Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

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

bijlage bij CP Domein Organisatie (g2)

Datum 3 februari 2020

Colofon

Versienummer	4.8
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 Trust Service Providers (TSP's) tot de PKI voor de overheid begeleiden en voorbereiden van de afhandeling;
- het toezicht houden op en controleren van de werkzaamheden van TSP'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
4.3	07-2016	Vastgesteld door BZK juni 2016
4.4	02-2017	Vastgesteld door BZK februari 2017
4.5	07-2017	Vastgesteld door BZK juni 2017
4.6	01-2018	Vastgesteld door BZK januari 2018
4.7	02-2019	Vastgesteld door BZK februari 2019
4.8	02-2020	Vastgesteld door BZK februari 2020

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 Trust Service Providers (TSP) 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 TSP'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 EN 319 411-1 waarbij
  - voor server certificaten (extendedKeyUsage client en server authentication) policies NCP in combinatie met OVCP, PTC-BR en Netsec van toepassing zijn.
- 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.

In dit CP zijn ook een aantal bepalingen opgenomen die niet als PKIo-eis zijn geformuleerd. Deze bepalingen stellen geen eisen aan de TSP'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 services certificaten opgenomen. De certificaat statusinformatie is in de basiseisen opgenomen.

1.1.2 Status

Dit is versie 4.8 van deel 3e van het PvE. De huidige versie is bijgewerkt tot en met 3 februari 2020.

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-256 algoritme (G2 en G3). Verder is er onder de stamcertificaten, een indeling gemaakt in verschillende domeinen.

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 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. Onder genoemd OID kunnen ook OCSP responder certificaten worden uitgegeven voor gebruik binnen de context van dit CP deel.

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 TSP 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 2.16.528.1.1003.1.2.5.6] 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. Certificaten uitgegeven met deze OID zijn conform de dan geldende versie van de Baseline Requirements. In het geval van discrepanties tussen dit PvE en de Baseline Requirements gaat de laatstgenoemde boven dit document.

Onder genoemd OID kunnen ook OCSP responder certificaten worden uitgegeven, alleen voor gebruik binnen het domein Organisatie Organisatie Services Server (G3). Genoemde certificaten kunnen worden gebruikt voor het tekenen van OCSP responses ter behoeve van verificatie van de geldigheid van een eindgebruikerscertificaat. Meer informatie is te vinden in bijlage A van de basiseisen.

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 TSP-informatie

RFC 3647	2.2 Publicatie van TSP-informatie
Nummer	2.2-pkio3

RFC 3647	2.2 Publicatie van TSP-informatie
Nummer	2.2-pkio156

RFC 3647	2.2 Publicatie van TSP-informatie
Nummer	2.2-pkio166

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	3.2.2 Authenticatie van organisatorische entiteit
Nummer	3.2.2-pkio186

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

RFC 3647	3.2.5 Autorisatie van certificaathouder
Nummer	3.2.5-pkio170

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.

4.2 Verwerking van certificaat aanvraag

RFC 3647	4.2 Verwerking van certificaat aanvraag
Nummer	4.2-pkio179

4.3 Uitgifte van certificaten

4.4 Acceptatie van certificaten

Bevat geen aanvullende eisen.

4.5 Sleutelpaar en certificaatgebruik

Bevat geen aanvullende eisen.

4.8 Compliance, audit en assessement

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-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-pkio125

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

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

RFC 3647	6.3.2 Gebruiksduur voor certificaten en publieke en private sleutels
Nummer	6.3.2-pkio178

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 TSP-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-pkio163

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio171

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio172

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio173

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio182

7.2 CRL-profielen

Bevat geen aanvullende eisen.

7.3 OCSP-profielen

Bevat geen aanvullende eisen.

8 Conformiteitbeoordeling

RFC 3647	8.1 Aantonen conformiteit ETSI/BR
Nummer	8.1-pkio183

RFC 3647	8.6 Aantonen conformiteit BR
Nummer	8.6-pkio158

Onderwerpen met betrekking tot de conformiteitbeoordeling van de TSP's binnen de PKI voor de overheid worden behandeld in PvE deel 2 en de Basiseisen.

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 TSP's
Nummer	9.6.1-pkio128

RFC 3647	9.6.1 Aansprakelijkheid van TSP'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.

RFC 3647	9.17 Overige bepalingen
Nummer	9.17-pkio180

Bijlage A Profielen certificaten

Profiel van server certificaten voor het domein 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 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	Zie eis 7.1-pkio171	RFC 5280, ETSI TS 119 312	OID	
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.
Issuer.countryName	V	zie eis 7.1-pkio174	ETSI TS101862, X520, ISO 3166	Printable String	

Veld / Attribuut	Criteria	Beschrijving	Norm refe-rentie	Type	Toelichting
Issuer.OrganizationName	V	zie eis 7.1-pkio174	ETSI TS 102280	UTF8String	
Issuer. organizationalUnitName	O	zie eis 7.1-pkio174	ETSI TS 102280	UTF8String	
Issuer.serialNumber	O	zie eis 7.1-pkio174	RFC 3739	Printable String	
Issuer.commonName	V	zie eis 7.1-pkio174	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).
Issuer.organizationIdentifier	V/N	In het organizationIdentifier veld wordt een identificatie van de uitgevende CA opgenomen. Dit veld is MOET worden opgenomen wanneer het veld subject.organizationIdentifier voorkomt in het TSP certificaat en MAG NIET worden opgenomen wanneer dit veld in het betreffende TSP certificaat niet voorkomt.	EN 319 412-1	String	De opmaak van de identificatiestring wordt gespecificeerd in paragraaf 5.1.4 van ETSI EN 319 412-1 en bevat: • 3 character legal person identity type reference; • 2 character ISO 3166 [2] country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier (according to country and identity type reference).

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 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 TSP 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.	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	Zie eis 7.1-pkio163 voor eisen aan de inhoud van dit veld Zie eis 3.2.5-pkio170 voor eisen validatie van de opgenomen gegevens in dit veld

Veld / Attribuut	Criteria	Beschrijving	Norm refe-rentie	Type	Toelichting
Subject.organizationName	V	Volledige naam van de organisatie van de abonnee conform geaccepteerd document of Basisregistratie.	PKIo	UTF8String	De abonnee-organisatie is de organisatie waarmee de TSP een overeenkomst heeft gesloten en namens welke de certificaathouder (server) communiceert of handelt.
Subject.organizationalUnitName	O	Optionele aanduiding van een organi-satieonderdeel. Dit attribuut MAG NIET een functieaanduiding of dergelijke bevat-ten.	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.serialNumber	O	Het is de verantwoordelijkheid van een TSP om de uniciteit van het subject (service) te waarborgen. Het	RFC 3739, X 520, PKIo	Printable String	Het nummer wordt door de TSP en/of de overheid bepaald. Het nummer kan per domein verschillen en voor meerdere toepassingen gebruikt worden.

Veld / Attribuut	Criteria	Beschrijving	Norm refe-rentie	Type	Toelichting
		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.			
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
SignedCertificate-TimestampList (OID 1.3.6.1.4.1.11129.2.4.2)	V	Nee	De Signed Certificate Timestamp List bevat één of meer Signed Certificate Timestamps.	RFC 6962	OCTET STRING	Zie eis 4.4.3-pkio154 voor de concrete invulling van de SignedCertificateTimestampList
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 TSP/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 en keyEncipherment zijn	RFC 3739, RFC 5280, ETSI TS 102 280	BitString	

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
			opgenomen en zijn aangemerkt als essentieel. Een ander keyUsage MAG hiermee NIET worden 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. Voor de gebruikersnotitie ZAL de TSP gebruik maken van UTF8String maar MAG er ook gebruik gemaakt worden van IA5String.	RFC 3739	OID, String, UTF8String of IA5String	Zie eis 7.1-pkio182 voor eisen aan de inhoud van dit veld
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.
SubjectAltName.dNSName	V		Naam die de server identificeert.	RFC2818, RFC5280	IA5String	Zie eis 7.1-pkio163 voor eisen aan de inhoud van dit veld

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
						Zie eis 3.2.5-pkio170 voor eisen validatie van de opgenomen gegevens in dit veld
SubjectAltName.iPAddress	A	Nee	Bevat een publiek IP-adres	RFC 5280, RFC 791, RFC 2460	Octet string	Zie eis 7.1-pkio163 voor eisen aan de inhoud van dit veld Zie eis 3.2.5-pkio170 voor eisen validatie van de opgenomen gegevens in dit veld
BasicConstraints	O	Ja	Het "CA" veld MOET 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	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 en MOET deze extensie de KeyPurposId's id-kp-serverAuth en id-kp-clientAuth bevatten.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
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 TSP tevens volledige CRL's publiceren met de geëiste uitgiftefrequentie.

Private extensies

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
authorityInfoAccess	V	Nee	Zie eis 7.1-pkio172			
SubjectInfoAccess	O	Nee		RFC 5280	OID, Generalname	Dit veld kan gebruikt worden om te verwijzen naar aanvullende informatie over het subject.

10 Revisies

10.1 Wijzigingen van versie 4.7 naar 4.8

10.1.1 Nieuw

- 6.3.2-pkio178 nwe eis geldigheid certificaten aangepast (ingangsdatum 1 november 2019)
- 4.2-pkio179 nwe eis maximale vervangingstermijn gesteld (ingangsdatum 1 november 2019)
- 9.17-pkio180 nwe eis informeren abonnees termijnen intrekking (ingangsdatum 29 augustus 2019)
- 7.1-pkio182 nwe eis CertificatePolicies tekst uit profiel naar deze eis verplaatst (ingangsdatum direct na publicatie PvE 4.8)
- 8.1-pkio183 nwe eis BR self-assesment (ingangsdatum direct na publicatie PvE 4.8)
- 3.2.2-pkio186 nwe eis omtrent het (her)valideren van organisatiegegevens (ingangsdatum direct na publicatie PvE 4.8)

10.1.2 Aanpassingen

- 2.2-pkio155 vervallen (ingangsdatum direct na publicatie PvE 4.8)
- 6.1.1-pkio91 vervallen (ingangsdatum direct na publicatie PvE 4.8)
- 7.1-pkio173 aanpassing serienummer eisen (ingangsdatum 29 augustus 2019)
- voetnoot bij subjectAltName.dNSName verwijderd (ingangsdatum direct na publicatie PvE 4.8)
- Subject.postaladdress uit profiel verwijderd (ingangsdatum direct na publicatie PvE 4.8)
- 9.17-pkio140 Vervallen (ingangsdatum direct na publicatie PvE 4.8)
- certificaatprofiel verborgen eis omtrent de opname van certificatepolicies (OID) in een end-user certificaat naar nwe eis 7.1-pkio 182 verplaatst (ingangsdatum direct na publicatie PvE 4.8)
- 7.1-pkio 182 verborgen eis omtrent de opname van certificatepolicies (OID) in een end-user certificaat uit certificaatprofiel deel 3e verplaatst naar deze eis ingangsdatum direct na publicatie PvE 4.8)

10.1.3 Redactioneel

- 3.2.5-pkio170 verwijzing (ingangsdatum direct na publicatie PvE 4.8)

10.2 Wijzigingen van versie 4.6 naar 4.7

10.2.1 Nieuw

- Eis 6.1.1-pkio90 (ingangsdatum direct na publicatie PvE 4.7)
- Eis 7.1-pkio171 (ingangsdatum direct na publicatie PvE 4.7)
- Eis 7.1-pkio171 (ingangsdatum 8 weken na publicatie PvE 4.7)
- Eis 7.1-pkio173 (ingangsdatum direct na publicatie PvE 4.7)
- Eis 7.1-pkio163 (ingangsdatum direct na publicatie PvE 4.7)
- Eis 3.2.5-pkio170 (ingangsdatum direct na publicatie PvE 4.7)

10.2.2 Aanpassingen

- Uitzonderingsbepaling voor "elk ander ExtKeyUsage behorend bij de keyusage G2" verwijderd uit het ExtKeyUsage veld in het certificaatprofiel. (ingangsdatum direct na publicatie PvE 4.7)
- Expliciet opnemen dat dat TSP aan de BRG moeten voldoen. Hoofdstuk 1.4 (ingangsdatum direct na publicatie PvE 4.7)
- Eis 4.8-pkio158 overgeheveld naar eis 8.6-pkio158 (ingangsdatum direct na publicatie PvE 4.7)
- Volledig normatief verklaren van Netsec (ingangsdatum direct na publicatie PvE 4.7)
- Beschrijving van een aantal certificaatattributen vervangen door verwijzing naar eis 7.1-pkio174 (ingangsdatum 8 weken na publicatie PvE 4.7)
- Verwijzing naar CWA 14 169 gewijzigd naar EN 419 211 voor QSCD's. Hiermee eveneens eisen gesteld aan uitgifte van QSCD's voor eisen 6.2.11-pkio105 en 6.4.1-pkio112 (ingangsdatum direct na publicatie PvE 4.7)

10.3 Wijzigingen van versie 4.5 naar 4.6

10.3.1 Nieuw

- Eis 4.8-pkio158 (uiterlijke ingangsdatum 1-9-2017, spoedchange)

10.3.2 Aanpassingen

- Verbod van opname van een e-mailadres in een server certificaat onder de velden Subject.AltName.rfc822Name en ExtKeyUsage (uiterlijke ingangsdatum 4 weken na publicatie PvE versie 4.6)

10.4 Wijzigingen van versie 4.4 naar 4.5

10.4.1 Nieuw

- Verplichting tot Engelstalig CPS (eis 2.2-pkio3, uiterlijke invoeringsdatum 1-10-2017)
- Verplichting tot jaarlijkse vernieuwing CPS (eis 2.2-pkio156, uiterlijke ingangsdatum 1-1-2017)
- Verplichting vermelding Baseline Requirements domein validatie methode (2.2-pkio155)

10.4.2 Aanpassingen

- Wijziging OID 2.16.528.1.1003.1.2.5.7 om ook OCSP responder certificaten te dekken (uiterlijke ingangsdatum 1-7-2017)
- Verplicht gebruik veld "NextUpdate" in OCSP responses (eis 4.9.9-pkio71, uiterlijke ingangsdatum 1-7-2017)

10.4.3 Redactioneel

- Enkele verwijzingen naar de term CSP omgezet naar TSP
- Aanpassing certificaatprofiel Issuer.organizationalIdentifier → Issuer.organizationidentifier.

10.5 Wijzigingen van versie 4.3 naar 4.4

10.5.1 Nieuw

- Eis 4.4.3-pkio154 toegevoegd & certificaatprofiel hierop aangepast (verplichting gebruik Certificate Transparancy, uiterlijke ingangsdatum 1-7-2017)

10.5.2 Aanpassingen

- Aanscherping gebruik optionele EKU's die conflicteren met bovenliggend TSP CA certificaat (uiterlijke ingangsdatum 1-2-2017)
- Verduidelijking aanwezigheid veld "Issuer.organizationalIdentifier" (uiterlijke ingangsdatum 1-2-2017)

10.5.3 Redactioneel

- Het veld "ExtKeyUsage" aangepast van critical naar non-critical (conflict tussen beschrijvende tekst en veldwaarde opgelost)
- Term CSP (Certificate service provider) vervangen door TSP (Trust Service Provider) n.a.v. eIDAS verordening

10.6 Wijzigingen van versie 4.2 naar 4.3

10.6.1 Nieuw

- Toevoeging Issuer.organizationalIdentifier in het certificaatprofiel (uiterlijke ingangsdatum 1-7-2016)

10.6.2 Aanpassingen

- Beschrijving bij het attribuut CertificatePolicies (uiterlijke ingangsdatum 1-7-2016)
- Verwijdering optioneel gebruik KeyAgreement bij Key Usage (uiterlijke ingangsdatum 4 weken na publicatie PvE 4.3)
- ETSI TS 102 176-1 vervangen door ETSI TS 119 312 (uiterlijke ingangsdatum 4 weken na publicatie PvE 4.3)
- Vervallen eis pkio95 i.v.m. dubbeling met ETSI EN 319 411-1
- Gebruik van waarden binnen het BasicConstraints veld niet meer toegestaan in eindgebruikerscertificaten (uiterlijke ingangsdatum 1-7-2016)
- ETSI TS 102 042 vervangen door ETSI EN 319 411-1 (uiterlijke ingangsdatum 1 juli 2016 of zoveel later als de accreditatie aan de certificerende instelling is verleend met een uiterste datum van 30 juni 2017)

10.6.3 Redactioneel

- Verwijzigingen naar G1 Root verwijderd (verlopen) en naar de G3 Root verduidelijkt.

10.7 Wijzigingen van versie 4.1 naar 4.2

10.7.1 Nieuw

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

10.7.2 Aanpassingen

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

10.7.3 Redactioneel

Niet van toepassing

10.8 Wijzigingen van versie 4.0 naar 4.1

10.8.1 Nieuw

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

10.8.2 Aanpassingen

Niet van toepassing

10.8.3 Redactioneel

Niet van toepassing

10.9 Wijzigingen van versie 3.7 naar 4.0

10.9.1 Nieuw

- Geen wijzigingen

10.9.2 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

10.9.3 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.