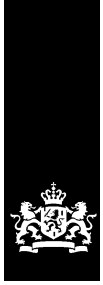

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

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

Datum 4 februari 2013

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 3.4
Contactpersoon Policy Authority PKIoverheid

Organisatie Logius

Bezoekadres
Wilhelmina van Pruisenweg 52

Postadres
Postbus 96810
2509 JE DEN HAAG

T 0900 - 555 4555
servicecentrum@logius.nl

Inhoud

De Policy Authority (PA) van de PKI voor de overheid ondersteunt de Minister van Binnenlandse Zaken en Koninkrijksrelaties bij het beheer over de PKI voor de overheid.

De PKI voor de overheid is een afsprakenstelsel. Dit maakt generiek en grootschalig gebruik mogelijk van de elektronische handtekening, en faciliteert voorts identificatie op afstand en vertrouwelijke communicatie. De taken van de PA PKIoverheid zijn:

- het leveren van bijdragen voor de ontwikkeling en het beheer van het normenkader dat aan de PKI voor de overheid ten grondslag ligt, het zogeheten Programma van Eisen (PvE);
- het proces van toetreding door Certification Service Providers (CSP's) tot de PKI voor de overheid begeleiden en voorbereiden van de afhandeling;
- het toezicht houden op en controleren van de werkzaamheden van CSP's die onder de root van de PKI voor de overheid certificaten uitgeven.

De doelstelling van de Policy Authority is:
Het handhaven van een werkbaar en betrouwbaar normenkader voor PKI-diensten dat voorziet in een vastgesteld beveiligingsniveau voor de communicatiebehoefte van de overheid en transparant is voor de gebruikers.

Revisiegegevens

Versie	**Datum**	**Omschrijving**
1.0	08-10-2009	Definitieve versie
2.0	09-10-2009	Vastgesteld door BZK oktober 2009
2.1	11-01-2010	Wijzigingen naar aanleiding van naamswijziging GBO.Overheid in Logius
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

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 Certification Service Provider (CSP) binnen de PKI voor de overheid worden gesteld. Binnen de PKI voor de overheid is onderscheid gemaakt tussen verschillende domeinen. Dit document heeft uitsluitend betrekking op de apparaatgebonden certificaten uitgegeven door CSP'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 eisen[1]:

- die voortkomen uit het Nederlandse wettelijke kader in relatie tot de elektronische handtekening;
- die voortkomen uit de standaard ETSI TS 102 042 waarbij gebruikt wordt gemaakt van een SUD V2.2.1 (2011-12) – niveau NCP+[2];
- die specifiek door en voor de PKIoverheid zijn opgesteld.

In de hoofdstukken 2 t/m 9 zijn de specifieke PKIoverheid-eisen opgenomen. In de onderstaande tabel is de structuur weergegeven waarin iedere PKIoverheid-eis (PKIo-eis) afzonderlijk wordt gespecificeerd.

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 Certi¬fication 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

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

	3647 paragraafnummer vormt dit een unieke aanduiding voor de PKIo-eis.
ETSI	Verwijzing naar de eis(en) uit ETSI TS 102 042 waarvan de PKIo-eis is afgeleid c.q. een nadere invulling is.
PKIo	De PKIo-eis die binnen de PKI voor de overheid van toepassing is. Indien in de tabel de aanduiding "PKIo-AA" is opgenomen, is de eis alleen van toepassing op certificaten die binnen het domein Autonome Apparaten worden uitgegeven.
Opmerking	Bij een aantal PKIo-eisen is, voor een beter begrip van de context waarin de eis moet worden geplaatst, een opmerking toegevoegd.

In dit CP is 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 apparatencertificaten 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 de eisen afkomstig uit de Nederlandse wetgeving, eisen uit ETSI TS 102 042 en de PKIo-eisen.

1.1.2 Status

Dit is versie 3.4 van deel 3d van het PvE. De huidige versie is bijgewerkt tot en met januari 2013.

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

Elke CP wordt uniek geïdentificeerd door een OID, conform het volgende schema[4].

Domein Autonome Apparaten:	
OID	**CP**
2.16.528.1.1003.1.2.6.1	voor het authenticiteitcertificaat voor apparaten binnen het domein Autonome Apparaten, dat de publieke sleutel bevat ten behoeve van identificatie en authenticatie.
2.16.528.1.1003.1.2.6.2	voor het vertrouwelijkheidcertificaat voor apparaten binnen het domein Autonome Apparaten, dat de publieke sleutel bevat ten behoeve van vertrouwelijkheid.
2.16.528.1.1003.1.2.6.3	voor het combinatiecertificaat voor apparaten binnen het domein Autonome Apparaten, dat de pu¬blieke sleutel bevat ten behoeve van authenticiteit & vertrouwelijkheid.

De OID is als volgt opgebouwd: {joint-iso-itu-t (2). country (16). nederland (528). Nederlandse organisatie (1). nederlandse-overheid (1003). pki voor de overheid (1). cp (2). domein 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 conformiteitcertificaat af aan elke fabrikant die en voor elk – door die fabrikant te produceren – type apparaat dat aan het normenkader conformeert (voor het uitvoeren van conformiteitbeoordelingen en het afgeven van conformiteitcertificaten kan de kadersteller een toezichthouder aanwijzen). Hiermee worden (gegadigde) apparaat-fabrikanten in staat gesteld aan het normenkader conformerende apparaten op de markt te brengen.

[4] Binnen de PKI voor de overheid is er sprake van een structuur c.q. root gebaseerd op het SHA-1 algoritme en een root gebaseerd op het SHA-256 algoritme. Verder is er, zowel voor de SHA-1 root als ook de SHA-256 root, een indeling gemaakt in verschillende domeinen. Voor de SHA-1 root is sprake van de domeinen Overheid/Bedrijven (deze twee domeinen zijn in de loop van de tijd samengevoegd) en Burger. Voor de SHA-256 root is er sprake van een domein Organisatie, een domein Burger en een domein Autonome Apparaten.

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 CSP 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] Authenticiteitcertificaten, 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.

[OID 2.16.528.1.1003.1.2.6.2] Vertrouwelijkheidcertificaten, 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

RFC 3647	2.1 Elektronische opslagplaats
Nummer	1
ETSI	NCP+ 7.3.5.e.ii
PKIo	De maximale tijdsduur, waarbinnen de beschikbaarheid van de dissemination service moet worden hersteld, is gesteld op 24 uur.

RFC 3647	2.1 Elektronische opslagplaats
Nummer	2
ETSI	NCP+ 7.3.1.c NCP+ 7.3.4.b NCP+ 7.3.5.f
PKIo	Het is verplicht dat er een elektronische opslagplaats is waar de informatie zoals genoemd in [2.2] wordt gepubliceerd. Deze opslagplaats kan worden beheerd door de CSP of door een afzonderlijke organisatie.
Opmerking	De informatie die moet worden gepubliceerd is opgenomen in ETSI TS 102 042. De relevante artikelen waar de informatie is gespecificeerd zijn te vinden in de verwijzingsmatrix in bijlage B.

2.2 Publicatie van CSP-informatie

RFC 3647	2.2 Publicatie van CSP-informatie
Nummer	1
ETSI	NCP+ 7.3.1.c
PKIo	Het CPS dient in het Nederlands te zijn opgesteld.

RFC 3647	2.2 Publicatie van CSP-informatie
Nummer	2
ETSI	NCP+ 5.2.b
PKIo	De CSP dient de OID's van de toegepaste CP's op te nemen in het CPS.

RFC 3647	2.2 Publicatie van CSP-informatie
Nummer	3
ETSI	NCP+ 7.3.1.c
PKIo	Alle informatie zal in het Nederlands beschikbaar moeten zijn.

2.4 Toegang tot gepubliceerde informatie

RFC 3647	2.4 Toegang tot gepubliceerde informatie
Nummer	1
ETSI	NCP+ 7.1.d.1
PKIo	Het CPS van een Certification Service Provider binnen de PKIoverheid dient voor een ieder raadpleegbaar te zijn.
PKIo-AA opmerking	Met een ieder wordt bedoeld dat, naast de in § 1.3 genoemde gebruikersgemeenschap, iedere potentiële vertrouwende partij het CPS moet kunnen raadplegen.

3 Identificatie en authenticatie

3.1 Naamgeving

RFC 3647	3.1.1 Soorten naamformaten
Nummer	1
ETSI	NCP+ 7.3.3.a NCP+ 7.3.6.i
PKIo-AA	De CSP dient te voldoen aan de eisen die aan naamformaten zijn gesteld in het Programma van Eisen, Programma van Eisen -bijlage A Certificaat- en CRL-profielen.
Opmerking	In bijlage A is een toelichting op de verschillende profielen opgenomen.

3.2 Initiële identiteitsvalidatie

RFC 3647	3.2.2 Authenticatie van organisatorische entiteit
Nummer	1
ETSI	NCP+ 7.3.1.g
PKIo-AA	De CSP dient te verifiëren dat de abonnee een bestaande organisatie is.

RFC 3647	3.2.2 Authenticatie van organisatorische entiteit
Nummer	2
ETSI	NCP+ 7.3.1.g
PKIo-AA	De CSP dient te verifiëren dat de door de abonnee aangemelde organisatienaam die in het certificaat wordt opgenomen juist en volledig is.

RFC 3647	3.2.3 Authenticatie van persoonlijke identiteit
Nummer	1
ETSI	NCP+ 7.3.1.e
PKIo-AA	De CSP dient overeenkomstig Nederlandse wet- en regelgeving de identiteit en, indien van toepassing, specifieke eigenschappen te controleren van de certificaatbeheerder. Bewijs van de identiteit dient te worden gecontroleerd aan de hand van fysieke verschijning van de persoon zelf, hetzij direct hetzij indirect, met behulp van middelen waarmee dezelfde zekerheid kan worden verkregen als bij persoonlijke aanwezigheid. Het bewijs van identiteit kan op

	papier dan wel langs elektronische weg worden aangeleverd.

RFC 3647	3.2.3 Authenticatie van persoonlijke identiteit
Nummer	2
ETSI	NCP+ 7.3.1.e
PKIo-AA	Ter verbijzondering van het in 3.2.3-1 gestelde, geldt dat de identiteit van de certificaatbeheerder slechts kan worden vastgesteld met de bij artikel 1 van de Wet op de identificatieplicht aangewezen geldige documenten. De CSP dient de geldigheid en echtheid hiervan te controleren.
Opmerking	Indien de controle van de persoonlijke identiteit van de certificaatbeheerder is uitgevoerd bij de aanvraag van een certificaat in het Domein Overheid, Bedrijven en Organisatie, dan wordt de controle van de identiteit van de certificaatbeheerder onder deze CP vermeend plaats te hebben gevonden.

RFC 3647	3.2.3 Authenticatie van persoonlijke identiteit
Nummer	3
ETSI	NCP+ 7.3.1.g
PKIo-AA	De certificaatbeheerder is een persoon van wie de identiteit dient vastgesteld te worden in samenhang met een organisatorische entiteit. Er dient bewijs te worden overlegd van: • volledige naam, met inbegrip van achternaam, eerste voornaam, initialen of overige voorna(a)m(en) (indien van toepassing) en tussenvoegsels (indien van toepassing); • geboortedatum en -plaats, een nationaal passend registratienummer, of andere eigenschappen van de certificaatbeheerder die kunnen worden gebruikt om, voor zover mogelijk, de persoon van andere personen met dezelfde naam te kunnen onderscheiden; • bewijs dat de certificaatbeheerder gerechtigd is voor een certificaathouder een certificaat te ontvangen namens de rechtspersoon of andere organisatorische entiteit.

RFC 3647	3.2.5 Autorisatie van de certificaathouder
Nummer	1
ETSI	NCP+ 7.3.1.d NCP+ 7.3.1.h NCP+ 7.3.1.i
PKIo-AA	De CSP dient te controleren dat: • het bewijs, dat de certificaathouder geautoriseerd is via de abonnee om een certificaat te ontvangen, authentiek is;

	• de certificaatbeheerder toestemming heeft verkregen van de abonnee om aan hem opgedragen handelingen uit te voeren (ingeval de certificaat-beheerder het registratieproces uitvoert);
	• het aangevraagde certificaat in combinatie met de in de certificaathouder (apparaat) permanent opgeslagen gegevens voldoende informatie bevat-ten om het volgende eenduidig te kunnen achterhalen:
	  ○ de identiteit van het apparaat (bijv. fabrikant en serienummer);
	  ○ het bewijs dat het apparaat en diens productieproces conformeren aan het door de kadersteller vastgelegde normenkader.

Opmerking	De "certificaatbeheerder" die handelingen overneemt van de certificaathouder behoeft niet noodzakelijkerwijs dezelfde persoon te zijn als degene die de certificaathouder (het apparaat) produceert of gebruikt. Tevens is het toegestaan dat de kennis van de activeringsgegevens van het sleutelmateriaal (bijvoorbeeld PIN) door verschillende personen wordt gedeeld als de inrichting van het beheer dat vereist. Echter, aangeraden wordt het aantal personen dat kennis heeft van de PIN zo beperkt mogelijk te houden. Ook is het verstandig maatregelen te treffen die de toegang tot de PIN beperken. Een voorbeeld hiervan is het plaatsen van de PIN in een kluis waartoe slechts geautoriseerde personen in bepaalde situaties toegang kunnen krijgen.

RFC 3647	3.2.5 Autorisatie van de certificaathouder
Nummer	2
ETSI	NCP+ 6.2.h
PKIo-AA	In de overeenkomst die de CSP sluit met de abonnee dient te zijn opgenomen dat de abonnee de verantwoordelijkheid heeft om, als er relevante wijzigingen plaats hebben in de relatie tussen abonnee en certificaatbeheerder en/of certificaathouder (autonoom apparaat), deze onmiddellijk aan de CSP door te geven. Wanneer het apparaat uitvalt, dient dit door middel van een intrekkingverzoek te geschieden.

3.3 Identificatie en authenticatie bij vernieuwing van het certificaat

RFC 3647	3.3.1 Identificatie en authenticatie bij routinematige vernieuwing van het certi-ficaat
Nummer	1
ETSI	NCP+ 7.3.2.d
PKIo	[OID 2.16.528.1.1003.1.2.6.2] NCP+ 7.3.2.d is van toepassing.
Opmerking	In NCP+ 7.3.2.d. wordt aangegeven onder welke voorwaarden hercertificering van vertrouwelijkheidsleutels is toegestaan.

RFC 3647	3.3.1 Identificatie en authenticatie bij routinematige vernieuwing van het certi-

	ficaat
Nummer	2
ETSI	NCP+ 7.3.2.d
PKIo	[OID 2.16.528.1.1003.1.2.6.1] en [OID 2.16.528.1.1003.1.2.6.3] NCP+ 7.3.2.d is niet van toepassing.
Opmerking	De eis houdt in dat certificaatvernieuwing zonder vernieuwing van de sleutels niet is toegestaan voor het authenticiteit- en combinatiecertificaat.

RFC 3647	3.3.1 Identificatie en authenticatie bij routinematige vernieuwing van het certificaat
Nummer	3
ETSI	NCP+ 7.3.2.a NCP+ 7.3.2.c
PKIo	Het vernieuwen van certificaten dient altijd vooraf te zijn gegaan door een controle of aan alle eisen die onder [3.1] en [3.2] zijn gesteld, is voldaan.
Opmerking	De relevante artikelen waarin de eisen zijn gespecificeerd zijn te vinden in de verwijzingsmatrix in bijlage B.

RFC 3647	3.3.2 Identificatie en authenticatie bij vernieuwing van het certificaat na intrekking
Nummer	1
ETSI	NCP+ 7.3.2.d
PKIo	Na intrekking van het certificaat mogen de desbetreffende sleutels niet opnieuw worden gecertificeerd. NCP+ 7.3.2.d is niet van toepassing.

4 Operationele eisen certificaatlevenscyclus

4.4 Acceptatie van certificaten

RFC 3647	4.4.1 Activiteiten bij acceptatie van certificaten
Nummer	1
ETSI	NCP+ 7.3.1.m
PKIo-AA	Na uitgifte van een certificaat, dient de certificaathouder of certificaatbeheerder expliciet de overhandiging van het sleutelmateriaal behorend bij het certificaat aan de CSP te bevestigen.

4.5 Sleutelpaar en certificaatgebruik

RFC 3647	4.5.2 Gebruik van publieke sleutel en certificaat door vertrouwende partij
Nummer	1
ETSI	NCP+ 6.3.a
PKIo	In de gebruikersvoorwaarden die aan de vertrouwende partijen ter beschikking worden gesteld dient te worden opgenomen dat de vertrouwende partij wordt geacht de geldigheid te controleren van de volledige keten van certificaten tot aan de bron (stamcertificaat) waarop wordt vertrouwd. Daarnaast dient te worden opgenomen dat de abonnee zelf zorg draagt voor een tijdige vervanging in het geval van een naderende afloop geldigheid, en noodvervanging in geval van compromittatie en/of andere soorten van calamiteiten met betrekking tot het certificaat of van bovenliggende certificaten. Van de abonnee wordt verwacht dat hij zelf adequate maatregelen neemt om de continuïteit van het gebruik van certificaten te borgen.
Opmerking	De geldigheid van een certificaat dient niet verward te worden met de bevoegdheid van de certificaathouder een bepaalde transactie namens een organisatie te doen. De PKI voor de overheid regelt geen autorisatie; daarvan moet een vertrouwende partij zichzelf op andere wijze overtuigen.

4.9 Intrekking en opschorting van certificaten

RFC 3647	4.9.1 Omstandigheden die leiden tot intrekking
Nummer	1
ETSI	NCP+ 7.3.6.a
PKIo-AA	Certificaten zullen worden ingetrokken wanneer: • de abonnee aangeeft dat het oorspronkelijke verzoek voor een certificaat niet was toegestaan en de abonnee verleent met terugwerkende kracht ook geen toestemming; • de CSP beschikt over voldoende bewijs dat de privésleutel van de

	abonnee (die overeenkomt met de publieke sleutel in het certificaat) is aangetast of er is het vermoeden van compromittatie, of er is sprake van inherente beveiligingszwakheid, of dat het certificaat op een andere wijze is misbruikt. Een sleutel wordt als aangetast beschouwd in geval van ongeautoriseerde toegang of vermoede ongeautoriseerde toegang tot de private sleutel, verloren of vermoedelijk verloren private sleutel of SUD, gestolen of vermoedelijk gestolen sleutel of SUD of vernietigde sleutel of SUD; • een abonnee niet aan zijn verplichtingen voldoet zoals verwoord in deze CP of het bijbehorende CPS van de CSP of de overeenkomst die de CSP met de abonnee heeft afgesloten; • de CSP op de hoogte wordt gesteld of anderszins zich bewust wordt dat het gebruik van de domeinnaam in het certificaat niet langer wettelijk toegestaan is (b.v. door een uitspraak van een rechter); • de CSP op de hoogte wordt gesteld of anderszins zich bewust wordt van een wezenlijke verandering in de informatie, die in het certificaat staat. Voorbeeld daarvan is: verandering van de naam van de certificaathouder (service); • de CSP bepaald dat het certificaat niet is uitgegeven in overeenstemming met deze CP of het bijbehorende CPS van de CSP of de overeenkomst die de CSP met de abonnee heeft gesloten; • de CSP bepaald dat informatie in het certificaat niet juist of misleidend is; • de CSP haar werkzaamheden staakt en de CRL en OCSP dienstverlening niet wordt overgenomen door een andere CSP; • De PA van PKIoverheid vaststelt dat de technische inhoud van het certificaat een onverantwoord risico met zich meebrengt voor abonnees, vertrouwende partijen en derden (b.v. browserpartijen).
Opmerking	Daarnaast kunnen certificaten worden ingetrokken als maatregel om een calamiteit te voorkomen, c.q. te bestrijden. Als calamiteit wordt zeker de aantasting of vermeende aantasting van de private sleutel van de CSP waarmee certificaten worden ondertekend, beschouwd.

RFC 3647	4.9.2 Wie mag een verzoek tot intrekking doen
Nummer	1
ETSI	NCP+ 7.3.6.a
PKIo-AA	De volgende partijen mogen een verzoek tot intrekking van een eindgebruikercertificaat doen: ▪ de certificaatbeheerder; ▪ de abonnee; ▪ de CSP; ▪ iedere andere, naar het oordeel van de kadersteller, belanghebbende partij/persoon.

RFC 3647	4.9.3 Procedure voor een verzoek tot intrekking
Nummer	1

ETSI	NCP+ 7.3.6.a
PKIo	De CSP mag additionele eisen stellen aan een intrekkingsverzoek. Deze additionele eisen moeten in de CPS van de CSP worden opgenomen.

RFC 3647	4.9.3 Procedure voor een verzoek tot intrekking
Nummer	2
ETSI	NCP+ 7.3.6
PKIo	De maximale tijdsduur, waarbinnen de beschikbaarheid van de revocation management services moet worden hersteld, is gesteld op vier uur.

RFC 3647	4.9.3 Procedure voor een verzoek tot intrekking
Nummer	3
ETSI	NCP+ 7.3.6.a
PKIo	De CSP moet de beweegreden voor de intrekking van een certificaat vastleggen.

RFC 3647	4.9.3 Procedure voor een verzoek tot intrekking
Nummer	4
ETSI	NCP+ 7.3.6.j (en BEH artikel 2 lid 1l)
PKIo	De CSP moet in ieder geval gebruik maken van een CRL om de certificaatstatus informatie beschikbaar te stellen.

RFC 3647	4.9.3 Procedure voor een verzoek tot intrekking
Nummer	5
ETSI	NCP+ 7.3.6
PKIo	De CSP moet de procedure voor intrekking publiceren en in die publicatie eenduidige definities geven van de volgende – in chronologische volgorde opgesomde – deelprocessen: • De ontvangst van een verzoek tot intrekking; • De identificatie en authenticatie van degene die het verzoek tot intrekking indient; • Het betrouwbaarheidsonderzoek met betrekking tot het verzoek tot intrekking;

	• De verwerking van (het betrouwbare verzoek tot) de intrekking; • De publicatie van de (verwerkte) intrekking. De definitie van elk deelproces dient minimaal de voorwaarden voor het doorlopen van het deelproces en de in dat deelproces te registreren gegevens te bevatten.

RFC 3647	4.9.5 Tijdsduur voor verwerking intrekkingsverzoek
Nummer	1
ETSI	NCP+ 7.3.6.a
PKIo	De maximale vertraging tussen een intrekkingsverzoek of intrek-kingsrapportage en de wijziging van de revocation status information, die voor alle vertrouwende partijen beschikbaar is, is gesteld op vier uur.
Opmerking	Deze eis is van toepassing op alle typen certificaat statusinformatie.

RFC 3647	4.9.6 Controlevoorwaarden bij raadplegen certificaat statusinformatie
Nummer	1
ETSI	NCP+ 6.3.a
PKIo	Een eindgebruiker die de certificaat statusinformatie raadpleegt, dient de authenticiteit van deze informatie te verifiëren door de elektronische handtekening waarmee de informatie is getekend en het bijbehorende certificatiepad te controleren.

RFC 3647	4.9.6 Controlevoorwaarden bij raadplegen certificaat statusinformatie
Nummer	2
ETSI	NCP+ 6.3.a
PKIo	De in [4.9.6-1] genoemde verplichting dient door de CSP te worden opgenomen in de gebruikersvoorwaarden die ter beschikking worden gesteld aan de vertrouwende partijen.

RFC 3647	4.9.7 CRL-uitgiftefrequentie
Nummer	1
ETSI	NCP+ 7.3.6
PKIo	De CSP moet de CRL ten behoeve van eindgebruiker certificaten tenminste een

	keer in de 7 kalenderdagen bijwerken en opnieuw uitgeven en de datum van het veld " Volgende update" mag niet meer dan 10 kalenderdagen zijn na de datum van het veld "Ingangsdatum".

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	1
ETSI	NCP+ 7.3.6.j
PKIo	Ondersteuning van de revocation management services van de CSP met het Online Certificate Status Protocol (OCSP) kan alleen plaatsvinden na expliciete toestemming van de PA.

RFC 3647	4.9.13 Omstandigheden die leiden tot opschorting
Nummer	1
ETSI	NCP+ 7.3.6.e
PKIo	Het is niet toegestaan om certificaatopschorting te ondersteunen.

4.10 Certificaat statusservice

RFC 3647	4.10.2 Beschikbaarheid certificaat statusservice
Nummer	1
ETSI	NCP+ 7.3.6.j
PKIo	De maximale tijdsduur, waarbinnen de beschikbaarheid van de revocation status information moet worden hersteld, is gesteld op vier uur.

5 Management, operationele en fysieke beveiligingsmaatregelen

5.2 Procedurele beveiliging

RFC 3647	5.2.4 Rollen die functiescheiding behoeven
Nummer	1
ETSI	NCP+ 7.4.3.d en 7.4.3.h
PKIo	De CSP dient functiescheiding te handhaven tussen tenminste de volgende functies: • Security officer De security officer ziet toe op de implementatie en naleving van de vastgestelde beveiligingsrichtlijnen. • Systeem auditor De systeem auditor vervult een toezichthoudende rol en geeft een onafhankelijk oordeel over de wijze waarop de bedrijfsprocessen zijn ingericht en over de wijze waarop aan de eisen ten aanzien van de betrouwbaarheid is voldaan. • Systeembeheerder De systeembeheerder beheert de CSP-systemen, waarbij het installeren, configureren en onderhouden van de systemen is inbegrepen. • CSP-operators De CSP-operators zijn verantwoordelijk voor het dagelijks bedienen van de CSP-systemen voor onder meer registratie, het genereren van certificaten, het leveren van een SSCD aan de certificaathouder en revocation management.
Opmerking	De hierboven genoemde functieomschrijvingen zijn niet limitatief en het staat de CSP vrij om binnen de eisen van functiescheiding de omschrijving uit te breiden of de functies verder op te splitsen of te verdelen tussen andere vertrouwde functionarissen.

RFC 3647	5.2.4 Rollen die functiescheiding behoeven
Nummer	2
ETSI	NCP+ 7.4.3.d en 7.4.3.h
PKIo	De CSP dient functiescheiding te handhaven tussen medewerkers die de uitgifte van een certificaat controleren en medewerkers die de uitgifte van een certificaat goedkeuren.

RFC 3647	5.2.5 Beheer en beveiliging
Nummer	1

ETSI	NCP+ 7.4.1.a NCP+ 7.4.5
PKIo	De CSP moet de risicoanalyse minimaal jaarlijks, of als de PA daartoe opdracht geeft, of het NCSC daartoe advies geeft, opnieuw uitvoeren. De risicoanalyse moet alle PKIoverheid processen raken die onder de verantwoordelijkheid van de CSP vallen. Op basis van de risicoanalyse moet de CSP een informatiebeveiligingsplan ontwikkelen, implementeren, onderhouden, handhaven en evalueren. Dit plan beschrijft een samenhangend geheel van passende administratieve, organisatorische, technische en fysieke maatregelen en procedures waarmee de CSP de beschikbaarheid, exclusiviteit en integriteit van alle PKIoverheid processen, aanvragen en de gegevens die daarvoor worden gebruikt, waarborgt.

RFC 3647	5.2.5 Beheer en beveiliging
Nummer	2
ETSI	NCP+ 7.4.1.b
PKIo	Naast een audit uitgevoerd door een geaccrediteerd auditor MAG de CSP een audit uitvoeren bij zijn externe leveranciers van PKIoverheid kerndiensten om zich ervan te verwittigen dat deze leveranciers de relevante eisen van het PVE van PKIoverheid conform de wensen van de CSP en rekening houdend met zijn bedrijfsdoelstellingen, -processen en -infrastructuur hebben geïmplementeerd en geoperationaliseerd. De CSP is vrij in de keuze om zelf een eigen audit uit te (laten) voeren dan wel gebruik te gaan maken van reeds bestaande audit resultaten zoals die van de formele certificeringsaudits, de diverse interne en externe audits, Third party mededelingen (TPM's) en (buitenlandse) compliancy rapportages. Ook is de CSP gerechtigd om inzage te verkrijgen in het onderliggende bewijsmateriaal zoals audit dossiers en overige, al dan niet systeem-, documentatie. Uiteraard beperkt zich het bovenstaande tot de bij de leveranciers gehoste CSP-processen, -systemen en –infrastructuur voor PKIo kerndiensten.

5.3 Personele beveiliging

RFC 3647	5.3 Geheimhoudingsverklaring
Nummer	1
ETSI	NCP+ 7.4.3.e
PKIo	Omdat het openbaar worden van vertrouwelijke informatie grote gevolgen kan hebben (o.a. voor de betrouwbaarheid) moet de CSP zich inspannen om er voor te zorgen dat vertrouwelijke informatie vertrouwelijk behandeld wordt en vertrouwelijk blijft. Eén van de inspanningen die hiervoor geleverd

	moet worden is het laten tekenen van een geheimhoudingsverklaring door personeelsleden en ingehuurde derden.

RFC 3647	5.3.2 Antecendentenonderzoek
Nummer	1
ETSI	7.4.3-j
PKIo	Voor het inschakelen van een persoon bij één of meerdere kerndiensten van PKIoverheid, ZAL de CSP of externe leverancier die een deel van deze werkzaamheden verricht de identiteit en de betrouwbaarheid van deze werknemer verifiëren.

5.4 Procedures ten behoeve van beveiligingsaudits

RFC 3647	5.4.1 Vastlegging van gebeurtenissen
Nummer	1
ETSI	NCP+ 7.4.5.j

PKIo	Logging dient plaats te vinden op minimaal:
	• Routers, firewalls en netwerk systeem componenten;
	• Database activiteiten en events;
	• Transacties;
	• Operating systemen;
	• Access control systemen;
	• Mail servers.
	
	De CSP dient minimaal de volgende events te loggen:
	• CA key life cycle management;
	• Certificate life cycle management;
	• Bedreigingen en risico's zoals:
	  • Succesvolle en niet succesvolle aanvallen PKI systeem;
	  • Activiteiten van medewerkers op het PKI systeem;
	  • Lezen, schrijven en verwijderen van gegevens;
	  • Profiel wijzigingen (Access Management);
	  • Systeem uitval, hardware uitval en andere abnormaliteiten;
	  • Firewall en router activiteiten;
	  • Betreden van- en vertrekken uit de ruimte van de CA.
	
	De log bestanden moeten minimaal het volgende registreren:
	• Bron adressen (IP adressen indien voorhanden);
	• Doel adressen (IP adressen indien voorhanden);
	• Tijd en datum;
	• Gebruikers ID's (indien voorhanden);
	• Naam van de gebeurtenis;
	• Beschrijving van de gebeurtenis.

Opmerking	Op basis van een risicoanalyse bepaalt de CSP zelf welke gegevens zij op-

	slaat.

RFC 3647	5.4.3 Bewaartermijn voor logbestanden
Nummer	1
ETSI	NCP+ 7.4.11.e
PKIo	De CSP moet logbestanden voor gebeurtenissen met betrekking tot: • CA key life cycle management en; • Certificate life cycle management; 7 jaar bewaren en daarna verwijderen. De CSP moet logbestanden voor gebeurtenissen met betrekking tot: • Bedreigingen en risico's; 18 maanden bewaren en daarna verwijderen. De logbestanden moeten zodanig worden opgeslagen, dat de integriteit en toegankelijkheid van de data gewaarborgd is.

5.5 Archivering van documenten

RFC 3647	5.5.1 Vastlegging van gebeurtenissen
Nummer	1
ETSI	NCP+ 7.3.1.j
PKIo-AA	De CSP dient alle informatie op te slaan die is gebruikt voor het verifiëren van de identiteit van de abonnee, certificaatbeheerder en indieners van verzoeken tot intrekking, met inbegrip van referentienummers van de documentatie die is gebruikt voor verificatie, evenals beperkingen ten aanzien van de geldigheid.

RFC 3647	5.5.2 Bewaartermijn archief
Nummer	2
ETSI	NCP+ 7.4.11.e
PKIo	Geen PKIo-eis van toepassing, alleen een opmerking.
Opmerking	Op verzoek van de rechthebbende kan worden overeengekomen dat de gewenste informatie langer door de CSP wordt bewaard. Dit is echter geen verplichting voor de CSP.

5.7 Aantasting en continuïteit

RFC 3647	5.7.1 Procedures voor afhandeling incidenten en aantasting
Nummer	1
ETSI	NCP+ 7.4.8.f
PKIo	De CSP dient de PA, het NCSC en de auditor onmiddellijk op de hoogte te stellen van een security breach en/of calamiteit, na analyse en vaststelling en dient de PA, het NCSC en de auditor van het verdere verloop op de hoogte te houden.
Opmerking	Onder security breach wordt in de PKIoverheid context verstaan: Een inbreuk op de CSP kerndiensten: registration service, certificate generation service, subject device provisioning service, dissemination service, revocation management service en revocation status service. Dit is in ieder geval maar niet limitatief: • het ongeoorloofd uitschakelen of onbruikbaar maken van een kerndienst; • ongeautoriseerde toegang tot een kerndienst t.b.v. het afluisteren, onderscheppen en of veranderen van berichtenverkeer; • ongeautoriseerde toegang tot een kerndienst t.b.v. het ongeoorloofd verwijderen, wijzigen of aanpassen van computergegevens.

RFC 3647	5.7.1 Procedures voor afhandeling incidenten en aantasting
Nummer	2
ETSI	NCP+ 7.4.8.e
PKIo	De CSP informeert de PA onmiddellijk over de risico's, gevaren of gebeurtenissen die op enigerlei wijze de betrouwbaarheid van de dienstverlening en/of het imago van de PKI voor de overheid kunnen bedreigen of beïnvloeden. Hieronder vallen in ieder geval ook, maar niet uitsluitend, security breaches en/of calamiteiten met betrekking tot andere, door de CSP uitgevoerde, PKI diensten, niet zijnde PKIoverheid.

RFC 3647	5.7.4 Continuïteit van de bedrijfsvoering na calamiteit
Nummer	1
ETSI	NCP+ 7.4.8.a
PKIo	De CSP moet een business continuity plan (BCP) opstellen voor minimaal de kerndiensten 'dissemination service', 'revocation management service' en 'revocation status service' met als doel, in het geval zich een security breach of calamiteit voordoet, het informeren en redelijkerwijs beschermen en continueren van de CSP dienstverlening ten behoeve van abonnees, vertrouwende partijen en derden (waaronder browserpartijen). De CSP moet het BCP jaarlijks testen, beoordelen en actualiseren. Het BCP moet in ieder geval de volgende zaken beschrijven:

	▪ Eisen aan inwerkingtreding; ▪ Noodprocedure / uitwijkprocedure; ▪ Eisen aan herstarten CSP dienstverlening; ▪ Onderhoudsschema en testplan dat voorziet in het jaarlijks testen, beoordelen en actualiseren van het BCP; ▪ Bepalingen over het onder de aandacht brengen van het belang van business continuity; ▪ Taken, verantwoordelijkheden en bevoegdheden van betrokken actoren; ▪ Beoogde hersteltijd c.q. Recovery Time Objective (RTO); ▪ Vastleggen van de frequentie van back-ups van kritische bedrijfsinformatie en software; ▪ Vastleggen van de afstand van de uitwijkfaciliteit tot de hoofdvestiging van de CSP; en ▪ Vastleggen van procedures voor het beveiligen van de faciliteit gedurende de periode na een security breach of calamiteit en voor de inrichting van een beveiligde omgeving bij de hoofdvestiging of de uitwijkfaciliteit.

6 Technische beveiliging

6.1 Genereren en installeren van sleutelparen

RFC 3647	6.1.1 Genereren van sleutelparen voor de CSP sub CA
Nummer	1
ETSI	NCP+ 7.2.1.c en 7.2.1.d
PKIo	Het algoritme en de lengte van de cryptografische sleutels die worden gebruikt voor het genereren van de sleutels voor de CSP sub CA dienen te voldoen aan de eisen, die daaraan zijn gesteld in de lijst van aanbevolen cryptografische algoritmes en sleutellengtes, zoals gedefinieerd in ETSI TS 102 176-1.
Opmerking	Hoewel in ETSI TS 102 176 over aanbevolen algoritmes en sleutellengtes wordt gesproken, worden deze binnen de PKI voor overheid verplicht gesteld. Verzoeken voor gebruik van andere algoritmes dienen, voorzien van een motivatie te worden gedaan bij de PA van de PKI voor de overheid.

RFC 3647	6.1.1 Genereren van sleutelparen van de certificaathouders
Nummer	2
ETSI	NCP+ 7.2.8.c
PKIo	Het genereren van de sleutels van certificaathouders dient te geschieden in een middel dat voldoet aan de eisen genoemd in {7} CWA 14169 Secure signature-creation devices "EAL 4+" of gelijkwaardige beveiligingscriteria.

RFC 3647	6.1.1 Genereren van sleutelparen van de certificaathouders
Nummer	3
ETSI	NCP+ 7.2.8.a en 7.2.8.b
PKIo	Het algoritme en de lengte van de cryptografische sleutels dat de CSP gebruikt voor het genereren van de sleutels van certificaathouders dient te voldoen aan de eisen, die daaraan zijn gesteld in de lijst van cryptografische algoritmes en sleutellengtes, zoals gedefinieerd in ETSI TS 102 176-1.
Opmerking	Hoewel in ETSI TS 102 176 over aanbevolen algoritmes en sleutellengtes wordt gesproken, worden deze binnen de PKI voor overheid verplicht gesteld. Verzoeken voor gebruik van andere algoritmes dienen, voorzien van een motivatie te worden gedaan bij de PA van de PKI voor de overheid.

RFC 3647	6.1.2 Overdracht van private sleutel en SUD aan certificaathouder

Nummer	1
ETSI	NCP+ 7.2.8.d en 7.2.8.e
PKIo-AA	[OID 2.16.528.1.1003.1.2.6.2] Indien het niet is vereist dat de CSP een kopie van de private sleutel van de certificaathouder bewaart (Key escrow) moet, nadat de private sleutel op een zodanige wijze is geleverd aan de certificaathouder of certificaatbeheerder dat de vertrouwelijkheid en integriteit van de sleutel niet is aangetast, alleen de certificaathouder of certificaatbeheerder toegang hebben tot de private sleutel. Elke kopie van de private sleutel van de certificaathouder, in bezit bij de CSP, dient te worden vernietigd.
Opmerking	Deze tekst komt overeen met NCP+ 7.2.8.e, maar is integraal opgenomen omdat deze eis alleen van toepassing is op het vertrouwelijkheidcertificaat.

RFC 3647	6.1.5 Sleutellengten van private sleutels van certificaathouders
Nummer	1
ETSI	NCP+ 7.2.8.b
PKIo	De lengte van de cryptografische sleutels van de certificaathouders dient te voldoen aan de eisen, die daaraan zijn gesteld in de lijst van cryptografische algoritmes en sleutellengtes, zoals gedefinieerd in ETSI TS 102 176-1.
Opmerking	Hoewel in ETSI TS 102 176 over aanbevolen algoritmes en sleutellengtes wordt gesproken, worden deze binnen de PKI voor overheid verplicht gesteld. Verzoeken voor gebruik van andere algoritmes dienen, voorzien van een motivatie te worden gedaan bij de PA van de PKI voor de overheid.

RFC 3647	6.1.7 Doelen van sleutelgebruik (zoals bedoeld in X.509 v3)
Nummer	1
ETSI	NCP+ 7.2.5
PKIo	De sleutelgebruiksextensie (key usage) in X.509 v3 certificaten (RFC5280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile) definieert het doel van het gebruik van de sleutel vervat in het certificaat. De CSP dient het gebruik van sleutels in het certificaat aan te geven, conform de eisen die daaraan zijn gesteld in bijlage A 'Certificaat- en CRL-profielen' van dit CP.

6.2 Private sleutelbescherming en cryptografische module engineering beheersmaatregelen

RFC 3647	6.2.3 Escrow van private sleutels van certificaathouders
Nummer	1

ETSI	NCP+ 7.2.4.a
PKIo	[OID 2.16.528.1.1003.1.2.6.1] en OID [2.16.528.1.1003.1.2.6.3] Escrow door de CSP is niet toegestaan voor de private sleutels van het authenticiteitcertificaat en combinatiecertificaat.

RFC 3647	6.2.3 Escrow van private sleutels van certificaathouders
Nummer	2
ETSI	NCP+ 7.2.4.b
PKIo	[OID 2.16.528.1.1003.1.2.6.2] De geautoriseerde personen, die toegang kunnen krijgen tot de door de CSP in escrow gehouden private sleutel van het vertrouwelijkheidcertificaat (indien van toepassing), moeten zich identificeren aan de hand van de bij artikel 1 van de Wet op de identificatieplicht aangewezen geldige documenten of een geldig gekwalificeerd certificaat (beperkt tot het PKIoverheid handtekeningcertificaat of gelijkwaardig).

RFC 3647	6.2.3 Escrow van private sleutels van certificaathouders
Nummer	3
ETSI	NCP+ 7.2.4.b
PKIo	[OID 2.16.528.1.1003.1.2.6.2] De CSP dient in de CPS te beschrijven welke partijen en onder welke voorwaarden, toegang tot de in escrow gehouden private sleutel van het vertrouwelijkheidcertificaat kunnen krijgen.

RFC 3647	6.2.4.2 Back-up van private sleutels van certificaathouders
Nummer	1
ETSI	NCP+ 7.2.4.a en 7.2.8.e
PKIo	Back-up door de CSP van de private sleutels van de certificaathouders, is niet toegestaan.

RFC 3647	6.2.5 Archivering van private sleutels van certificaathouders
Nummer	1
ETSI	NCP+ 7.2.4.a en 7.2.8.e
PKIo	Archivering door de CSP van de private sleutels van de certificaathouders, is niet toegestaan

RFC 3647	6.2.11 Eisen voor veilige middelen voor het aanmaken van elektronische hand-tekeningen
Nummer	1
ETSI	NCP+ 3.1
PKIo	Door de CSP uitgegeven of aanbevolen veilige middelen voor opslag van sleutels (SUD's) moeten voldoen aan de eisen gesteld in document {7} CWA 14169 Secure signature-creation devices "EAL 4+".

RFC 3647	6.2.11 Eisen voor veilige middelen voor het aanmaken van elektronische hand-tekeningen
Nummer	2
ETSI	NCP+ 3.1
PKIo	In plaats van conformiteit aan CWA 14169 aan te tonen mogen CSP's SUD's uitgeven of aanbevelen die volgens een ander protection profile zijn gecertificeerd tegen de Common Criteria (ISO/IEC 15408) op niveau EAL4+ of die een vergelijkbaar betrouwbaarheidsniveau hebben. Dit dient te worden vastgesteld door een testlaboratorium dat geaccrediteerd is voor het uitvoeren van Common Criteria evaluaties.

6.3 Andere aspecten van sleutelpaarmanagement

RFC 3647	6.3.2 Gebruiksduur voor certificaten en publieke en private sleutels
Nummer	1
ETSI	NCP+ 7.2.6
PKIo	Private sleutels die door een certificaathouder worden gebruikt en die zijn uitgegeven onder verantwoordelijkheid van deze CP dienen niet langer dan tien jaar te worden gebruikt. De certificaten, die zijn uitgegeven onder de verantwoordelijkheid van deze CP, dienen een geldigheid te hebben van niet meer dan tien jaar.
Opmerking	De CSP's binnen het domein Autonome Apparaten van de PKI voor de overheid mogen pas certificaten uitgeven met een maximale geldigheidsduur van tien jaar nadat de PA hiervoor expliciet toestemming heeft gegeven.

RFC 3647	6.3.2 Gebruiksduur voor certificaten en publieke en private sleutels
Nummer	2

ETSI	NCP+ 7.2.6
PKIo	Op het moment van uitgifte van een eindgebruikercertificaat dient de resterende geldigheidsduur van het bovenliggende CSP-certificaat langer te zijn dan de beoogde geldigheidsduur van het eindgebruikercertificaat.

6.4 Activeringsgegevens

RFC 3647	6.4.1 Genereren en installeren van activeringsgegevens
Nummer	1
ETSI	NCP+ 7.2.9.d
PKIo-AA	De CSP verbindt activeringsgegevens aan het gebruik van een SUD, ter bescherming van de private sleutels van de certificaathouders.
Opmerking	De eisen waaraan de activeringsgegevens (bijvoorbeeld de PIN-code) moet voldoen, kunnen door de CSP's zelf worden bepaald op basis van bijvoorbeeld een risicoanalyse. Eisen waaraan kan worden gedacht zijn lengte van de PIN-code en gebruik van vreemde tekens.

RFC 3647	6.4.1 Genereren en installeren van activeringsgegevens
Nummer	2
ETSI	NCP+ 7.2.9.d
PKIo	Het is alleen toegestaan om gebruik te maken van een deblokkeringscode als de CSP kan garanderen dat daarbij tenminste wordt voldaan aan de betrouwbaarheidseisen, die aan het gebruik van de activeringsgegevens zijn gesteld.

6.5 Logische toegangsbeveiliging van CSP-computers

RFC 3647	6.5.1 Specifieke technische vereisten aan computerbeveiliging
Nummer	1
ETSI	NCP+ 7.4.6
PKIo	De CSP moet multi-factor authenticatie gebruiken (b.v. smartcard met persoonsgebonden certificaten en een persoonsgebonden wachtwoord of biometrie en een persoonsgebonden wachtwoord) voor het systeem of de gebruiker accounts waarmee uitgifte of goedkeuring van certificaten kan worden verricht.
Opmerking	Multi-factor authenticatie tokens mogen niet op een permanente of semi-permanente wijze zijn aangesloten op het systeem (b.v. een permanent geactiveerde smartcard). Hiermee zou het namelijk mogelijk zijn dat

	certificaten (semi)-automatisch worden uitgegeven of goedgekeurd of dat niet geautoriseerde medewerkers certificaten uitgeven of goedkeuren.

RFC 3647	6.5.1 Specifieke technische vereisten aan computerbeveiliging
Nummer	2
ETSI	NCP+ 7.4.6
PKIo	Medewerkers van externe Registration Authorities (RA) of Resellers mogen geen toegang hebben tot het systeem of de gebruiker accounts van de CSP waarmee uitgifte of goedkeuring van certificaten kan worden verricht. Dit is alleen voorbehouden aan geautoriseerde medewerkers van de CSP. Als een RA of een Reseller wel deze toegang heeft dan wordt de RA of de Reseller als een onderdeel van de CSP beschouwd en moet zij onverkort en aantoonbaar voldoen aan het Programma van Eisen van de PKI voor de overheid.

RFC 3647	6.5.1 Specifieke technische vereisten aan computerbeveiliging
Nummer	3
ETSI	NCP+ 7.4.6.a
PKIo	De CSP voorkomt ongeautoriseerde toegang tot de kerndiensten registration service, certificate generation service, subject device provision service, dissemination service, revocation management service en revocation status service. Hiertoe worden deze kerndiensten fysiek of logisch gescheiden van niet-PKI netwerkdomeinen, of worden de verschillende kerndiensten op separate netwerkdomeinen uitgevoerd waarbij er sprake moet zijn van een unieke authenticatie per kerndienst. Als kerndiensten gebruik maken van hetzelfde netwerkdomein dwingt de CSP een unieke authenticatie per kerndienst af. De CSP documenteert de inrichting van de netwerkdomeinen ten minste op grafische wijze.
Opmerking	Deze eis geldt zowel voor de productie omgeving als voor de uitwijk omgeving. Deze eis geldt niet voor andere omgevingen zoals acceptatie en test.

6.6 Beheersmaatregelen technische levenscyclus

RFC 3647	6.6.1 Beheersmaatregelen ten behoeve van systeemontwikkeling
Nummer	1
ETSI	NCP+ 7.4.7
PKIo	Bij deze ETSI-eis heeft de PKIoverheid alleen een opmerking geformuleerd en is geen specifieke PKIo-eis van toepassing.
Opmerking	Conformiteit aan NCP+ 7.4.7. en BEH art. 2 lid 1c kan worden aangetoond

	door: • een auditverklaring van de leverancier van de producten, die een onafhankelijke EDP audit heeft laten uitvoeren op basis van CWA 14167-1; • een auditverklaring van een interne auditor van de CSP op basis van CWA 14167-1; • een auditverklaring van een externe auditor op basis van CWA 14167-1.

6.7 Netwerkbeveiliging

RFC 3647	6.7.1 Netwerkbeveiliging
Nummer	1
ETSI	NCP+ 7.4.6
PKIo	De CSP moet er zorg voor dragen dat alle PKIoverheid ICT systemen met betrekking tot de registration service, certificate generation service, subject device provision service, dissemination service, revocation management service en revocation status service: • zijn voorzien van de laatste updates en; • de webapplicatie alle invoer van gebruikers controleert en filtert en; • de webapplicatie de dynamische uitvoer codeert en; • de webapplicatie een veilige sessie met de gebruiker onderhoudt en; • de webapplicatie op een veilige manier gebruik maakt van een database.
Opmerking	De CSP moet hiervoor de "Checklist beveiliging webapplicaties[5]" van het NCSC als guidance gebruiken. Daarnaast wordt geadviseerd dat de CSP alle overige aanbevelingen uit de laatste versie van de whitepaper "Raamwerk Beveiliging Webapplicaties" van het NCSC implementeert.

RFC 3647	6.7.1 Netwerkbeveiliging
Nummer	2
ETSI	NCP+ 7.4.6
PKIo	De CSP voert minimaal maandelijks, met behulp van een audit tool, een security scan uit op haar PKIoverheid infrastructuur. De CSP documenteert het resultaat van elke security scan en de maatregelen die hierop zijn genomen.
Opmerking	Enkele voorbeelden van commerciële en niet-commerciële audit tools zijn GFI LanGuard, Nessus, Nmap, OpenVAS en Retina.

[5] http://www.govcert.nl/binaries/live/govcert/hst%3Acontent/dienstverlening/kennis-en-publicaties/factsheets/checklist-webapplicatie-beveiliging/checklist-webapplicatie-beveiliging/govcert%3AdocumentResource/govcert%3Aresource

RFC 3647	6.7.1 Netwerkbeveiliging
Nummer	3
ETSI	NCP+ 7.4.6
PKIo	De CSP laat minimaal een keer per jaar een pentest uitvoeren op de PKIoverheid internet facing omgeving door een onafhankelijke, ervaren, externe leverancier. De CSP moet de bevindingen van de pentest, en de maatregelen die hierop worden genomen, (laten) documenteren.
Opmerking	Voor de leverancierselectie kan de CSP de aanbevelingen in hoofdstuk 4 ("Leverancierselectie") zoals beschreven in de laatste versie van de whitepaper "Pentesten doe je zo[6]" van het NCSC, als guidance gebruiken. Indien noodzakelijk kan de PA een opdracht geven aan de CSP tot het laten uitvoeren van extra pentesten.

[6] http://www.govcert.nl/binaries/live/govcert/hst%3Acontent/dienstverlening/kennis-en-publicaties/whitepapers/pentesten-doe-je-zo/pentesten-doe-je-zo/govcert%3AdocumentResource/govcert%3Aresource

7 Certificaat- en CRL-profielen

7.1 Certificaatprofielen

RFC 3647	7.1 Certificaatprofielen
Nummer	1
ETSI	NCP+ 7.3.3.a
PKIo	De CSP dient certificaten uit te geven conform de eisen, die daaraan zijn gesteld in bijlage A van dit document, te weten "Certificaat- en CRL-profielen".

7.2 CRL-profielen

RFC 3647	7.2 CRL-profielen
Nummer	1
ETSI	NCP+ 7.3.6.i
PKIo	De CSP dient CRL's uit te geven conform de eisen, die daaraan zijn gesteld in bijlage A van dit document, te weten "Certificaat- en CRL-profielen".

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, 9.2.2 Overige bezittingen
Nummer	1
ETSI	NCP+ 7.5.d
PKIo	De CSP moet aantoonbaar in staat zijn, bijvoorbeeld door middel van verzekeringen dan wel zijn financiële positie, een verhaalbaarheid op basis van genoemde vormen van aansprakelijkheid in artikel 6:196b Burgerlijk Wetboek (die betrekking hebben op zowel directe als indirecte schade) af te dekken ten bedrage van tenminste EUR 1.000.000 per jaar.
Opmerking	De hierboven beschreven verhaalbaarheid is gebaseerd op een maximaal aantal af te geven certificaten van 100.000 per CSP, hetgeen past bij de huidige situatie. Wanneer CSP's meer certificaten gaan uitgeven zal worden bepaald of een passende, hogere, verhaalbaarheid zal worden gevorderd.

9.5 Intellectuele eigendomsrechten

RFC 3647	9.5 Intellectuele eigendomsrechten
Nummer	1
ETSI	In ETSI wordt schending van intellectuele eigendomsrechten niet behandeld
PKIo	De CSP vrijwaart de abonnee ten aanzien van aanspraken door derden vanwege schendingen van intellectuele eigendomsrechten door de CSP.

9.6 Aansprakelijkheid

RFC 3647	9.6.1 Aansprakelijkheid van CSP's
Nummer	1
ETSI	NCP+ 6.4
PKIo	[OID 2.16.528.1.1003.1.2.6.1] In de overeenkomst tussen de CSP en de abonnee wordt een beding (een bepaling als bedoeld in artikel 6:253 BW) opgenomen waarin de CSP zich sterk maakt voor een op het certificaat vertrouwende derde. Dit beding strekt tot een aansprakelijkheid van de CSP overeenkomstig artikel 6:196b, eerste tot en met derde lid, van het Burgerlijk Wetboek, met dien verstande dat: a. voor "een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss Telecommunicatiewet" gelezen wordt: "een authenticiteitcertificaat uit het PKIoverheid–domein Autonome Apparaten"; b. voor "ondertekenaar" gelezen wordt: "certificaathouder"; c. voor "elektronische handtekeningen" gelezen wordt:

	"authenticiteitskenmerken".

RFC 3647	9.6.1 Aansprakelijkheid van CSP's
Nummer	2
ETSI	NCP+ 6.4
PKIo	[OID 2.16.528.1.1003.1.2.6.2] In de overeenkomst tussen de CSP en de abonnee wordt een beding (een bepaling als bedoeld in artikel 6:253 BW) opgenomen waarin de CSP zich sterk maakt voor een op het certificaat vertrouwende derde. Dit beding strekt tot een aansprakelijkheid van de CSP overeenkomstig artikel 6:196b, eerste tot en met derde lid, van het Burgerlijk Wetboek, met dien verstande dat: a. voor "een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss Telecommunicatiewet" gelezen wordt: "een vertrouwelijkheidcertificaat uit het PKIoverheid–domein Autonome Apparaten"; b. voor "ondertekenaar" gelezen wordt: "certificaathouder"; c. voor "aanmaken van elektronische handtekeningen" gelezen wordt: "aanmaken van vercijferde data"; d. voor "verifiëren van elektronische handtekeningen" gelezen wordt: "ontcijferen van vercijferde data".

RFC 3647	9.6.1 Aansprakelijkheid van CSP's
Nummer	3
ETSI	NCP+ 6.4
PKIo-AA	[OID 2.16.528.1.1003.1.2.6.3] In de overeenkomst tussen de CSP en de abonnee wordt een beding (een bepaling als bedoeld in artikel 6:253 BW) opgenomen waarin de CSP zich sterk maakt voor een op het certificaat vertrouwende derde. Dit beding strekt tot een aansprakelijkheid van de CSP overeenkomstig artikel 6:196b, eerste tot en met derde lid, van het Burgerlijk Wetboek, met dien verstande dat: a. voor "een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss Telecommunicatiewet" gelezen wordt: "een combinatiecertificaat uit het PKIoverheid–domein Autonome Apparaten"; b. voor "ondertekenaar" gelezen wordt: "certificaathouder"; c. voor "aanmaken van elektronische handtekeningen" gelezen wordt: "verifiëren van authenticiteitskenmerken en aanmaken van vercijferde data"; d. voor "verifiëren van elektronische handtekeningen" gelezen wordt: "ontcijferen van authenticiteitskenmerken en vercijferde data".

RFC 3647	9.6.1 Aansprakelijkheid van CSP's
Nummer	4

ETSI	NCP+ 6.4
PKIo	De CSP sluit alle aansprakelijkheid uit voor schade indien het certificaat niet conform het in paragraaf 1.4 beschreven certificaatgebruik wordt gebruikt.

9.8 Beperkingen van aansprakelijkheid

RFC 3647	9.8 Beperkingen van aansprakelijkheid
Nummer	1
ETSI	NCP+ 6.4
PKIo	Het is de CSP toegestaan om binnen het toepassingsgebied van certificaten, zoals benoemd in paragraaf 1.4 in deze CP, beperkingen te stellen aan het gebruik van certificaten.

RFC 3647	9.8 Beperkingen van aansprakelijkheid
Nummer	2
ETSI	NCP+ 6.4
PKIo	Het is de CSP niet toegestaan om binnen het toepassingsgebied van certificaten, zoals benoemd in paragraaf 1.4 in deze CP, beperkingen te stellen aan de waarde van de transacties, waarvoor certificaten kunnen worden gebruikt.

9.12 Wijzigingen

9.12.1 Wijzigingsprocedure

De volgende partijen kunnen een wijzigingsvoorstel betreffende een onderdeel of een bepaling van deze CP indienen:

a. Het ministerie van BZK;
b. De PA PKIoverheid (PA);
c. CSP's binnen de PKI voor de overheid die deze CP hanteren;
d. Overige belanghebbende partijen.

Het indienen van een wijzigingsvoorstel dient te geschieden door het aanvraagformulier "Wijzigingsvoorstel Programma van Eisen" in te vullen en dit bij de PA aan te bieden. Dit formulier kan worden gevonden op de website van de PA of kan direct worden aangevraagd bij de PA.

De PA behandelt een ingediend wijzigingsvoorstel betreffende een onderdeel of een bepaling van deze CP conform gedocumenteerde interne processen. In het geval van een wijziging van inhoudelijke aard geeft de PA een advies, inclusief tekstvoorstel, impactanalyse (onder meer voor een overgangsregeling en dispensaties) en motivatie. Deze worden aan het Afnemersoverleg PKIoverheid voorgelegd, die een standpunt hierover inneemt. Het standpunt van het Afnemersoverleg wordt als advies met het wijzigingsvoorstel en het advies van de PA ter besluitvorming voorgelegd aan een door de Minister van Binnenlandse Zaken en Koninkrijksrelaties

daartoe aangewezen functionaris. Een door deze functionaris genomen besluit wordt door de PA duidelijk herkenbaar en in begrijpelijke taal gepubliceerd op haar website. Bij de publicatie wordt tevens vermeld wanneer de wijziging van kracht zal worden. Aanvullend stelt de PA het Afnemersoverleg PKIoverheid en de indiener van het wijzigingsvoorstel actief schriftelijk en/of elektronisch op de hoogte van het genomen besluit.

De PA is gerechtigd om zelfstandig een voorstel uit te werken over een wijziging van redactionele aard of een correctie van kennelijke schrijf- en/of spelfouten. Een dergelijk wijzigingsvoorstel zal ter besluitvorming worden voorgelegd aan de door de Minister van Binnenlandse Zaken en Koninkrijksrelaties daartoe aangewezen functionaris en kan zonder voorafgaande bekendmaking in werking treden. Een kopie van deze wijziging wordt na besluitvorming aan de leden van het Afnemersoverleg PKIoverheid toegestuurd. Daarnaast wordt de wijziging duidelijk herkenbaar en in begrijpelijke taal gepubliceerd op de website van de PA.

Op het moment dat zich een calamiteit voordoet, zoals gedefinieerd en beschreven in het Calamiteitenplan PA PKIoverheid, heeft de door de Minister van Binnenlandse Zaken en Koninkrijksrelaties aangewezen functionaris het recht om, zonder tussenkomst van andere organisaties en zonder aankondiging vooraf een wijziging aan te laten brengen die tot doel heeft de betrouwbaarheid te waarborgen. Een dergelijke wijziging zal achteraf worden gepubliceerd door de PA.

RFC 3647	9.12.2 Notificatie van wijzigingen
Nummer	1
ETSI	In ETSI wordt dit onderwerp niet behandeld.
PKIo	Indien een gepubliceerde wijziging van het CP consequenties kan hebben voor de eindgebruikers, zullen de CSP's de wijziging bekend dienen te maken aan de bij hen geregistreerd zijnde abonnees en/of certificaathouders conform hun CPS.

RFC 3647	9.12.2 Notificatie van wijzigingen
Nummer	2
ETSI	In ETSI wordt dit onderwerp niet behandeld.
PKIo	De CSP dient de PA informatie te verstrekken over het voornemen de CA-structuur te wijzigen. Hierbij moet gedacht worden aan bijvoorbeeld de creatie van een sub-CA.

Deze CP en de geaccordeerde wijzigingen hierop kunnen in elektronische vorm worden verkregen via Internet op de website van de PA. Het adres hiervan is: http://www.logius.nl/pkioverheid.

9.13 Geschillenbeslechting

RFC 3647	9.13 Geschillenbeslechting
Nummer	1
ETSI	NCP+ 7.5.f
PKIo	De door de CSP gehanteerde klachtenafhandeling- en geschillenbeslechtingsprocedures mogen het instellen van een procedure bij de gewone rechter niet beletten.

9.14 Van toepassing zijnde wetgeving

Op deze CP is het Nederlands recht van toepassing.

9.17 Overige bepalingen

RFC 3647	9.17 Overige bepalingen
Nummer	1
ETSI	In ETSI wordt dit onderwerp niet behandeld.
PKIo-AA	De CSP moet in staat zijn om minimaal één onder [1.2] genoemde typen certificaten uit te geven.

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 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.
- 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.

Referenties

1. Richtlijn 1999/93/EC van het Europees Parlement en van de Europese Ministerraad van 13 december 1999 betreffende een Europees raamwerk voor elektronische handtekeningen.
2. ITU-T Aanbeveling X.509 (1997) | ISO/IEC 9594-8: "Information Technology – Open Systems Interconnection – The directory: Public-key and attribute certificate frameworks".
3. ITU-T Aanbeveling X.520 (2001) ISO/IEC 9594-6: "Information Technology – Open Systems Interconnection – The directory: Selected Attribute Types".
4. RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".
5. RFC 3739: "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".
6. OID RA management_PKI overheid – OID scheme.
7. ETSI TS 101 862: "Qualified certificate profile", versie 1.3.3 (2006-01).
8. ETSI TS 102 280 : "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons", versie 1.1.1 (2004-03).
9. ETSI TS 102 176-1 : "Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms", versie 2.0.0 (2007-11).
10. ISO 3166 "English country names and code elements".

Algemene eisen

- Eindgebruikercertificaten MOETEN in overeenstemming zijn met de X.509v3 norm voor publieke sleutel certificaten. Algemene eisen aan certificaten staan in RFC5280.
- De [X.509] standaard staat een onbeperkt uitbreiden van de attributen binnen een certificaat toe. I.v.m. interoperabiliteitseisen is het binnen de PKI voor de overheid niet toegestaan om deze te gebruiken. Alleen attributen die in deze bijlage als Verplicht, Optioneel of Afgeraden worden aangeduid mogen gebruikt worden.

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 20 bits aan niet te voorspellen willekeurige data bevatten in, bij voorkeur, 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 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 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	UTF8String	Meerdere instanties van dit attribuut MOGEN gebruikt worden.
Issuer.localityName	N	Gebruik is niet toegestaan.	PKIo	UTF8String	-

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
Issuer.serialNumber	O	MOET, conform RFC 3739, worden gebruikt INDIEN eenduidige naamgeving dit vereist.	RFC 3739	Printable String	
Issuer.commonName	V	MOET de naam van de CA bevatten conform geaccepteerd document of basisregistratie, MAG worden aangevuld met de Domein aanduiding en/of de typen certificaat die worden ondersteund.	PKIo, RFC 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).
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 *context* van de PKI voor de (Nederlandse) overheid.
Subject.commonName	V	MOET het normenkader waaraan het apparaat conformeert identificeren OF MOET het aan het normenkader conformerende model/type van het apparaat identificeren.	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	De abonnee MOET aantonen dat diens organisatie deze naam mag toekennen. 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.Surname	N	Wordt voor autonome apparaten-certificaten niet	PKIo		Apparatencertificaten zijn niet persoonsgebonden. Gebruik van dit attribuut wordt

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
		gebruikt.			daarom niet toegestaan om verwarring te voorkomen.
Subject.givenName	N	Wordt voor autonome apparaten-certificaten niet gebruikt.	PKIo		Apparatencertificaten zijn niet persoonsgebonden. Gebruik van dit attribuut wordt daarom niet toegestaan om verwarring te voorkomen.
Subject.pseudonym	N	Het gebruik van pseudoniemen is niet toegestaan.	ETSI TS 102 280, RFC 3739, PKIo		
Subject.organization-Name	V	Volledige naam van de organisatie van de abonnee conform geaccepteerd document of Basisregistratie.	PKIo	UTF8String	De abonneeorganisatie is de organisatie waarmee de CSP 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.stateOrProvin-ceName	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 be-vatten.	PKIo, RFC 3739	UTF8String	Naam van de vestigingsplaats MOET in overeenstemming zijn met het adres van de abonnee volgens geaccepteerd document of registratie.

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
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.
Subject.emailAddress	N	Gebruik is niet toegestaan.	RFC 5280	IA5String	Dit veld MAG NIET worden gebruikt in nieuwe certificaten.
Subject.serialNumber	O	Het is de verantwoordelijkheid van een CSP 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 CSP 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.
IssuerUniqueIdentifier	N	Wordt niet gebruikt.	RFC 5280		Gebruik hiervan is niet toegestaan (RFC 5280).
subjectUniquIdentifier	N	Wordt niet gebruikt.	RFC 5280		Gebruik hiervan is niet toegestaan (RFC 5280).

Standaard extensies

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
authorityKeyIdentifier	V	Nee	Het algoritme om de AuthorityKey te genereren MOET worden ingesteld op een algoritme zoals door de PA is bepaald.	ETSI TS 102 280, RFC 5280	BitString	De waarde MOET de SHA-1 hash van de authorityKey (publieke sleutel van de CSP/CA) bevatten.
SubjectKeyIdentifier	V	Nee	Het algoritme om de subjectKey te genereren MOET worden ingesteld op een algoritme zoals door de PA is bepaald.	RFC 5280	BitString	De waarde MOET de SHA-1 hash van de subjectKey (publieke sleutel van de certificaathouder) bevatten.
KeyUsage	V	Ja	Dit attribuut extensie specificeert het beoogde doel van de in het certificaat opgenomen sleutel. In de PKI voor de overheid zijn per certificaatsoort verschillende bits opgenomen in the keyUsage extensie. In authenticiteitcertificaten MOET het digitalSignature bit zijn opgenomen. Een andere keyUsage MAG hiermee NIET worden gecombineerd. In vertrouwelijkheidcertificaten MOETEN de keyEncipherment en dataEncipherment bits zijn opgenomen. Optioneel MAG dit worden gecombineerd met het keyAgreement bit. Een andere keyUsage MAG hiermee NIET worden gecombineerd.	RFC 3739, RFC 5280, ETSI TS 102 280	BitString	

			In combinatiecertificaten MOETEN de digitalSignature, keyEncipherment en keyAgreement bits 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 beschreven in de CP.	RFC 3739	OID, String, String	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. 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. 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).
PolicyMappings	N		Wordt niet gebruikt.			Deze extensie wordt niet gebruikt in eindgebruikercertificaten
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		MOET worden gebruikt met daarin een nummer dat de certificaathouder (subject) wereldwijd uniek identificeert.	RFC 4043, PKIo	IA5String, Microsoft UPN, IBM Principal-	Bevat een door PKIoverheid aan de CSP (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:

			In het authenticiteitcertificaat MAG daarnaast als othername een PrincipalName (UPN) worden opgenomen voor gebruik met SSO (Single Sign On).		Name of Permanent-Identifier	MS UPN: [nummer]@[OID] IA5String: [OID].[nummer] IA5String: [OID]-[nummer] Permanent Identifier: Identifiervalue = [nummer] Assigner = [OID] 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 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.
IssuerAltName	N		Wordt niet gebruikt.	RFC 5280		Mogelijke invullingen voor dit veld zijn DNS naam, IP adres en URI. Gebruik van een rfc822 naam (e-mail adres) is NIET toegestaan.
subjectDirectoryAttributes	N		Wordt niet gebruikt.	RFC 5280; RFC 3739		Het gebruik van deze extensie is niet toegestaan.
BasicConstraints	O	Ja	Het "CA" veld MOET op "FALSE" staan of worden weggelaten (default waarde is dan "FALSE").	RFC 5280		In een (Nederlandstalige) browser zal dan te zien zijn: "Subjecttype = Eindentiteit", "Beperking voor padlengte = Geen".
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	Ja / Nee	Wordt alleen gebruikt indien nodig voor de specifieke toepassing.	RFC 5280	KeyPurposeId's	Apparatencertificaten MOGEN ExtendedKeyUsage gebruiken indien dit wordt vereist door de toepassing waarvoor het certificaat wordt gebruikt.Indien gebruikt, zijn de volgende voorwaarden allen van kracht. Een ExtKeyUsage: • MAG worden opgenomen in elk ander certificaat; • MAG NIET als critical worden aangemerkt; • MOET minimaal een (1) KeyPurposeId bevatten. 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. Opmerking: Authenticiteitcertificaten die worden gebruikt voor SSO (Single Sign On) MOETEN voor een goede werking van de toepassing worden voorzien van de KeyPurposeId voor Smart Card Logon (1.3.6.1.4.1.311.20.2.2).
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 accessMethod (id-ad-caIssuers)	O		Een AccessDescription item met accessMethod id-ad-caIssuers verwijst naar de online locatie waar het certificaat van de CSP 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.
BiometricInfo	N		Wordt niet gebruikt in autonome apparatencertificaten.	PKIo		Biometrische informatie is niet zinvol in niet persoonsgebonden certificaten zoals apparatencertificaten.
QcStatement	N	Nee	Wordt niet gebruikt in autonome apparatencertificaten.	RFC 3739, ETSI TS 102 280, ETSI TS 101 862	OID	Dit attribuut wordt alleen gebruik in persoonsgebonden certificaten en is niet toegestaan in apparatencertificaten.

Profiel van de CRL

Algemene eisen aan de CRL

- De CRL's moeten voldoen aan de X.509v3 stan¬daard voor publieke sleutel certificaten en CRL's.
- Een CRL bevat informatie over ingetrokken certificaten die binnen de huidige geldig¬heidsperiode vallen of waarvan de geldigheidsperiode min¬der dan 6 maanden geleden is verlopen (conform Wet Elektronische Handtekeningen).

CRL attributen

Veld / Attribuut	**Criteria**	**Beschrijving**	**Norm refe-rentie[1]**	**Type**	**Toelichting**
Version	V	MOET ingesteld worden op 1 (X.509v2 CRL profiel).	RFC 5280	Integer	Beschrijft de versie van het CRL profiel, waarde 1 staat voor X.509 versie 2.
Signature	V	MOET worden ingesteld op het algoritme, zoals deze door de PA is bepaald.	RFC 5280	OID	MOET gelijk zijn aan het veld signatureAlgorithm. Voor certificaten onder het G2 stamcertificaat wordt alleen sha-256WithRSAEncryption toegestaan.
Issuer	V	MOET een Distinguished Name (DN) bevatten. Veld heeft attributen zoals beschreven in de volgende rijen.	PKIo, RFC 5280		Andere attributen dan hieronder genoemd MOGEN NIET worden gebruikt. De attributen die worden gebruikt MOETEN gelijk zijn aan de gelijknamige attributen in het Subject veld van het CSP certificaat (ten behoeve van validatie).
Issuer.countryName	V	MOET de landcode bevatten van het land waar de uitgevende organisatie van het certificaat is gevestigd.	ISO3166, X.520	Printable String	C = NL voor CSP's gevestigd in Nederland.
Issuer.stateOrProvinceName	N	Wordt niet gebruikt.	PKIo	UTF8String	-
Issuer.organizationName	V	Volledige naam conform geaccepteerd	ETSI TS	UTF8String	

		document of basisregistratie.	102280: 5.2.4		
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	Wordt niet gebruikt.	PKIo	UTF8String	-
Issuer.serialNumber	O	MOET, conform RFC 3739, worden gebruikt INDIEN eenduidige naamgeving dit vereist	RFC 3739	Printable String	
Issuer.commonName	V	MOET de naam van de CA bevatten conform geaccepteerd document of basisregistratie, MAG worden aangevuld met de Domein aanduiding en/of de typen certificaat die worden ondersteund.	PKIo, RFC 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).
ThisUpdate	V	MOET datum en tijdstip aangeven waarop de CRL is gewijzigd.	RFC 5280	UTCTime	Moet uitgavedatum bevatten van de CRL conform het van toepassing zijnde beleid vastgelegd in het CPS.
NextUpdate	V	MOET datum en tijdstip aangeven van de volgende versie van de CRL (waarop deze verwacht mag worden).	PKIo, RFC 5280	UTCTime	Dit is het uiterste tijdstip waarop een update verwacht mag worden, eerdere update is mogelijk. Moet worden ingevuld conform het van toepassing zijnde beleid vastgelegd in het CPS.
revokedCertificates	V	MOET de lijst van ingetrokken certificaten bevatten.	RFC 5280	Serial-Numbers, UTCTime	Als er geen ingetrokken certificaten zijn MAG de revokedCertificates lijst NIET aanwezig zijn. Als er minimaal één ingetrokken certificaat bestaat, dan MOET de revokedCertificates lijst wel aanwezig zijn. De lijst is een reeks van CRL entries. De opbouw van een CRL entry is beschreven in de sectie

					"CRL entry" die volgt na de sectie "CRL extensies" hier direct onder.
crlExtensions	V	Bevat een reeks van CRL extensies.	RFC 5280	Extensions	Dit veld bevat een reeks extensies die op de gehele CRL van toepassing zijn. Zie de sectie "CRL extensies" hier direct onder.

CRL extensies

Veld / Attribuut	Criteria	Critical	Beschrijving	Norm refe-rentie[1]	Type	Toelichting
authority-KeyIdentifier	O	Nee	Dit attribuut is interessant als een CSP over meer handtekening certificaten beschikt waarmee een CRL getekend zou kunnen worden (m.b.v. dit attribuut is dan te achterhalen welke publieke sleutel gebruikt moet worden om de handtekening van de CRL te kunnen controleren).	RFC 5280	Key-Identifier	De waarde MOET de SHA-1 hash van de authorityKey (publieke sleutel van de CSP/CA) bevatten.
IssuerAltName	A	Nee	Dit attribuut geeft de mogelijkheid om alternatieve namen voor de CSP (als uitgevende instantie van de CRL) te gebruiken (het gebruik wordt afgeraden).	RFC 5280		Mogelijke invullingen voor dit veld zijn DNS naam, IP adres en URI. Gebruik van een rfc822 naam (e-mail adres) is NIET toegestaan.
CRLNumber	V	Nee	Dit attribuut MOET een oplopend nummer bevatten dat het bepalen van de volgorde van CRL's ondersteunt (de CSP voorziet de CRL van de nummering).	RFC 5280	Integer	RFC 5280 stelt bepaalde eisen aan de wijze van nummeren van CRL's en delta-CRL's. De CSP MOET aan die eisen voldoen.
DeltaCRLIndicator	O	Ja	Aanwezigheid van deze extensie duidt aan dat onderhavige CRL een delta-CRL betreft.	RFC 5280	Base-CRLNum-ber	DeltaCRLIndicator MAG NIET worden opgenomen in een basis-, noch een volledige CRL. DeltaCRLIndicator MOET worden opgenomen in een delta-CRL en MOET dan als Critical worden aangemerkt en MOET dan ook het nummer van die basis-CRL bevatten waarop deze delta-CRL een uitbreiding vormt.
issuing-DistributionPoint	O	Ja	Als gebruik wordt gemaakt van deze extensie identificeert dit attribuut het CRL distributie punt. Het kan ook additionele informatie bevatten (zoals een gelimiteerde reden waarom het certificaat is ingetrokken).	RFC 5280		Indien gebruikt MOET dit veld voldoen aan de specificaties in RFC 5280.

FreshestCRL	O	Nee	Dit attribuut staat ook bekend onder de naam 'Delta CRL Distribution Point'. Indien gebruikt MOET het de URI van een Delta-CRL distributiepunt bevatten. Het komt nooit voor in een Delta-CRL.	RFC 5280		Dit veld wordt gebruikt in volledige CRL's en geeft aan waar Delta-CRL informatie te vinden is die een update vormt op de volledige CRL. In delta-CRL's MAG deze extensie NIET worden opgenomen.
authorityInfoAccess	O	Nee	Dit veld verwijst naar aanvullende informatie over de CSP CA die de onderhavige CRL ondertekende (uitgaf).	RFC 5280		Bevat een reeks van AccessDescription items die elk naar een bepaald(e) aanvullend(e) gegeven / service verwijst. Indien deze extensie wordt gebruikt, MOET er minimaal één AccessDescription item met de accessMethod id-ad-caIssuers in worden opgenomen. Deze extensie MAG NIET AccessDescription items met andere accessMethods dan id-ad-caIssuers bevatten.
authorityInfoAccess accessMethod (id-ad-caIssuers)	V		Een AccessDescription item met accessMethod id-ad-caIssuers verwijst naar de online locatie waar het certificaat van de CSP CA die de onderhavige CRL 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".

CRL entry

Veld / Attribuut	Criteria	Beschrijving	Norm refe-rentie1	Type	Toelichting
userCertificate	V	Identificeert het (ingetrokken) certificaat	RFC 5280	Certificate-Serial-Number	Bevat het (integer) serienummer van het ingetrokken certificaat.
revocationDate	V	Specificeert het tijdstip (datum en tijd) waarop het certificaat in de CRL werd opgenomen.	RFC 5280	UTCTime	Bevat hetzelfde tijdstip als het veld ThisUpdate van die CRL die het eerst na het intrekken van het certificaat werd gegenereerd.
crlEntryExtensions	O	Bevat een reeks van CRL entry extensies.	RFC 5280	Extensions	Dit veld bevat een reeks extensies die op uitsluitend deze CRL entry van toepassing zijn. Zie de sectie "CRL entry extensies" hier direct onder.

CRL entry extensies

Veld / Attribuut	Criteria	Critical	Beschrijving	Norm referentie1	Type	Toelichting
CRLReason	O	Nee	Indien gebruikt geeft dit de reden aan waarom een certificaat is ingetrokken.	RFC 5280, PKIo	reasonCode	Als geen reden wordt opgegeven MOET deze extensie worden weggelaten. Als deze extensie wordt gebruikt, MAG deze NIET meer dan één keer voorkomen. De gebruikte reasonCode MOET één van de volgende zijn: keyCompromise (1); affiliationChanged (3); superseded (4); privilegeWithdrawn (9).
invalidityDate	O	Nee	Dit attribuut kan gebruikt worden om een datum en tijdstip aan te geven waarop het certificaat gecompromitteerd is geworden indien dit afwijkt van (eerder is dan) de datum en tijdstip waarop de CSP de revocatie heeft verwerkt.	RFC 5280	Generalized-Time	Wanneer een verzoek tot intrekking bij de CSP wordt ingediend, kan het zijn dat de verzoeker meldt dat de reden tot intrekken (bijvoorbeeld diefstal) enige tijd in het verleden ligt. Ook het valideren van het verzoek kan nog enige tijd in beslag nemen. Deze extensie biedt de mogelijkheid om het daadwerkelijke (gemelde) starttijdstip van ongeldigheid te registreren, ondanks het feit dat het verwerkingstijdstip (en het in de CRL opnemen) pas later plaatsvindt.
certificateIssuer	A	Ja	Als gebruik wordt gemaakt van een indirecte CRL MOET dit attribuut worden gebruikt om de oorspronkelijke uitgever van certificaten te identificeren.	RFC 5280	General-Names	De Distinguished Name (DN) van de issuer van het desbetreffende (ingetrokken) certificaat moet overgenomen worden in deze extensie en wel op exact dezelfde wijze als dat die Issuer.DN in het desbetreffende (ingetrokken) certificaat is gecodeerd.

BIJLAGE B Verwijzingsmatrix

Op basis van de hoofdstukken 1 t/m 9 is in deze bijlage 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 de Nederlandse wetgeving, ETSI TS 102 042 NCP+en de PKIo-eisen.

In de navolgende tabel komen de eerste en tweede kolom overeen met de in RFC 3647 gehanteerde hoofdstuk- en paragraafindeling. In de kolom 'ETSI-eis' is vervolgens aangegeven welke eisen uit ETSI van toepassing zijn op de betreffende paragraaf uit de binnen de PKIoverheid gehanteerde Certificate Policy. Wanneer een ETSI-eis van toepassing is op meerdere paragrafen uit RFC 3647 is de referentie naar de betreffende ETSI-eis eenmalig opgenomen. zoals als in PvE deel 1 is opgenomen zijn de eisen uit ETSI van toepassing op alle typen certificaten tenzij anders is aangegeven.

Daarnaast wordt in de tabel aangegeven welke eisen uit het wettelijk kader niet worden afgedekt door ETSI en op welke onderdelen uit de CP deze wettelijke eisen van toepassing zijn. Hierbij wordt aansluiting bij de Regeling Elektronische Handtekeningen gezocht, waarin is aangegeven welke eisen uit het Besluit Elektronische Handtekeningen niet worden afgedekt door ETSI. Tevens zijn in de onderstaande tabel de artikelen uit de Wet Elektronische Handtekeningen opgenomen met betrekking tot aansprakelijkheid. Dit is gedaan omdat deze artikelen nader zijn uitgewerkt in PKIo-eisen.

In de laatste kolom is voor de PKIo-eisen aangegeven op welke paragraaf uit de CP deze eisen van toepassing zijn. De cursief weergegeven ETSI-eisen zijn nader uitgewerkt in PKIo-eisen. In de onderstaande tabel kan het voorkomen dat een PKIo-eis is opgenomen zonder dat daaraan een ETSI-eis is gekoppeld. Dit wordt veroorzaakt door het feit dat een PKIo-eis soms is gebaseerd op een gedeelte van een ETSI-eis terwijl die ETSI-eis in zijn geheel beter past bij een andere RFC-paragraaf. Ook kunnen meerdere PKIo-eisen soms dezelfde ETSI-eis als bron gebruiken, terwijl elke ETSI-eis slechts eenmalig wordt genoemd. Bij een aantal RFC-paragrafen zijn in het geheel geen eisen opgenomen. Dit houdt in dat er geen eisen van toepassing zijn op de betreffende RFC-paragraaf of dat de eisen al zijn opgenomen bij een andere RFC-paragraaf[7]. De PA heeft er bewust voor gekozen om alle eisen maar eenmalig op te nemen.

[7] *Dit wordt mede veroorzaakt door het feit dat ETSI TS 102 042 niet volgens de RFC 3647 structuur is opgebouwd.*

Nr.	CP-referentie	ETSI-eis	Wettelijke eis	PKIo-eis
1	**Introductie op de Certificate Policy**			
1.1	**Achtergrond**			1.1
1.2	**Verwijzingen naar deze CP**			1.2
1.3	**Gebruikersgemeenschap**			1.3
1.4	**Certificaatgebruik**			1.4
1.5	**Contactgegevens Policy Authority**			1.5
2	**Publicatie en elektronische opslagmogelijkheden**			
2.1	**Elektronische opslagplaats**	7.3.1.c 7.3.4.b 7.3.5.e.ii 7.3.5.f		2.1-1 2.1-2
2.2	**Publicatie van CSP-informatie**	*5.2.b* 7.1.a 7.1.c 7.1.e 7.3.2.b		2.2-1 2.2-2 2.2-3

		7.3.4 7.3.4.a 7.3.5 7.3.5.c 7.3.5.d 7.3.6.a		
2.3	**Frequentie van publicatie**			
2.4	**Toegang tot gepubliceerde informatie**	*7.1.d.1* 7.3.6.o		2.4-1
3	**Identificatie en authenticatie**			
3.1	**Naamgeving**			
3.1.1	Soorten naamformaten			3.1.1-1
3.1.2	Noodzaak voor betekenisvolle namen			
3.1.3	Anonimiteit of pseudonimiteit van certificaathouders			
3.1.4	Richtlijnen voor het interpreteren van de diverse naamvormen			
3.1.5	Uniciteit van namen	7.3.3.e		

3.1.6	Erkenning, authenticatie en de rol van handelsmerken			
3.2	**Initiële identiteitsvalidatie**			
3.2.1	Methode om bezit van de private sleutel aan te tonen	7.3.1.o		
3.2.2	Authenticatie van organisatorische entiteit			3.2.2-1 3.2.2-2
3.2.3	Authenticatie van persoonlijke identiteit	6.2 6.2.a 7.3.1 7.3.1.a 7.3.1.d *7.3.1.e* *7.3.1.g* 7.3.1.l		3.2.3-1 3.2.3-2 3.2.3-3
3.2.4	Niet-geverifieerde abonnee informatie			
3.2.5	Autorisatie van de certificaathouder	*7.3.1.h* *7.3.1.i* *6.2.h*		3.2.5-1 3.2.5-2
3.2.6	Criteria voor interoperabiliteit			

3.3	**Identificatie en authenticatie bij vernieuwing van het certificaat**			
3.3.1	Identificatie en authenticatie bij routinematige vernieuwing van het certificaat	7.3.2 7.3.2.a 7.3.2.c 7.3.2.d		3.3.1-1 3.3.1-2 3.3.1.3
3.3.2	Identificatie en authenticatie bij vernieuwing van het certificaat na intrekking			3.3.2-1
3.4	**Identificatie en authenticatie van verzoeken tot intrekking**	**7.3.6.d**		
4	**Operationele eisen**			
4.1	**Aanvraag van certificaten**			
4.2	**Verwerken van een certificaat aanvraag**			
4.3	**Uitgifte van certificaten**			
4.3.1	CSP taken met betrekking tot certificaat uitgifte	7.3.3 7.3.3.a 7.3.3.b 7.3.3.c 7.3.3.d		
4.3.2	CSP notificatie van certificaat uitgifte aan abonnee	7.3.5.a		

4.4	**Acceptatie van certificaten**			
4.4.1	Activiteiten bij acceptatie van certificaten			4.4.1-1
4.4.2	Publicatie van het certificaat door CSP			
4.4.3	CSP notificatie van certificaat uitgifte aan overige entiteiten			
4.5	**Gebruik van sleutelparen en certificaten**			
4.5.1	Gebruik van private sleutel en certificaat door abonnee	6.2 6.2.b 6.2.c 6.2.f 6.2.g 6.2.i 6.2.j		
4.5.2	Gebruik van publieke sleutel en certificaat door vertrouwende partij	6.3 *6.3.a* 6.3.b 6.3.c		4.5.2-1
4.6	**Vernieuwing van het certificaat**			
4.7	**Vernieuwen van de sleutels van een certificaat**			

4.8	**Certificaat aanpassingen**			
4.9	**Intrekking van certificaten**	7.3.6 7.3.6.g		
4.9.1	Omstandigheden die leiden tot intrekking			4.9.1-1
4.9.2	Wie mag een verzoek tot intrekking doen			4.9.2-1
4.9.3	Procedure voor een verzoek tot intrekking	7.3.6.f	BEH[8] artikel 2 lid 1l	4.9.3-1 4.9.3-2 4.9.3-3 4.9.3-4 4.9.3-5
4.9.4	Tijdsduur waarbinnen certificaathouder intrekkingsverzoek moet indienen			
4.9.5	Tijdsduur voor verwerking intrekkingsverzoek	*7.3.6.a* 7.3.6.b		4.9.5-1
4.9.6	Controlevoorwaarden bij raadplegen certificaat statusinformatie			4.9.6-1 4.9.6-2
4.9.7	CRL-uitgiftefrequentie	*7.3.6.h* *7.3.6.i*		4.9.7-1

[8] *BEH staat voor Besluit Elektronische Handtekeningen.*

4.9.8	Maximale latentie voor CRL's			
4.9.9	Online intrekking/statuscontrole			4.9.9-1
4.9.10	Eisen inzake Online intrekking/statuscontrole			
4.9.11	Overige mogelijkheden tot status publicatie			
4.9.12	Specifieke eisen bij compromittering sleutel			
4.9.13	Omstandigheden die leiden tot opschorting	*7.3.6.e*		4.9.13-1
4.10	**Certificaat Status service**			
4.10.1	Operationele eigenschappen	7.3.6.n 7.3.6.p		
4.10.2	Beschikbaarheid certificaat statusservice	*7.3.6.j*		4.10.2-1
4.10.3	Additionele functies			
4.11	**Einde van afname CSP-dienstverlening**			
4.12	**Escrow van sleutels en recovery**	Zie par. 6.2.3		
5	**Management, operationele en fysieke beveiligingsmaatregelen**	7.4.1		

		7.4.1.a 7.4.1.b 7.4.1.c 7.4.1.d 7.4.1.e 7.4.1.f 7.4.1.g		
5.1	**Fysieke beveiliging**	7.4.4		
5.1.1	Locatie en constructie van gebouwen	7.4.4.d 7.4.4.f		
5.1.2	Fysieke toegang	7.4.4.a 7.4.4.b 7.4.4.c 7.4.4.e 7.4.4.h		
5.1.3	Energievoorziening en airconditioning	7.4.4.g		
5.1.4	Overstromingsmaatregelen			
5.1.5	Brandpreventie en protectie			
5.1.6	Opslag van gegevensdragers	7.4.5.c		

		7.4.5.d 7.4.5.f		
5.1.7	Verwijderen gegevensdragers			
5.1.8	Externe opslag van back-ups			
5.2	**Procedurele beveiliging**	7.4.5		
5.2.1	Vertrouwelijke functies	7.4.3.g *7.4.3.h* 7.4.3.i		
5.2.2	Aantal personen benodigd per taak			
5.2.3	Identificatie en authenticatie met betrekking tot CSP-functies			
5.2.4	Rollen die functiescheiding behoeven	7.4.5.k		5.2.4-1 5.2.4-2
5.2.5	Beheer en beveiliging	7.4.5.a 7.4.5.b 7.4.5.g 7.4.5.h		5.2.5-1 5.2.5.2
5.3	**Personele beveiliging**			

5.3	Personele beveiliging	7.4.3 7.4.3.c *7.4.3.d* 7.4.3.e 7.4.5.e 7.5.h 7.5.i		5.3-1
5.3.1	Vakkennis, ervaring en kwalificaties	7.4.3.a 7.4.3.f		
5.3.2	Antecedentenonderzoek	7.4.3.j	BEH art.2, lid 1s BEH art.2, lid 2 BEH art.2, lid 3	5.3.2-1
5.3.3	Trainingseisen			
5.3.4	Bijscholing frequentie en eisen			
5.3.5	Baanrotatie frequentie en volgorde			
5.3.6	Sancties voor ongeoorloofde activiteiten	7.4.3.b		
5.3.7	Eisen met betrekking tot externe medewerkers			
5.3.8	Documentatie verstrekking aan personeel			

5.4	**Procedures ten behoeve van beveiligingsaudits**			
5.4.1	Vastlegging van gebeurtenissen	7.4.5.i 7.4.11.g 7.4.11.h 7.4.11.d 7.4.11.k 7.4.11.l 7.4.11.m 7.4.11.n 7.4.11.o		5.4.1-1
5.4.2	Frequentie van verwerking audit-log	7.4.5.j		
5.4.3	Bewaartermijn audit-log	Zie 5.5.2		5.4.3-1
5.4.4	Bescherming van audit-log	7.4.11.a 7.4.11.f		
5.4.5	Audit-log back-up procedure			
5.4.6	Intern of extern auditsysteem			
5.4.7	Notificatie van entiteit die audit-log veroorzaakt			
5.4.8	Analyse van audit-log			

5.5	**Archivering van documenten**			
5.5.1	Vastlegging van gebeurtenissen	7.4.11 7.4.11.i *7.3.1.j* *7.3.1.m*		5.5.1-1
5.5.2	Bewaartermijn archief	*7.4.11.e* 7.3.1.n		5.5.2-1
5.5.3	Bescherming van archieven	7.4.10.a 7.4.11.b		
5.5.4	Archief back-up procedure			
5.5.5	Voorwaarden aan tijdsaanduiding van vastgelegde gebeurtenissen			
5.5.6	Intern of extern archiefsysteem			
5.5.7	Procedures ten behoeve van het verkrijgen en verifiëren van archiefinformatie			
5.6	**Vernieuwen van sleutels**			
5.7	**Aantasting en continuïteit**			

5.7.1	Procedures voor afhandeling incidenten en aantasting	*7.4.8.f*		5.7.1-1 5.7.1-2
5.7.2	Herstelprocedure in geval van aantasting hardware, software en/of data			
5.7.3	Herstelprocedure in geval van aantasting van de private sleutel van de CSP	7.4.8.d 7.4.8.g		
5.7.4	Continuïteit van de bedrijfsvoering na calamiteit	7.4.8 7.4.8.a 7.4.8.b 7.4.8.c		5.7.4-1
5.8	**CSP-beëindiging**	7.4.9 7.4.9.a 7.4.9.b 7.4.9.c	BEH art.2, lid 1p BEH art. 2, lid 1q	
6	**Technische beveiliging**			
6.1	**Genereren en installeren van sleutelparen**			
6.1.1	Genereren van sleutelparen voor de CSP sub CA	7.2.1 7.2.1.a *7.2.1.c* *7.2.1.d*		6.1.1-1

	Genereren van sleutelparen van de certificaathouders	6.2.d 6.2.e 7.2.8 *7.2.8.a*		6.1.1-2 6.1.1-3
6.1.2	Overdracht van private sleutel en SSCD aan certificaathouder	*7.2.8.c* *7.2.8.d* 7.2.8.e 7.2.9 7.2.9.a 7.2.9.b 7.2.9.c		6.1.2-1
6.1.3	Overdracht van de publieke sleutel van de eindgebruiker aan de CSP			
6.1.4	Overdracht van de publieke sleutel van de CSP aan gebruikers	7.2.3 7.2.3.a		
6.1.5	Sleutellengten van private sleutels van certificaathouders	*7.2.8.b*		6.1.5-1
6.1.6	Genereren en controleren van parameters voor publieke sleutels			
6.1.7	Doelen van sleutelgebruik (zoals bedoeld in X.09 v3)	*7.2.5* 7.2.5.a 7.2.5.b		6.1.7-1

6.2	**Private sleutel bescherming en beheersmaatregelen cryptografische modulen**			
6.2.1	Standaarden voor cryptografische modulen en beheersmaatregelen	7.2.1.b 7.2.2 7.2.2.a 7.2.2.b		
6.2.2	Private CSP-sleutel controle door meerdere personen			
6.2.3	Escrow van private sleutels van certificaathouders	7.2.4 *7.2.4.a* *7.2.4.b*		6.2.3-1 6.2.3-2 6.2.3-3
6.2.4	Back-up van private sleutel			
6.2.4.1	Back-up van private sleutels van de CSP	7.2.2.c 7.2.2.d		
6.2.4.2	Back-up van private sleutel van certificaathouders			6.2.4.2-1
6.2.5	Archivering van private sleutels van certificaathouders			6.2.5-1
6.2.6	Toegang tot private sleutels in cryptografische module	7.2.2.e		
6.2.7	Opslag van private sleutels in cryptografische module			

6.2.8	Activering van de private sleutels van de CSP			
6.2.9	Deactivering van de private sleutels van de CSP			
6.2.10	Methode voor het vernietigen van private sleutels	7.2.6.b		
6.2.11	Eisen voor veilige middelen voor het aanmaken van elektronische handtekeningen	*5.3.1.c*		6.2.11-1 6.2.11-2
6.3	**Andere apsecten van sleutelpaarmanagement**			
6.3.1	Archiveren van publieke sleutels			
6.3.2	Gebruiksduur voor certificaten en publieke en private sleutels	7.2.1.e *7.2.6*		6.3.2-1 6.3.2-2
6.4	**Activeringsgegevens**			
6.4.1	Genereren en installeren van activeringsgegevens	*7.2.9.d*		6.4.1-1 6.4.1-2
6.4.2	Activeringsgegevens bescherming			
6.4.3	Andere aspecten van activeringsgegevens			
6.5	**Logische toegangsbeveiliging van CSP-computers**			

6.5.1	Specifieke technische vereisten aan computerbeveiliging	7.4.6 7.4.6.c 7.4.6.d 7.4.6.e 7.4.6.f 7.4.6.j 7.4.6.l		6.5.1-1 6.5.1-2 6.5.1-3
6.5.2	Beheer en classificatie van middelen	7.4.2 7.4.2.a		
6.6	**Beheersmaatregelen technische levenscyclus**			
6.6.1	Beheersmaatregelen ten behoeve van systeemontwikkeling	*7.4.7* 7.4.7.a 7.4.7.b		6.6.1-1
6.6.2	Management van maatregelen ten behoeve van beveiliging			
6.6.3	Levenscyclus beveiligingsclassificatie			
6.6.4	Levenscyclus van cryptografische hardware voor het ondertekenen van certificaten	7.2.7 7.2.7.a 7.2.7.b 7.2.7.c 7.2.7.d 7.2.7.e		

6.7	**Netwerkbeveiliging**	7.4.6.a 7.4.6.b 7.4.6.g 7.4.6.h 7.4.6.i 7.4.6.k 7.3.3.f 7.3.3.g		6.7.1-1 6.7.1-2 6.7.1-3
6.8	**Time-stamping**			
7	**Certificaat- en CRL-profielen**			
7.1	**Certificaatprofielen**			7.1-1
7.2	**CRL-profielen**			7.2-1
8	**Conformiteitbeoordeling**			Zie hoofdstuk 8
9	**Algemene bepalingen**			
9.1	**Tarieven**			
9.2	**Financiële verantwoordelijkheid en aansprakelijkheid**			
9.2.1	Verzekeringsdekking	*7.5.d*		9.2.1-1

9.2.2	Overige bezittingen			9.2.2-1
9.3	**Vertrouwelijkheid**			
9.4	**Bescherming persoonsgegevens**			
9.4.1	Beleid met betrekking tot bescherming van persoonsgegevens			
9.4.2	Informatie behandeld als privé	7.4.11.j		
9.4.3	Informatie niet behandeld als privé			
9.4.4	Verantwoordelijkheden voor bescherming van privé informatie	7.4.10.c		
9.4.5	Notificatie en toestemming van eindgebruiker voor gebruik en publicatie persoonlijke informatie	7.3.5.b 7.4.10.b 7.4.10.d		
9.4.6	Vrijgeven van informatie in geval van gerechtelijke of administratieve procedure	7.4.11.c		
9.4.7	Andere omstandigheden wanneer informatie mag worden vrijgegeven			
9.5	**Intellectuele eigendomsrechten**			9.5-1
9.6	**Aansprakelijkheid**			

9.6.1	Aansprakelijkheid van CSP's	*6.4*		9.6.1-1 9.6.1-2 9.6.1-3 9.6.1-4
9.6.2 t/m 9.6.5	Diverse artikelen omtrent aansprakelijkheid			
9.7	**Verwerping van aansprakelijkheid**			
9.8	**Beperkingen van aansprakelijkheid**			9.8-1 9.8-2
9.9	**Vrijwaring**			
9.10	**Geldigheidsduur en beëindiging overeenkomst**			
9.11	**Afspraken en communicatie tussen entiteiten uit de PKIoverheid-hiërarchie**			
9.12	**Wijzigingen**			
9.12.1	Wijzigingsprocedure			9.12.1
9.12.2	Notificatie van wijzigingen			9.12.2-1 9.12.2-2
9.12.3	Omstandigheden waardoor de OID dient te worden gewijzigd			

9.13	**Geschillenbeslechting**	*7.5.f*	BEH art.2, lid 1n	9.13-1
9.14	**Van toepassing zijnde wetgeving**			9.14
9.15	**Het in overeenstemming zijn met de van toepassing zijnde wet**	7.4.10		
9.16	**Diverse bepalingen**			
9.17	**Overige bepalingen**	6.1 7.1.f 7.1.g 7.1.j 7.5 7.5.a 7.5.b 7.5.c 7.5.e 7.5.g		9.17-1

10 Revisies

10.1 Wijzigingen van versie 3.3 naar 3.4

10.1.1 Nieuw

- Eis 5.2.5-2 (uiterlijke ingangsdatum 4 weken na datum publicatie PVE 3.4);
- Eis 5.3.2-1 (uiterlijke ingangsdatum 4 weken na datum publicatie PVE 3.4);

10.1.2 Aanpassingen

- Toelichting bij ExtKeyusage;

10.1.3 Redactioneel

- Eis 5.4.1-1 (uiterlijke ingangsdatum 4 weken na datum publicatie PVE 3.4);

10.2 Wijziging van versie 3.2 naar 3.3

10.2.1 Nieuw

- Eis 5.2.5-1 (uiterlijke ingangsdatum 1-12-2012)
- Eis 5.4.3-1
- Eis 5.7.4-1 (uiterlijke ingangsdatum 1-12-2012)

10.2.2 Aanpassingen

- Eis 4.9.1-1
- Eis 5.4.1-1
- Eis 5.7.1-1 (uiterlijke ingangsdatum 1-10-2012)
- Eis 5.7.1-2 (uiterlijke ingangsdatum 1-10-2012)
- Eis 6.5.1.3
- Eis 6.7.1.1

10.2.3 Redactioneel

Een aantal redactionele aanpassingen zijn doorgevoerd maar deze hebben geen gevolgen voor de inhoud van de informatie.

10.3 Wijzigingen van versie 3.1 naar 3.2

10.3.1 Nieuw

- Eis 5.2.4-2;
- Eis 5.4.1-1 (uiterlijke ingangsdatum 1-6-2012);
- Eis 6.5.1-3 (uiterlijke ingangsdatum is 1-7-2012);
- Eis 6.7.1-1 (uiterlijke ingangsdatum 1-7-2012);
- Eis 6.7.1-2 (uiterlijke ingangsdatum 1-7-2012);
- Eis 6.7.1-3.

10.3.2 Aanpassingen

- Eis 4.5.2-1 (uiterlijke ingangsdatum is 1-2-2012);
- Eis 5.7.1-2;
- Eis 6.2.3-2.

10.3.3 Redactioneel

Een aantal redactionele aanpassingen zijn doorgevoerd maar deze hebben geen gevolgen voor de inhoud van de informatie.

10.4 Wijzigingen van versie 3.0 naar 3.1

10.4.1 Nieuw

- Eis 4.9.7-1, 6.5.1-1 en 6.5.1-2.

10.4.2 Aanpassingen

- Eis 4.9.1-1;
- Toelichting bij attribuut SerialNumber.

10.4.3 Redactioneel

Een aantal redactionele aanpassingen zijn doorgevoerd maar deze hebben geen gevolgen voor de inhoud van de informatie.

10.5 Wijzigingen van versie 2.1 naar 3.0

Geen wijzigingen.

10.6 Wijzigingen van versie 2.0 naar 2.1

10.6.1 Redactioneel

Alleen een aantal redactionele aanpassingen zijn doorgevoerd maar deze hebben geen gevolgen voor de inhoud van de informatie.

10.7 Versie 2.0

Eerste versie.