Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programma van Eisen deel 3f: Certificate Policy – Extended Validation

Datum 18 januari 2016

EV policy OID 2.16.528.1.1003.1.2.7

Colofon

Versienummer 4.2
Contactpersoon Policy Authority PKIoverheid

Organisatie Logius

Bezoekadres
Wilhelmina van Pruisenweg 52

Postadres
Postbus 96810
2509 JE DEN HAAG

T 0900 - 555 4555
servicecentrum@logius.nl

Inhoud

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

Revisiegegevens

Versie	**Datum**	**Omschrijving**
1.0	07-12-2010	Definitieve versie
3.0	25-01-2011	Vastgesteld door BZK januari 2011
3.1	01-07-2011	Vastgesteld door BZK juni 2011
3.2	27-01-2012	Vastgesteld door BZK januari 2012
3.3	01-07-2012	Vastgesteld door BZK juni 2012
3.4	04-02-2013	Vastgesteld door BZK januari 2013
3.5	06-07-2013	Vastgesteld door BZK juli 2013
3.6	27-01-2014	Vastgesteld door BZK januari 2014
3.7	06-2014	Vastgesteld door BZK juni 2014
4.0	12-2014	Vastgesteld door BZK december 2014
4.1	07-2015	Vastgesteld door BZK juli 2015
4.1	08-2015	Correctie aan foutief doorgevoerde wijziging aan eis 3.2.2-pkio147
4.2	01-2016	Vastgesteld door BZK januari 2016

1 Introductie op de Certificate Policy

1.1 Achtergrond

Dit is deel 3f van het Programma van Eisen (PvE) van de PKI voor de overheid en wordt aangeduid als Certificate Policy (CP) Extended Validation (EV). In het PvE zijn de normen voor de PKI voor de overheid vastgelegd. Dit deel heeft betrekking op de eisen die aan de dienstverlening van een Certification Service Provider (CSP) binnen de PKI voor de overheid worden gesteld. Dit document heeft uitsluitend betrekking op de Extended Validation (EV) SSL certificaten en EV issuing subordinate CA certificaten uitgegeven door CSP's onder de Staat der Nederlanden EV Root CA.

In dit hoofdstuk is een beknopte toelichting opgenomen op de CP. Een uitgebreide toelichting op de achtergrond en structuur van de PKI voor de overheid, evenals de samenhang tussen de verschillende delen uit het PvE is opgenomen in deel 1 van het PvE.

Voor een overzicht van de in dit deel gehanteerde definities en afkortingen wordt verwezen naar deel 4 van het PvE.

1.1.1 Opzet van de Certificate Policy

Zoals in deel 1 van het PvE is aangegeven bestaan de eisen die onderdeel uitmaken van de CP uit eisen[1]:

- die voortkomen uit het Nederlandse wettelijke kader in relatie tot de elektronische handtekening;
- die voortkomen uit de vigerende versie van de standaard ETSI TS 102 042 EVCP, gecombineerd met de PTC-BR en Netsec. **Voor Netsec geldt dat eisen 1h, 3a, 3e, 4c.i en 4f niet normatief zijn** (ETSI CP OID 0.4.0.2042.1.4);
- die specifiek door en voor de PKIoverheid Extended Validation zijn opgesteld.

In de hoofdstukken 2 t/m 9 is voor de specifieke PKIoverheid-eisen een verwijzing opgenomen naar de Aanvullende eisen. In de onderstaande tabel is de structuur van de verwijzing naar de inhoudelijke PKIoverheid-eis (PKIo-eis) weergegeven.

RFC 3647	Verwijzing naar de paragraaf uit de RFC 3647-structuur waarop de PKIo-eis betrekking heeft. RFC 3647 is een PKIX raamwerk van de Internet Engineering Task Force (IETF) en is de de facto standaard voor de structuur van Certificate Policies en Certification Practice Statements[2].
Nummer	Uniek nummer van de PKIo-eis. Per paragraaf wordt een doorlopende nummering gehanteerd voor de PKIo-eisen. In combinatie met het RFC 3647 paragraafnummer vormt dit een unieke aanduiding voor de PKIo-eis.

In dit CP zijn ook een aantal bepalingen opgenomen die niet als PKIo-eis zijn geformuleerd. Deze bepalingen stellen geen eisen aan de CSP's

[1] *Voor een toelichting op positionering van de binnen de PKI voor de overheid geldende eisen wordt verwezen naar deel 1 van het PvE.*

[2] *In de hoofdstukken 2 t/m 9 zijn alleen die paragrafen uit RFC 3647 opgenomen waarvoor een PKIo-eis van toepassing is.*

binnen de PKI voor de overheid maar zijn als beleid wel van toepassing op de PKI voor de overheid. Het betreft hier bepalingen uit de paragrafen 1.1, 1.1.1, 1.1.2, 1.2, 1.3, 1.4, 1.5, 8, 9.12.1, 9.12.2, 9.14 en 9.17.

In bijlage A zijn de binnen de PKIoverheid gehanteerde profielen met betrekking tot de EV SSL certificaten opgenomen. De certificaat statusinformatie is in de basiseisen opgenomen.

1.1.2 Verhouding CP en CPS

Voorliggend CP beschrijft de minimumeisen die zijn gesteld aan de dienstverlening, op het gebied van EV SSL certificaten, van een Certification Service Provider (CSP) binnen de PKI voor de overheid. De Certification Practice Statement EV certificaten binnen de PKI voor de overheid geeft aan op welke wijze invulling wordt gegeven aan deze dienstverlening, voor zover dit valt onder directe verantwoordelijkheid van de PA.

1.1.3 Status

Dit is versie 4.2 van deel 3f van het PvE. De huidige versie is bijgewerkt tot en met 18 januari 2016.

De PA heeft de grootst mogelijke aandacht en zorg besteed aan de gegevens en informatie, die zijn opgenomen in deze CP. Desalniettemin is het mogelijk dat onjuistheden en onvolkomenheden voorkomen. De PA aanvaardt geen enkele aansprakelijkheid voor schade als gevolg van deze onjuistheden of onvolkomenheden, noch voor schade die wordt veroorzaakt door het gebruik of de verspreiding van deze CP, indien deze CP wordt gebruikt buiten het in paragraaf 1.4 van deze CP beschreven certificaatgebruik.

1.2 Verwijzingen naar deze CP

Elke CP wordt uniek geïdentificeerd door een OID. De volgende OID is geregistreerd door PKIoverheid voor opname in alle EV certificaten:

EV policy OID **2.16.528.1.1003.1.2.7**

De OID is als volgt opgebouwd: {joint-iso-itu-t (2). country (16). nederland (528). Nederlandse organisatie (1). nederlandse-overheid (1003). pki voor de overheid (1). cp (2). ev (7).

1.3 Gebruikersgemeenschap

De gebruikersgemeenschap bestaat uit in Nederland gevestigde abonnees, die organisatorische entiteiten binnen overheid en bedrijfsleven zijn (zie PKIo 3.2.2-pkio15) en uit certificaathouders, die bij deze abonnees behoren. Daarnaast zijn er vertrouwende partijen, die handelen in vertrouwen op certificaten van de betreffende certificaathouders.

De partijen binnen de gebruikersgemeenschap zijn abonnees, certificaatbeheerders, certificaathouders en vertrouwende partijen.

- Een abonnee is een natuurlijke of rechtspersoon die met een CSP een overeenkomst sluit namens een of meer certificaathouders voor het laten certificeren van de publieke sleutels.
- Een certificaathouder is een entiteit, gekenmerkt in een certificaat als de houder van de private sleutel die is verbonden met de publieke sleutel die in het certificaat is gegeven. De certificaathouder is

onderdeel van een organisatorische entiteit waarvoor een abonnee de contracterende partij is.

Binnen de Certificate Policy Extended Validation wordt de volgende invulling aan de term certificaathouder gegeven:
”een apparaat of een systeem (een niet-natuurlijke persoon), bediend door of namens een organisatorische entiteit.”

In deze CP gebruiken we de naam "service" voor dergelijke certificaathouders. Voor het uitvoeren van de handelingen ten aanzien van de levensloop van het certificaat van de certificaathouder is tussenkomst door een andere partij dan de certificaathouder vereist. De abonnee is hiervoor verantwoordelijk en dient een certificaatbeheerder aan te wijzen om deze handelingen te verrichten.

- Een certificaatbeheerder is een natuurlijke persoon die namens de abonnee handelingen uitvoert ten aanzien van het certificaat van de certificaathouder. De abonnee geeft de certificaatbeheerder opdracht de betreffende handelingen uit te voeren en legt dit vast in een bewijs van certificaatbeheer.
- Een vertrouwende partij is iedere natuurlijke of rechtspersoon die ontvanger is van een certificaat en die handelt in vertrouwen op dat certificaat. Anders dan bij persoonsgebonden certificaten ontlenen vertrouwende partijen vooral zekerheid aan de verbondenheid van een service (apparaat of functie) met de organisatorische entiteit waartoe de service behoort. De CP Extended Validation legt derhalve de nadruk op het bieden van zekerheid over de verbondenheid van een door een apparaat, systeem of functie verzonden bericht of geleverde webdienst met de betreffende organisatie. Het vaststellen van de identiteit van de certificaathouder (apparaat of functie) is in dit licht gezien minder van belang dan het vaststellen van diens verbondenheid met de organisatorische entiteit.

1.4 Certificaatgebruik

Het gebruik van certificaten uitgegeven onder deze CP heeft betrekking op communicatie van certificaathouders die handelen namens de abonnee.

[OID 2.16.528.1.1003.1.2.7] EV SSL certificaten die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het beveiligen van een verbinding tussen een bepaalde client en een server, via het TLS/SSL protocol, die behoort bij de organisatorische entiteit die als abonnee wordt genoemd in het betreffende certificaat.

1.5 Contactgegevens Policy Authority

De PA is verantwoordelijk voor deze CP. Vragen met betrekking tot deze CP kunnen worden gesteld aan de PA, waarvan het adres gevonden kan worden op: http://www.logius.nl/pkioverheid.

2 Publicatie en verantwoordelijkheid voor elektronische opslagplaats

2.1 Elektronische opslagplaats

Bevat geen aanvullende eisen.

2.2 Publicatie van CSP-informatie

RFC 3647	2.2 Publicatie van CSP-informatie
Nummer	2.2-pkio9

3 Identificatie en authenticatie

3.1 Naamgeving

Bevat geen aanvullende eisen.

3.2 Initiële identiteitsvalidatie

RFC 3647	3.2.1. Methode om bezit van de private sleutel aan te tonen
Nummer	3.2.1-pkio13

RFC 3647	3.2.2. Authenticatie van organisatorische entiteit
Nummer	3.2.2-pkio147

RFC 3647	3.2.3 Authenticatie van persoonlijke identiteit
Nummer	3.2.3-pkio27

RFC 3647	3.2.5 Autorisatie van de certificaathouder
Nummer	3.2.5-pkio30

RFC 3647	3.2.5 Autorisatie van de certificaathouder
Nummer	3.2.5-pkio33

RFC 3647	3.2.5 Autorisatie van de certificaathouder
Nummer	3.2.5-pkio35

RFC 3647	3.2.5 Autorisatie van de certificaathouder
Nummer	3.2.5-pkio146

3.3 Identificatie en authenticatie bij vernieuwing van het certificaat

Bevat geen aanvullende eisen.

4 Operationele eisen certificaatlevenscyclus

4.1 Aanvraag van certificaten

RFC 3647	4.1 Aanvraag van certificaten
Nummer	4.1-pkio48

4.4 Acceptatie van certificaten

Bevat geen aanvullende eisen.

4.5 Sleutelpaar en certificaatgebruik

RFC 3647	4.5.2 Gebruik van publieke sleutel en certificaat door vertrouwende partij
Nummer	4.5.2-pkio145

4.9 Intrekking en opschorting van certificaten

RFC 3647	4.9.3 Procedure voor een verzoek tot intrekking
Nummer	4.9.3-pkio57

RFC 3647	4.9.3 Procedure voor een verzoek tot intrekking
Nummer	4.9.3-pkio60

RFC 3647	4.9.5 Tijdsduur voor verwerking intrekkingsverzoek
Nummer	4.9.5-pkio62

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	4.9.9-pkio152

4.10 Certificaat statusservice

Bevat geen aanvullende eisen.

5 Management, operationele en fysieke beveiligingsmaatregelen

5.2 Procedurele beveiliging

Bevat geen aanvullende eisen.

5.3 Personele beveiliging

Bevat geen aanvullende eisen.

5.4 Procedures ten behoeve van beveiligingsaudits

Bevat geen aanvullende eisen.

5.5 Archivering van documenten

RFC 3647	5.5.1 Vastlegging van gebeurtenissen
Nummer	5.5.1-pkio82

5.7 Aantasting en continuïteit

Bevat geen aanvullende eisen.

6 Technische beveiliging

6.1 Genereren en installeren van sleutelparen

RFC 3647	6.1.1 Genereren van sleutelparen voor de CSP sub CA
Nummer	6.1.1-pkio87

RFC 3647	6.1.1 Genereren van sleutelparen van de certificaathouders
Nummer	6.1.1-pkio90

RFC 3647	6.1.1 Genereren van sleutelparen van de certificaathouders
Nummer	6.1.1-pkio92

6.2 Private sleutelbescherming en cryptografische module engineering beheersmaatregelen

RFC 3647	6.2.11 Eisen voor veilige middelen voor het aanmaken van elektronische handtekeningen
Nummer	6.2.11-pkio107

6.3 Andere aspecten van sleutelpaarmanagement

Bevat geen aanvullende eisen.

6.4 Activeringsgegevens

Bevat geen aanvullende eisen.

6.5 Logische toegangsbeveiliging van CSP-computers

Bevat geen aanvullende eisen.

6.6 Beheersmaatregelen technische levenscyclus

Bevat geen aanvullende eisen.

6.7 Netwerkbeveiliging

Bevat geen aanvullende eisen.

7 Certificaat-, CRL- en OCSP-profielen

7.1 Certificaatprofielen

Bevat geen aanvullende eisen.

7.2 CRL-profielen

Bevat geen aanvullende eisen.

7.3 OCSP-profielen

RFC 3647	7.3 OCSP-profielen
Nummer	7.3-pkio123

8 Conformiteitbeoordeling

Alle onderwerpen met betrekking tot de conformiteitbeoordeling van de CSP's binnen de PKI voor de overheid worden behandeld in PvE deel 2: Toetreding tot en Toezicht binnen de PKI voor de overheid.

9 Algemene en juridische bepalingen

9.2 Financiële verantwoordelijkheid en aansprakelijkheid

Bevat geen aanvullende eisen.

9.5 Intellectuele eigendomsrechten

Bevat geen aanvullende eisen.

9.6 Aansprakelijkheid

RFC 3647	9.6.1 Aansprakelijkheid van CSP's
Nummer	9.6.1-pkio128

9.8 Beperkingen van aansprakelijkheid

RFC 3647	9.8 Beperkingen van aansprakelijkheid
Nummer	9.8-pkio134

9.12 Wijzigingen

Bevat geen aanvullende eisen.

9.13 Geschillenbeslechting

Bevat geen aanvullende eisen.

9.14 Van toepassing zijnde wetgeving

Bevat geen aanvullende eisen.

9.17 Overige bepalingen

Bevat geen aanvullende eisen.

Als één of meerdere bepalingen van deze CP bij gerechtelijke uitspraak ongeldig of anderszins niet van toepassing wordt verklaard, laat dit de geldigheid en toepasselijkheid van alle overige bepalingen onverlet.

Bijlage A Profielen certificaten

Profiel van Extended Validation van het EV stamcertificaat

Criteria
Bij de beschrijving van de velden en attributen binnen een certificaat worden de volgende codes gebruikt:
V : Verplicht; geeft aan dat het attribuut verplicht is en MOET worden gebruikt in het certificaat.
: Optioneel; geeft aan dat het attribuut optioneel is en KAN worden opgenomen in het certificaat.
A : Afgeraden; geeft aan dat het attribuut afgeraden wordt maar KAN worden opgenomen in het certificaat.
Het is niet toegestaan velden te gebruiken die niet in de certificaatprofielen staan beschreven.

Bij de extensies worden velden/attributen die volgens de internationale standaarden critical zijn in de 'Critical' kolom met ja gemerkt om aan te geven dat het betreffende attribuut MOET worden gecontroleerd door middel van een proces waarmee een certificaat wordt geëvalueerd. Overige velden/attributen worden met nee gemerkt.

Extended Validation certificaten

Basisattributen

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
Version	V	MOET ingesteld worden op 2 (X.509v3).	RFC 5280	Integer	Beschrijft de versie van het certificaat, de waarde 2 staat voor X.509 versie 3.
SerialNumber	V	Een serienummer dat op unieke wijze het certificaat binnen het uitgevende CA domein MOET identificeren.	RFC 5280	Integer	Alle eindgebruiker certificaten moeten tenminste 8 bytes aan niet te voorspellen willekeurige data bevatten in het serienummer (SerialNumber) van het certificaat.
Signature	V	MOET worden ingesteld op het algoritme, zoals deze door de PA is bepaald.	RFC 5280, ETSI TS 102176	OID	MOET gelijk zijn aan het veld signatureAlgorithm. Ten behoeve van maximale interoperabiliteit worden voor certificaten uitgegeven onder deze CP alleen sha-256WithRSAEncryption toegestaan. Zie voor de sleutellengtes het PKIoverheid CPS EV certificaten.
Issuer	V	MOET een Distinguished Name (DN) bevatten. Veld heeft de onderstaande attributen:	PKIo, RFC3739, ETSI TS 102280		Andere attributen dan hieronder genoemd MOGEN NIET worden gebruikt. De attributen die worden gebruikt MOETEN gelijk zijn aan de gelijknamige attributen in het Subject veld van het CSP certificaat (ten behoeve van validatie).
Issuer.countryName	V	MOET de landcode bevatten van het land	ETSI TS101862,	Printable String	C = NL voor CSP's gevestigd in Nederland.

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
		waar de uitgevende organisatie van het certificaat is gevestigd.	X520, ISO 3166		
Issuer.OrganizationName	V	Volledige naam conform geaccepteerd document of basisregistratie.	ETSI TS 102280	UTF8String	
Issuer.organizationalUnitName	O	Optionele aanduiding van een organisatieonderdeel. Dit veld MAG NIET een functieaanduiding of dergelijke bevatten. Wel eventueel de typen certificaten die worden ondersteund.	ETSI TS 102280	UTF8String	Meerdere instanties van dit attribuut MOGEN gebruikt worden.
Issuer.serialNumber	O	MOET, conform RFC 3739, worden gebruikt indien eenduidige naamgeving dit vereist.	RFC 3739	Printable String	
Issuer.commonName	V	MOET de naam van de CA te bevatten conform geaccepteerd document of basisregistratie, MAG worden aangevuld met de Domein aanduiding en/of de typen certificaat die worden ondersteund.	PKIo, RFC 3739	UTF8String	Het commonName attribuut MAG NIET nodig zijn om de uitgevende instantie te identificeren (geen onderdeel van de Distinguished Name, eis uit RFC 3739).

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
Validity	V	MOET de geldigheidsperiode (validity) van het certificaat definiëren volgens RFC 5280.	RFC 5280	UTCTime	MOET begin- en einddatum bevatten voor geldigheid van het certificaat conform het van toepassing zijnde beleid vastgelegd in het EV CPS.
Subject	V	De attributen die worden gebruikt om het subject (service) te beschrijven MOETEN het subject op unieke wijze benoemen en gegevens bevatten over de abonnee-organisatie. Veld heeft de volgende attributen:	PKIo, RFC3739, ETSI TS 102 280		MOET een Distinguished Name (DN) bevatten. Andere attributen dan hieronder genoemd MOGEN NIET worden gebruikt.
Subject.businessCategory	V	MOET een van de volgende waarden bevatten: 2.5.4.15 = Private Organization 2.5.4.15 = Government Entity 2.5.4.15 = Business Entity 2.5.4.15 = Non-Commercial Entity	PKIo		▪ Private Organization is van toepassing op privaatrechtelijke organisaties met rechtspersoonlijkheid; ▪ Government Entity is van toepassing op organisaties binnen de overheid; ▪ Business Entity is van toepassing op privaatrechtelijke organisaties zonder rechtspersoonlijkheid. Ook formele samenwerkingsverbanden tussen bedrijven vallen onder deze categorie; ▪ Non-Commercial Entity is van toepassing bij internationale organisaties die niet behoren tot één land of regering (b.v. de NAVO (http://www.nato.int) of de Verenigde Naties (http://www.un.int)). Aan dit soort organisaties MOGEN GEEN PKIoverheid EV SSL

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
					certificaten worden uitgegeven.
Subject.countryName	V	C vullen met tweeletterige landcode conform ISO 3166-1. Indien een officiële alpha-2 code ontbreekt, MAG de CSP de user-assigned code XX gebruiken.	RFC 3739, X520, ISO 3166, PKIo	PrintableString	De landcode die wordt gehanteerd in Subject.countryName MOET in overeenstemming zijn met het adres van de abonnee volgens geaccepteerd document of registratie.
Subject.commonName	A	Naam die de server identificeert. Het gebruik van dit veld wordt afgeraden. Als dit veld wordt gebruikt MOET deze maximaal 1 "fully-qualified domain name (FQDN)" (zie de definitie in deel 4) bevatten. Deze FQDN MOET ook in het SubjectAltName.dNSName veld worden opgenomen.	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	Het is niet toegestaan in dit attribuut wildcards, private IP adressen en/of hostnames, internationalized domain names (IDN's) en null characters \0 te gebruiken.
Subject.organizationName	V	MOET de volledige naam van de organisatie van de abonnee bevatten conform geaccepteerd document (Staatsalmanak) of Basisregistratie (Handelsregister).	PKIo	UTF8String	De abonnee-organisatie is de organisatie waarmee de CSP een overeenkomst heeft gesloten en namens welke de certificaathouder (service / server) communiceert of handelt.

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
					De CSP MAG de volledige naam van de organisatie van de abonnee aanpassen als deze groter is dan 64 posities. De CSP MOET hierover in overleg treden met de abonnee. De aanpassing MOET zodanig plaatsvinden dat voorkomen wordt dat vertrouwende partijen denken met een andere organisatie te maken te hebben. Mocht een dergelijke aanpassing niet mogelijk zijn dan MAG de CSP het EV SSL certificaat NIET uitgeven.
Subject.organizationalUnitName	O/V	Optionele aanduiding van een organisatieonderdeel. Dit attribuut MAG NIET een functieaanduiding of dergelijke bevatten. Verplichte aanduiding van een overheidsorganisatie.	PKIo		Dit attribuut MAG meerdere malen voorkomen. Het veld MOET een geldige naam van een organisatieonderdeel van de abonnee bevatten conform geaccepteerd document of registratie. Alleen in die gevallen waarbij een organisatorische entiteit binnen de overheid nog niet is ingeschreven in het Handelsregister MOET de CSP in dit veld het woord “overheidsorganisatie” opnemen.
Subject.stateOrProvinceName	V	MOET de provincie van vestiging van de abonnee bevatten conform geaccepteerd document (Staatsalmanak) of Basisregistratie (Handelsregister).	PKIo, RFC 3739	UTF8String	

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
Subject.localityName	V	MOET de vestigingsplaats van de abonnee bevatten conform geaccepteerd document (Staatsalmanak) of Basisregistratie (Handelsregister).	PKIo, RFC 3739	UTF8String	.
Subject.streetAddress	O	Indien aanwezig MOET dit veld de straatnaam van de abonnee bevatten conform geaccepteerd document (Staatsalmanak) of Basisregistratie (Handelsregister).	PKIo, RFC 3739	UTF8String	
Subject.postalCode	O	Indien aanwezig MOET dit veld de postcode gerelateerd aan de straatnaam van de abonnee bevatten conform geaccepteerd document (Staatsalmanak) of Basis-registratie (Handelsregister).	PKIo, RFC 3739	UTF8String	
Subject:jurisdictionOfIncorporationCountryName	V	Vaste waarde: 1.3.6.1.4.1.311.60.2.1.3 = NL	RFC 5280, ISO 3166	OID	
Subject.postalAddress	A	Het gebruik wordt afgeraden. Indien	PKIo, RFC 3739	UTF8String	Adres MOET in overeenstemming zijn met het adres van de abonnee

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
		aanwezig MOET dit veld het postadres van de abonnee conform geaccepteerd document of Basisregistratie te bevatten.			volgens geaccepteerd document of registratie.
Subject.serialNumber	V	Het is de verantwoordelijkheid van een CSP om de uniciteit van het subject (service) te waarborgen. Het Subject.serialNumber MOET gebruikt worden om het subject uniek te identificeren.	RFC 3739, X 520, PKIo	Printable String	In dit veld MOET het KvK-nummer worden opgenomen. In die gevallen waarbij een organisatorische entiteit binnen de overheid nog niet is ingeschreven in het Handelsregister MOET de CSP zelf het nummer bepalen waarmee de uniciteit van het subject (service) wordt gewaarborgd. Tevens MOET de CSP dan in het veld Subject.organizationalUnitName het woord “overheidsorganisatie” opnemen.
subjectPublicKeyInfo	V	Bevat o.a. de publieke sleutel.	ETSI TS 102 280, RFC 3279		Bevat de publieke sleutel, identificeert het algoritme waarmee de sleutel kan worden gebruikt.

Standaard extensies

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
authorityKeyIdentifier	V	Nee	Het algoritme om de AuthorityKey te genereren MOET worden ingesteld op een algoritme zoals door de PA is bepaald.	ETSI TS 102 280, RFC 5280	BitString	De waarde MOET de SHA-1 hash van de authorityKey (publieke sleutel van de CSP CA) bevatten.
SubjectKeyIdentifier	V	Nee	Het algoritme om de subjectKey te genereren MOET worden ingesteld op een algoritme zoals door de PA is bepaald.	RFC 5280	BitString	De waarde MOET de SHA-1 hash van de subjectKey (publieke sleutel van de certificaathouder) bevatten.
KeyUsage	V	Ja	In EV subordinate CA certificaten die onder een EV CSP CA certificaat worden uitgegeven MOET het keyCertSign en cRLSign zijn opgenomen en zijn aangemerkt als essentieel. Een ander keyUsage MAG hiermee NIET worden gecombineerd. In EV SSL certificaten MOETEN de digitalSignature en keyEncipherment bits zijn opgenomen en zijn aangemerkt als essentieel. Een ander keyUsage MAG	RFC 3739, RFC 5280, ETSI TS 102 280	BitString	

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
			hiermee NIET worden gecombineerd.			
CertificatePolicies	V	Nee	MOET de OID bevatten van de voorliggende EV certificate policy (CP) en de EV OID van het CA/B forum. policyIdentifier ▪ EV policy identifier policyQualifiers:policyQualifierId ▪ id-qt 1 [RFC 5280] In EV subordinate CA certificaten die onder een EV CSP CA certificaat worden uitgegeven MOET de HTTP URL van het EV Certification Practice Statement van de PA van PKIoverheid worden opgenomen. policyQualifiers:qualifier:cPSuri ▪ HTTP URL van het Certification Practice Statement van de PA van PKIoverheid In EV SSL certificaten MOET de HTTP URL	RFC 3739 RFC 5280	OID, String, String	De volgende OID's zijn van toepassing: • 2.16.528.1.1003.1.2.7 en • 2.23.140.1.1 Dit OID MOET worden opgenomen in EV SSL certificaten én in EV subordinate CA certificaten die onder een EV CSP CA certificaat worden uitgegeven. De HTTP URL van het EV Certification Practice Statement van de PA van PKIoverheid is: http://www.logius.nl/producten/toegang/pkioverheid/documentatie/cps/

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
			van het certification practice statement (CPS) van de CSP worden opgenomen policyQualifiers:qualifier:cPSuri ▪ HTTP URL van het Certification Practice Statement van de CSP In EV SSL certificaten MOET een gebruikersnotitie worden opgenomen.			
SubjectAltName	V	Nee	MOET worden gebruikt en voorzien zijn van een wereldwijd uniek nummer dat de service identificeert.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		MOET een unieke identifier bevatten in het othername attribuut. Andere attributen dan hieronder genoemd MOGEN NIET worden gebruikt.
SubjectAltName.dNSName	V		Naam die de server identificeert. Dit veld MOET minimaal 1 "fully-qualified domain name (FQDN)" (zie de definitie in deel 4) bevatten. In dit veld MOGEN meerdere FQDN’s	RFC2818, RFC5280	IA5String	Het is niet toegestaan in dit attribuut wildcards, private IP adressen en/of hostnames, internationalized domain names (IDN’s) en null characters \0 te gebruiken.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
			worden gebruikt. Deze FQDN's MOETEN uit dezelfde domeinnaam range komen. (b.v. www.logius.nl, applicatie.logius.nl, secure.logius.nl etc. etc.).			
SubjectAltName.rfc822Name	A		MAG worden gebruikt voor een e-mail adres van de service, ten behoeve van applicaties die het e-mail adres nodig hebben om goed te functioneren.	RFC 5280	IA5String	Voor EV SSL certificaten wordt het gebruik van e-mail adressen afgeraden, omdat e-mail adressen van certificaathouders vaak wisselen en gevoelig zijn voor spam.
BasicConstraints	V	Ja	In EV SSL certificaten MOET het "CA" veld op "FALSE" staan of worden weggelaten (default waarde is dan "FALSE"). In EV subordinate CA certificaten die onder een EV CSP CA certificaat worden uitgegeven MOET het "CA" veld op "TRUE" staan. Het veld pathLenConstraint MAG aanwezig zijn.	RFC 5280		In een (Nederlandstalige) browser zal dan bij EV SSL certificaten te zien zijn: "Subjecttype = Eindentiteit", "Beperking voor padlengte = Geen". Bij EV subordinate CA certificaten die onder een EV CSP CA certificaat worden uitgegeven zal te zien zijn: "Subjecttype = CA", "Beperking voor padlengte = Geen".
CRLDistributionPoints	V	Nee	MOET de HTTP URL van een CRL distributie-	RFC 5280, ETSI		

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
			punt bevatten.	TS 102 280		
ExtKeyUsage	V	Nee	In EV SSL certificaten MOETEN de attributen id-kp-serverAuth (Verificatie van de server) en id-kp-clientAuth (Clientverificatie) zijn opgenomen. De waarde id-kp-emailProtection MAG hiermee worden gecombineerd. Andere extKeyUsage MOGEN hiermee NIET worden gecombineerd.	RFC 5280	KeyPurposeId's	
FreshestCRL	O	Nee	MOET de URI van een Delta-CRL distributiepunt bevatten, indien gebruik wordt gemaakt van Delta-CRL's.	RFC 5280, PKIo		Delta-CRL's zijn een optionele uitbreiding. Om aan de eisen van PKIoverheid te voldoen MOET een CSP tevens volledige CRL's publiceren met de geëiste uitgiftefrequentie.

Private extensies

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
authorityInfoAccess	V	Nee	Dit attribuut MOET de HTTP URL van een OCSP responder bevatten als Online Certificate Status Protocol (OCSP).			In het issuing EV CA certificaat (EV CSP CA of EV subordinate CA certificaat) MAG daarnaast ook de HTTP URL van de Staat der Nederlanden EV Root CA certificaat worden opgenomen. In het EV SSL certificaat MAG daarnaast ook de HTTP URL van het issuing EV CA certificaat (EV CSP CA of EV subordinate CA certificaat) worden opgenomen.
SubjectInfoAccess	O	Nee		RFC 5280	OID, General-name	Dit veld kan gebruikt worden om te verwijzen naar aanvullende informatie over het subject.

10 Revisies

10.1 Wijzigingen van versie 4.1 naar 4.2

10.1.1 Nieuw

- Eis 4.9.9-pkio152 (Uiterlijke ingangsdatum 01-07-2016)

10.1.2 Aanpassingen

- Toevoeging van OID aan CertificatePolicies (uiterlijke ingangsdatum 1 april 2016)

10.1.3 Redactioneel

Niet van toepassing

10.2 Wijzigingen van versie 4.0 naar 4.1

10.2.1 Nieuw

- Eis 3.2.5-pkio146 (Uiterlijke ingangsdatum 31-12-2015)

10.2.2 Aanpassingen

- Eis 3.2.5-pkio35
- De volgende eisen zijn komen te vervallen:
  - Eis 3.2.0-pkio12;
  - Eis 3.2.2-pkio15 (samengevoegd op 27-8-2015 met eis 3.2.3-pkio23 onder nieuwe eis 3.2.2-pkio147);
  - Eis 3.2.2-pkio17;
  - Eis 3.2.2-pkio18;
  - Eis 3.2.2-pkio19;
  - Eis 3.2.2-pkio20;
  - Eis 3.2.3-pkio23 (samengevoegd op 27-8-2015 met eis 3.2.3-pkio23 onder nieuwe eis 3.2.2-pkio147);
  - Eis 3.2.3-pkio25;
  - Eis 3.2.3-pkio28;
  - Eis 4.4.1-pkio50;
  - Eis 4.9.3-pkio59;
  - Eis 9.6.1-pkio130.
- Verbod op gebruik SubjectAltName.otherName (uiterlijke ingangsdatum 4 weken na publicatie PvE 4.1)

10.2.3 Redactioneel

- Kleine redactionele wijzigingen aan de volgende eisen:
  - Eis 3.2.3-pkio27.

10.3 Wijzigingen van versie 3.7 naar 4.0

10.3.1 Nieuw

- Eis 2.2-pkio9
- Eis 4.5.2-pkio145
- Eis 5.2.4-pkio77

10.3.2 Aanpassingen

- PvE eisen zijn omgenummerd volgens een nieuwe naming convention;
- De creatie van een baseline en een aanvullende eisen document;

- Inhoudelijke wijzigingen aan eisen zijn terug te vinden in de baseline en het aanvullende eisen document.

10.3.3 Redactioneel

Redactionele wijzigingen aan eisen zijn terug te vinden in de baseline en het aanvullende eisen document. Deze hebben echter geen gevolgen voor de inhoud van de informatie.