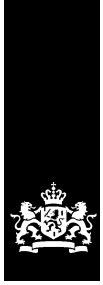

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programma van Eisen deel 3e: Certificate Policy server certificaten - Domein Organisatie Services (g3)

bijlage bij CP Domeinen Overheid/Bedrijven (g1) en Organisatie (g2)

Datum 18 januari 2016

Domein Overheid / Bedrijven (g1):
Services - Server 2.16.528.1.1003.1.2.2.6

Domein Organisatie (g2) / Organisatie Services (g3):
Services - Server 2.16.528.1.1003.1.2.5.6

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	09-11-2005	Vastgesteld door BZK november 2005
1.1	25-01-2008	Vastgesteld door BZK januari 2008
1.2	13-01-2009	Vastgesteld door BZK januari 2009
2.0	09-10-2009	Vastgesteld door BZK oktober 2009
2.1	11-01-2010	Vastgesteld door BZK januari 2010
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	Vastegesteld door BZK 2012
3.5	06-07-2013	Vastgesteld door BZK juli 2013
3.6	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
4.2	01-2016	Vastgesteld door BZK januari 2016

1 Introductie op de Certificate Policy

1.1 Achtergrond

Dit is deel 3e van het Programma van Eisen (PvE) van de PKI voor de overheid en wordt aangeduid als Certificate Policy (CP). 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. Binnen de PKI voor de overheid is onderscheid gemaakt tussen verschillende domeinen. Dit document heeft uitsluitend betrekking op de server certificaten uitgegeven door CSP's in het domein Overheid/Bedrijven en Organisatie.

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 waarbij
  - voor server certificaten (extendedKeyUsage client en server authentication) policies NCP in combinatie met OVCP, PTC-BR en Netsec van toepassing zijn. **Voor Netsec geldt dat eisen 1h, 3a, 3e, 4c.i en 4f niet normatief zijn** (ETSI CP OID 0.4.0.2042.1.7);
- die specifiek door en voor de PKIoverheid 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.

[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.

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 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 services certificaten opgenomen. De certificaat statusinformatie is in de basiseisen opgenomen.

1.1.2 Status

Dit is versie 4.2 van deel 3e 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

Binnen de PKI voor de overheid is er sprake van een structuur gebaseerd op het SHA-1 algoritme (G1) en op het SHA-256 algoritme (G2 en G3). Verder is er onder de stamcertificaten, een indeling gemaakt in verschillende domeinen.

Voor de G1 root is sprake van de domeinen Overheid/Bedrijven (deze twee domeinen zijn in de loop van de tijd samengevoegd) en Burger.
Voor de G2 root is er sprake van een domein Organisatie, een domein Burger en een domein Autonome Apparaten.
Voor de G3 root is sprake van een domein Organisatie Persoon, een domein Organisatie Services, een domein Burger en een domein Autonome Apparaten.

Elke CP wordt uniek geïdentificeerd door een OID, conform het onderstaande schema.

Domein Overheid / Bedrijven:	
OID	**CP**
2.16.528.1.1003.1.2.2.6	voor het servercertificaat binnen het domein Overheid/Bedrijven, dat de publieke sleutel bevat ten behoeve van authenticiteit & vertrouwelijkheid.

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). domein overheid en bedrijven (2). server (6). versienummer}.

Domein Organisatie / Organisatie Services:	
OID	**CP**
2.16.528.1.1003.1.2.5.6	voor het servercertificaat binnen het domein Organisatie, dat de publieke sleutel bevat ten behoeve van authenticiteit & vertrouwelijkheid.

De OID is als volgt opgebouwd: {joint-iso-itu-t (2). country (16). nederland (528). Nederlandse or-
ganisatie (1). nederlandse-overheid (1003). pki voor de overheid (1). cp (2). domein organisatie
(5). server (6). versienummer}.

Als eisen slechts voor één of twee typen certificaten van toepassing zijn, dan is dat nadrukkelijk aangegeven door de Object Identifier (OID) te vermelden van de van toepassing zijnde CP of CP's.

1.3 Gebruikersgemeenschap

Binnen de domeinen Overheid/Bedrijven en Organisatie bestaat de gebruikersgemeenschap uit abonnees, die organisatorische entiteiten binnen overheid en bedrijfsleven zijn (zie PKIo 3.2.2-pkio4) 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 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 Services 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; of
  - een functie van 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 Services 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 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6]
Servercertificaten die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het beveiligen van een verbinding tussen een bepaalde client en een server 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

Bevat geen aanvullende eisen.

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-pkio4

RFC 3647	3.2.2 Authenticatie van organisatorische entiteit
Nummer	3.2.2-pkio144

RFC 3647	3.2.3 Authenticatie van persoonlijke identiteit
Nummer	3.2.3-pkio22

RFC 3647	3.2.3 Authenticatie van persoonlijke identiteit
Nummer	3.2.3-pkio24

RFC 3647	3.2.3 Authenticatie van persoonlijke identiteit
Nummer	3.2.3-pkio26

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-pkio146

3.3 Identificatie en authenticatie bij vernieuwing van het certificaat

Bevat geen aanvullende eisen.

4 Operationele eisen certificaatlevenscyclus

4.1 Aanvraag van certificaten

Bevat geen aanvullende eisen.

4.4 Acceptatie van certificaten

Bevat geen aanvullende eisen.

4.5 Sleutelpaar en certificaatgebruik

Bevat geen aanvullende eisen.

4.9 Intrekking en opschorting van certificaten

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	4.9.9-pkio70

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 van de certificaathouders
Nummer	6.1.1-pkio89

RFC 3647	6.1.1 Genereren van sleutelparen van de certificaathouders
Nummer	6.1.1-pkio91

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

RFC 3647	6.1.2 Overdracht van private sleutel en SUD aan certificaathouder
Nummer	6.1.2-pkio95

6.2 Private sleutelbescherming en cryptografische module engineering beheersmaatregelen

RFC 3647	6.2.11 Eisen voor veilige middelen voor het aanmaken van elektronische hand-tekeningen
Nummer	6.2.11-pkio125

RFC 3647	6.2.11 Eisen voor veilige middelen voor het aanmaken van elektronische hand-tekeningen
Nummer	6.2.11-pkio105

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

6.3 Andere aspecten van sleutelpaarmanagement

Bevat geen aanvullende eisen.

6.4 Activeringsgegevens

RFC 3647	6.4.1 Genereren en installeren van activeringsgegevens
Nummer	6.4.1-pkio112

RFC 3647	6.4.1 Genereren en installeren van activeringsgegevens
Nummer	6.4.1-pkio113

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

Bevat geen aanvullende eisen.

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

RFC 3647	9.2.1 Verzekeringsdekking
Nummer	9.2-pkio124

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

RFC 3647	9.6.1 Aansprakelijkheid van CSP's
Nummer	9.6.1-pkio132

9.8 Beperkingen van aansprakelijkheid

RFC 3647	9.8 Beperkingen van aansprakelijkheid
Nummer	9.8-pkio133

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

RFC 3647	9.17 Overige bepalingen
Nummer	9.17-pkio140

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 server certificaten voor het domein Overheid/Bedrijven, Organisatie en Organisatie Services

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.
- O : 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.

Server 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 wordt voor certificaten onder het G1 stamcertificaat alleen sha-1WithRSAEncryption toegestaan. Vanaf 01-01-2011 MAG de CSP alleen in zeer uitzonderlijke situaties nog een certificaat op basis van sha-1WithRSAEncryption onder het G1 stamcertificaat uitgeven. Dit certificaat MOET een 2048 bit RSA sleutel bevatten. Dit certificaat MAG maar maximaal geldig zijn tot en met 31-12-2011. Voor certificaten onder het G2 stamcertificaat wordt alleen sha-256WithRSAEncryption toegestaan.

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
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 waar de uitgevende organisatie van het certificaat is gevestigd.	ETSI TS101862, X520, ISO 3166	Printable String	C = NL voor CSP's gevestigd in Nederland.
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	

Veld / Attribuut	Criteria	Beschrijving	Norm refe-rentie	Type	Toelichting
Issuer.commonName	V	MOET de naam van de CA 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).
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 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.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.

Veld / Attribuut	Criteria	Beschrijving	Norm refe-rentie	Type	Toelichting
Subject.commonName	A	Naam die de server identificeert. Bij server certificaten wordt het gebruik van dit veld 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 zijn opgenomen.	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	Indien de subject.commonname wordt gebruikt voor server certificaten, dient hier een FQDN te worden opgenomen. Het is niet toegestaan in dit attribuut wildcard FQDN's, locale domeinnamen, private IP adressen, alleen een hostname, internationalized domain names (IDN's) en null characters \0 te gebruiken. De abonnee MOET aantonen dat de organisatie deze naam mag voeren. Bij server certificaten MOET de CSP bij erkende registers (Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA)) controleren of de abonnee de eigenaar is van de domeinnaam of dat de abonnee exclusief geautoriseerd is door de geregistreerde domeinnaam eigenaar om, namens de geregistreerde domeinnaam eigenaar, de domeinnaam te gebruiken. De CSP MAG in uitzonderlijke situaties nog een server certificaat uitgeven zonder FQDN. Hierbij gelden de volgende aanvullende eisen: met ingang van 1 juli 2012 MOET de CSP de abonnee informeren dat het gebruik van server certificaten zonder FQDN wordt afgeraden en dat uiterlijk met ingang van 1 oktober 2016 alle nog geldige server certificaten zonder

Veld / Attribuut	Criteria	Beschrijving	Norm refe-rentie	Type	Toelichting
					FQDN zullen worden ingetrokken. In het geval een CSP op of na 1 juli 2012 een server certificaat uitgeeft zonder FQDN dan MOET als "datum geldigheid tot", uiterlijk 1 november 2015 worden aangehouden. Voor de uitgifte van een server certificaat zonder FQDN moet door de CSP een registratie worden bijgehouden die maandelijks aan de PA wordt overhandigd. De non-FQDN mag geen nieuwe generieke Top Level Domains (gTLD's) bevatten die door ICANN in overweging zijn genomen (https://gtldresult.icann.org/application-result/applicationstatus/viewstatus). Na goedkeuring van een nieuwe gTLD worden door de CSP binnen 120 dagen alle certificaten ingetrokken die reeds een non-FQDN bevatten waar de gTLD een onderdeel van uitmaakt, tenzij de Abonnee de eigenaar is van de domeinnaam of door de eigenaar exclusief geautoriseerd de domeinnaam te gebruiken. Goedkeuring van nieuwe gTLD's wordt bekend gemaakt via de ICANN mailing lijst op https://mm.icann.org/mailman/listinfo/gtldnotification.
Subject.organizationName	V	Volledige naam van de organisatie van de	PKIo	UTF8String	De abonnee-organisatie is de organisatie waarmee de CSP een

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
		abonnee conform geaccepteerd document of Basisregistratie.			overeenkomst heeft gesloten en namens welke de certificaathouder (server) communiceert of handelt.
Subject.organizationalUnitName	O	Optionele aanduiding van een organisatieonderdeel. Dit attribuut MAG NIET een functieaanduiding of dergelijke bevatten.	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.
Subject.stateOrProvinceName	V	MOET de provincie van de vestiging van de abonnee bevatten conform geaccepteerd document of Basisregistratie.	PKIo, RFC 3739	UTF8String	Naam van de provincie MOET in overeenstemming zijn met het adres van de abonnee volgens geaccepteerd document of registratie.
Subject.localityName	V	MOET de vestigingsplaats van de abonnee bevatten conform geaccepteerd document of Basisregistratie.	PKIo, RFC 3739	UTF8String	Naam van de vestigingsplaats MOET in overeenstemming zijn met het adres van de abonnee volgens geaccepteerd document of registratie.
Subject.postalAddress	A	Het gebruik wordt afgeraden. Indien aanwezig MOET dit veld het postadres van de abonnee conform geaccepteerd document of Basisregistratie te bevatten.	PKIo, RFC 3739	UTF8String	Adres MOET in overeenstemming zijn met het adres van de abonnee volgens geaccepteerd document of registratie.

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
Subject.serialNumber	O	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. Het gebruik van 20 posities is uitsluitend toegestaan voor OIN en HRN na aanvullende afspraken met Logius.	RFC 3739, X 520, PKIo	Printable String	Het nummer wordt door de CSP en/of de overheid bepaald. Het nummer kan per domein verschillen en voor meerdere toepassingen gebruikt worden.
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	Dit attribuut extensie specificeert het beoogde doel van de in het certificaat opgenomen sleutel. In de PKI voor de overheid zijn per certificaatsoort verschillende bits opgenomen in the keyUsage extensie. In servercertificaten MOETEN het digitalSignature, keyEncipherment en de keyAgreement bits zijn opgenomen en zijn aangemerkt als essentieel. Een ander keyUsage MAG hiermee NIET worden	RFC 3739, RFC 5280, ETSI TS 102 280	BitString	

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
			gecombineerd.			
CertificatePolicies	V	Nee	MOET de OID bevatten van de certificate policy (CP), de OV OID van het CA/B Forum, de URI van het certification practice statement (CPS), en een gebruikersnotitie. Het te gebruiken OID schema in de PKI voor de overheid wordt beschreven in de CP.	RFC 3739	OID, String, String	Voor server certificaten in domein Overheid/Bedrijven zijn de OID's: 2.16.528.1.1003.1.2.2.6. Voor server certificaten in het domein Organisatie en Organisatie Services zijn de OID's: 2.16.528.1.1003.1.2.5.6 De verplichte CA/B Forum OV OID is: 2.23.140.1.2.2 Verwijzen naar paragraafnummers van het PvE / CP in de gebruikersnotitie wordt afgeraden omdat persistentie hiervan niet kan worden gegarandeerd (in tegenstelling tot het OID nummer van de CP).
SubjectAltName	V	Nee	MOET worden gebruikt en voorzien zijn van een wereldwijd uniek nummer dat de server identificeert.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		MOET een unieke identifier bevatten in het het dnsName voor server certifcaten. Andere attributen dan hieronder genoemd MOGEN NIET worden gebruikt.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
SubjectAltName.dNSName[3]	V		Naam die de server identificeert. Bij server certificaten MOET dit veld minimaal 1 "fully-qualified domain name (FQDN)" (zie de definitie in deel 4) bevatten. Een server certificaat mag meerdere FQDN's bevatten van verschillende domeinen op voorwaarde dat deze domeinen geregistreerd zijn op naam van dezelfde abonnee of een machtiging van dezelfde abonnee afkomstig is. Het is dus NIET toegestaan FQDN's in één certificaat te combineren die én afkomstig zijn uit verschillende domeinen én geregistreerd staan op naam van verschillende eigenaren.	RFC2818, RFC5280	IA5String	De abonnee MOET aantonen dat de organisatie deze naam mag voeren. Bij server certificaten is het niet toegestaan in dit attribuut wildcard FQDN's, locale domeinnamen, private IP adressen, alleen een hostname, internationalized domain names (IDN's) en null characters \0 te gebruiken. Bij server certificaten MOET de CSP bij erkende registers (Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA)) controleren of de abonnee de eigenaar is van de domeinnaam of dat de abonnee exclusief geautoriseerd is door de geregistreerde domeinnaam eigenaar om, namens de geregistreerde domeinnaam eigenaar, de domeinnaam te gebruiken. De CSP MAG in uitzonderlijke situaties nog een server certificaat uitgeven zonder FQDN. Hierbij gelden de volgende aanvullende eisen: met ingang van 1 juli 2012 MOET de CSP de abonnee

[3] Dit veld/attribuut moet uiterlijk zijn opgenomen in certificaten die vanaf 1-7-2011 worden uitgegeven.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
						informeren dat het gebruik van server certificaten zonder FQDN wordt afgeraden en dat uiterlijk met ingang van 1 oktober 2016 alle nog geldige server certificaten zonder FQDN zullen worden ingetrokken. In het geval een CSP op of na 1 juli 2012 een server certificaat uitgeeft zonder FQDN dan MOET als "datum geldigheid tot", uiterlijk 1 november 2015 worden aangehouden. Voor de uitgifte van een server certificaat zonder FQDN moet door de CSP een registratie worden bijgehouden die maandelijks aan de PA wordt overhandigd. De non-FQDN mag geen nieuwe generieke Top Level Domains (gTLD's) bevatten die door ICANN in overweging zijn genomen (https://gtldresult.icann.org/application-result/applicationstatus/viewstatus). Na goedkeuring van een nieuwe gTLD worden door de CSP binnen 120 dagen alle certificaten ingetrokken die reeds een non-FQDN bevatten waar de gTLD een onderdeel van uitmaakt, tenzij de Abonnee de eigenaar is van de domeinnaam of door de eigenaar exclusief geautoriseerd de domeinnaam te gebruiken. Goedkeuring van nieuwe gTLD's wordt bekend gemaakt via de ICANN mailing lijst op https://mm.icann.org/mailman/listinfo/gtldnotification.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
SubjectAltName.iPAddress	A	Nee	MAG het publieke IP adres van de server bevatten waarvan de abonnee de eigenaar is of die in opdracht van de abonnee, wordt gehost door een leverancier.	RFC 5280, RFC 791, RFC 2460	Octet string	De CSP MOET verifiëren dat de abonnee de eigenaar is van het publieke IP adres of dat een leverancier het publieke IP adres mag gebruiken in opdracht van de abonnee. Het is niet toegestaan in dit attribuut private IP adressen op te nemen.
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 PKIoverheid certificaten wordt het gebruik van e-mail adressen afgeraden, omdat e-mail adressen van certificaathouders vaak wisselen en gevoelig zijn voor spam.
BasicConstraints	O	Ja	Het "CA" veld MOET op "FALSE" staan of worden weggelaten (default waarde is dan "FALSE").	RFC 5280		In een (Nederlandstalige) browser zal dan te zien zijn: "Subjecttype = Eindentiteit", "Beperking voor padlengte = Geen".
CRLDistributionPoints	V	Nee	MOET de URI van een CRL distributiepunt bevatten.	RFC 5280, ETSI TS 102 280		De aanwezige referentie MOET via http of ldap protocol toegankelijk zijn. Het attribuut Reason MAG NIET worden gebruikt, er MOET naar 1 CRL worden verwezen voor alle soorten intrek-

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
						kingsredenen. Naast CRL MOGEN ook andere vormen van certificaatstatus informatiediensten worden ondersteund.
ExtKeyUsage	V	Ja	Extensie die aangeeft voor welke toepassingen het certificaat kan worden gebruikt.	RFC 5280	KeyPurposeId's	Bij server certificaten MOET deze extensie worden opgenomen, MAG deze extensie NIET als "critical" worden gemerkt, MOET deze extensie de KeyPurposId's id-kp-serverAuth en id-kp-clientAuth bevatten, MAG aanvullend de KeyPurposeId id-kp-emailProtection worden opgenomen, MAG eveneens aanvullend elke andere, in een open of geaccepteerde standaard gedefinieerde KeyPurposeId die bedoeld is voor het identificeren van een service op basis van zijn FQDN worden opgenomen en MOGEN andere KeyPurposeId's NIET worden opgenomen.
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 URI van een OCSP responder bevatten als Online Certificate Status Protocol (OCSP) een rol speelt.			Dit veld kan verder optioneel gebruikt worden om te verwijzen naar andere aanvullende informatie over de CSP.
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

Niet van toepassing

10.2.3 Redactioneel

Niet van toepassing

10.3 Wijzigingen van versie 3.7 naar 4.0

10.3.1 Nieuw

- Geen wijzigingen

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;
- Criteria en toelichting bij SubjectAltName.otherName

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.