



Programma van Eisen deel 3d: Certificate Policy - Domein Autonome Apparaten

Datum 1 juli 2017

| | |
|----------------------------------------|-------------------------|
| Domein autonome apparaten: | |
| Autonome Apparaten – Authenticiteit | 2.16.528.1.1003.1.2.6.1 |
| Autonome Apparaten – Vertrouwelijkheid | 2.16.528.1.1003.1.2.6.2 |
| Autonome Apparaten – Combinatie | 2.16.528.1.1003.1.2.6.3 |

Colofon

Versienummer 4.5
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

| | |
|-------------------------------------------------------------------------------------|-----------|
| Colofon | 2 |
| Inhoud | 3 |
| 1 Introductie op de Certificate Policy | 8 |
| 1.1 <i>Achtergrond</i> | 8 |
| 1.1.1 <i>Opzet van de Certificate Policy</i> | 8 |
| 1.1.2 <i>Status</i> | 9 |
| 1.2 <i>Verwijzingen naar deze CP</i> | 9 |
| 1.3 <i>Gebruikersgemeenschap</i> | 10 |
| 1.4 <i>Certificaatgebruik</i> | 12 |
| 1.5 <i>Contactgegevens Policy Authority</i> | 13 |
| 2 Publicatie en verantwoordelijkheid voor elektronische opslagplaats | 14 |
| 2.1 <i>Elektronische opslagplaats</i> | 14 |
| 2.2 <i>Publicatie van TSP-informatie</i> | 14 |
| 3 Identificatie en authenticatie | 15 |
| 3.4 <i>Naamgeving</i> | 15 |
| 3.5 <i>Initiële identiteitsvalidatie</i> | 15 |
| 3.6 <i>Identificatie en authenticatie bij vernieuwing van het certificaat</i> | 16 |
| 4 Operationele eisen certificaatlevenscyclus | 17 |
| 4.1 <i>Aanvraag van certificaten</i> | 17 |
| 4.4 <i>Acceptatie van certificaten</i> | 17 |
| 4.5 <i>Sleutelpaar en certificaatgebruik</i> | 17 |
| 4.9 <i>Intrekking en opschorting van certificaten</i> | 17 |
| 4.10 <i>Certificaat statusservice</i> | 17 |
| 5 Management, operationele en fysieke beveiligingsmaatregelen | 18 |
| 5.2 <i>Procedurele beveiliging</i> | 18 |
| 5.3 <i>Personele beveiliging</i> | 18 |
| 5.4 <i>Procedures ten behoeve van beveiligingsaudits</i> | 18 |
| 5.5 <i>Archivering van documenten</i> | 18 |
| 5.7 <i>Aantasting en continuïteit</i> | 18 |
| 6 Technische beveiliging | 19 |
| 6.1 <i>Genereren en installeren van sleutelparen</i> | 19 |

| | | |
|------------------|--------------------------------------------------------------------------------------------------|-----------|
| 6.2 | <i>Private sleutelbescherming en cryptografische module engineering beheersmaatregelen</i> | 19 |
| 6.3 | <i>Andere aspecten van sleutelpaarmanagement</i> | 20 |
| 6.4 | <i>Activeringsgegevens</i> | 20 |
| 6.5 | <i>Logische toegangsbeveiliging van TSP-computers</i> | 20 |
| 6.6 | <i>Beheersmaatregelen technische levenscyclus</i> | 20 |
| 6.7 | <i>Netwerkbeveiliging</i> | 20 |
| 7 | Certificaat- en CRL-profielen | 21 |
| 7.1 | <i>Certificaatprofielen</i> | 21 |
| 7.2 | <i>CRL-profielen</i> | 21 |
| 8 | Conformiteitbeoordeling | 22 |
| 9 | Algemene en juridische bepalingen | 23 |
| 9.2 | <i>Financiële verantwoordelijkheid en aansprakelijkheid</i> | 23 |
| 9.5 | <i>Intellectuele eigendomsrechten</i> | 23 |
| 9.6 | <i>Aansprakelijkheid</i> | 23 |
| 9.8 | <i>Beperkingen van aansprakelijkheid</i> | 23 |
| 9.12 | <i>Wijzigingen</i> | 24 |
| 9.13 | <i>Geschillenbeslechting</i> | 24 |
| 9.14 | <i>Van toepassing zijnde wetgeving</i> | 24 |
| 9.17 | <i>Overige bepalingen</i> | 24 |
| Bijlage A | Profielen certificaten | 25 |
| 10 | Revisies | 34 |
| 10.1 | <i>Wijzigingen van versie 4.4 naar 4.5</i> | 34 |
| 10.1.1 | <i>Nieuw</i> | 34 |
| 10.1.2 | <i>Aanpassingen</i> | 34 |
| 10.1.3 | <i>Redactioneel</i> | 34 |
| 10.2 | <i>Wijzigingen van versie 4.3 naar 4.4</i> | 34 |
| 10.2.1 | <i>Aanpassingen</i> | 34 |
| 10.2.2 | <i>Redactioneel</i> | 34 |
| 10.3 | <i>Wijzigingen van versie 4.2 naar 4.3</i> | 34 |
| 10.3.1 | <i>Nieuw</i> | 34 |
| 10.3.2 | <i>Aanpassingen</i> | 34 |
| 10.3.3 | <i>Redactioneel</i> | 35 |
| 10.4 | <i>Wijzigingen van versie 4.1 naar 4.2</i> | 35 |
| 10.4.1 | <i>Nieuw</i> | 35 |
| 10.4.2 | <i>Aanpassingen</i> | 35 |
| 10.4.3 | <i>Redactioneel</i> | 35 |
| 10.5 | <i>Wijzigingen van versie 4.0 naar 4.1</i> | 35 |
| 10.5.1 | <i>Nieuw</i> | 35 |
| 10.5.2 | <i>Aanpassingen</i> | 35 |
| 10.5.3 | <i>Redactioneel</i> | 35 |

| | | |
|-------------|--------------------------------------------------|----|
| <i>10.6</i> | <i>Wijzigingen van versie 3.7 naar 4.0</i> | 35 |
| 10.6.1 | Nieuw..... | 35 |
| 10.6.2 | Aanpassingen | 35 |
| 10.6.3 | Redactioneel | 35 |

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 Trusted 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 |
|---------------|--------------|------------------------------------|
| 1.0 | 08-10-2009 | Definitieve versie |
| 2.0 | 09-10-2009 | Vastgesteld door BZK oktober 2009 |
| 2.1 | 11-01-2010 | Vastgesteld door BZK januari 2010 |
| 3.0 | 25-01-2011 | Vastgesteld door BZK januari 2011 |
| 3.1 | 01-07-2011 | Vastgesteld door BZK juni 2011 |
| 3.2 | 27-01-2012 | Vastgesteld door BZK januari 2012 |
| 3.3 | 01-07-2012 | Vastgesteld door BZK juni 2012 |
| 3.4 | 04-02-2013 | Vastgesteld door BZK januari 2013 |
| 3.5 | 06-07-2013 | Vastgesteld door BZK juli 2013 |
| 3.6 | 01-2014 | Vastgesteld door BZK januari 2014 |
| 3.7 | 06-2014 | Vastgesteld door BZK juni 2014 |
| 4.0 | 12-2014 | Vastgesteld door BZK december 2014 |
| 4.1 | 07-2015 | Vastgesteld door BZK juli 2015 |
| 4.2 | 01-2016 | Vastgesteld door BZK januari 2016 |

| | | |
|-----|---------|------------------------------------|
| 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 |

1 Introductie op de Certificate Policy

1.1 Achtergrond

Dit is deel 3d 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 Trusted Service Provider (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 apparaatgebonden certificaten uitgegeven door TSP's in het domein Autonome Apparaten.

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 eisen¹:

- 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 policy NCP+² van toepassing is, zodat gebruikt 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 |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

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 De CP Autonome Apparaten is gebaseerd op een andere onderliggende standaard dan de CP's voor persoonsgebonden certificaten. Omdat apparatencertificaten niet persoonsgebonden zijn en geen gekwalificeerde certificaten zijn zoals bedoeld in de Wet Elektronische Handtekeningen wijken de eisen aan apparatencertificaten op bepaalde punten af van de eisen aan andere soorten certificaten. Voor certificaten met een ExtkeyUsage client- and server authentication zijn de policies NCP in combinatie met OVCP, PTC-BR en Netsec van toepassing. Dit komt omdat deze certificaten volgens het CABforum worden beschouwd als SSL certificaten. Voor Netsec geldt dat eisen 1h, 3a, 3e, 4c.i en 4f niet normatief zijn (ETSI CP OID 0.4.0.2042.1.7).

| | |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Certificate Policies en Certification Practice Statements ³ . |
| 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 is ook een aantal bepalingen opgenomen die niet als PKIo-eis zijn geformuleerd. Deze bepalingen stellen geen eisen aan de TSP'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 apparatencertificaten opgenomen. De certificaat statusinformatie is in de basiseisen opgenomen.

1.1.2

Status

Dit is versie 4.5 van deel 3d van het PvE. De huidige versie is bijgewerkt tot en met 1 juli 2017.

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 Autonome Apparaten: | |
| OID | CP |

³ In de hoofdstukken 2 t/m 9 zijn alleen die paragrafen uit RFC 3647 opgenomen waarvoor een PKIo-eis van toepassing is.

| | |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.16.528.1.1003.1.2.6.1 | <p>voor het authenticiteitcertificaat voor apparaten binnen het domein Autonome Apparaten, dat de publieke sleutel bevat ten behoeve van identificatie en authenticatie.</p> <p>Onder genoemd OID kunnen ook OSCP responder certificaten worden uitgegeven voor gebruik binnen de context van dit CP deel.</p> |
| 2.16.528.1.1003.1.2.6.2 | <p>voor het vertrouwelijkheidcertificaat voor apparaten binnen het domein Autonome Apparaten, dat de publieke sleutel bevat ten behoeve van vertrouwelijkheid.</p> |
| 2.16.528.1.1003.1.2.6.3 | <p>voor het combinatiecertificaat voor apparaten binnen het domein Autonome Apparaten, dat de publieke sleutel bevat ten behoeve van authenticiteit & vertrouwelijkheid.</p> |

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 autonome apparaten (6). authenticiteit (1)/ vertrouwelijkheid (2)/ combinatie (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 het domein Autonome Apparaten zijn de certificaathouders apparaten die in hun operationele levensfase zelfstandig de integriteit en authenticiteit van (meet)gegevens waarborgen ten behoeve van (een specifiek doel binnen een kerntaak van) een bepaalde overheidsinstantie. De betreffende overheidsinstantie publiceert een normenkader voor de voor het gespecificeerde doel te fabriceren apparaten en wordt daarmee als de "kadersteller" gekenmerkt.

Op basis van dat normenkader geeft de kadersteller een conformiteitscertificaat af aan elke fabrikant die en voor elk – door die fabrikant te produceren – type apparaat dat aan het normenkader conformeert (voor het uitvoeren van conformiteitsbeoordelingen en het afgeven van conformiteitscertificaten kan de kadersteller een toezichthouder aanwijzen). Hiermee worden (gegadigde) apparaat-fabrikanten in staat gesteld aan het normenkader conformerende apparaten op de markt te brengen.

Voorafgaand aan de operationeelstelling van een (aan het normenkader conformerend) apparaat, dient er een certificaat uit het domein Autonome Apparaten aan dat apparaat te worden toegekend (gekoppeld). Gedurende de operationele levensduur van een autonoom apparaat kan het apparatencertificaat worden vervangen c.q. ingetrokken. De kadersteller dient een of meer organisaties te autoriseren voor het uitvoeren van deze taken. Een dergelijke organisatie wordt in deze CP aangemerkt als Abonnee.

Een Abonnee kan een of meer certificaatbeheerders aanwijzen voor het (namens de Abonnee) uitvoeren van een of meer handelingen met betrekking tot certificaten uit het domein Autonome Apparaten.

Certificaatbeheerders kunnen in twee vormen voorkomen:

- Natuurlijke personen met een directe relatie tot de Abonneeorganisatie;
- Natuurlijke personen met een relatie tot een of meer rechtspersonen die een overeenkomst met de Abonneeorganisatie hebben.

Rekening houdend met wat hierboven beschreven is, bestaat in het domein Autonome Apparaten de gebruikersgemeenschap uit kaderstellers, fabrikanten, abonnees, certificaatbeheerders, certificaathouders (de apparaten zelf) en vertrouwende partijen (waaronder de kaderstellers zelf).

- Een *Kadersteller* is een overheidsinstantie die:
 - voor een bepaalde kerntaak de behoefte heeft aan – van buiten haar directe invloedssfeer afkomstige – (meet)gegevens;
 - voor het waarborgen van de integriteit en authenticiteit van die (meet)gegevens gebruik wenst te maken van autonoom handelende apparaten van een bepaalde soort;
 - voor het waarborgen van de betrouwbaarheid van exemplaren van die apparaatsoort:
 - een normenkader voor de productie, activering, operatie, onderhoud, inname en gebruik opstelt en in wet- en regelgeving vastlegt;
 - op basis van dat normenkader organisaties autoriseert voor:
 - het produceren en verspreiden van apparaten van betreffende soort;
 - het koppelen van certificaten aan apparaten van betreffende soort;
 - het vervangen van certificaten op apparaten van betreffende soort;
 - het intrekken van certificaten van apparaten van betreffende soort.
- Een *Fabrikant* is een in Nederland erkende organisatie, die aantoonbaar conformeert aan het Normenkader voor het produceren en in Nederland verspreiden van een specifieke soort Autonome Apparaten en daarvoor dan ook is geautoriseerd door de Kadersteller.
- Een *Abonnee* is een natuurlijke of rechtspersoon die met een TSP een overeenkomst sluit namens een of meer Certificaathouders voor het laten certificeren van de publieke sleutels. In het kader van het domein Autonome Apparaten is een Abonnee een in Nederland erkende organisatie, die aantoonbaar conformeert aan de toelatingseisen voor het koppelen van certificaten (uit het domein Autonome Apparaten) aan een specifieke soort Autonome Apparaten.
- Een *Certificaathouder* is een entiteit, gekenmerkt via een beschermde koppeling met een certificaat als de houder van de private sleutel die is verbonden met de publieke sleutel die in het certificaat is gegeven.

Een Certificaathouder is een apparaat waarvan de werking en de wijze van produceren aantoonbaar conformeren aan het normenkader van een specifieke soort autonome apparaten en dat in die hoedanigheid door de kadersteller geautoriseerd is gebruik te maken van een aan dat apparaat gekoppeld Autonome Apparatencertificaat.

De koppeling tussen certificaat en apparaat is gemaakt en beschermd door een organisatorische entiteit waarvoor een abonnee de contracterende partij is.

- Een *Certificaatbeheerder* is een natuurlijke persoon of een combinatie van een natuurlijke en een rechtspersoon die namens de Abonnee handelingen (koppelen, vervangen en/of intrekken) 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 andere CP's ontlenen vertrouwende partijen zekerheid aan zowel de verbondenheid van een autonoom apparaat met diens certificaat, als aan de met dat certificaat aangeduide goedkeuring van de werking van het autonome apparaat. De CP Autonome Apparaten legt derhalve even veel nadruk op het bieden van zekerheid over de verbondenheid van een door een autonoom apparaat ondertekend bericht met enerzijds de identiteit van het autonome apparaat en anderzijds diens goedgekeurde werking. Het vaststellen van de identiteit van de certificaathouder (apparaat) is in dit licht net zo van belang als het vaststellen van de goedkeuring van diens werking.

1.4 Certificaatgebruik

Het gebruik van certificaten uitgegeven onder deze CP heeft betrekking op communicatie van certificaathouders die handelen conform hun gecertificeerde werking.

[OID 2.16.528.1.1003.1.2.6.1] Authenticiteitscertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het langs elektronische weg betrouwbaar identificeren en authenticeren van het Autonome Apparaat en diens gecertificeerde werking.

Onder genoemd OID kunnen ook OCSP responder certificaten worden uitgegeven, alleen voor gebruik binnen het domein Organisatie Autonome Apparaten (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.

[OID 2.16.528.1.1003.1.2.6.2] Vertrouwelijkheidscertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het beschermen van de vertrouwelijkheid van gegevens, die worden uitgewisseld met het Autonome Apparaat en/of daarin worden opgeslagen in elektronische vorm.

[OID 2.16.528.1.1003.1.2.6.3] Combinatiecertificaten die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het beveiligen van een verbinding tussen een bepaalde client en een Autonoom Apparaat.

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 |

3 Identificatie en authenticatie

3.4 Naamgeving

Bevat geen aanvullende eisen.

3.5 Initiële identiteitsvalidatie

| | |
|-----------------|---------------------------------------------------|
| 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-pkio31 |

| | |
|-----------------|--------------------------------------------|
| RFC 3647 | 3.2.5 Autorisatie van de certificaathouder |
| Nummer | 3.2.5-pkio34 |

3.6 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 | 4.9.3 Procedure voor een verzoek tot intrekking |
| Nummer | 4.9.3-pkio58 |

| | |
|-----------------|------------------------------|
| 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 |

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

| | |
|-----------------|--------------------------------------|
| 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 TSP 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 |

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 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 |

6.3 Andere aspecten van sleutelpaarmanagement

| | |
|-----------------|----------------------------------------------------------------------|
| RFC 3647 | 6.3.2 Gebruiksduur voor certificaten en publieke en private sleutels |
| Nummer | 6.3.2-pkio111 |

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- en CRL-profielen

7.1 Certificaatprofielen

| | |
|-----------------|--------------------------|
| RFC 3647 | 7.1 Certificaatprofielen |
| Nummer | 7.1-pkio151 |

7.2 CRL-profielen

Bevat geen aanvullende eisen.

8 Conformiteitbeoordeling

Alle onderwerpen met betrekking tot de conformiteitbeoordeling van de TSP'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 TSP's |
| Nummer | 9.6.1-pkio127 |

| | |
|-----------------|-----------------------------------|
| RFC 3647 | 9.6.1 Aansprakelijkheid van TSP's |
| Nummer | 9.6.1-pkio142 |

| | |
|-----------------|-----------------------------------|
| 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-pkio143 |

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-pkio141 |

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 apparatencertificaten voor het domein Autonome Apparaten

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.

Apparatencertificaten

Basisattributen

| Veld / Attribuut | Criteria | Beschrijving | Norm referentie | Type | Toelichting |
|-------------------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version | V | MOET ingesteld worden op 2 (X.509v3). | RFC 5280 | Integer | Beschrijft de versie van het certificaat, de waarde 2 staat voor X.509 versie 3. |
| SerialNumber | V | Een serienummer dat op unieke wijze het certificaat binnen het uitgevende CA domein MOET identificeren. | RFC 5280 | Integer | Alle eindgebruiker certificaten moeten tenminste 8 bytes aan niet te voorspellen willekeurige data bevatten in het serienummer (SerialNumber) van het certificaat. |
| Signature | V | MOET worden ingesteld op het algoritme, zoals deze door de PA is bepaald. | RFC 5280, ETSI TS 102176 | OID | MOET gelijk zijn aan het veld signatureAlgorithm. Voor certificaten onder het G2 en G3 stamcertificaat wordt alleen sha-256WithRSAEncryption toegestaan. |
| Issuer | V | MOET een Distinguished Name (DN) bevatten. Veld heeft de onderstaande attributen: | PKIo, RFC3739, ETSI TS 102280 | | Andere attributen dan hieronder genoemd MOGEN NIET worden gebruikt. De attributen die worden gebruikt MOETEN gelijk zijn aan de gelijknamige attributen in het Subject veld van het TSP 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 TSP's gevestigd in Nederland. |
| Issuer.organizationName | V | Volledige naam conform geaccepteerd document of basisregistratie. | ETSI TS 102280 | UTF8String | |
| Issuer.organizationalUnitName | O | Optionele aanduiding van een organisatieonderdeel. Dit veld MAG NIET een functieaanduiding of dergelijke bevatten. Wel eventueel de typen certificaten die worden ondersteund. | ETSI TS 102280 | UTF8String | Meerdere instanties van dit attribuut MOGEN gebruikt worden. |
| Issuer.serialNumber | O | MOET, conform RFC 3739, worden gebruikt INDIEN eenduidige naamgeving dit vereist. | RFC 3739 | Printable String | |

| Veld / Attribuut | Criteria | Beschrijving | Norm referentie | Type | Toelichting |
|-------------------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Issuer.commonName | V | MOET de naam van de CA bevatten conform geaccepteerd document of basisregistratie, MAG worden aangevuld met de Domein aanduiding en/of de typen certificaat die worden ondersteund. | PKIo, RFC 5280, 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: <ul style="list-style-type: none"> • 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). |
| Validity | V | MOET de geldigheidsperiode (validity) van het certificaat definiëren. | 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 (apparaat) te beschrijven MOETEN het subject op unieke wijze benoemen en gegevens bevatten over de abonneeorganisatie. 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 | Vaste waarde: C=NL, conform ISO 3166. | RFC 3739, X520, ISO 3166, PKIo | PrintableString | Met countryname wordt aangegeven dat het certificaat is uitgegeven binnen de <i>context</i> van de PKI voor de (Nederlandse) overheid. |
| Subject.commonName | V | MOET het normenkader waaraan het apparaat | RFC 3739, ETSI TS | UTF8String | De abonnee MOET aantonen dat diens organisatie deze naam mag toekennen. |

| Veld / Attribuut | Criteria | Beschrijving | Norm referentie | Type | Toelichting |
|---------------------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | conformeert identificeren OF MOET het aan het normenkader conformerende model/type van het apparaat identificeren. | 102 280, PKIo | | Het is niet toegestaan in dit attribuut wildcards te gebruiken. Voorbeelden van een correcte invulling zijn: Het typegoedkeuringsnummer van het betreffende apparaat; De (korte) omschrijving van de specifieke soort Autonoom Apparaten |
| Subject.organizationName | V | Volledige naam van de organisatie van de abonnee conform geaccepteerd document of Basisregistratie. | PKIo | UTF8String | De abonneeorganisatie is de organisatie waarmee de TSP een overeenkomst heeft gesloten voor het binnen het door de kadersteller opgestelde normenkader koppelen/toekennen van certificaten aan apparaten. |
| Subject.organizational-UnitName | O | Optionele aanduiding van een organisatieonderdeel binnen de abonneeorganisatie. MOET overeenstemmen met een door de abonneeorganisatie gedocumenteerde naam van een organisatieonderdeel. | PKIo | | Dit attribuut MAG meerdere malen voorkomen. Uit bij de abonneeorganisatie opvraagbare documentatie MOET blijken dat de in dit attribuut gebruikte naam dat organisatieonderdeel vermeldt waarin de certificaatbeheerder(s) van de abonneeorganisatie werkzaam is (zijn). |
| 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 | 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 |
|----------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | conform geaccepteerd document of Basisregistratie te bevatten. | | | |
| Subject.serialNumber | O | Het is de verantwoordelijkheid van een TSP om de uniciteit van het subject (apparaat) te waarborgen. Het Subject.serialNumber MOET gebruikt worden om het subject uniek te identificeren. | 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. In aanvulling op de definitie in RFC 3739 MAG het nummer worden aangevuld om naast het subject, bijvoorbeeld het SUD te identificeren. |
| Subject.title | O | Geeft de binnen het normenkader geldende autorisatie van het (autonome) apparaat aan. | ETSI TS 102 280, RFC 3739, RFC 5280 | | De kadersteller bepaalt of dit attribuut wordt gebruikt en legt dat gebruik vast in het door hem op te stellen normenkader. |
| 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 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 | <p>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.</p> <p>In authenticiteitcertificaten MOET het digitalSignature bit zijn opgenomen. Een andere keyUsage MAG hiermee NIET worden gecombineerd.</p> <p>In vertrouwelijkheidcertificaten MOETEN de keyEncipherment en dataEncipherment bits zijn opgenomen.. Een andere keyUsage MAG hiermee NIET worden gecombineerd.</p> <p>In combinatiecertificaten MOETEN de digitalSignature, keyEncipherment en keyAgreement bits zijn opgenomen en zijn aangemerkt als essentieel. Een ander keyUsage MAG hiermee NIET worden gecombineerd</p> | RFC 3739, RFC 5280, ETSI TS 102 280 | BitString | |

| | | | | | | |
|--------------------------|---|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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. 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 | <p>Voor apparatencertificaten in domein Autonome Apparaten zijn de OID's: 2.16.528.1.1003.1.2.6.1, 2.16.528.1.1003.1.2.6.2 en 2.16.528.1.1003.1.2.6.3.</p> <p>Een eventuele verdere beperking ten aanzien van het certificaatgebruik MOET worden opgenomen in het CPS waarnaar deze extensie verwijst en wordt bij voorkeur ook vermeld in de in deze extensie opgenomen gebruikersnotitie.</p> <p>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).</p> |
| SubjectAltName | V | Nee | Bevat een of meer alternatieve namen/identificatienummers van de certificaathouder | RFC 5280, PKIo, ETSI 102 280 | | Andere attributen dan hieronder genoemd MOGEN NIET worden gebruikt. |
| SubjectAltName.otherName | V | | <p>MOET worden gebruikt met daarin een nummer dat de certificaathouder (subject) wereldwijd uniek identificeert.</p> <p>In het authenticiteitcertificaat MAG daarnaast als othername een PrincipalName (UPN) worden opgenomen voor gebruik met SSO (Single Sign On).</p> | RFC 4043, PKIo | IA5String, Microsoft UPN, IBM Principal-Name of Permanent-Identifier | <p>Bevat een door PKIoverheid aan de TSP (issuer) toegewezen OID en een binnen de namespace van die OID uniek nummer dat blijvend de certificaathouder (subject) identificeert, op een van de volgende manieren:</p> <p>MS UPN: [nummer]@[OID] IA5String: [OID].[nummer] IA5String: [OID]-[nummer] Permanent Identifier: Identifiervalue = [nummer] Assigner = [OID]</p> <p>Variant 1. is tevens geschikt voor SSO (Single Sign On). 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</p> |

| | | | | | | |
|---------------------------|---|----------|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | | | | | mechanisme te waarborgen. |
| 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 worden weggelaten (default waarde is dan "FALSE"). | RFC 5280 | | In een (Nederlandstalige) browser zal dan te zien zijn: "Subjecttype = Eidentiteit", "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 intrekingsredenen. Naast CRL MOGEN ook andere vormen van certificaatstatus informatiediensten worden ondersteund. |
| ExtKeyUsage | V | Ja / Nee | | RFC 5280 | KeyPurposeId's | Zie eis 7.1-pkio151 |
| 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 accessMethod (id-ad-caIssuers) | O | | Een AccessDescription item met accessMethod id-ad-caIssuers verwijst naar de online locatie waar het certificaat van de TSP CA die het onderhavige certificaat ondertekende (uitgaf) zich bevindt. | RFC 5280 | URI | Dit attribuut MOET de URI van het desbetreffende certificaatbestand/-object bevatten. Indien het een HTTP-URI betreft, is het bestand waarnaar verwezen wordt: bij voorkeur een DER-gecodeerd CA-certificaatbestand, dat door de desbetreffende HTTP server is aangemerkt als zijnde van het MIME type "application/pkix-cert". |
| 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 4.4 naar 4.5

10.1.1 *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)

10.1.2 *Aanpassingen*

- Wijziging OID 2.16.528.1.1003.1.2.6.1 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)

10.1.3 *Redactioneel*

- Enkele typfouten gecorrigeerd in het certificaatprofiel
- CRL extensies en CRL entry verwijderd (staan in bijlage A van de basiseisen)

10.2 Wijzigingen van versie 4.3 naar 4.4

10.2.1 *Aanpassingen*

- Eis 5.3.2-pkio79 is vervallen (uiterlijke ingangsdatum 1-2-2017)
- Eis 7.1-pkio151 aangepast; gebruik van EKU's uitgesplitst naar diverse certificaattypen (uiterlijke ingangsdatum 1-2-2017)
- 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)

10.2.2 *Redactioneel*

- Term TSP (Certificate service provider) vervangen door TSP (Trust Service Provider) n.a.v. eIDAS verordening

10.3 Wijzigingen van versie 4.2 naar 4.3

10.3.1 *Nieuw*

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

10.3.2 *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 (ingangsdatum 1-7-2016)

10.3.3 *Redactioneel*

- Verwijzingen naar de G1 Root verwijderd (verlopen)

10.4 **Wijzigingen van versie 4.1 naar 4.2**

10.4.1 *Nieuw*

- Eis 7.1-pkio151 (uiterlijke ingangsdatum 1 juli 2016)

10.4.2 *Aanpassingen*

Niet van toepassing

10.4.3 *Redactioneel*

Niet van toepassing

10.5 **Wijzigingen van versie 4.0 naar 4.1**

10.5.1 *Nieuw*

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

10.5.2 *Aanpassingen*

Niet van toepassing

10.5.3 *Redactioneel*

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

10.6 **Wijzigingen van versie 3.7 naar 4.0**

10.6.1 *Nieuw*

- Eis 4.9.9-pkio69

10.6.2 *Aanpassingen*

- PvE eisen zijn omgenummerd volgens een nieuwe naming convention;
- De creatie van een baseline en een aanvullende eisen document;
- Inhoudelijke wijzigingen aan eisen zijn terug te vinden in de baseline en het aanvullende eisen document.

10.6.3 *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.