wordt een gedetailleerd draaiboek opgesteld waarin alle uit te voeren handelingen zijn vermeld. Het gestelde in dit draaiboek is confidentieel en wordt daarom niet in detail beschreven in dit CPS. Het draaiboek is met name bedoeld om invoerfouten tijdens de ceremonie te voorkomen. Een creatieceremonie wordt uitgevoerd conform het draaiboek in aanwezigheid van onafhankelijke getuigen. De identiteit van de aanwezige personen wordt gecontroleerd aan de hand van bij artikel 1 van de Wet op de identificatieplicht aangewezen geldige documenten.

De creatieceremonies verlopen voor alle genoemde typen certificaten op vergelijkbare wijze. Hierbij is de certificaathouder de PA of de CSP. Tijdens de ceremonie vinden onder meer de volgende stappen plaats:

1. opbouwen van het computersysteem;
2. installeren en configureren van de PKI-software;
3. activeren van de Hardware Security Module (HSM), waarbij meerdere sleutelhouders elk een deel van de activeringsgegevens inbrengen;
4. genereren van de sleutelparen;
5. genereren van certificaten voor elk sleutelpaar;
6. ontmantelen van het computersysteem en
7. veiligstellen van het computersysteem en de kritieke componenten.

4.3 Uitgifte van certificaten

Uitsluitend een CSP die (voorlopig) is toegetreden tot de PKI voor de overheid kan en mag EV SSL certificaten aan derden uitgeven onder de EV hiërarchie van de PKI voor de overheid.

De eisen waaraan een CSP dient te voldoen bij de uitgifte van de certificaten zijn geformuleerd in vigerende versie van ETSI EN 319 411-1 (policy EVCP), de basiseisen PKIoverheid en PvE deel 3f. De wijze waarop een CSP uitvoering geeft aan deze eisen dient door de CSP zelf beschreven te worden in een separate CPS Extended Validation. De beschrijving van de dienstverlening door CSP's valt derhalve buiten het bestek van dit CPS.

Voor het uitgeven van certificaten door de PA is geen separaat CP opgesteld, aangezien de PA geen eindgebruikercertificaten uitgeeft. De maatregelen die de PA heeft getroffen om de betrouwbaarheid van de door de PA uit te geven EV certificaten te waarborgen zijn in dit CPS beschreven.

4.4 Acceptatie van certificaten

Het draaiboek behorende bij de creatieceremonies bevat tevens de procedure voor het vaststellen van de juistheid en het accepteren van de gecreëerde certificaten. Daarnaast zijn in het draaiboek ook de namen van de betrokken functionarissen vermeld. De PA stelt de juistheid van de certificaten vast. De CSP accepteert vervolgens het EV CSP CA certificaat.

4.5 Sleutelpaar en certificaatgebruik

Het Staat der Nederlanden EV Root CA, Staat der Nederlanden EV Intermediair CA en de EV CSP CA certificaten kunnen uitsluitend worden gebruikt voor het verifiëren van de handtekening van de uitgever en worden uitgegeven door de PA. Het is niet toegestaan deze certificaten voor andere doeleinden te gebruiken. Het eindgebruiker EV SSL certificaat wordt uitgegeven door de CSP's.

4.6 Vernieuwen van certificaten

Certificaten dienen te worden vernieuwd wanneer (een deel van) de informatie die aan het certificaat ten grondslag ligt is veranderd of verouderd. Hierbij valt te denken aan het wijzigen van de naam van een CSP die in het certificaat is vermeld of het verminderen van de sterkte van een cryptografisch algoritme.

Certificate Renewal waarbij het bestaande sleutelpaar wordt gehandhaafd en de geldigheidsduur van het certificaat wordt verlengd wordt niet toegepast binnen PKIoverheid.

Ongeveer 3 á 4 jaar voor het einde van de geldigheidsduur van het Staat der Nederlanden EV Root CA en het Staat der Nederlanden EV Intermediair CA certificaat zal de PA van PKIoverheid een nieuwe generatie (G2) creëren van de EV Root CA en de EV Intermediair CA.

Een nieuwe (G2) EV CSP CA certificaat moet worden aangevraagd en zijn uitgegeven ruim voor het moment dat onder een bestaande EV CSP CA het niet meer mogelijk zou zijn om een eindgebruiker EV SSL certificaat uit te geven met een maximale geldigheidsduur van 27 maanden. Dit betekent dat ongeveer 2,5 á 3 jaar voor het einde van de geldigheidsduur een nieuwe EV CSP CA moet worden gecreëerd.

Een CSP dient hiertoe, rekening houdend met een vereiste verificatieperiode, nieuwe signing keys aan te (laten) maken en tevens een verzoek in te dienen bij de PA om het nieuwe EV CSP CA certificaat aan te laten maken.

Dit verzoek is de eerste stap van de interne procedure CSP-certificaat-vernieuwing. Op hoofdlijnen bestaat deze procedure verder uit de volgende stappen:

- Indienen van een aanvraagformulier tot vernieuwing van een EV CSP CA onder de nieuwe root door de bevoegd vertegenwoordiger van de CSP;Controleren van de geldigheid van de aanvraag door de PA;
- Validatie van de gegevens in het aanvraagformulier;
- Indienen van het Naming Document voor het nieuwe EV CSP CA certificaat door de CSP;
- Controleren van het Naming Document door de PA;

- Indienen Certificate Signing Request (CSR) door CSP t.b.v. test CSP CA;
- Creëren Test EV CSP CA certificaat door technisch beheerder van de EV root;
- Controleren Test EV CSP CA certificaat door de PA en CSP;
- Indienen Certificate Signing Request (CSR) door CSP t.b.v. Productie CSP CA;
- Opdracht van de PA aan de technisch beheerder van de EV Root voor creatie nieuwe EV CSP CA certificaat;
- Uitvoering creatie ceremonie van nieuwe EV CSP CA certificaat door de technisch beheerder van de root;
- Controle PA van nieuwe EV CSP CA certificaat;
- Overhandiging PA van nieuwe EV CSP CA certificaat aan de CSP;
- Decharge PA aan de technisch beheerder van de EV Root.

Het aanvragen, de uitgifte, de acceptatie en de publicatie van het nieuwe CSP-certificaat volgen dezelfde stappen als bij de oorspronkelijke toetreding van een CSP, zie 4.2 t/m 4.5. De nieuwe signing keys

vervangen de voorgaande versies[5]. Het oorspronkelijke CSP EV CA certificaat blijft, gedurende een bepaalde periode, bestaan naast het nieuwe EV CSP CA certificaat.

4.7 Rekey van certificaten

Certificate Rekey waarbij de bestaande publieke sleutel in een certificaat wordt gewijzigd, wordt binnen de centrale hiërarchie van de PKI voor de overheid niet toegepast.

4.8 Aanpassing van certificaten

Certificate Modification wordt alleen in uitzonderlijke gevallen toegepast. Normaliter zal de voorkeur worden gegeven aan het opnieuw uitgeven van een certificaat wanneer de inhoud van het certificaat (publieke sleutel) niet meer correct is.

4.9 Intrekking en opschorting van certificaten

Intrekking van het Staat der Nederlanden EV Root CA en het Staat der Nederlanden EV Intermediair CA certificaat en een EV CSP CA certificaat zal in ieder geval worden overwogen als de signing key behorende bij het certificaat is gecompromitteerd of daarvan wordt verdacht. Van compromittatie is onder meer sprake als ongeautoriseerd toegang is verkregen tot deze signing key of wanneer dragers hiervan zijn gestolen of verloren gegaan. Om dit te bewerkstelligen houdt de PA een registratie bij van de meldingen die kunnen leiden tot intrekking van het Staat der Nederlanden EV Root CA en het Staat der Nederlanden EV Intermediair CA certificaat en een EV CSP CA certificaat. Alle meldingen worden door de PA geregistreerd en in behandeling genomen. De Wet bescherming persoonsgegevens is van toepassing en wordt in acht genomen.

De PA merkt compromittatie van de signing key aan als een calamiteit. Doet zich een calamiteit voor, dan treedt het calamiteitenplan in werking en worden alle relevante partijen onmiddellijk op de hoogte gesteld. In paragraaf 6.7 van dit CPS wordt het calamiteitenplan behandeld.

Voorafgaand aan het intrekken van het Staat der Nederlanden EV Root CA certificaat, het Staat der Nederlanden EV Intermediair CA certificaat of een EV CSP CA certificaat wordt een zorgvuldig beoordelingsproces doorlopen. Het calamiteitenteam zal deze beoordeling uitvoeren en zal eventuele hieruit voortvloeiende activiteiten (laten) initiëren.

Indien een CSP niet langer voldoet aan de voorwaarden voor deelname aan PKIoverheid Extended Validation, dan kan de PA overgaan tot het intrekken van het betreffende EV CSP CA certificaat. De intrekking van een certificaat kan binnen één dag worden geëffectueerd. De PA informeert de CSP vooraf over het intrekken van het certificaat.

In geval van het intrekken van het Staat der Nederlanden EV Root CA certificaat en/of het Staat der Nederlanden EV Intermediair CA certificaat informeert de PA de CSP's waarmee samenwerking is overeengekomen. Van het intrekken van het Staat der Nederlanden EV Root CA certificaat

5 De PA staat niet toe dat dezelfde signing keys gebruikt worden als in het oude CSP-certificaat.

wordt mededeling gedaan in de Staatscourant en via andere media waar het stamcertificaat formeel is of zal worden gepubliceerd.

Het besluit het Staat der Nederlanden EV Root CA certificaat en/of het Staat der Nederlanden EV Intermediair CA certificaat in te trekken zal gepaard gaan met een uitspraak over het al dan niet uitgeven van een nieuw certificaat ter vervanging van het ingetrokken certificaat.

Het intrekken van het Staat der Nederlanden EV Intermediair CA certificaat of een EV CSP CA certificaat leidt altijd tot ad hoc publicatie van de betreffende gewijzigde CRL. Het intrekken van certificaten en het uitgeven van CRL's geschiedt conform een vooraf opgesteld draaiboek. Maximaal 24 uur na intrekking van domein of CSP CA zal de nieuwe CRL worden gepubliceerd.

Opschorting van certificaten wordt binnen de PKI voor de overheid niet ondersteund.

4.10 Certificaat statusservice

4.10.1 Operationele eigenschappen van de certificaat statusservice

De geldigheid van certificaten is raadpleegbaar middels de gepubliceerde CRL die verkrijgbaar is via de elektronische opslagplaats (zie 2.1). De PA hanteert voor de CRL's het X.509 versie 2 formaat.

Naast de publicatie van de CRL voert de PA een Online Certificate Status Protocol (OCSP) dienst. De OCSP service wordt standaard elke 12 uur bijgewerkt. Een OCSP response van deze dienst heeft een geldigheid van maximal 7 dagen. In het geval van de intrekking van een EV CSP CA certificaat wordt de OCSP dienst ad hoc bijgewerkt. De OCSP dienst ondersteunt de GET methode voor het opvragen van een response.

De CSP zal met betrekking tot zijn CRL en OCSP dienstverlening passende server capaciteit aanhouden waarmee een response tijd wordt gegarandeerd van 10 seconden of minder onder normale omstandigheden.

De status van ingetrokken certificaten blijft gedurende de levensduur van de bovenliggende CA beschikbaar op de CRL en via OCSP.

4.10.2 Beschikbaarheid certificaat statusservice

De CRL en OCSP zijn 24 uur per dag en 7 dagen per week beschikbaar.

De maximale tijdsduur, waarbinnen de beschikbaarheid van de revocation status information (de status van een ingetrokken certificaat) moet worden hersteld, is gesteld op vier uur.

4.10.3 Optionele kenmerken van de certificaat statusservice

Geen nadere bepalingen voor de certificaatdienstverlening van CSP.

4.11 Beëindiging

Indien BZK besluit de dienst PKIoverheid Extended Validation te beëindigen, dan zullen de volgende stappen worden gevolgd:

1. Alle betrokken partijen (abonnees, cross certifying CA's, hoger gelegen CA's en vertrouwenspartijen) van de dienst PKIoverheid Extended Validation, zullen een half jaar voor het beëindigen van de dienst worden geïnformeerd.
2. Alle EV certificaten die zijn uitgeven na bekendmaking van het beëindigen van de dienst, zullen in het certificaat een einddatum bevatten gelijk aan de geplande einddatum van PKIoverheid Extended Validation.
3. Bij het beëindigen van de dienst zullen alle nog geldige certificaten worden ingetrokken.
4. PKIoverheid Extended Validation stopt op de einddatum met het distribueren van certificaten en CRL's.

4.12 Key escrow en key recovery

De PA PKIoverheid heeft de stam-en domeincertificaten gekloond en deze backup wordt bewaard op de uitwijklocatie van PKIoverheid.

4.12.1 Overdracht PKIoverheid (geen RFC 3647)

Indien BZK besluit de dienst PKIoverheid Extended Validation over te dragen aan een andere organisatie, dan zullen alle betrokken partijen (abonnees, cross certifying CA's, hoger gelegen CA's en vertrouwenspartijen) van de dienst PKIoverheid Extended Validation minimaal 3 maanden van tevoren worden geïnformeerd over de overdracht. De nieuwe organisatie zal de bepalingen uit dit CPS in haar eigen CPS overnemen.

5 Fysieke, procedurele en personele beveiliging

In dit CPS zijn de door de PA getroffen beveiligingsmaatregelen op hoofdlijnen beschreven.

De PA heeft beheersmaatregelen geïmplementeerd om verlies, diefstal, beschadiging of compromittatie van infrastructurele middelen en onderbreking van de activiteiten te voorkomen. Daarbij is onder meer voorzien in fysieke toegangscontrole. De fysieke inrichting kent verschillende lagen die aparte toegangscontrole vereisen met steeds een hoger niveau van beveiliging. Daarnaast is een reeks van maatregelen getroffen ter bescherming tegen brand, natuurrampen, uitval van ondersteunende faciliteiten (zoals elektriciteit en telecommunicatie-voorzieningen), instortingsgevaar, lekkages, et cetera.

5.1 Fysieke beveiliging

De beveiligde omgeving van de Staat der Nederlanden EV Root CA is ingericht op basis van eisen die geformuleerd zijn in het Programma van Eisen en de eisen uit het Voorschrift Informatiebeveiliging Rijksdienst voor Bijzondere Informatie (VIR-BI)

5.2 Procedurele beveiliging

Voor afhandeling van incidenten en calamiteiten zijn specifieke processen en procedures geïmplementeerd.

De Policy Authority voert jaarlijks een stelselbrede risicoanalyse uit en beschrijft de beheersmaatregelen die zijn genomen om risico's binnen het stelsel te verkleinen. Tevens wordt er een risicoanalyse uitgevoerd bij significante wijzigingen in interne of externe factoren.

Daarnaast wordt jaarlijks een risico-analyse uitgevoerd voor het technisch beheer van de centrale hiërarchie van PKIoverheid.

De computersystemen voor productie worden niet voor andere doeleinden gebruikt. Er zijn aparte systemen ingericht, uitsluitend bedoeld voor het testen of accepteren van nieuwe of gewijzigde software. Behalve deze hardwarematige scheiding zijn er procedures van kracht die ervoor zorgen dat alle medewerkers het principe van een strikte scheiding tussen de acceptatie- en de productieomgeving respecteren.

De verantwoordelijkheden bij de PA zijn verdeeld over verschillende functies en personen. De software controleert de functiescheiding en dwingt deze af. In algemene zin is ervoor gezorgd dat de uitvoering van beveiligingstaken en van toezicht en controle onafhankelijk plaatsvinden van de uitvoering van productiewerkzaamheden. Meer PKI-specifieke maatregelen zijn getroffen rondom het maken van het sleutelmateriaal en EV certificaten. De PA kan slechts sleutelmateriaal en EV certificaten genereren in gelijktijdige aanwezigheid van verschillende sleutelhouders. Elke sleutelhouder heeft toegang tot slechts een deel van de activeringsgegevens die nodig zijn om de signing key te kunnen

gebruiken. Ook bij het maken en publiceren van CRL's is dit zogenaamde N out of M principe toegepast[6]. Andere randvoorwaarden zijn:

- De CA systemen zijn stand-alone systemen zonder netwerkkoppelingen naar buiten;
- Tijdens operationeel gebruik staan de CA systemen in een beveiligde ruimte die alleen door daartoe bevoegde personen betreden kan worden;
- Na gebruik wordt het CA systeem met alle randapparatuur en sleuteldelen opgeborgen in een kluis die in bovenliggende beveiligde ruimte is geplaatst;
- De CA systemen worden door een keymanager bediend, waarbij er strikt volgens de scripts wordt gewerkt en onder constant toezicht van een getuige. Afhankelijk van de ceremonie is dit een onafhankelijke externe getuige of een vertegenwoordiger van de PA. Eventuele afwijkingen van het script worden zorgvuldig opgetekend;
- De complete ceremonie wordt van het begin (ophalen CA systemen en sleuteldelen) tot het eind (inpakken CA systemen en sleuteldelen) opgenomen en opgeslagen. De opnames worden bewaard;
- Tijdens de ceremonie zijn de sleuteldelen in het bezit van de betreffende sleutelhouders. De verdeling van de sleuteldelen over de sleuteldragers is zodanig dat het uitvoeren van een bepaalde activiteit niet kan worden uitgevoerd door de technisch beheerder zonder aanwezigheid van minimaal 2 ambtenaren. Het M out of N principe zorgt ervoor dat er meerdere sleuteldelen en sleuteldragers noodzakelijk zijn.
- Een verzoek tot certificering wordt door de PA aan de technisch beheerder overhandigd.

5.3 Personele beveiliging

De PA ziet erop toe dat de medewerkers in vertrouwensfuncties vrij zijn van tegengestelde belangen, zodat de onpartijdigheid van de activiteiten van de PA is gewaarborgd. Indien dit noodzakelijk wordt geacht worden bij de PA alleen personen aangenomen op vertrouwensfuncties wanneer op basis van een veiligheidsonderzoek uitgevoerd door de Algemene Inlichtingen en Veiligheidsdienst (AIVD) een verklaring van geen bezwaar is afgegeven.

Door de PA is personeel aangenomen dat beschikt over de voor de betreffende functies vereiste vakkennis, ervaring en kwalificaties.

5.4 Audit logging procedures ten behoeve van beveiligingsaudits

De PA houdt voor audit-doeleinden afschriften van computerloggings bij met de mutaties in de systemen die onderdeel uitmaken van de technische infrastructuur van de top van de hiërarchie en die voor de betrouwbaarheid van de dienstverlening van belang zijn. Voorbeelden hiervan zijn het aanmaken van accounts, installatie van software, back-

6 Vanwege de vertrouwelijkheid wordt in dit CPS niet aangegeven over hoeveel sleutelhouders de activeringsgegevens zijn verdeeld.

ups, het afsluiten en (her)starten van het systeem, hardware wijzigingen en veiligstelling van audit-logbestanden. Alle activiteiten van de PA met betrekking tot het genereren van sleutels en maken van certificaten en CRL's worden gelogd op zodanige wijze dat reconstructie van de systeemhandelingen achteraf mogelijk is.
Tijdens een CSP ceremonie wordt bij het opstarten van de informatiesystemen gecontroleerd of hierin (ongeautoriseerde) wijzigingen zijn aangebracht.

Na elke ceremonie wordt een volledige back-up gemaakt van systeem en database. De back-ups worden voor een periode van minimaal 7 jaren opgeslagen. Dit geldt alleen voor de laatste twee images van het systeem.

5.5 Archiveren van documenten

Als de signing keys aan het einde van de levensduur buiten gebruik zijn gesteld, vindt uit veiligheidsoverwegingen geen archivering van deze signing keys plaats. De signing keys worden op adequate wijze vernietigd, zodat het onmogelijk is ze weer in gebruik te nemen.

Van alle signing keys is een back-up gemaakt. Deze back-ups zijn opgeslagen in een andere ruimte dan waar de operationele signing keys zijn opgeslagen. Op de back-ups zijn dezelfde beveiligingsmaatregelen van toepassing als op de operationele signing keys.

De PA zal, nadat de geldigheid van het EV CSP certificaat is verlopen, voor tenminste 7 jaren alle informatie opslaan met betrekking tot de aanvraag en eventuele revocatie van het EV CSP certificaat en alle gegevens die zijn gebruikt voor het verifiëren van de identiteit van de CSP, Bevoegde Vertegenwoordiger en certificaatbeheerder.

5.6 Vernieuwen sleutels

Sleutels van certificaathouders mogen niet opnieuw worden gebruikt na het verstrijken van de geldigheidsduur of na het intrekken van het bijbehorende certificaat. Met het vernieuwen van certificaten wordt ook het sleutelpaar vernieuwd.

5.7 Compromittatie en continuïteit

De PA treft voorzieningen om de continuïteit van de eigen dienstverlening zodanig te waarborgen, dat mogelijke verstoringen minimaal blijven. Hiertoe behoort het in stand houden van kritieke diensten, waaronder het aanbieden van de revocation management service, de revocation status service en het via de gebruikelijke kanalen beschikbaar stellen van certificate status information.

De voorzieningen die de PA heeft getroffen betreffen o.a. het dubbel uitvoeren van systemen, installeren van Intrusion Detection Systemen en uitvoeren van back-ups.

Om te kunnen anticiperen op eventuele calamiteiten die zich kunnen voordoen binnen PKIoverheid Extended Validation heeft de PA een calamiteitenplan opgesteld. In dit plan zijn de maatregelen beschreven om een calamiteit zo spoedig mogelijk op te lossen. Het calamiteitenplan voorziet derhalve in het onmiddellijk bijeenroepen van een

calamiteitenteam met bepaalde bevoegdheden en middelen, teneinde passend te handelen.

Binnen PKIoverheid Extended Validation zijn meerdere partijen actief (Ministerie van BZK, PA, CSP's en de technisch beheerder van de root). Bij ieder van deze partijen kan een calamiteit optreden, die mogelijke gevolgen kan hebben voor de andere delen binnen de PKIoverheid Extended Validation keten. Om op een gecoördineerde wijze te kunnen optreden bij een calamiteit zijn de calamiteitenplannen van de verschillende partijen op elkaar afgestemd.

Om goed voorbereid te zijn op eventuele calamiteiten en om de gevolgen van een calamiteit te beperken wordt het calamiteitenplan van de PA periodiek getest. De afstemming en communicatie met betrokken partijen uit de PKIoverheid Extended Validation keten wordt hierbij ook getest.

6 Technische beveiliging

6.1 Genereren en installeren van sleutelparen

Het genereren van de sleutelparen van de PA vindt plaats tijdens de verschillende creatieceremonies. Daarbij worden slechts stand-alone computersystemen gebruikt. Deze computersystemen hebben geen verbinding met een netwerk, alle communicatie tussen systemen vindt plaats via media als CD-ROM, floppydisk of smartcard. Omdat het genereren en het gebruik van de signing key van de PA incidenteel plaatsvindt, zijn de computersystemen uitsluitend voor dit doel in gebruik. De meeste tijd zijn de kritische componenten van de computersystemen opgeborgen in een kluis.

De volgende sleutellengtes zijn van toepassing:

EV CSP sub-CA certificaten	4096 bit RSA sleutels
EV CSP CA certificaten	4096 bit RSA sleutels
Staat der Nederlanden EV Intermediair CA	4096 bit RSA sleutels
Staat der Nederlanden EV Root CA	4096 bit RSA sleutels

6.2 Private sleutelbescherming en beheersmaatregelen cryptografische modulen

De actieve signing keys van de PA bevinden zich altijd in de veilige behuizing van een cryptografische module (HSM) die voldoet aan:

- de eisen zoals beschreven in de standaard FIPS PUB 140-2 niveau 3 of hoger, of de eisen zoals beschreven in de standaard CWA 14167-2, of;
- een betrouwbaar systeem dat minimaal is gecertificeerd conform ISO 15408op evaluatiegarantieniveau EAL 4+ of gelijkwaardige beveiligingscriteria.

Alle handelingen met de signing keys van de PA vinden plaats volgens vooraf vastgestelde procedures. Vooraf zijn de personen aangewezen die bij deze handelingen aanwezig moeten zijn. Alleen als deze personen aanwezig zijn, kunnen de signing keys van de PA voor gebruik worden ontsloten.

De signing keys van de PA worden nimmer ter bewaring in handen gegeven van een derde partij.

Als de signing keys aan het einde van de levensduur buiten gebruik zijn gesteld, vindt uit veiligheidsoverwegingen geen archivering van deze signing keys plaats. De signing keys worden op adequate wijze vernietigd, zodat het onmogelijk is ze weer in gebruik te nemen.

Van alle signing keys is een back-up gemaakt. Deze back-ups zijn opgeslagen in een andere ruimte dan waar de operationele signing keys zijn opgeslagen. Op de back-ups zijn dezelfde beveiligingsmaatregelen van toepassing als op de operationele signing keys.

6.3 Andere aspecten van sleutelpaar management

Alle EV certificaten hebben een maximale periode van geldigheid:

EV CSP sub-CA certificaten	12 jaar minus 3 dagen
EV CSP certificaten	12 jaar minus 2 dagen
Staat der Nederlanden EV Intermediair CA	12 jaar minus 1 dag
Staat der Nederlanden EV Root CA	12 jaar

6.4 Activeringsgegevens

Activeringsgegevens voor de informatiesystemen zoals wachtwoorden en pincodes worden net als de sleuteldelen opgeslagen in aparte sealbags in de PKIoverheid kluis.

6.5 Beheersingsmaatregelen computersystemen

De computers van de PA die worden gebruikt om handelingen met een signing key van de PA uit te voeren zijn slechts toegankelijk voor geautoriseerde medewerkers. In de systemen zijn daarvoor softwarematige controles ingebouwd die zorg dragen voor de toegangscontrole. De software controleert de bevoegdheid van de medewerker voordat de betreffende handelingen op het computersysteem kunnen worden verricht. De op de computersystemen uitgevoerde handelingen worden gelogd op een zodanige wijze dat later kan worden vastgesteld welke medewerker de gelogde handelingen heeft uitgevoerd. De bijgehouden logs worden periodiek, ten minste eenmaal per jaar, gecontroleerd door de PA.

De hier bedoelde computersystemen van de PA zijn zodanig ingericht dat slechts de noodzakelijke handelingen kunnen worden uitgevoerd. Alle in dat opzicht overbodige componenten, zoals hulpprogramma's, zijn verwijderd. De computersystemen zijn stand-alone systemen, zodat bepalingen met betrekking tot netwerkbeveiliging niet van toepassing zijn.

De PA ziet erop toe dat de cryptografische hard- en software die de PA gebruikt voor het tekenen van certificaten nooit ongemerkt kan worden gewijzigd. Dit toezicht wordt gedurende de gehele levensloop van de cryptografische hard- en software gehouden.

6.6 Beheersingsmaatregelen technische levenscyclus

De hard- en software die wordt gebruikt in de centrale hiërarchie t.b.v. het keymanagement zijn meegenomen in de evaluatie door het NBV op stg. confidentieel. Bij wijzigingen in de informatiesystemen wordt opnieuw een evaluatie uitgevoerd.

CA systemen worden na uitvoerig testen in gebruik genomen en onderhouden door de technisch beheerder. Software updates worden zorgvuldig doorgevoerd na overleg met en in het bijzijn van de PA PKIoverheid.

6.7 Netwerkbeveiliging

De Staat der Nederlanden EV Root CA is off-line. De Staat der Nederlanden EV Intermediair CA is on-line ten behoeve van het signen van de CRL. De in dit CPS beschreven CRL’s staan ook online in de Certificate Status Service. De technisch beheerder van de EV Root van Logius heeft maatregelen genomen om de stabiliteit, de betrouwbaarheid en de veiligheid van het netwerk te waarborgen. Dit omvat bijvoorbeeld maatregelen om gegevensverkeer te reguleren en ongewenst

gegevensverkeer onmogelijk te maken, alsmede de plaatsing van firewalls om de integriteit en exclusiviteit van het netwerk te garanderen. Tevens zijn er maatregelen getroffen om ongewenste toegangspogingen tot de systemen tijdig te detecteren.

De Certificate Status Service is onderdeel van de jaarlijkse Webtrust audit. Deze wordt uitgevoerd door een externe IT-auditor. Daarnaast ondergaat de Certificate Status Service jaarlijks een penetratietest. Deze wordt uitgevoerd door een extern IT security bedrijf.

6.8 Tijdstempelen

De PA ondersteunt geen tijdstempeldienst als onderdeel van haar dienstverlening.

6.9 Cryptografische algoritmes (geen RFC 3647)

Binnen de PKIoverheid Extended validation is, met het oog op de betrouwbaarheid van de PKIoverheid Extended Validation, een beperkt aantal cryptografische algoritmes toegestaan. De PA zal, gelet op de te verwachten ontwikkelingen, regelmatig nagaan of de gehanteerde standaarden nog voldoen aan onder meer de aanbevelingen in ETSI TS 102 176-1. Mocht een overstap naar een ander algoritme noodzakelijk zijn dan zal hierover vooraf ook advies worden gevraagd aan het Nationaal Bureau voor Verbindingsbeveiliging (NBV-AIVD). Op basis van de ETSI standaard is in de certificaatprofielen, die zijn opgenomen in deel 3f van het Programma van Eisen, aangegeven welke algoritme is toegestaan.

7 Certificaat- en CRL profielen

7.1 Certificaatprofielen

De PA hanteert voor het formaat van de Staat der Nederlanden EV Root CA, het Staat der Nederlanden EV Intermediair CA certificaat en de EV CSP CA certificaten de standaard ITU-T Rec. X.509 (1997).

In Bijlage A is in een overzicht de inhoud weergegeven van de velden van het EV stamcertificaat en van het EV intermediair certificaat.

Binnen de hiërarchie van de EV root maakt de PA gebruik van zowel CRL als OCSP.

7.2 CRL profielen

Een CRL bevat informatie over ingetrokken certificaten die binnen de huidige geldigheidsperiode vallen of waarvan de geldigheidsperiode minder dan 6 maanden geleden is verlopen.
De CRL's voldoen aan de X.509v2 standaard voor publieke sleutel certificaten en CRL's.

De CRL voor statuscontrole van de EV intermediair CA is een jaar geldig.
De CRL voor statuscontrole van de CSP CA's is een half jaar geldig.

Er is een overgangsperiode van twee weken voordat de CRL verloopt, waarbinnen een nieuwe CRL wordt gepubliceerd.

Attribuut	
Versie	V2 Beschrijft de versie van het CRL profiel. Waarde 1 staat voor X.509 versie 2 CRL profiel.
Verlener	CN = Staat der Nederlanden EV Root CA O = Staat der Nederlanden C = NL
Ingangsdatum	Ingangsdatum van de CRL
Volgende update	Uiterste tijdstip waarop een update verwacht mag worden, eerdere update is mogelijk. Bevat datum en tijdstip waarop de volgende versie van de CRL (uiterlijk) verwacht mag worden.
Algoritme voor de handtekening	sha256 De waarde is gelijk aan het veld signatureAlgorithm en bevat het algoritme dat voor signing toegepast wordt. Het signing algoritme is SHA-256WithRSAEncryption.
intrekkingslijst	Ingetrokken certificaten met datum van revocatie. Bevat datum en tijdstip van revocatie en serialNumber van de ingetrokken certificaten.
CRL-nummer	Opeenvolgend nummer van publicatie van de CRL in hexadecimale

7.3 OCSP profielen

De EV root CA en de EV intermediair CA maken gebruik van OCSP en OCSP signing certificaten. OCSP signing certificaten zijn 14 maanden geldig en worden jaarlijks opnieuw getekend.

De OCSP responses en OCSPSigning certificates voldoen aan de eisen die hieraan worden gesteld in IETF RFC 2560. OCSPSigning certificaten zijn in overeenstemming met de X.509v3 norm voor publieke sleutel certificaten.

Basis Extensies	OID	Critical	Waarde
Certificate			N/a
SignatureAlgorithm	{ pkcs-1 5 }		N/a
Algorithm			sha256WithRSAEncryption (1.2.840.113549.1.1.11)
SignatureValue			Handtekening door Staat der Nederlanden EV Root CA
TBSCertificate			N/a
Version			2
serial number			SHA1 hash of public key door Staat der Nederlanden <Domein> CA – G<nummer> gegenereerd
Issuer DN			C=NL O=Staat der Nederlanden CN=Staat der Nederlanden EV Root CA – G<nummer>
Subject DN			C=NL O=Staat der Nederlanden CN=Staat der Nederlanden EV Root CA – G<nummer> OCSP Responder n (n= 1, 2, 3)
Validity			
notBefore			dd-mm-yyyy (Datum van de ceremonie)
notAfter			dd-mm-yyyy (14 maanden na de datum van de ceremonie)
Public Key Algorithm			sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Public Key Length			4096
Standaard Extenties	**OID**	**Critical**	**Waarde**
basicConstraints	{id-ce 19}	TRUE	n/a
cA			Clear (FALSE)
pathLenConstraint			n/a
keyUsage	{id-ce 15}	TRUE	n/a
Digital Signature			Set
SubjectKeyIdentifier	{id-ce 14}	FALSE	n/a
KeyIdentifier			Method-1
AuthorityKeyIdentifier	{id-ce 35}	FALSE	n/a
KeyIdentifier			Hash of public key of Issuing CA
CrlDistributionPoints	{id-ce 31}	FALSE	n/a
DistributionPoint			n/a
Full Name (URI)			http://crl.pkioverheid.nl/EVIntermediairLatestCRL.crl
extendedKeyUsage	{id-ce 37 }	TRUE	n/a
Key Purpose - OCSPsigning	{id-kp 9}		1.3.6.1.5.5.7.3.9
PrivateExtenties	**OID**	**Critical**	**Waarde**
id-pkix-ocsp-nocheck	1.3.6.1.5.5.7	FALSE	05 00 (Null)

	.48.1.5		

8 Conformiteitbeoordeling

8.1 Frequentie en omstandigheden van de conformiteitsbeoordeling

De PA van PKIoverheid zal zich houden aan de eisen zoals beschreven in de laatste versie van het WebTrust program for CA – Extended Validation. De PA van PKIoverheid ondergaat hiervoor jaarlijks een WebTrust for CA Audit – Extended Validation audit.[7]

Daarnaast conformeert de PA PKIoverheid zich tevens aan de *SSL Baseline Requirements Audit Criteria* van Webtrust.

De PA PKIoverheid zal actief de wijzigingen in het Webtrust program for CA monitoren die van invloed zijn op dit CPS. Eveneens zal de PA PkIoverheid actief wijzigingen in de *Baseline Requirements* van het CA/Browserforum monitoren die van invloed zijn op dit CPS en op het Programma van Eisen van PKIoverheid. Deze wijzigingen zullen worden beoordeeld op hun impact op het CPS en PvE van PKIoverheid.

Tevens conformeert de PA PKIoverheid zich aan vastgesteld rijksbeleid op het gebied van informatiebeveiliging en privacy.

8.2 Identiteit, kwalificaties van de auditor

Audits worden uitgevoerd door een externe gecertificeerde WebTrust for CAs auditor.

8.3 Onderwerpen behandeld door de conformiteitbeoordeling

Bij deze audit wordt nagegaan of de kwaliteit en de beveiligingsmaatregelen van de ingerichte organisatie voldoen aan de gestelde Webtrust normen.

8.4 Acties op basis van afwijkingen

Indien additionele beveiligingsmaatregelen worden aanbevolen, dan zal de PA terstond acties ondernemen om deze maatregelen te implementeren.

8.5 Communiceren van de resultaten

Door middel van een Webtrustzegel dat wordt gepubliceerd op de website van Logius toont de PA PKIoverheid jaarlijks aan te voldoen aan de Webtrust normen.

8.6 Toetreden CSP's tot de PKI voor de overheid

Zie "deel 2 van het Programma van Eisen PKIoverheid"[8]

7 http://www.webtrust.org/

8 https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-csp/programma-van-eisen/

9 Algemene en juridische bepalingen

9.1 Tarieven

Het Staat der Nederlanden EV Intermediair CA en de EV CSP CA-certificaten bevatten een verwijzing naar dit CPS. Er worden geen kosten in rekening gebracht voor het raadplegen van deze certificaten of de informatie waarnaar wordt verwezen. Dit geldt voor:

- het raadplegen van de certificaten;
- het raadplegen van de revocation status information (CRL's) en;
- het raadplegen van de Programma van Eisen, deel 3: Certificate Policies;
- het raadplegen van dit CPS.

9.2 Financiële verantwoordelijkheid en aansprakelijkheid

In het kader van aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van de wettelijke verplichting tot schadevergoeding.

BZK en een CSP sluiten een overeenkomst dan wel convenant over het deelnemen van de betreffende CSP aan PKIoverheid Extended Validation. Inhoudelijk betekent dit dat de CSP verplicht is haar diensten te verlenen binnen de door BZK gestelde voorwaarden, met name de voorwaarden zoals gesteld in het Programma van Eisen deel 3: basiseisen en deel3f. De PA is hierbij het aanspreekpunt voor de CSP.

Bepalingen omtrent aansprakelijkheid van BZK jegens een CSP zijn opgenomen in een overeenkomst dan wel convenant tussen BZK en de CSP. De eisen waaraan de aansprakelijkheid van de CSP moet voldoen zijn geformuleerd in het Programma van Eisen deel3: basiseisen en deel 3f.

De CSP sluit overeenkomsten met abonnees en vertrouwende partijen. In deze overeenkomsten wordt ook de aansprakelijkheid van de CSP jegens abonnees en vertrouwende partijen geregeld. De eisen waaraan deze aansprakelijkheid moet voldoen zijn opgenomen in de Algemene bepalingen van het Programma van Eisen deel 3:basiseisen en deel 3f.

De Staat der Nederlanden heeft voor schadeclaims in het kader van eventuele aansprakelijkheid geen verzekering afgesloten.

9.3 Vertrouwelijkheid van organisatiegegevens

De Policy Authority PKIoverheid gaat vertrouwelijk om met organisatiegegevens. Alleen medewerkers van de PA PKIoverheid hebben toegang tot deze gegevens.

Organisatiegegevens zoals auditrapporten en Corrective Action Plans van CSP’s worden versleuteld uitgewisseld.

9.4 Vertrouwelijkheid van persoonsgegevens

De PA PKIoverheid geeft in tegenstelling tot de CSP geen certificaten uit aan natuurlijke personen. Een registratie met persoonsgegevens van certificaathouders is derhalve niet aanwezig.

9.5 Intellectuele eigendomsrechten

Voorliggend CPS is eigendom van Logius. Ongewijzigde kopieën van dit CPS mogen zonder toestemming verspreid en gepubliceerd worden mits dit met bronvermelding geschiedt.

9.6 Aansprakelijkheid en verplichtingen

Zie paragraaf 9.2.

9.7 Verwerping van aansprakelijkheid

Zie paragraaf 9.2.

9.8 Beperkingen van aansprakelijkheid

Zie paragraaf 9.2.

9.9 Vrijwaring

Zie paragraaf 9.2.

9.10 Geldigheidsduur en ontbinding CPS

Dit is versie 1.5 van het document "CERTIFICATION PRACTICE STATEMENT (CPS) Policy Authority PKIoverheid voor Extended Validation certificaten uit te geven door de Policy Authority van de PKI voor overheid", oktober 2016.

Dit CPS is geldig vanaf de datum inwerkingtreding. Het CSP is geldig zolang de dienstverlening van de PKI voor de overheid voortduurt of tot dat het CPS wordt vervangen door een nieuwere versie. Nieuwere versies worden aangeduid met een hoger versienummer (vX.x). Bij ingrijpende wijzigingen wordt het versienummer opgehoogd met 1, bij overige minder ingrijpende aanpassingen wordt het versienummer opgehoogd met 0.1. Nieuwere versies worden gepubliceerd op de website van de PA (https://cps.pkioverheid.nl).

9.11 Afspraken en communicatie tussen entiteiten uit de PKIoverheid-hiërarchie

Indien CSP's vragen hebben kan contact worden opgenomen met de PA PKIoverheid.

Er wordt op regelmatige basis gecommuniceerd via e-mail met de contactpersonen van de aan het PKIoverheid stelsel deelnemende CSP's. CPS's worden terstond op de hoogte gesteld van de publicatie van een nieuwe versie van het CPS of Programma van Eisen. Ook worden voorgenomen wijzigingen zo snel mogelijk kenbaar gemaakt.

Naast communicatie met de CSP's is er tevens geregeld contact met de ACM en de auditor(s) van de deelnemende CSP's.

9.12 Wijzigingen

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor dit CPS. Het ministerie heeft deze taak gedelegeerd aan Logius. Dit omvat ook het goedkeuren van wijzigingen op dit CPS.

Alle wijzigingendie niet tot de categorie van wijzigingen van redactionele aard behoren worden bekend gesteld en leiden tot een nieuwe versie van het CPS. Wijzigingen van redactionele aard zijn geen aanleiding een nieuwe versie van het CPS te publiceren.

9.13 Geschillenbeslechting

Zie hiervoor de individuele overeenkomsten tussen Logius PKIoverheid en CSP's.

9.14 Van toepassing zijnde wetgeving

Het Nederlands recht is van toepassing.

9.15 Naleving relevante wetgeving

De PA-functie wordt uitgevoerd door Logius. Logius is een baten- en lastendienst onderdeel van het Directoraat-Generaal Bestuur en Koninkrijksrelaties. Op Logius is de Awb van toepassing.

Bijlage A. Inhoud velden EV Root- & Intermediair-certificaat

Attribuut	**Staat der Nederlanden EV Root CA**	**Staat der Nederlanden EV Intermediair CA**
Versie	V3	
Serienummer	0098968D	0098969a
Algoritme voor handtekening	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Verlener	CN = Staat der Nederlanden EV Root CA O = Staat der Nederlanden C = NL	
Geldig van	woensdag 8 december 2010 12:19:29	woensdag 8 december 2010 13:41:43
Geldig tot	donderdag 8 december 2022 12:10:28	woensdag 7 december 2022 13:38:55
Onderwerp	CN = Staat der Nederlanden EV Root CA O = Staat der Nederlanden C = NL	CN = Staat der Nederlanden EV Intermediair CA O = Staat der Nederlanden C = NL
Openbare sleutel	RSA (4096 Bits) Betreft cijferreeks. Bevat o.a. de publieke sleutel.	RSA (4096 Bits) Betreft cijferreeks. Bevat o.a. de publieke sleutel.
Certificate Policies	n.v.t.	PolicyQualifiers:policyQualifierId: 2.16.528.1.1003.1.2.7 (PKIoverheid explicit EV policy identifier) Qualifier:cPSuri: http://www.logius.nl/producten/toegang/pkioverheid/documentatie/cps/
Sleutel ID van CA	n.v.t.	Sleutel-ID= fe ab 00 90 98 9e 24 fc a9 cc 1a 8a fb 27 b8 bf 30 6e a8 3b
CRL distributie	n.v.t.	http://crl.pkioverheid.nl/EVRootLatestCRL.crl
Sleutel ID van onderwerp	fe ab 00 90 98 9e 24 fc a9 cc 1a 8a fb 27 b8 bf 30 6e a8 3b	25 80 eb d8 9f a6 c3 11 41 37 c7 78 59 88 1e 69 ef b1 d3 ea
Essentiële	Subjecttype=CA	

Attribuut	**Staat der Nederlanden EV Root CA**	**Staat der Nederlanden EV Intermediair CA**
beperkingen	Beperking voor padlengte=Geen	
Sleutelgebruik	Certificaatondertekening, Off line CRL-ondertekening, CRL-ondertekening	
Vingerafdruk algoritme	sha1	
SHA-1 Vingerafdruk	76 e2 7e c1 4f db 82 c1 c0 a6 75 b5 05 be 3d 29 b4 ed db bb	ed a4 7d 89 71 81 88 bd 00 14 66 fc db bc ae ed 29 24 39 cc

Bijlage B. Tekst Staatscourant bekendmaking stamcertificaat PKI Staat der Nederlanden EV Root CA

De Minister van Binnenlandse Zaken en Koninkrijksrelaties maakt bekend dat 8 december 2010 een nieuw stamcertificaat van de PKI voor de overheid is gecreëerd onder de naam

Staat der Nederlanden EV Root CA

Dit stamcertificaat is het centrale deel van PKIoverheid Extended Validation. Het stamcertificaat is het ankerpunt van vertrouwen voor PKIoverheid Extended Validation SSL certificaten die gebruikt kunnen worden voor het beveiligen van een verbinding tussen een bepaalde client en een server, via het TLS/SSL protocol.

De houder van het stamcertificaat is geïdentificeerd als de Staat der Nederlanden EV Root CA (Common name), Staat der Nederlanden (Organisation), NL (Country).

Het serienummer van het stamcertificaat is 10000013 (hexadecimaal 0098 968d).

Het stamcertificaat is geldig tot: donderdag 8 december 2022 11:10:28 (GMT)

De identificatie van het stamcertificaat (de vingerafdruk in hexadecimale vorm) op basis van het SHA1-algoritme is: 76E2 7EC1 4FDB 82C1 C0A6 75B5 05BE 3D29 B4ED DBBB

Dit stamcertificaat, de documenten die aan dit certificaat ten grondslag liggen en nadere informatie over dit stamcertificaat zijn in elektronische vorm beschikbaar op de website: https://cert.pkioverheid.nl. Op deze website is toegelicht op welke wijze de identificatie van het stamcertificaat kan plaatsvinden.

Het beheer van het stamcertificaat is opgedragen aan de Policy Authority van de PKI voor de overheid. Deze organisatie is ondergebracht bij Logius, dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
P.H. Donner.

Bijlage C. Procedures voor het wijzigingenbeheer van het PvE PKIoverheid

Overlegstructuur

1. Het PKIoverheidstelsel kent de volgende overleggen ten behoeve van het wijzingenbeheer van het Programma van Eisen: het PKIoverheid wijzigingenoverleg en PKIoverheid stelseloverleg.

2. Het stelseloverleg bestaat uit een afvaardiging van de PA en de CSP's die deelnemen aan het PKIoverheidstelsel. Het wijzigingenoverleg wordt eveneens gevormd door een afvaardiging van de PA en CSP's waarbij de mogelijkheid wordt geboden om experts uit te nodigen.

3. Auditors van CSP's die deelnemen aan het PKIoverheidstelsel mogen als toehoorder aanschuiven bij het wijzigingenoverleg en / of stelseloverleg. Wanneer een auditor aanwezig is heeft deze kennis genomen van de wijzigingsvoorstellen en kan tenminste aangeven of een nieuwe of gewijzigde norm auditeerbaar is.

4. Beide overleggen zijn in het bijzonder bedoeld om wijzigingen in het Programma van Eisen (PVE) af te stemmen.
   Het wijzigingenoverleg wordt gebruikt om conceptwijzigingsvoorstellen te bespreken en zoveel mogelijk consensus te bereiken over definitieve wijzigingsvoorstellen.
   Het stelseloverleg wordt gebruikt voor mededelingen omtrent het PKIoverheidstelsel en om een voorgenomen besluit te nemen over opname van definitieve wijzigingsvoorstellen in een eerstvolgende versie van het PVE met daarbij een ingangsdatum.

5. Het stelseloverleg vindt in principe 2 keer per jaar plaats ten behoeve van de publicatie van een nieuwe versie van het Programma van Eisen van PKIoverheid.

6. Een wijzigingenoverleg vindt in ieder geval een maand voorafgaand aan het stelseloverleg plaats, maar kan ook vaker plaatsvinden om wijzigingsvoorstellen met een grote impact te bespreken.

7. Voor het bespreken van specifieke onderwerpen, niet direct gerelateerd aan actuele PVE wijzigingen kunnen aparte bijeenkomsten worden georganiseerd.

Besluitvorming

1. In het stelseloverleg wordt getracht om op basis van consensus een voorgenomen besluit te nemen over de inhoud en ingangsdatum van wijzigingen in het Programma van Eisen.

2. Wijzigingen in het PVE worden doorgevoerd door Het Ministerie van Binnenlandse Zaken die als opdrachtgever eindverantwoordelijk is voor het PKIoverheid stelsel en beslist over het doorvoeren van wijzigingsvoorstellen, al dan niet via een versnelde wijzigingsprocedure. De PA adviseert de opdrachtgever hierbij.

3. Elk voorgenomen besluit naar aanleiding van een stelseloverleg of versnelde wijzigingsprocedure, wordt door de PA ter goedkeuring voorgelegd aan een door de Minister van Binnenlandse Zaken en Koninkrijksrelaties daartoe aangewezen functionaris tezamen met een advies van de PA en het standpunt van de CSP's.9

4. Tevens zal de door de Minister van Binnenlandse Zaken en Koninkrijksrelaties daartoe aangewezen functionaris worden geïnformeerd over wijzigingsvoorstellen die (tijdelijk) zijn ingetrokken.

5. Indien sprake is van een verschil van inzicht met de CSP's over een wijzigingsvoorstel, zal de beslissing door de functionaris van het Ministerie van Binnenlandse Zaken worden gemotiveerd.

6. Bij goedkeuring door de Minister van Binnenlandse Zaken en Koninkrijksrelaties aangewezen functionaris wordt de wijziging door de PA duidelijk herkenbaar en in begrijpelijke taal gepubliceerd op de website van Logius. Bij publicatie wordt tevens vermeld wanneer de wijziging van kracht zal worden.

7. Aanvullend stelt de PA de CSP contactpersonen en de indiener van het wijzigingsvoorstel actief elektronisch en/of schriftelijk op de hoogte van het genomen besluit.

8. Indien sprake is van een nieuwe versie van het PVE zal voor publicatie een formele handtekening nodig zijn van zowel de directeur van Logius als de door de Minister van Binnenlandse Zaken en Koninkrijksrelaties aangewezen functionaris. Indien sprake is van een versnelde wijzigingsprocedure zal goedkeuring van wijzigingen per e-mail volstaan.

---

9 Momenteel is dat de directeur van B&I van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

9. De door de Minister van Binnenlandse Zaken en Koninkrijksrelaties aangewezen functionaris behoudt zich het recht voor om autonoom wijzigingen door te voeren in het PVE in het kader van een (dreigend) incident, calamiteit of crisis.

Normenkader

1. CSP's zijn verplicht zich te houden aan de inhoud en ingangsdatum van wijzigingen die door de Minister van Binnenlandse Zaken en Koninkrijksrelaties aangewezen functionaris zijn goedgekeurd dan wel afgekondigd.

2. Wanneer een CSP niet kan voldoen aan de ingangsdatum van een nieuwe of gewijzigde eis, zal de CSP hiervoor formeel dispensatie moeten aanvragen bij de PA PKIoverheid.

3. Een verzoek tot dispensatie wordt uiterlijk een week na het stelsoverleg formeel ingediend en aangekondigd tijdens het overleg.

4. Dispensatie moet elektronisch en/of schriftelijk aangevraagd worden bij de PA PKIoverheid.

5. Het verlenen van dispensatie wordt door de PA ter goedkeuring voorgelegd aan de door de Mi*n*ister van Binnenlandse Zaken en Koninkrijksrelaties daartoe aangewezen functionaris.

6. De PA zal elektronisch en/of schriftelijk reageren met een afschrift naar de auditor van de CSP waarin het verzoek wordt gehonoreerd of afgewezen.

Wijzigingsvoorstellen

1. De volgende partijen kunnen een wijzigingsvoorstel betreffende een onderdeel of een bepaling van het Programma van Eisen (PVE) indienen via de reguliere of versnelde wijzigingsprocedure:

   • Het ministerie van BZK;
   • De PA PKIoverheid (PA);
   • CSP's binnen de PKI voor de overheid die het PVE hanteren.

2. De PA kan wijzigingsvoorstellen indienen op basis van input van eindgebruikers of andere belanghebbenden. Dit zal duidelijk worden aangeven bij het wijzigingsverzoek.

3. Wijzigingsverzoeken worden normaliter afgestemd via een wijzigingenoverleg en stelseloverleg. Indien een wijziging niet kan wachten tot een volgende versie van het PVE kan een versnelde

wijzigingsprocedure worden gevolgd.

4. Het indienen van een wijzigingsvoorstel dient te geschieden door het aanvraagformulier "Wijzigingsvoorstel Programma van Eisen" in te vullen en dit bij de PA aan te bieden. Dit formulier kan worden gevonden op de website van de PA of kan direct worden aangevraagd bij de PA.

5. De PA behandelt een ingediend wijzigingsvoorstel betreffende een onderdeel of een bepaling van het PVE conform gedocumenteerde interne processen. In het geval van een wijziging van inhoudelijke aard geeft de PA een advies, inclusief tekstvoorstel, impactanalyse (onder meer voor een overgangsregeling, ingangsdata en eventuele dispensatie) en motivatie. Deze worden aan de CSP's ter afstemming voorgelegd.

Reguliere wijzigingsprocedure

1. In principe wordt twee keer per jaar een nieuwe versie van het PVE gepubliceerd. Een voorgenomen besluit omtrent opname van een nieuwe of gewijzigde eis in het PVE wordt genomen in het stelseloverleg voorafgaand aan de publicatie.

2. Een wijzigingsvoorstel wordt door de PA direct verspreid onder de CSP's en de auditoren van de CSP's zodra een concept hiervan gereed is.

3. Wijzigingsvoorstellen worden, ten minste tien weken voor het stelseloverleg plaatsvindt, verstuurd naar de CSP's.

4. Wijzigingsverzoeken die na deze datum worden ingediend kunnen niet meer in behandeling worden genomen voor publicatie in de eerstvolgende versie van het PVE, tenzij de PA en CSP's unaniem van mening zijn dat deze wijziging nog kan worden meegenomen.

5. CSP's hebben vijf weken de tijd om wijzigingsvoorstellen te analyseren en feedback te geven aan de PA.

6. Deze feedback wordt meegenomen in een wijzigingenoverleg voorafgaand aan het stelseloverleg.

7. Naar aanleiding van het wijzigingenoverleg worden wijzigingsvoorstellen definitief gemaakt.

8. De data voor het wijzigingen- en stelseloverleg worden zo snel mogelijk na het versturen van de laatste conceptvoorstellen t.b.v. van een volgende versie van het PVE door de PA vastgesteld, waarbij er mimimaal 4 weken zitten tussen het wijzigingenoverleg en het stelseloverleg.

9. Definitieve wijzigingsvoorstellen worden uiterlijk twee weken na het wijzigingenoverleg verstuurd aan de CSP's en de auditors tezamen met de agenda voor het stelseloverleg.

10. De reactietermijn van CSP's op de agenda en de definitieve wijzigingsvoorstellen bedraagt mimimaal een week en is maximaal een week voor aanvang van het stelseloverleg.

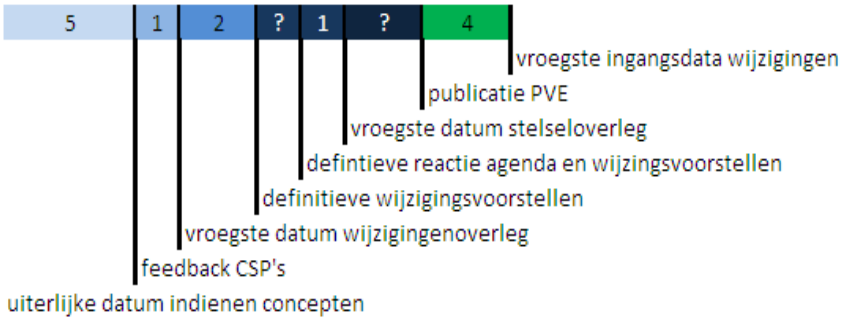
11. CSP's worden geacht om niet met nieuwe inhoudelijke inzichten te komen nadat de definitieve wijzigingsvoorstellen zijn afgerond en verstuurd. Hiermee wordt beoogd te voorkomen dat de PA en overige CSP's tijdens het stelseloverleg worden gedwongen een beslissing te nemen zonder een goede afweging te hebben gemaakt over het inhoudelijk nieuwe voorstel.

12. Indien de afvaardiging van een CSP niet aanwezig kan zijn bij een wijzigingenoverleg of stelseloverleg, wordt de CSP contactpersoon geacht vooraf zijn standpunt schriftelijk toe te lichten aangaande de inhoud en ingangsdatum van wijzigingen.

13. Na het stelseloverleg wordt het PVE zo spoedig mogelijk gepubliceerd. De ingangsdata van de nieuwe of gewijzigde wijzigingen zijn minimaal vier weken na publicatie van de nieuwe versie van het PVE.

14. Ingangsdata van wijzigingen worden expliciet opgenomen in het PVE.

I Regulier wijzigingenproces in weken



Versnelde wijzigingsprocedure

1. Wijzigingen worden normaliter via de reguliere wijzigingsprocedure afgehandeld. Bij een (dreigend) incident,

calamiteit of crisis zal de Minister van Binnenlandse Zaken en Koninkrijksrelaties aangewezen functionaris autonoom wijzigingen kunnen doorvoeren. Daarnaast kan ook een versnelde wijzigingsprocedure worden gevolgd, indien het noodzakelijk is om een wijziging door te voeren ruim voor publicatie van een nieuwe versie van het PVE.

2. De PA besluit wanneer het noodzakelijk is om een versnelde wijzigingsprocedure te volgen en zal bij zijn afweging de grootst mogelijke zorgvuldigheid betrachten.

3. Bij een versnelde wijzigingsprocedure wordt het volgende proces gevolgd:

    a) De intentie van de PA om een wijziging via een versnelde wijzigingsprocedure te publiceren op de website van Logius wordt aan de CSP's, de auditors van de CSP's en de door de minister van Binnelandse Zaken en Koninkrijksrelaties aangewezen functionaris kenbaar gemaakt via e-mail tezamen met het wijzigingsverzoek.
    b) CSP's hebben minimaal een week de tijd om bezwaar aan te tekenen tegen de inhoud en / of ingangsdatum van deze wijziging.
    c) Een bezwaar wordt in behandeling genomen door de PA PKioverheid die zal pogen om in goed overleg tot een gedragen advies te komen.
    d) Besluitvorming door het Ministerie van Binnenlandse Zaken geschiedt zoals beschreven in de paragraaf "Besluitvorming".
    e) De PA publiceert de wijziging op de website en communiceert dit naar de CSP's. CSP's zijn verplicht zich te houden aan de inhoud en de ingangsdatum van de op de website van Logius gepubliceerde wijziging.

Overigen

1. Het PVE en de geaccordeerde wijzigingen hierop kunnen in elektronische vorm worden verkregen via Internet op de website van de PA. Het adres hiervan is: http://www.logius.nl/pkioverheid.

2. In het PVE zal worden verwezen naar deze wijzigingenprocedure, die wordt opgenomen in het CPS van PKIoverheid.

Bijlage D. Certificaatprofiel CSP CA

Basis Extensies	OID	Critical	Waarde
Certificate			N/a
SignatureAlgorithm•Algorithm	{ pkcs-1 5 }		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
SignatureValue			Handtekening door EV Intermediair CA
TBSCertificate			N/a
Version			2
SerialNumber			door EV Intermediair CA gegenereerd
Signature			sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer•CountryName	C		NL
Issuer•OrganisationName	O		Staat der Nederlanden
Issuer• CommonName	CN		Staat der Nederlanden EV Intermediair CA
Validity•NotBefore			dd-mm-yyyy
Validity•NotAfter			dd-mm-yyyy
SubjectCountryName	C		NL
Subject•OrganisationName	O		[naam CSP]
Subject•CommonName	CN		[naam CSP] PKIoverheid EV CA
SubjectPublicKeyInfo			Publieke sleutel CSP-CA (Keylength=4096)
Standaard Extenties	**OID**	**Critical**	**Waarde**
CertificatePolicies	{id-ce 32}	FALSE	N/a
PolicyIdentifier			2.16.528.1.1003.1.2.7
PolicyQualifierId			1.3.6.1.5.5.7.2.1 (id-qt-cps)
Qualifier			https://cps.pkioverheid.nl
KeyUsage	{id-ce 15}	TRUE	N/a
KeyCertSign			Set
CRLSign			Set
AuthorityKeyIdentifier	{id-ce 35}	FALSE	N/a
KeyIdentifier			160-bit SHA-1 Hashwaarde van de EV Intermediair CA
SubjectKeyIdentifier	{id-ce 14}	FALSE	N/a
KeyIdentifier			160-bit SHA-1 Hashwaarde van deze CSP CA
AuthorityInfoAccess	{id-pe 1}	FALSE	
accessMethod	1.3.6.1.5.5.7.48.1		OCSP
accessLocation: URI			http://ocsp.pkioverheid.nl
accessMethod	1.3.6.1.5.5.48.2		Certification Authority Issuer
accessLocation: URI			https://cert.pkioverheid.nl/EVIntermediairCA.cer
CRLDistributionPoints	{id-ce 31}	FALSE	N/a
DistributionPoint•FullName			http://crl.pkioverheid.nl/EVIntermediairLatestCRL.crl
ExtendedKeyUsage	{id-ce 37 }	FALSE	n/a
Id-kp-serverAuth	{id-kp 1}		1.3.6.1.5.5.7.3.1

Id-kp-clientAuth	{id-kp 2}		1.3.6.1.5.5.7.3.2
Id-kp-OCSPsigning	{id-kp 9}		1.3.6.1.5.5.7.3.9
BasicConstraints	{id-ce 19}	TRUE	N/a
CA			Set
PathLenConstraint			0