Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programma van Eisen deel 3g: Certificate Policy Authenticiteit en Vertrouwelijkheid-certificaten – Domein Private Services

Datum 18 januari 2016

Domein Private services (g1):

Services - Authenticiteit	2.16.528.1.1003.1.2.8.4
Services - Vertrouwelijkheid	2.16.528.1.1003.1.2.8.5

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**
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 3g 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 stamcertificaten en daaronder ressorterende domeinen. Dit document heeft uitsluitend betrekking op services authenticiteit- en vertrouwelijkheidcertificaten uitgegeven door CSP's in het domein private services onder het private stamcertificaat.

Certificaten uitgegeven onder het private stamcertificaat worden niet publiekelijk vertrouwd door browsers of andere applicaties. Het toepassingsgebied van deze certificaten is primair een besloten gebruikersgroep waarbinnen afspraken zijn gemaakt over het gebruik van de private root van PKIoverheid.

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 de policy NCP+ van toepassing is, zodat gebruik wordt gemaakt van een SUD (ETSI CP OID 0.4.0.2042.1.2);
- 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

[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.

	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 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 3g 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 zijn meerdere stamcertificaten in gebruik voor de reguliere - publiekelijk vertrouwde – root, de TRIAL root de EV root en de private - niet-publiekelijk vertrouwde - root. Onder deze stamcertificaten is een hiërarchie gemaakt met domeinen. Elke hiërarchie heeft zijn eigen specifieke domeinindeling.
Daarnaast zijn van deze stamcertificaten vaak meerdere generaties of versies actief (g1, g2, g3). Tevens is er binnen de PKI voor de overheid is sprake van een structuur gebaseerd op het SHA-1 algoritme (reguliere root G1) en op het SHA-256 algoritme (reguliere root G2 en G3).

Elk certifcaattype binnen PKIoverheid wordt uniek geïdentificeerd door een OID. De OID's van de Certifcate Policies van dit deel van het Programma van Eisen zijn conform onderstaand schema:

Domein Private services:	
OID	**CP**
2.16.528.1.1003.1.2.8.4	voor het authenticiteitcertificaat voor services binnen het domeinPrivate services, dat de publieke sleutel bevat ten behoeve van identificatie en authenticatie.
2.16.528.1.1003.1.2.8.5	voor het vertrouwelijkheidcertificaat voor services binnen het domeinPrivate services, dat de publieke sleutel bevat ten behoeve van 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). private root (8). Services authenticiteit (4)/vertrouwelijkheid (5). 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 het domein Private Services 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 2.16.528.1.1003.1.2.8.4] Authenticiteitcertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het langs elektronische weg betrouwbaar identificeren en authenticeren van de service als behorende bij de organisatorische entiteit, die verantwoordelijk is voor de betreffende service. Uitgfite van code signing certificaten waarmee, door het zetten van een digitale handtekening, de integriteit en authenticiteit van programmatuur kan worden gewaarborgd, is onder deze CP NIET toegestaan.

[OID 2.16.528.1.1003.1.2.8.5] Vertrouwelijkheidcertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het beschermen van de vertrouwelijkheid van gegevens, die worden uitgewisseld en/of opgeslagen in elektronische vorm.

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-pkio8

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

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-pkio47

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	4.9.1 Omstandigheden die leiden tot intrekking
Nummer	4.9.1-pkio52

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

RFC 3647	4.9.7 CRL-uitgiftefrequentie
Nummer	4.9.7-pkio65

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	4.9.9-pkio66

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	4.9.9-pkio67

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-pkio71

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

RFC 3647	5.3.2 Antecendentenonderzoek
Nummer	5.3.2-pkio79

5.4 Procedures ten behoeve van beveiligingsaudits

RFC 3647	5.4.1 Vastlegging van gebeurtenissen
Nummer	5.4.1-pkio80

5.5 Archivering van documenten

RFC 3647	5.5.1 Vastlegging van gebeurtenissen
Nummer	5.5.1-pkio82

5.7 Aantasting en continuïteit

RFC 3647	5.7.4 Continuïteit van de bedrijfsvoering na calamiteit
Nummer	5.7.4-pkio86

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-pkio88

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-pkio92

RFC 3647	6.1.1 Genereren van sleutelparen van de certificaathouders
Nummer	6.1.1-pkio93

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	6.2.3 Escrow van private sleutels van certificaathouders
Nummer	6.2.3-pkio99

RFC 3647	6.2.3 Escrow van private sleutels van certificaathouders
Nummer	6.2.3-pkio100

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

6.3 Andere aspecten van sleutelpaarmanagement

RFC 3647	6.3.2 Gebruiksduur voor certificaten en publieke en private sleutels
Nummer	6.3.2-pkio109

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

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio150

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

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-pkio127

RFC 3647	9.6.1 Aansprakelijkheid van CSP's
Nummer	9.6.1-pkio129

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	9.8.1-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 services authenitciteit- en vertrouwelijkheidcertificaten voor het domein private 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.

Services authenticiteit- en vertrouwelijkheidcertificaten – domein private services

Basisattributen

Veld / Attribuut	Criteria	Beschrijving	Norm refe-rentie	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	Dit certificaat MOET minimaal een 2048 bit RSA sleutel bevatten.
Issuer	V	MOET een Distinguished Name (DN) bevatten. Dit veld bevat 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.

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
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 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	RFC 5280	UTCTime	MOET begin- en einddatum bevatten voor geldigheid van het certificaat conform het van toepassing zijnde beleid vastgelegd in het CPS.

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
		5280.			
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. Dit veld heeft de onderstaande 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.
Subject.commonName	V	Naam die de service identificeert. Bij services certificaten is dit veld verplicht	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	In de subject.commonname wordt de functie van een organisatorische entiteit of de naam waarmee de service, apparaat of systeem wordt aangeduid opgenomen. Dit MAG een lokcale domein naam of hostname zijn.
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 (service / 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	A	Het gebruik wordt afgeraden. Indien aanwezig MOET dit veld de provincie van vestiging van de abonnee conform geaccepteerd document of Basisregistratie bevatten.	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	A	Het gebruik wordt afgeraden. Indien aanwezig MOET dit veld de vestigingsplaats van de abonnee conform geaccepteerd document of Basisregistratie bevatten.	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	PKIo, RFC 3739	UTF8String	Adres MOET in overeenstemming zijn met het adres van de abonnee

Veld / Attribuut	Criteria	Beschrijving	Norm refe-rentie	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	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 authenticiteitcertificaten MOET het digitalSignature bit zijn opgenomen en zijn aangemerkt als essentieel. Een ander keyUsage MAG hiermee NIET worden gecombineerd.	RFC 3739, RFC 5280, ETSI TS 102 280	BitString	

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
			In vertrouwelijkheidcertificaten MOETEN keyEncipherment en dataEncipherment bits zijn opgenomen en zijn aangemerkt als essentieel. Optioneel MAG dit worden gecombineerd met het keyAgreement bit. Een ander keyUsage MAG hiermee NIET worden gecombineerd.			
CertificatePolicies	V	Nee	MOET de OID bevatten van de certificate policy (CP), 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	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 service identificeert.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		MOET een unieke identifier bevatten in het othername attribuut voor services certificaten. Andere attributen dan hieronder genoemd MOGEN NIET worden gebruikt.
SubjectAltName.dNSName	N		Naam die de server identificeert. Bij	RFC2818,	IA5String	De abonnee MOET aantonen dat de organisatie deze FQDN mag

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
			services authenticicatie en vertrouwelijkheidcertificaten wordt dit veld niet gebruikt.	RFC5280		voeren.
SubjectAltName.iPAddress	N	Nee	Het publieke IP adres die de service identificeert. Bij services certificaten MAG dit veld NIET gebruikt worden.	RFC 5280, RFC 791, RFC 2460	Octet string	
SubjectAltName.otherName	V		MOET worden gebruikt met daarin een uniek nummer dat de certificaathouder identificeert.	PKIo	IA5String, Microsoft UPN, IBM Principal-Name of Permanent-Identifier	Bevat de OID van de CSP en een nummer dat op unieke wijze blijvend het subject (service) identificeert, gescheiden door een punt of liggend streepje ('-'). Het is aan te bevelen een bestaand registratienummer uit backoffice systemen te gebruiken samen met een code voor de organisatie. In combinatie met het CSP OID-nummer is deze identifier wereldwijd uniek. Dit nummer MOET persistent zijn.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
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 intrekkingsredenen. Naast CRL MOGEN ook andere vormen van certificaatstatus informatiediensten worden ondersteund.
ExtKeyUsage	V	Nee		RFC 5280	KeyPurposeId's	Zie eis 7.1-pkio150
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	O	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 7.1-pkio150 (uiterlijke ingangsdatum 1 juli 2016)

10.1.2 Aanpassingen

- Wijziging in subjectAltname in het certificaatprofiel (uiterlijke ingangsdatum direct na publicatie PvE)

10.1.3 Redactioneel

Niet van toepassing

10.2 Wijzigingen van versie 4.0 naar 4.1

10.2.1 Nieuw

- Certificering tegen ETSI TS 102 042 (uiterlijke ingangsdatum 4 weken na publicatie PvE 4.1)

10.2.2 Aanpassingen

Niet van toepassing

10.2.3 Redactioneel

- Kleine redactionele wijzigingen aan de volgende eisen:
    - Eis 5.7.4-pkio86.