Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programma van Eisen deel 3i: Certificate Policy – Domein private personen

Datum 05 januari 2015

Domein Private Personen (g1):

Authenticiteit	2.16.528.1.1003.1.
Onweerlegbaarheid	2.16.528.1.1003.1.
Vertrouwelijkheid	2.16.528.1.1003.1.

Colofon

Versienummer 4.0
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

1 Introductie op de Certificate Policy

1.1 Achtergrond

Dit is deel 3i 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 stamcertificaten en daaronder ressorterende domeinen. Dit document heeft uitsluitend betrekking op de persoonsgebonden certificaten uitgegeven door CSP's in het domein private personen 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 EN 319 411-2, QCP public + SSCD (ETSI CP OID 0.4.0.1456.1.1);
- 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].

[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.

Nummer	Uniek nummer van de PKIo-eis. Per paragraaf wordt een doorlopende nummering gehanteerd voor de PKIo-eisen. In combinatie met het RFC 3647 paragraafnummer vormt dit een unieke aanduiding voor de PKIo-eis.

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

Op basis van de hoofdstukken 1 t/m 9 is in bijlage B een verwijzingsmatrix opgenomen. In de matrix is conform de RFC 3647 structuur een verwijzing opgenomen naar de van toepassing zijnde eisen binnen de PKI voor de overheid. Hierbij is een onderscheid gemaakt tussen eisen afkomstig uit de Nederlandse wetgeving, eisen uit ETSI EN 319 411-2 en de PKIo-eisen.

1.1.2 Status

Dit is versie 4.0 van deel 3a van het PvE. De huidige versie is bijgewerkt tot en met januari 2015.

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 Personen	
OID	**CP**
2.16.528.1.1003.1.2.8.1	voor het authenticiteitcertificaat binnen het domein Private Personen, dat de publieke sleutel bevat ten behoeve van identificatie en authenticatie
2.16.528.1.1003.1..8.2	voor het handtekeningcertificaat binnen het domein Private Personen, dat de publieke sleutel bevat ten behoeve van de gekwalificeerde elektronische handtekening/onweerlegbaarheid
2.16.528.1.1003.1.2.8.3	voor het vertrouwelijkheidcertificaat binnen het domein Private Personen, 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). domein private personen (8). authenticiteit (1)/onweerlegbaarheid (2)/vertrouwelijkheid (3). 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 Private Personen bestaat de gebruikersgemeenschap uit abonnees, die organisatorische entiteiten binnen overheid en bedrijfsleven zijn (zie PKIo 3.2.2-pkio14) en uit certificaathouders, die bij deze abonnees behoren. Tevens zijn er beroepsbeoefenaars die zowel abonnee als certificaathouder zijn. 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 abonnee kan tevens certificaathouder zijn.
- 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 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 ofwel onderdeel van een organisatorische entiteit waarvoor een abonnee de

contracterende partij is (organisatiegebonden certificaathouder), ofwel de beoefenaar van een erkend beroep en in die hoedanigheid zelf een abonnee en daarmee de contracterende partij (beroepsgebonden certificaathouder).Een vertrouwende partij is iedere natuurlijke of rechtspersoon die ontvanger is van een certificaat en die handelt in vertrouwen op dat certificaat.

1.4 Certificaatgebruik

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

[OID 2.16.528.1.1003.1.2.2.1 en 2.16.528.1.1003.1.2.5.1]
Authenticiteitcertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het betrouwbaar identificeren en authenticeren van personen, organisaties en middelen langs elektronische weg. Dit betreft zowel de identificatie van personen onderling als tussen personen en geautomatiseerde middelen.

[OID 2.16.528.1.1003.1.2.2.2 en 2.16.528.1.1003.1.2.5.2]
Handtekeningcertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt om elektronische handtekeningen te verifiëren, die "dezelfde rechtsgevolgen hebben als een handgeschreven handtekening", zoals wordt aangegeven in artikel 15a, eerste en tweede lid, in Titel 1 van Boek 3 van het Burgerlijk Wetboek onder afdeling 1A en zijn gekwalificeerde certificaten zoals bedoeld in artikel 1.1, lid ss van de Telecomwet.

[OID 2.16.528.1.1003.1.2.2.3 en 2.16.528.1.1003.1.2.5.3]
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. Dit betreft zowel de uitwisseling tussen personen onderling als tussen personen en geautomatiseerde middelen.

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:

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.

2.4 Toegang tot gepubliceerde informatie

Bevat geen aanvullende eisen.

3 Identificatie en authenticatie

3.1 Naamgeving

RFC 3647	3.1.3 Anonimiteit of pseudonimiteit van certificaathouders
Nummer	3.1.3-pkio11

3.2 Initiële identiteitsvalidatie

RFC 3647	3.2.2 Authenticatie van organisatorische entiteit
Nummer	3.2.2-pkio14

RFC 3647	3.2.2 Authenticatie van organisatorische entiteit
Nummer	3.2.2-pkio16

RFC 3647	3.2.3 Authenticatie van persoonlijke identiteit
Nummer	3.2.3-pkio21

RFC 3647	3.2.5 Autorisatie van de certificaathouder
Nummer	3.2.5-pkio29

RFC 3647	3.2.5 Autorisatie van de certificaathouder
Nummer	3.2.5-pkio32

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	4.9.1 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-pkio68

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 Antecedentenonderzoek
Nummer	5.3.2pkio79

5.4 Procedures ten behoeve van beveiligingsaudits

RFC 3647	5.4.1 Vastlegging van gebeurtenissen
Nummer	5.4.1-pkio80

RFC 3647	5.5.1 Vastlegging van gebeurtenissen
Nummer	5.5.1-pkio82

5.5 Archivering van documenten

Bevat geen aanvullende eisen.

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	6.1.2 Overdracht van private sleutel en SSCD aan certificaathouder
Nummer	6.1.2-pkio94

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	6.2.3 Escrow van private sleutels van certificaathouders
Nummer	6.2.3-pkio101

RFC 3647	6.2.11 Eisen voor veilige middelen voor het aanmaken van elektronische handtekeningen
Nummer	6.2.11-pkio104

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-pkio106

6.3 Andere aspecten van sleutelpaarmanagement

RFC 3647	6.3.1 Archiveren van publieke sleutels
Nummer	6.3.1-pkio108

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

Bevat geen aanvullende eisen.

7.2 CRL-profielen

Bevat geen aanvullende eisen.

7.3 OCSP-profielen

RFC 3647	7.3 OCSP-profielen
Nummer	7.3-pkio123

8 Conformiteitbeoordeling

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

9 Algemene en juridische bepalingen

9.2 Financiële verantwoordelijkheid en aansprakelijkheid

RFC 3647	9.2.1 Verzekeringsdekking
Nummer	9.2.1-pkio124

9.5 Intellectuele eigendomsrechten

Bevat geen aanvullende eisen.

9.6 Aansprakelijkheid

RFC 3647	9.6.1 Aansprakelijkheid van CSP's
Nummer	9.61-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-pkio131

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-pkio139

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 en certificaat statusinformatie

Profiel van persoonsgebonden certificaten voor het domein private personen

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.
- N : Niet toegestaan; geeft aan dat gebruik van het attribuut in de PKI voor de overheid niet is toegestaan.

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.

Naamconventie Subject.commonName
De volgende eisen gelden ten aanzien van de CommonName van het Subject veld. Het belangrijkste uitgangspunt is dat de CSP verantwoordelijk is voor een adequate vermelding van de CommonName. Dat betekent dat voor een goede uitvoering hiervan elk onderdeel dat wordt ingevoerd gecontroleerd moet kunnen worden door de CSP. De CommonName heeft de volgende vorm[3]:

[adellijk predicaat] **[Volledige eerste voornaam]** [*initialen verdere voornamen OF volledige verdere voornamen*] [tussenvoegsels + achternaam partner '-'] [adellijke titel] **[tussenvoegsels + geboorteachternaam]**

waarbij:
dikgedrukt = verplicht onderdeel, schrijfwijze conform WID document of gepresenteerd GBA uittreksel
cursief = verplicht onderdeel, keuze uit twee opties (volledige voornamen of initialen)
normaal = optioneel onderdeel; indien vermeld moet schrijfwijze gelijk zijn aan WID document of gepresenteerd GBA uittreksel

Keuze voor wel of niet toestaan van optionele onderdelen ligt in principe bij de CSP. Deze kan indien gewenst de keuze voor een optie overlaten aan de abonnee of de certificaataanvrager. Indien de Commonname te lang wordt voor het aantal toegestane tekens, dienen optionele onderdelen te worden weggelaten (beginnend met het van achter naar

[3] *De getoonde volgorde is niet verplicht, het is ook toegestaan eerst achternamen te vermelden en dan pas voornamen / initialen.*

voren vervangen van verdere voornamen door initialen) tot de naam past binnen de maximale veldlengte.

Persoonsgebonden certificaten – Domein private personen

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	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.
Issuer	V	MOET een Distinguished Name (DN) bevat-	PKIo, RFC3739,		Andere attributen dan hieronder genoemd MOGEN NIET worden gebruikt.

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
		ten. Veld heeft de onderstaande attributen	ETSI TS 102280		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.stateOrProvinceName	N	Gebruik is niet toegestaan.	PKIo	UTF8String	-
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: 5.2.4	UTF8String	Meerdere instanties van dit attribuut MOGEN gebruikt worden.
Issuer.localityName	N	Gebruik is niet toegestaan.	PKIo	UTF8String	-
Issuer.serialNumber	O	MOET, conform RFC 3739, worden gebruikt	RFC 3739	Printable String	

Veld / Attribuut	Criteria	Beschrijving	Norm refe-rentie	Type	Toelichting
		indien eenduidige naamgeving dit vereist			
Issuer.commonName	V	MOET de naam van de CA te bevatten conform geaccepteerd document of basisregistratie, optioneel 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 (eindgebruiker) te beschrijven MOETEN het subject op unieke wijze benoemen en gegevens bevatten over de abonnee. 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	Printable String	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 referentie	Type	Toelichting
Subject.commonName	V	Het commonName attribuut MOET worden ingevoerd conform de paragraaf *Naamconventie Subject.commonName* hierboven.	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	Zie bij naamconventie Subject.commonName.
Subject.Surname	A	Een juiste weergave van de in het CN vastgelegde element van de naam. Gebaseerd op WID document.	RFC 3739	UTF8String	Het gebruik van dit veld wordt afgeraden. Indien dit veld wordt gebruikt MOET het een juiste weergave te zijn van de achternaam van het subject, inclusief tussenvoegsels. De surname MAG NIET in strijd zijn met de informatie in de commonname
Subject.givenName	A	Een juiste weergave van de in het CN vastgelegde element van de naam. Gebaseerd op WID document.	RFC 3739	UTF8String	Het gebruik van dit veld wordt afgeraden. Indien dit veld wordt gebruikt MOET het een juiste weergave te zijn van de voorna(a)m(en) van het subject. De givenName MAG NIET in strijd zijn met de informatie in de commonname.
Subject.pseudonym	N	Het gebruik van pseudoniemen is niet toegestaan.	ETSI TS 102 280, RFC 3739, PKIo		
Subject.organizationName	V	Volledige naam van de abonnee conform geaccepteerd document of Basisregistratie	PKIo	UTF8String	De abonnee is de entiteit waarmee de CSP een overeenkomst heeft gesloten en namens welke of uit hoofde van wie, de certificaathouder handelt bij het gebruik van het certificaat.

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
Subject.organizationalUnitName	O	Optionele aanduiding van een organisatieonderdeel. Dit attribuut MAG NIET een functieaanduiding of dergelijke bevatten.	PKIo		Dit attribuut MAG bij organisatiegebonden certificaathouders meerdere malen voorkomen. Het veld MOET een geldige naam van een organisatieonderdeel van de abonnee bevatten conform geaccepteerd document of registratie. Bij beroepsgebonden certificaathouders MAG dit attribuut NIET worden opgenomen.
Subject.stateOrProvinceName	A	Het gebruik wordt afgeraden. Indien aanwezig MOET dit veld de provincie van vestiging van de abonnee conform geaccepteerd document of Basisregistratie te 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 te 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 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.emailAddress	N	Gebruik is niet toegestaan.	RFC 5280	IA5String	Dit veld MAG NIET worden gebruikt in nieuwe certificaten.
Subject.serialNumber	V	Door de CSP te bepalen nummer. De combinatie van CommonName, OrganizationName en Serialnumber MOET binnen de context van de CSP uniek zijn.	RFC 3739, X 520, PKIo	Printable String	Het serialnumber is bedoeld om onderscheid te kunnen maken tussen subjects met dezelfde commonName en dezelfde OrganizationName. Om gevoeligheden te vermijden MOET aan elk subject een serialNumber attribuut worden toegekend.
Subject.title	O	Bevat de positie/functie/beroep(sgroep) van een subject.	ETSI TS 102 280, RFC 3739, RFC 5280		Dit attribuut vermeldt bij voorkeur statische, toetsbare beroepstitels (arts, apotheker etc.), NIET de aanspreektitel (Dhr., mw., etc.).
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.
IssuerUniqueIdentifier	N	Wordt niet gebruikt.	RFC 5280		Gebruik hiervan is niet toegestaan (RFC 5280)
subjectUniqueIdentifier	N	Wordt niet gebruikt.	RFC 5280		Gebruik hiervan is niet toegestaan (RFC 5280)

Standaard extensies

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	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 ver-schillende 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. In certificaten voor de elektronische handtekening MOET het non-repudiation bit zijn opgenomen en zijn aangemerkt als essentieel. Een ander keyUsage MAG hiermee NIET worden gecombineerd.			
privateKeyUsagePeriod	N		Wordt niet gebruikt.	RFC 5280		
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	RFC 3739	OID, String, String	Voor domein Overheid/Bedrijven zijn de OID's: 2.16.528.1.1003.1.2.2.1, 2.16.528.1.1003.1.2.2.2 en 2.16.528.1.1003.1.2.2.3.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
			beschreven in de CP.			Voor het domein Organisatie en Organisatie Persoon zijn de OID's: 2.16.528.1.1003.1.2.5.1, 2.16.528.1.1003.1.2.5.2 en 2.16.528.1.1003.1.2.5.3. 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). Indien het een beroepsgebonden certificaat betreft, verdient het voorkeur in de gebruikersnotitie melding te maken van het feit dat de certificaathouder handelt uit hoofde van diens beroep.
PolicyMappings	N		Wordt niet gebruikt.			Deze extensie wordt niet gebruikt in eindgebruikercertificaten
SubjectAltName	V	Nee	MOET worden gebruikt en voorzien zijn van een persoonlijk wereldwijd uniek nummer.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		MOET een unieke identifier bevatten in het othername attribuut. Andere attributen dan hieronder genoemd MOGEN NIET worden gebruikt.
SubjectAltName.otherName	V		MOET worden gebruikt met daarin een	PKIo	IA5String, Mi-	Bevat een door PKIoverheid aan de CSP toegewezen *OID* van de

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
			uniek nummer dat de certificaathouder identificeert. In het authenticatiecertificaat MAG daarnaast nog een othername worden opgenomen voor gebruik met ŧSingle Sign On (SSO).		crosoft UPN, IBM Principal-Name, Kerberos PrincipalName of Permanent-Identifier	CSP en een binnen de namespace van die OID uniek *nummer* dat blijvend het subject identificeert, op een van de volgende manieren: 1. MS UPN: [*nummer*]@[*OID*] 2. MS UPN: [*OID*].[*nummer*] 3. IA5String: [*OID*]-[*nummer*] 4. Permanent Identifier: Identifiervalue = [*nummer*] Assigner = [*OID*] Variant 1. is tevens geschikt voor SSO. Als er een tweede othername voor SSO in het certificaat staat MOET de SSO othername als eerste in de SubjectAltName te staan, vóór de hierboven beschreven PKIoverheid formaat othername, teneinde een goede werking van het SSO mechanisme te waarborgen. Het is aan te bevelen een bestaand registratienummer uit backoffice systemen te gebruiken zoals een personeelsnummer in combinatie met een code voor de organisatie. In combinatie met de CSP OID is deze identifier wereldwijd uniek. Dit nummer MOET persistent te zijn.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
SubjectAltName.rfc822Name	A		MAG worden gebruikt voor het e-mail adres van de certificaathouder, ten behoeve van applicaties die het e-mail adres nodig hebben om goed te functioneren.	RFC 5280	IA5String	Voor PKIoverheid certificaten in domein Overheid/Bedrijven en Organisatie wordt het gebruik van e-mail adressen afgeraden, omdat e-mail adressen van certificaathouders vaak wisselen en bovendien privacygevoelig zijn (spam). Als het e-mail adres wel in het certificaat wordt opgenomen MOET de CSP: • de abonnee hiervoor akkoord laten tekenen en; • controleren of het e-mail adres behoort tot het domein van de abonnee of; • controleren of het mailadres behoort aan de abonnee (b.v. de beroepsbeoefenaar) en deze toegang heeft tot het mailadres (bijvoorbeeld door het uitvoeren van een challenge response).
IssuerAltName	N		Wordt niet gebruikt.	RFC 5280		
subjectDirectoryAttributes	O	Nee		RFC 5280; RFC 3739		Het gebruik van deze extensie is toegestaan. Deze attributen MOGEN GEEN persoonsgegevens bevatten die de privacy van het subject kunnen schaden.
BasicConstraints	O	Ja	Het "CA" veld MOET op "FALSE" staan of	RFC 5280		In een (Nederlandstalige) browser zal dan te zien zijn:

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
			worden weggelaten (default waarde is dan "FALSE").			"Subjecttype = Eindentiteit", "Beperking voor padlengte = Geen"
NameConstraints	N		Wordt niet gebruikt.	RFC 5280		Wordt niet gebruikt in eindgebruiker certificaten.
PolicyConstraints	N		Wordt niet gebruikt.	RFC 5280		Wordt niet gebruikt in eindgebruiker certificaten.
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	O / N	Nee	ExtKeyUsage MAG NIET worden gebruikt in certificaten voor de elektronische handtekening. In andere certificaten is, voor de ondersteuning van bepaalde toepassingen, het gebruik van ExtKeyUsage toegestaan.	RFC 5280	KeyPurposeId's	Indien gebruikt, zijn de volgende voorwaarden allen van kracht. Een ExtKeyUsage: • MAG NIET worden opgenomen in certificaten voor de elektronische handtekening [OID 2.16.528.1.1003.1.2.2.2 en 2.16.528.1.1003.1.2.5.2]; • MAG worden opgenomen in elk ander certificaat; • MAG NIET als critical worden aangemerkt; • MOET minimaal een (1) KeyPurposeId bevatten.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
						Elke in een ExtKeyUsage opgenomen KeyPurposeId: • MAG NIET strijdig zijn met de KeyUsage extensie; • MOET toepasselijk zijn op de soort certificaathouder; • MOET gedefinieerd zijn in een wereldwijd erkende standaard, zoals een RFC.
InhibitAnyPolicy	N		Wordt niet gebruikt.	RFC 5280		Wordt niet gebruikt in eindgebruiker certificaten.
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 referentie	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, Generalname	Dit veld kan gebruikt worden om te verwijzen naar aanvullende informatie over het subject, mits de aangeboden informatie geen inbreuk maakt op de privacy van het subject.
BiometricInfo	O	Nee	Bevat de hash van een biometrische template en optioneel een URI die verwijst naar een bestand met de biometrische template zelf.	RFC 3739		
QcStatement	V/N	Nee	Certificaten voor de elektronische handtekening MOETEN aangeven dat zij zijn uitgegeven als gekwalificeerde certificaten overeenstemmend met annex I en annex II van de Europese Richtlijn. Deze overeenstemming wordt aangegeven door het opnemen van de *id-etsi-qcs-QcCompliance* statement in deze extensie.	RFC 3739, ETSI TS 102 280, ETSI TS 101 862	OID	De genoemde QcStatement identifiers betreffen de volgende OIDs: id-etsi-qcs-QcCompliance { id-etsi-qcs 1 } 0.4.0.1862.1.1 id-etsi-qcs-QcSSCD { id-etsi-qcs 4 } 0.4.0.1862.1.4

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
			Certificaten voor de elektronische handtekening MOGEN aangeven dat de private sleutel behorende bij de publieke sleutel in het certificaat is opgeslagen op een secure signature-creation device (SSCD) overeenstemmend met annex III van de Europese Richtlijn. Deze overeenstemming wordt aangegeven door het (additioneel) opnemen van de *id-etsi-qcs-QcSSCD* statement in deze extensie. De certificaten voor authenticiteit en de certificaten voor vertrouwelijkheid MOGEN deze extensie NIET gebruiken.			

10 Revisies

Er zijn nog geen wijzigingen voor dit CP deel. Het gaat hier om de initiele versie.