Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programma van Eisen deel 3b: Certificate Policy - Services
Bijlage bij CP Domeinen Overheid/Bedrijven en Organisatie

Datum 4 februari 2013

Domein Overheid/Bedrijven:	
Services - Authenticiteit	2.16.528.1.1003.1.2.2.4
Services - Vertrouwelijkheid	2.16.528.1.1003.1.2.2.5
Services - Server	2.16.528.1.1003.1.2.2.6
Domein Organisatie:	
Services - Authenticiteit	2.16.528.1.1003.1.2.5.4
Services - Vertrouwelijkheid	2.16.528.1.1003.1.2.5.5
Services - Server	2.16.528.1.1003.1.2.5.6

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	09-11-2005	Vastgesteld door BZK november 2005
1.1	25-01-2008	Vastgesteld door BZK januari 2008
1.2	13-01-2009	Vastgesteld door BZK januari 2009
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	Vastegesteld door BZK 2012

1 Introductie op de Certificate Policy

1.1 Achtergrond

Dit is deel 3b 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 services certificaten uitgegeven door CSP's in het domein Overheid/Bedrijven en Organisatie.

In dit hoofdstuk is een beknopte toelichting opgenomen op de CP. Een uitgebreide toelichting op de achtergrond en structuur van de PKI voor de overheid, evenals de samenhang tussen de verschillende delen uit het PvE is opgenomen in deel 1 van het PvE.

Voor een overzicht van de in dit deel gehanteerde definities en afkortingen wordt verwezen naar deel 4 van het PvE.

1.1.1 Opzet van de Certificate Policy

Zoals in deel 1 van het PvE is aangegeven bestaan de eisen die onderdeel uitmaken van de CP uit eisen[1]:

- die voortkomen uit het Nederlandse wettelijke kader in relatie tot de elektronische handtekening;
- die voortkomen uit de standaard ETSI TS 102 042 waarbij gebruikt wordt gemaakt van een SUD V2.3.1 (2012-11) – 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 Certification Practice Statements[3].
Nummer	Uniek nummer van de PKIo-eis. Per paragraaf wordt een doorlopende nummering gehanteerd voor de PKIo-eisen. In combinatie met het RFC 3647 paragraafnummer vormt dit een unieke aanduiding voor de PKIo-eis.
ETSI	Verwijzing naar de eis(en) uit ETSI TS 102 042 waarvan de PKIo-eis is afgeleid c.q. een nadere invulling is.

[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 services is gebaseerd op een andere onderliggende standaard dan de CP's voor persoonsgebonden certificaten. Omdat services certificaten niet persoonsgebonden zijn en geen gekwalificeerde certificaten zijn zoals bedoeld in de Wet Elektronische Handtekeningen wijken de eisen aan services certificaten 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.

PKIo	De PKIo-eis die binnen de PKI voor de overheid van toepassing is. Indien in de tabel de aanduiding "PKIo-Sv" is opgenomen, is de eis alleen van toepassing op services certificaten die binnen het domein Overheid/Bedrijven en Organisatie worden uitgegeven. Indien in de tabel de aanduiding "PKIo-OO" is opgenomen, is de eis alleen van toepassing. binnen het domein Overheid/Bedrijven en Organisatie, zowel voor de persoonsgebonden, als de services certificaten.
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 zijn ook een aantal bepalingen opgenomen die niet als PKIo-eis zijn geformuleerd. Deze bepalingen stellen geen eisen aan de CSP's binnen de PKI voor de overheid maar zijn als beleid wel van toepassing op de PKI voor de overheid. Het betreft hier bepalingen uit de paragrafen 1.1, 1.1.1, 1.1.2, 1.2, 1.3, 1.4, 1.5, 8, 9.12.1, 9.12.2, 9.14 en 9.17.

In bijlage A zijn de binnen de PKIoverheid gehanteerde profielen met betrekking tot de services certificaten 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 3b 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].

[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 twee 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.*

Domein Overheid/Bedrijven:	
OID	**CP**
2.16.528.1.1003.1.2.2.4	voor het authenticiteitcertificaat voor services binnen het domein Overheid/Bedrijven, dat de publieke sleutel bevat ten behoeve van identificatie en authenticatie.
2.16.528.1.1003.1.2.2.5	voor het vertrouwelijkheidcertificaat voor services binnen het domein Overheid/Bedrijven, dat de publieke sleutel bevat ten behoeve van vertrouwelijkheid.
2.16.528.1.1003.1.2.2.6	voor het servercertificaat binnen het domein Overheid/Bedrijven, dat de publieke 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 overheid en bedrijven (2). authenticiteit (4)/ vertrouwelijkheid (5)/ server (6). versienummer}.

Domein Organisatie:	
OID	**CP**
2.16.528.1.1003.1.2.5.4	voor het authenticiteitcertificaat voor services binnen het domein Organisatie, dat de publieke sleutel bevat ten behoeve van identificatie en authenticatie.
2.16.528.1.1003.1.2.5.5	voor het vertrouwelijkheidcertificaat voor services binnen het domein Organisatie, dat de publieke sleutel bevat ten behoeve van vertrouwelijkheid.
2.16.528.1.1003.1.2.5.6	voor het servercertificaat binnen het domein Organisatie, dat de publieke sleutel bevat ten behoeve van authenticiteit & vertrouwelijkheid.

De OID is als volgt opgebouwd: {joint-iso-itu-t (2). country (16). nederland (528). Nederlandse or-
ganisatie (1). nederlandse-overheid (1003). pki voor de overheid (1). cp (2). domein organisatie
(5). authenticiteit (4)/ vertrouwelijkheid (5)/ server (6). versienummer}.

Als eisen slechts voor één of twee typen certificaten van toepassing zijn, dan is dat nadrukkelijk aangegeven door de Object Identifier (OID) te vermelden van de van toepassing zijnde CP of CP's.

1.3 Gebruikersgemeenschap

Binnen de domeinen Overheid/Bedrijven en Organisatie bestaat de gebruikersgemeenschap uit abonnees, die organisatorische entiteiten binnen overheid en bedrijfsleven zijn (zie PKIo 3.2.2-1) en uit certificaathouders, die bij deze abonnees behoren. Daarnaast zijn er

vertrouwende partijen, die handelen in vertrouwen op certificaten van de betreffende certificaathouders.

De partijen binnen de gebruikersgemeenschap zijn abonnees, certificaatbeheerders, certificaathouders en vertrouwende partijen.

- Een abonnee is natuurlijke of rechtspersoon die met een CSP een overeenkomst sluit namens een of meer certificaathouders voor het laten certificeren van de publieke sleutels.
- Een certificaathouder is een entiteit, gekenmerkt in een certificaat als de houder van de private sleutel die is verbonden met de publieke sleutel die in het certificaat is gegeven. De certificaathouder is onderdeel van een organisatorische entiteit waarvoor een abonnee de contracterende partij is.

  Binnen de Certificate Policy Services wordt de volgende invulling aan de term certificaathouder gegeven:
  - een apparaat of een systeem (een niet-natuurlijke persoon), bediend door of namens een organisatorische entiteit; of
  - een functie van een organisatorische entiteit.
    In deze CP gebruiken we de naam "service" voor dergelijke certificaathouders. Voor het uitvoeren van de handelingen ten aanzien van de levensloop van het certificaat van de certificaathouder is tussenkomst door een andere partij dan de certificaathouder vereist. De abonnee is hiervoor verantwoordelijk en dient een certificaatbeheerder aan te wijzen om deze handelingen te verrichten.
- Een certificaatbeheerder is een natuurlijke persoon die namens de abonnee handelingen uitvoert ten aanzien van het certificaat van de certificaathouder. De abonnee geeft de certificaatbeheerder opdracht de betreffende handelingen uit te voeren en legt dit vast in een bewijs van certificaatbeheer.
- Een vertrouwende partij is iedere natuurlijke of rechtspersoon die ontvanger is van een certificaat en die handelt in vertrouwen op dat certificaat. Anders dan bij persoonsgebonden certificaten ontlenen vertrouwende partijen vooral zekerheid aan de verbondenheid van een service (apparaat of functie) met de organisatorische entiteit waartoe de service behoort. De CP Services legt derhalve de nadruk op het bieden van zekerheid over de verbondenheid van een door een apparaat, systeem of functie verzonden bericht of geleverde webdienst met de betreffende organisatie. Het vaststellen van de identiteit van de certificaathouder (apparaat of functie) is in dit licht gezien minder van belang dan het vaststellen van diens verbondenheid met de organisatorische entiteit.

1.4 Certificaatgebruik

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

[OID 2.16.528.1.1003.1.2.2.4 en 2.16.528.1.1003.1.2.5.4]
Authenticiteitcertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het langs elektronische weg betrouwbaar identificeren en authenticeren van de service als behorende bij de organisatorische entiteit, die verantwoordelijk is voor de betreffende

service. Code signing certificaten waarmee, door het zetten van een digitale handtekening, de integriteit en authenticiteit van programmatuur kan worden gewaarborgd, vallen ook onder deze CP.

[OID 2.16.528.1.1003.1.2.2.5 en 2.16.528.1.1003.1.2.5.5]
Vertrouwelijkheidcertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het beschermen van de vertrouwelijkheid van gegevens, die worden uitgewisseld en/of opgeslagen in elektronische vorm.

[OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6]
Servercertificaten die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het beveiligen van een verbinding tussen een bepaalde client en een server die behoort bij de organisatorische entiteit die als abonnee wordt genoemd in het betreffende certificaat.

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.

RFC 3647	2.2 Publicatie van CSP-informatie
Nummer	4
ETSI	NCP+ 7.1.a
PKIo	[2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] De volgende clausule moet worden opgenomen in de CPS en in alle overeenkomsten met partijen die betrokken zijn bij de uitgifte van de services server certificaten van de CSP (zoals b.v. de Registration Authority): "CSP [naam] conformeert zich aan de huidige versie van de Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates zoals gepubliceerd op http://www.cabforum.org. Mocht er een inconsistentie aanwezig zijn tussen het PKIoverheid Programma van Eisen deel 3b en de betreffende Requirements, waardoor niet tenminste tegemoet wordt gekomen aan de hierin beschreven minimale eisen, dit ter beoordeling door de PA, dan prevaleert het gestelde in de Requirements."

RFC 3647	2.2 Publicatie van CSP-informatie
Nummer	5
ETSI	NCP+ 7.1.d.3
PKIo	De certificate policy statement van de CSP moet worden gestructureerd volgens RFC 2527, RFC 3647 of het Programma van Eisen van PKIoverheid dat is gebaseerd op RFC 3647 en moet alle relevante hoofdstukken bevatten zoals beschreven in RFC 2527, RFC 3647 of het PVE PKIoverheid.

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-Sv	Met een ieder wordt bedoeld dat, naast de abonnees, certificaathouders en -

opmerking	beheerders, 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	De CSP dient te voldoen aan de eisen die aan naamformaten zijn gesteld in het Programma van Eisen, deel 3 – bijlage A Certificaat-, CRL- en OCSP-profielen.
Opmerking	In bijlage A is een toelichting op de verschillende profielen opgenomen.

3.2 Initiële identiteitsvalidatie

RFC 3647	3.2.1. Methode om bezit van de private sleutel aan te tonen
Nummer	1
ETSI	NCP+ 7.3.1
PKIo	De CSP waarborgt dat de abonnee het certificate signing request (CSR) op een veilige manier aanlevert. Het op een veilige manier aanleveren moet als volgt plaatsvinden: • het invoeren van het CSR op de daartoe speciaal ontwikkelde applicatie van de CSP waarbij gebruik wordt gemaakt van een SSL verbinding die gebruikt maakt van een PKIoverheid SSL certificaat of gelijkwaardig of; • het invoeren van het CSR op de HTTPS website van de CSP die gebruikt maakt van een PKIoverheid SSL certificaat of gelijkwaardig of; • het via e-mail verzenden van het CSR voorzien van een gekwalificeerde elektronische handtekening van de certificaatbeheerder die gebruik maakt van een PKIoverheid gekwalificeerd certificaat of gelijkwaardig of; • het invoeren of verzenden van een CSR op een wijze minimaal gelijkwaardig aan bovenstaande manieren.
Opmerking	Als er sprake is van een calamiteit, waarbij een vooraf met de abonnee afgesproken noodprocedure in werking treedt, mag worden afgeweken van deze eis. In dergelijke gevallen moet de CSP, zodra het CSR is ontvangen, tenminste telefonisch contact opnemen met de abonnee opdat de abonnee het CSR accordeert.

RFC 3647	3.2.2 Authenticatie van organisatorische entiteit
Nummer	1
ETSI	NCP+ 7.3.1.g

PKIo-Sv	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-Sv	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-Sv	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-Sv	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-Sv	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-Sv	De CSP dient te controleren dat: • het bewijs, dat de certificaathouder geautoriseerd is namens de abonnee om een certificaat te ontvangen, authentiek is; • of de certificaatbeheerder toestemming heeft verkregen van de abonnee om aan hem opgedragen handelingen uit te voeren (ingeval de certificaatbeheerder het registratieproces uitvoert).
Opmerking	De "certificaatbeheerder" die handelingen overneemt van de certificaathouder behoeft niet noodzakelijkerwijs dezelfde persoon te zijn als de systeembeheerder of personeelsfunctionaris. 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-Sv	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 service, deze onmiddellijk aan de CSP door te geven. Wanneer de service ophoudt te bestaan, dient dit door middel van een intrekkingsverzoek te

	geschieden.

RFC 3647	3.2.5 Autorisatie van de certificaathouder
Nummer	3
ETSI	NCP+ 7.3.1.i.i
PKIo-Sv	[OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] De CSP moet verifiëren dat de domeinnaam niet voorkomt op een spam- en/of phishing blacklist. Gebruik hiervoor ten minste http://www.phishtank.com. Als de domeinnaam voorkomt op phishtank of eventueel een andere blacklist die is geraadpleegd, dient de CSP tijdens het verificatieproces extra zorgvuldig om te gaan met de aanvraag van het betreffende services server certificaat.

3.3 Identificatie en authenticatie bij vernieuwing van het certificaat

RFC 3647	3.3.1 Identificatie en authenticatie bij routinematige vernieuwing van het certificaat
Nummer	1
ETSI	NCP+ 7.3.2.d
PKIo	[OID 2.16.528.1.1003.1.2.2.5 en 2.16.528.1.1003.1.2.5.5] NCP+ 7.3.2.d is van toepassing.
Opmerking	In NCP+ 7.3.2.d. wordt aangegeven onder welke voorwaarden hercertificering van sleutels is toegestaan.

RFC 3647	3.3.1 Identificatie en authenticatie bij routinematige vernieuwing van het certificaat
Nummer	2
ETSI	NCP+ 7.3.2.d
PKIo	[OID 2.16.528.1.1003.1.2.2.4 en 2.16.528.1.1003.1.2.5.4] en [OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] 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 servercertificaat.

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

4.1 Aanvraag van certificaten

RFC 3647	4.1 Aanvraag van certificaten
Nummer	1
ETSI	NCP+ 6.2
PKIo-Sv	[OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] De CSP dient, voorafgaand aan de uitgifte van een services server certificaat, een overeenkomst af te sluiten met de abonnee en een, door de certificaatbeheerder ondertekende, certificaataanvraag te ontvangen. De overeenkomst moet tenminste aan de volgende voorwaarden voldoen: • de overeenkomst moet ondertekend worden door de Bevoegde Vertegenwoordiger of Vertegenwoordiging van de abonnee; • de abonnee moet verklaren dat de gegevens die worden verstrekt in het kader van een services server certificaat aanvraagproces volledig en juist zijn; • de abonnee moet verklaren dat passende maatregelen zullen worden genomen om de private sleutel (en de daarbij behorende toegangsinformatie b.v. een PINcode), behorend bij de publieke sleutel in het betreffende services server certificaat, onder zijn controle en geheim te houden en te beschermen; • de abonnee moet verklaren dat het niet het services server certificaat zal installeren en gebruiken alvorens het op juistheid en volledigheid gecontroleerd te hebben; • Indien de domeinnaam (FQDN) zoals vermeld in een services server certificaat identificeerbaar en adresseerbaar is via het internet, moet de abonnee verklaren dat het services server certificaat alleen op een server wordt gezet die ten minste bereikbaar is met een van de FQDN's in dit services server certificaat; • de abonnee moet verklaren dat het services server certificaat alleen wordt gebruikt in overeenstemming met de regelgeving die op haar bedrijfsvoering van toepassing is en alleen in relatie met de werkzaamheden van de abonnee en in overeenstemming met de bepalingen van de voorliggende overeenkomst; • de abonnee moet verklaren dat het per direct geen gebruik meer zal maken van het services server certificaat als duidelijk is dat de gegevens in het services server certificaat onjuist of onvolledig zijn of als er aanwijzingen zijn dat de private sleutel, behorend bij de publieke sleutel van het betreffende services server certificaat, gecompromitteerd is geraakt; • de abonnee moet verklaren dat het per direct geen gebruik meer zal maken van de private sleutel, behorend bij de publieke sleutel van het betreffende services server certificaat, als de geldigheid van het services server certificaat is verlopen of als het services server certificaat is ingetrokken; • De abonnee moet verklaren te reageren op instructies van de CSP binnen de door de CSP gestelde termijn in geval van aantasting van de private sleutel of certificaatmisbruik; • De abonnee moet aanvaarden dat de CSP gerechtigd is om het certificaat

	in te trekken indien de abonnee de gebruikersovereenkomst heeft geschonden of de CSP heeft ontdekt dat het certificaat wordt gebruikt voor criminele activiteiten zoals phishing, fraude of het verspreiden van malware.

4.4 Acceptatie van certificaten

RFC 3647	4.4.1 Activiteiten bij acceptatie van certificaten
Nummer	1
ETSI	NCP+ 7.3.1.m
PKIo-Sv	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.
Opmerking	Indien gebruik wordt gemaakt van softwarematig beschermde sleutels (zie [6.2.11-3]) waarbij de private sleutel door de certificaatbeheerder wordt gegenereerd en niet door de CSP, is overdracht van het sleutelmateriaal en ontvangstbevestiging niet van toepassing. Wel dienen nog steeds de gegevens te worden vastgelegd die worden vereist in NCP+ 7.3.1.m.

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-Sv	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 abonnee een “code signing” certificaat gebruikt om “hostile code” (waaronder spyware, malware, trojans etc.) digitaal te ondertekenen. • 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-Sv	De volgende partijen mogen een verzoek tot intrekking van een eindgebruikercertificaat doen: • de certificaatbeheerder;

	• de abonnee; • de CSP; • ieder andere, naar het oordeel van de CSP, 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, indien de intrekking geïnitieerd is door de CSP.

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-Sv	De CSP moet in ieder geval gebruik maken van een CRL om de certificaatstatus informatie beschikbaar te stellen. [OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] De CSP moet gebruik maken van een OCSP en een CRL om de certificaatstatus informatie beschikbaar te stellen.

RFC 3647	4.9.5 Tijdsduur voor verwerking intrekkingsverzoek
Nummer	1
ETSI	NCP+ 7.3.6.a
PKIo	De maximale vertraging tussen de ontvangst van een intrekkingsverzoek of intrekkingsrapportage 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 (CRL en OCSP)

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	[OID 2.16.528.1.1003.1.2.2.4 en 2.16.528.1.1003.1.2.5.4] en [OID 2.16.528.1.1003.1.2.2.5 en 2.16.528.1.1003.1.2.5.5] De revocation management services van de CSP kunnen als aanvulling op de publicatie van CRL informatie het Online Certificate Status Protocol (OCSP) ondersteunen. Indien deze ondersteuning aanwezig is moet deze in het CPS worden vermeld.

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	2
ETSI	NCP+ 7.3.6.j
PKIo	Indien de CSP het Online Certificate Status Protocol (OCSP) ondersteunt, dient dit te gebeuren in overeenstemming met {16} IETF RFC 2560.

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	3
ETSI	NCP+ 7.3.6.j
PKIo	Ter verbijzondering van het in {16} IETF RFC 2560 gestelde dienen OCSP responses digitaal te worden ondertekend door ofwel: • de private (CA) sleutel waarmee ook het certificaat is ondertekend waarvan de status wordt gevraagd; • de private sleutel van een door de CSP aangewezen responder die beschikt over een OCSP-Signing certificaat dat voor dit doel is ondertekend door de private (CA) sleutel waarmee ook het certificaat is ondertekend waarvan de status wordt gevraagd; Indien een CSP voor de tweede optie kiest, dan MOET het OCSP-Signing certificaat waarover de responder beschikt aan de navolgende additionele voorwaarde voldoen (zie RFC2560 en de eis PvE deel 3b, 4.9.9-6): • Het OCSP-Signing certificaat is voorzien van de extensie id-pkix-ocsp-nocheck die niet is gemarkeerd als “critical” en is voorzien van de waarde “NULL”.

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	4
ETSI	NCP+ 7.3.6.j

PKIo	Ter verbijzondering van het in {16} IETF RFC 2560 gestelde is het gebruikt van vooraf berekende OCSP responses (precomputed responses) niet toegestaan.

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	5
ETSI	NCP+ 7.3.6.j
PKIo	Indien de CSP OCSP ondersteunt, dient de informatie die wordt verstrekt middels OCSP ten minste even actueel en betrouwbaar te zijn als de informatie die wordt gepubliceerd door middel van een CRL, gedurende de geldigheid van het afgegeven certificaat en bovendien tot ten minste zes maanden na het tijdstip waarop de geldigheid van het certificaat is verlopen of, indien dat tijdstip eerder valt, na het tijdstip waarop de geldigheid is beëindigd door intrekking.

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	6
ETSI	NCP+ 7.3.6.j
PKIo	Indien de CSP OCSP ondersteunt, moet de CSP de OCSP service tenminste een keer in de 4 kalenderdagen bijwerken. De maximale vervaltermijn van de OCSP responses is 10 kalenderdagen.

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	7
ETSI	NCP+ 7.3.6.h.iv
PKIo	[OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] De CSP MOET de GET methode ondersteunen bij het aanbieden van OCSP responses volgens RFC5019.
Opmerking	Http gebaseerde OCSP verzoeken kunnen zowel de GET als de POST methode gebruiken voor het indienen van een verzoek. Om http caching mogelijk te maken wordt de CSP verplicht om de GET methode te ondersteunen.

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	4.10.1 Operationele eigenschappen
Nummer	1
ETSI	NCP+ 7.3.6
PKIo	[OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] De CSP moet met betrekking tot zijn OCSP en CRL dienstverlening passende server capaciteit aanhouden waarmee een response tijd wordt gegarandeerd van 10 seconden of minder onder normale omstandigheden.

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.
Opmerking	Deze eis is alleen van toepassing op de CRL en niet op andere mechanismen zoals OCSP.

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	5.3.1 Vakkennis, ervaring en kwalificaties
Nummer	1
ETSI	NCP+ 7.4.3.l
PKIo	[OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] Alvorens tot uitgifte van services server certificaten kan worden overgegaan moet de CSP: ▪ al het personeel dat zich gaat bezighouden met het controleren en goedkeuren van een services server certificaat een training laten ondergaan waarbij algemene kennis over PKI, authenticatie en verificatie policies en procedures met betrekking tot het controle- en goedkeuringsproces en dreigingen waaronder phishing en andere social engineering tactieken, aan bod komen; ▪ al het personeel een intern examen afnemen dat succesvol moet worden afgerond; ▪ een administratie bijhouden van de training(en) en het examen en waarborgen dat de vaardigheden van het betreffende personeel op het juiste niveau blijft.

RFC 3647	5.3.2 Antecendentenonderzoek
Nummer	1
ETSI	NCP + 7.4.3-l
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-Sv	De CSP dient alle informatie op te slaan die is gebruikt voor het verifiëren van

	de identiteit van de abonnee en certificaatbeheerder, met inbegrip van referentienummers van de documentatie die is gebruikt voor verificatie, evenals beperkingen ten aanzien van de geldigheid.

RFC 3647	5.5.1 Vastlegging van gebeurtenissen
Nummer	2
ETSI	NCP+ 7.4.11
PKIo-Sv	[OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] De CSP dient een registratie bij te houden van alle ingetrokken services server certificaten en alle afgewezen aanvragen voor een services server certificaat in verband met de verdenking van phishing of ander mogelijk misbruik, zulks ter beoordeling aan de CSP en dient deze aan te melden bij http://www.phishtank.com.

RFC 3647	5.5.2 Bewaartermijn archief
Nummer	1
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.

RFC 3647	5.5.2 Bewaartermijn archief
Nummer	2
ETSI	NCP+ 7.4.11.e
PKIo-Sv	[OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] De CSP dient, nadat de geldigheid van het service server certificaat is verlopen, voor tenminste 7 jaren alle informatie op te slaan met betrekking tot de aanvraag en eventuele revocatie van het services server certificaat en alle gegevens die zijn gebruikt voor het verifiëren van de identiteit van de abonnee en certificaatbeheerder.

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 (c.q. gegevens voor het aanmaken van elektronische handtekeningen) 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.
PKIo-Sv Opmerking	Zie paragraaf 6.2.11 voor de mogelijkheden van softwarematige generatie en opslag van het sleutelmateriaal van de certificaathouders.

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	6.1.1 Genereren van sleutelparen van de certificaathouders
Nummer	4
ETSI	NCP+ 7.2.8.d
PKIo-Sv	[OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] Indien de CSP de private sleutel genereert ten behoeve van de abonnee MOET deze versleuteld worden aangeleverd aan de abonnee zodat integriteit en vertrouwelijkheid van de private sleutel geborgd is. De volgende maatregelen moeten daarbij in acht worden genomen: a. De CSP MOET de private sleutel ten behoeve van de abonnee generen in de beveiligde omgeving waarop de PKIoverheid PvE en de bijbehorende audit van toepassing is; b. Nadat de private sleutel ten behoeve van de abonnee is gegeneerd MOET deze met behulp van een sterk algoritme (conform eisen ETSI TS 102 176) versleuteld worden opgeslagen binnen de beveiligde omgeving van de CSP; c. De CSP MOET daarbij de P12 standaard toepassen waarbij gebruik wordt gemaakt van de privacy mode en de integrity mode. Hiertoe MAG de CSP het P12 bestand versleutelen met een persoonsgebonden PKI certificaat van de abonnee / certificaatbeheerder. Indien deze niet beschikbaar is MOET de CSP een wachtwoord gebruiken die door de abonnee is aangeleverd. Dit wachtwoord MOET door de abonnee zijn aangeleverd via de website van de CSP waarbij gebruik wordt gemaakt van een SSL/TLS verbinding of via een gelijkwaardige procedure waarmee dezelfde betrouwbaarheid en veiligheid wordt gewaarborgd; d. Indien een wachtwoord wordt gebruikt om de P12 te versleutelen moet dit wachtwoord minimaal 8 posities bevatten waaronder minimaal één getal en twee bijzondere tekens; e. De CSP MAG het wachtwoord dat wordt gebruikt om de P12 te versleutelen / ontsleutelen NOOIT in cleartext over een netwerk verzenden of op een server opslaan. Het wachtwoord MOET worden versleuteld met behulp van sterk algoritme (conform eisen ETSI TS 102 176); f. Het P12 bestand MOET over een met SSL/TLS beveiligd netwerk aan de abonnee worden gezonden of out-of-band op een informatiedrager (b.v. USB-stick of CD-rom) worden aangeleverd. g. Als de p12 out-of-band wordt aangeleverd moet deze additioneel versleuteld zijn met een andere sleutel dan het P12 bestand. Daarnaast MOET de p12 via een door de OPTA gecertificeerde koerier of door een vertegenwoordiger van de CSP in een sealbag worden afgeleverd bij de abonnee, h. Als het P12 bestand over een met SSL/TLS beveiligd netwerk wordt

	aangeboden MOET de CSP waarborgen dat het P12 bestand maximaal één keer succesvol wordt gedownload. Toegang tot het P12 bestand bij de overdracht via SSL/TLS moet na drie pogingen worden geblokkeerd.
Opmerking	Best practice is dat de abonnee zelf de private sleutel behorend bij de publieke sleutel genereert. Wanneer de CSP ten behoeve van de abonnee de private sleutel behorend bij de publieke sleutel genereert moet deze voldoen aan bovenstaande eisen. Het is hierbij van belang te onderkennen dat niet alleen het P12 bestand wordt versleuteld, maar ook de toegang tot het P12 bestand bij de overdracht wordt beveiligd.

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-Sv	[OID 2.16.528.1.1003.1.2.2.5 en 2.16.528.1.1003.1.2.5.5] 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- en OCSP-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 2.16.528.1.1003.1.2.2.4 en 2.16.528.1.1003.1.2.5.4] en OID [2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] Escrow door de CSP is niet toegestaan voor de private sleutels van het authenticiteitcertificaat en servercertificaat.

RFC 3647	6.2.3 Escrow van private sleutels van certificaathouders
Nummer	2
ETSI	NCP+ 7.2.4.b
PKIo	[OID 2.16.528.1.1003.1.2.2.5 en 2.16.528.1.1003.1.2.5.5] 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 2.16.528.1.1003.1.2.2.5 en 2.16.528.1.1003.1.2.5.5] 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.

RFC 3647	6.2.11 Eisen voor veilige middelen voor het aanmaken van elektronische hand-tekeningen

Nummer	3
ETSI	NCP+ 3.1
PKIo	[OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] In plaats van gebruik te maken van een hardwarematige SUD mogen de sleutels van een services certificaat softwarematig worden beschermd indien compenserende maatregelen worden getroffen in de omgeving van het systeem dat de sleutels bevat. De compenserende maatregelen moeten van een dusdanige kwaliteit zijn dat het praktisch onmogelijk is de sleutels ongemerkt te stelen of te kopiëren. De beheerder van de services certificaten die gebruik maakt van deze mogelijkheid voor softwarematige opslag dient bij registratie ten minste een schriftelijke verklaring te overleggen dat compenserende maatregelen zijn getroffen die voldoen aan de hiervoor gestelde voorwaarde. In de overeenkomst tussen abonnee en CSP dient te worden opgenomen dat de CSP het recht heeft om een controle uit te voeren naar de getroffen maatregelen.
Opmerking	Bij compenserende maatregelen moet bijvoorbeeld worden gedacht aan een combinatie van fysieke toegangsbeveiliging, logische toegangsbeveiliging, logging en audit en functiescheiding.

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	[OID 2.16.528.1.1003.1.2.2.4 en 2.16.528.1.1003.1.2.5.4] en [OID 2.16.528.1.1003.1.2.2.5 en 2.16.528.1.1003.1.2.5.5] Private sleutels die door een certificaathouder worden gebruikt en die zijn uitgegeven onder verantwoordelijkheid van deze CP, dienen niet langer dan vijf jaar te worden gebruikt. De certificaten, die zijn uitgegeven onder de verantwoordelijkheid van deze CP, dienen een geldigheid te hebben van niet meer dan vijf jaar.
Opmerking	De CSP's binnen de PKI voor de overheid mogen pas certificaten uitgeven met een maximale geldigheidsduur van vijf jaar nadat de PA hiervoor expliciet toestemming heeft gegeven. Dit in verband met het te gebruiken algoritme dat door een groot aantal applicaties nog niet wordt ondersteund. Van de expliciete toestemming zal melding worden gemaakt bij dit artikel.

RFC 3647	6.3.2 Gebruiksduur voor certificaten en publieke en private sleutels
Nummer	2
ETSI	NCP+ 7.2.6
PKIo	[OID 2.16.528.1.1003.1.2.2.4 en 2.16.528.1.1003.1.2.5.4 alleen voor wat betreft code signing certificaten] en [OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] Private sleutels die door een certificaathouder

	worden gebruikt en die zijn uitgegeven onder verantwoordelijkheid van deze CP, dienen niet langer dan drie jaar te worden gebruikt. De certificaten, die zijn uitgegeven onder de verantwoordelijkheid van deze CP, dienen een geldigheid te hebben van niet meer dan drie jaar.

RFC 3647	6.3.2 Gebruiksduur voor certificaten en publieke en private sleutels
Nummer	3
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-Sv	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

[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

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.

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-, CRL- en OCSP-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-, CRL- en OCSP-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-, CRL- en OCSP-profielen".

7.3 OCSP-profielen

RFC 3647	7.3 OCSP-profielen
Nummer	1
ETSI	In ETSI wordt OCSP in het geheel niet behandeld.
PKIo	Indien de CSP het Online Certificate Status Protocol (OCSP) ondersteunt, dient de CSP OCSP certificaten en responses te hanteren conform de eisen, die daaraan zijn gesteld in bijlage A van dit document, te weten "Certificaat-, CRL- en OCSP-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 2.16.528.1.1003.1.2.2.4 en 2.16.528.1.1003.1.2.5.4] 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"; 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 2.16.528.1.1003.1.2.2.5 en 2.16.528.1.1003.1.2.5.5] 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"; 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-Sv	[OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] 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 servercertificaat"; 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 niet 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 procedures voor het wijzigingenbeheer van het PvE van PKIoverheid zijn opgenomen in het Certificate Policy Statement van PKIoverheid. Het CPS kan in elektronische vorm worden verkregen op de website van de PA:

https://www.logius.nl/producten/toegang/pkioverheid/documentatie/cps/

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 geschillenbeslechtings-procedures 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-Sv	De CSP moet in staat zijn om alle onder [1.2] genoemde typen services certificaten uit te geven.

RFC 3647	9.17 Overige bepalingen
Nummer	2
ETSI	In ETSI wordt dit onderwerp niet behandeld.
PKIo-Sv	In de overeenkomst die de CSP sluit met de abonnee dient te zijn opgenomen dat, m.b.t. code signing certificaten, de gegevens (naam applicatie, URL en beschrijving applicatie) die de abonnee afgeeft over de applicatie, waarheidsgetrouw, nauwkeurig en niet misleidend zijn.

RFC 3647	9.17 Overige bepalingen
Nummer	3
ETSI	In ETSI wordt dit onderwerp niet behandeld.
PKIo-Sv	• Code signing certificaten die zijn ingetrokken als gevolg van een compromittatie of omdat zij zijn uitgegeven aan onbevoegden moeten voor ten minste 20 jaar worden opgenomen in de database van de CSP die wordt gebruikt ten behoeve van de CRL en, indien van toepassing, OCSP of; • de CSP moet de lifetime signing OID 1.3.6.1.4.1.311.10.3.13 (szOID_KP_LIFETIME_SIGNING) opnemen i.c.m. met de code signing OID 1.3.6.1.5.5.7.3.3 (id_kp_codeSigning) in het ExtKeyUsage veld van het code signing certificaat.

RFC 3647	9.17 Overige bepalingen
Nummer	4
ETSI	In ETSI wordt dit onderwerp niet behandeld.
PKIo-Sv	Deze eis gaat in vanaf 31-10-2011: Indien de CSP een code signing service aanbiedt moet dit plaatsvinden i.c.m. een timestamp server authority (TSA). De CSP moet de abonnee adviseren om een " timestamp" te plaatsen over de digitale handtekening nadat de "code" getekend is. De TSA moet voldoen aan RFC 3161, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)."

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 services certificaten voor het domein Overheid/Bedrijven en Organisatie

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 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".
5. RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".
6. RFC 3739: "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".
7. OID RA management_PKI overheid – OID scheme.
8. ETSI TS 101 862: "Qualified certificate profile", versie 1.3.3 (2006-01).
9. ETSI TS 102 280 : "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons", versie 1.1.1 (2004-03).
10. ETSI TS 102176-1 : "Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms", versie 2.0.0 (2007-11).
11. 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.

Services certificaten

Basisattributen

Veld / Attribuut	Criteria	Beschrijving	Norm refe-rentie	Type	Toelichting
Version	V	MOET ingesteld worden op 2 (X.509v3).	RFC 5280	Integer	Beschrijft de versie van het certificaat, de waarde 2 staat voor X.509 versie 3.
SerialNumber	V	Een serienummer dat op unieke wijze het certificaat binnen het uitgevende CA domein MOET identificeren.	RFC 5280	Integer	Alle eindgebruiker certificaten moeten tenminste 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. Ten behoeve van maximale interoperabiliteit wordt voor certificaten onder het G1 stamcertificaat alleen sha-1WithRSAEncryption toegestaan. Vanaf 01-01-2011 MAG de CSP alleen in zeer uitzonderlijke situaties nog een certificaat op basis van sha-1WithRSAEncryption onder het G1 stamcertificaat uitgeven. Dit certificaat MOET een 2048 bit RSA sleutel bevatten. Dit certificaat MAG maar maximaal geldig zijn tot en met 31-12-2011. Voor certificaten onder het G2 stamcertificaat wordt alleen sha-256WithRSAEncryption toegestaan.
Issuer	V	MOET een Distinguished Name (DN)	PKIo, RFC3739,		Andere attributen dan hieronder genoemd MOGEN NIET worden gebruikt.

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
		bevatten. Veld heeft de onderstaande attributen:	ETSI TS 102280		De attributen die worden gebruikt MOETEN gelijk zijn aan de gelijknamige attributen in het Subject veld van het CSP certificaat (ten behoeve van validatie).
Issuer.countryName	V	MOET de landcode bevatten van het land waar de uitgevende organisatie van het certificaat is gevestigd.	ETSI TS101862, X520, ISO 3166	Printable String	C = NL voor CSP's gevestigd in Nederland.
Issuer.stateOrProvinceName	N	Gebruik is niet toegestaan.	PKIo	UTF8String	-
Issuer.OrganizationName	V	Volledige naam conform geaccepteerd document of basisregistratie.	ETSI TS 102280	UTF8String	
Issuer. organizationalUnitName	O	Optionele aanduiding van een organisatieonderdeel. Dit veld MAG NIET een functieaanduiding of dergelijke bevatten. Wel eventueel de typen certificaten die worden ondersteund.	ETSI TS 102280	UTF8String	Meerdere instanties van dit attribuut MOGEN gebruikt worden.
Issuer.localityName	N	Gebruik is niet toegestaan.	PKIo	UTF8String	-

Veld / Attribuut	Criteria	Beschrijving	Norm refe-rentie	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 te bevatten conform geaccepteerd document of basisregistratie, MAG worden aangevuld met de Domein aanduiding en/of de typen certificaat die worden ondersteund.	PKIo, RFC 3739	UTF8String	Het commonName attribuut MAG NIET nodig zijn om de uitgevende instantie te identificeren (geen onderdeel van de Distinguished Name, eis uit RFC 3739).
Validity	V	MOET de geldigheidsperiode (validity) van het certificaat definiëren volgens RFC 5280.	RFC 5280	UTCTime	MOET begin- en einddatum bevatten voor geldigheid van het certificaat conform het van toepassing zijnde beleid vastgelegd in het CPS.
Subject	V	De attributen die worden gebruikt om het subject (service) te beschrijven MOETEN het subject op unieke wijze benoemen en gegevens bevatten over de abonnee-organisatie. Veld heeft de volgende attributen:	PKIo, RFC3739, ETSI TS 102 280		MOET een Distinguished Name (DN) bevatten. Andere attributen dan hieronder genoemd MOGEN NIET worden gebruikt.

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
Subject.countryName	V	C vullen met tweeletterige landcode conform ISO 3166-1. Indien een officiële alpha-2 code ontbreekt, MAG de CSP de user-assigned code XX gebruiken.	RFC 3739, X520, ISO 3166, PKIo	PrintableString	De landcode die wordt gehanteerd in Subject.countryName MOET in overeenstemming zijn met het adres van de abonnee volgens geaccepteerd document of registratie.
Subject.commonName	V/A	Naam die de service of server identificeert. Verplicht: Bij services certificaten is dit veld verplicht Afgeraden: Bij services server certificaten [OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] wordt het gebruik van dit veld afgeraden. Als dit veld wordt gebruikt MOET deze maximaal 1 "fully-qualified domain name (FQDN)" (zie de definitie in deel 4) bevatten. Deze FQDN MOET ook in het	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	De abonnee MOET aantonen dat de organisatie deze naam mag voeren. Het is niet toegestaan in dit attribuut wildcard FQDN's, locale domeinnamen, private IP adressen, alleen een hostname, internationalized domain names (IDN's) en null characters \0 te gebruiken. Bij services server certificaten [OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] MOET de CSP bij erkende registers (Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA)) controleren of de abonnee de eigenaar is van de domeinnaam of dat de abonnee exclusief geautoriseerd is door de geregistreerde domeinnaam eigenaar om, namens de geregistreerde domeinnaam eigenaar, de domeinnaam te gebruiken. [OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] De CSP MAG

Veld / Attribuut	Criteria	Beschrijving	Norm refe-rentie	Type	Toelichting
		SubjectAltName.dNSName veld zijn opgenomen.			in uitzonderlijke situaties nog een services server certificaat uitgeven zonder FQDN. Hierbij gelden de volgende aanvullende eisen: met ingang van 1 juli 2012 MOET de CSP de abonnee informeren dat het gebruik van server certificaten zonder FQDN wordt afgeraden en dat uiterlijk met ingang van 1 oktober 2016 alle nog geldige server certificaten zonder FQDN zullen worden ingetrokken. In het geval een CSP op of na 1 juli 2012 een server certificaat uitgeeft zonder FQDN dan MOET als "datum geldigheid tot", uiterlijk 1 november 2015 worden aangehouden.
Subject.Surname	N	Wordt voor services certificaten niet gebruikt.			Services certificaten zijn niet persoonsgebonden. Gebruik van dit attribuut wordt daarom niet toegestaan om verwarring te voorkomen.
Subject.givenName	N	Wordt voor services certificaten niet gebruikt.			Services certificaten 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.organizationName	V	Volledige naam van de organisatie van de abonnee conform geaccepteerd document	PKIo	UTF8String	De abonnee-organisatie is de organisatie waarmee de CSP een overeenkomst heeft gesloten en namens welke de certificaathouder

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
		of Basisregistratie.			(service / server) communiceert of handelt.
Subject.organizationalUnitName	O	Optionele aanduiding van een organisatieonderdeel. Dit attribuut MAG NIET een functieaanduiding of dergelijke bevatten.	PKIo		Dit attribuut MAG meerdere malen voorkomen. Het veld MOET een geldige naam van een organisatieonderdeel van de abonnee bevatten conform geaccepteerd document of registratie.
Subject.stateOrProvinceName	V/A	[OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] MOET de provincie van de vestiging van de abonnee bevatten conform geaccepteerd document of Basisregistratie. [OID 2.16.528.1.1003.1.2.2.4 en 2.16.528.1.1003.1.2.5.4] en [OID 2.16.528.1.1003.1.2.2.5 en 2.16.528.1.1003.1.2.5.5] Het gebruik wordt afgeraden. Indien aanwezig MOET dit veld de provincie van vestiging van de abonnee conform	PKIo, RFC 3739	UTF8String	Naam van de provincie MOET in overeenstemming zijn met het adres van de abonnee volgens geaccepteerd document of registratie.

Veld / Attribuut	Criteria	Beschrijving	Norm refe-rentie	Type	Toelichting
		geaccepteerd document of Basisregistratie bevatten.			
Subject.localityName	V/A	[OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] MOET de vestigingsplaats van de abonnee bevatten conform geaccepteerd document of Basisregistratie. [OID 2.16.528.1.1003.1.2.2.4 en 2.16.528.1.1003.1.2.5.4] en [OID 2.16.528.1.1003.1.2.2.5 en 2.16.528.1.1003.1.2.5.5] Het gebruik wordt afgeraden. Indien aanwezig MOET dit veld de vestigingsplaats van de abonnee conform geaccepteerd document of Basisregistratie bevatten.	PKIo, RFC 3739	UTF8String	Naam van de vestigingsplaats MOET in overeenstemming zijn met het adres van de abonnee volgens geaccepteerd document of registratie.
Subject.postalAddress	A	Het gebruik wordt afgeraden. Indien aanwezig MOET dit veld het postadres van	PKIo, RFC 3739	UTF8String	Adres MOET in overeenstemming zijn met het adres van de abonnee volgens geaccepteerd document of registratie.

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
		de abonnee conform geaccepteerd document of Basisregistratie te bevatten.			
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 (service) te waarborgen. Het Subject.serialNumber MOET gebruikt worden om het subject uniek te identificeren. Het gebruik van 20 posities is uitsluitend toegestaan voor OIN en HRN na aanvullende afspraken met Logius.	RFC 3739, X 520, PKIo	Printable String	Het nummer wordt door de CSP en/of de overheid bepaald. Het nummer kan per domein verschillen en voor meerdere toepassingen gebruikt worden.
Subject.title	N	Voor services certifcaten is gebruik van het title attribuut niet toegestaan.	ETSI TS 102 280, RFC 3739, RFC 5280		Dit attribuut wordt alleen gebruikt in persoonsgebonden certificaten en dus niet in services certificaten.
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.

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

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
			In vertrouwelijkheidcertificaten MOETEN keyEncipherment en dataEncipherment bits zijn opgenomen en zijn aangemerkt als essentieel. Optioneel MAG dit worden gecombineerd met het keyAgreement bit. Een ander keyUsage MAG hiermee NIET worden gecombineerd. In servercertificaten MOETEN het digitalSignature, keyEncipherment en de 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	RFC 3739	OID, String, String	Voor services certificaten in domein Overheid/Bedrijven zijn de OID's: 2.16.528.1.1003.1.2.2.4,

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
			gebruikersnotitie. Het te gebruiken OID schema in de PKI voor de overheid wordt beschreven in de CP.			2.16.528.1.1003.1.2.2.5 en 2.16.528.1.1003.1.2.2.6. Voor services certificaten in het domein Organisatie zijn de OID's: 2.16.528.1.1003.1.2.5.4 2.16.528.1.1003.1.2.5.5 en 2.16.528.1.1003.1.2.5.6 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	MOET worden gebruikt en voorzien zijn van een wereldwijd uniek nummer dat de service identificeert.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		MOET een unieke identifier bevatten in het othername attribuut. Andere attributen dan hieronder genoemd MOGEN NIET worden gebruikt.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
SubjectAltName.dNSName[7]	V/N		Naam die de service of server identificeert. Verplicht: Bij services server certificaten [OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] MOET dit veld minimaal 1 "fully-qualified domain name (FQDN)" (zie de definitie in deel 4) bevatten. In dit veld MOGEN meerdere FQDN's worden gebruikt. Deze FQDN's MOETEN uit dezelfde domeinnaam range komen. (b.v. www.logius.nl, applicatie.logius.nl, secure.logius.nl etc. etc.). Niet toegestaan: Bij overige services certificaten [OID 2.16.528.1.1003.1.2.2.4 en	RFC2818, RFC5280	IA5String	De abonnee MOET aantonen dat de organisatie deze naam mag voeren. Het is niet toegestaan in dit attribuut wildcard FQDN's, locale domeinnamen, private IP adressen, alleen een hostname, internationalized domain names (IDN's) en null characters \0 te gebruiken. Bij services server certificaten [OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] MOET de CSP bij erkende registers (Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA)) controleren of de abonnee de eigenaar is van de domeinnaam of dat de abonnee exclusief geautoriseerd is door de geregistreerde domeinnaam eigenaar om, namens de geregistreerde domeinnaam eigenaar, de domeinnaam te gebruiken. [OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] De CSP MAG in uitzonderlijke situaties nog een services server certificaat

[7] Dit veld/attribuut moet uiterlijk zijn opgenomen in certificaten die vanaf 1-7-2011 worden uitgegeven.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
			2.16.528.1.1003.1.2.5.4] en [OID 2.16.528.1.1003.1.2.2.5 en 2.16.528.1.1003.1.2.5.5] MAG dit veld NIET gebruikt worden.			uitgeven zonder FQDN. Hierbij gelden de volgende aanvullende eisen: met ingang van 1 juli 2012 MOET de CSP de abonnee informeren dat het gebruik van server certificaten zonder FQDN wordt afgeraden en dat uiterlijk met ingang van 1 oktober 2016 alle nog geldige server certificaten zonder FQDN zullen worden ingetrokken. In het geval een CSP op of na 1 juli 2012 een server certificaat uitgeeft zonder FQDN dan MOET als "datum geldigheid tot", uiterlijk 1 november 2015 worden aangehouden.
SubjectAltName.iPAddress	A	Nee	MAG het publieke IP adres van de server bevatten waarvan de abonnee de eigenaar is of die in opdracht van de abonnee, wordt gehost door een leverancier.	RFC 5280, RFC 791, RFC 2460	Octet string	De CSP MOET verifiëren dat de abonnee de eigenaar is van het publieke IP adres of dat een leverancier het publieke IP adres mag gebruiken in opdracht van de abonnee. Het is niet toegestaan in dit attribuut private IP adressen op te nemen.
SubjectAltName.otherName	V		MOET worden gebruikt met daarin een uniek nummer dat de certificaathouder identificeert. In het authenticatiecertificaat MAG	PKIo	IA5String, Microsoft UPN, IBM Principal-Name of Permanent-Identifier	Bevat de OID van de CPS en een nummer dat op unieke wijze blijvend het subject (service) identificeert, gescheiden door een punt of liggend streepje ('-'). Het is aan te bevelen een bestaand registratienummer uit backoffice systemen te gebruiken samen met een code voor de organisatie. In combinatie met het CSP OID-

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
			daarnaast als othername een Principal-Name (UPN) worden opgenomen voor gebruik met SSO (Single Sign On).			nummer is deze identifier wereldwijd uniek. Dit nummer MOET persistent te zijn. Als er ook een othername voor Single Sign On 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		
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	RFC 5280		In een (Nederlandstalige) browser zal dan te zien zijn: "Subjecttype = Eindentiteit", "Beperking voor padlengte = Geen".

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
			"FALSE").			
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	V/O	Ja / Nee	Wordt alleen gebruikt indien nodig voor de specifieke service.	RFC 5280	KeyPurposeId's	Bij services authenticatie certificaten [OID 2.16.528.1.1003.1.2.2.4 en 2.16.528.1.1003.1.2.5.4 alleen voor wat betreft code signing certificaten] MOET ExtkeyUsage worden opgenomen, MOET deze extensie als “critical” worden gemerkt, MOET in deze extensie de KeyPurposeId id-kp-codeSigning worden opgenomen en MOGEN andere KeyPurposeId’s NIET worden opgenomen. Bij services server certificaten [OID 2.16.528.1.1003.1.2.2.6 en 2.16.528.1.1003.1.2.5.6] MOET deze extensie worden opgenomen,

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
						MAG deze extensie NIET als "critical" worden gemerkt, MOET deze extensie de KeyPurposId's id-kp-serverAuth en id-kp-clientAuth bevatten, MAG aanvullend de KeyPurposeId id-kp-emailProtection worden opgenomen, MAG eveneens aanvullend elke andere, in een open of geaccepteerde standaard gedefinieerde KeyPurposeId die bedoeld is voor het identificeren van een service op basis van zijn FQDN worden opgenomen en MOGEN andere KeyPurposeId's NIET worden opgenomen. Overige servicecertificaten MOGEN ExtendedKeyUsage gebruiken, waarbij geldt dat de KeyPurposeId id-kp-serverAuth NIET MAG worden opgenomen, dat de KeyPurposeId id-kp-codeSigning NIET MAG worden opgenomen, dat de KeyPurposeId AnyextendedKeyusage NIET MAG worden opgenomen, dat elke KeyPurposeId die uitsluitend bedoeld is voor het identificeren van een service op basis van zijn FDQN NIET MAG worden opgenomen maar dat wel MAG worden opgenomen: elke andere, in een open of geaccepteerde standaard gedefinieerde, KeyPurposeId die correspondeert met het sleutelgebruik zoals aangeduid in de KeyUsage extensie.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
InhibitAnyPolicy	N		Wordt niet gebruikt.	RFC 5280		Wordt niet gebruikt in eindgebruiker certificaten.
FreshestCRL	O	Nee	MOET de URI van een Delta-CRL distributiepunt bevatten, indien gebruik wordt gemaakt van Delta-CRL's.	RFC 5280, PKIo		Delta-CRL's zijn een optionele uitbreiding. Om aan de eisen van PKIoverheid te voldoen MOET een CSP tevens volledige CRL's publiceren met de geëiste uitgiftefrequentie.

Private extensies

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
authorityInfoAccess	O	Nee	Dit attribuut MOET de URI van een OCSP responder bevatten als Online Certificate Status Protocol (OCSP) een rol speelt.			Dit veld kan verder optioneel gebruikt worden om te verwijzen naar andere aanvullende informatie over de CSP.
SubjectInfoAccess	O	Nee		RFC 5280	OID, Generalname	Dit veld kan gebruikt worden om te verwijzen naar aanvullende informatie over het subject.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
BiometricInfo	N		Wordt niet gebruikt in services certificaten.	PKIo		Biometrische informatie is niet zinvol in niet persoonsgebonden certificaten zoals services certificaten.
QcStatement	N	Nee		RFC 3739, ETSI TS 102 280, ETSI TS 101 862	OID	Dit attribuut wordt alleen gebruik in persoonsgebonden certificaten en is niet toegestaan in services certificaten.

Profiel van de CRL

Algemene eisen aan de CRL
De CRL's moeten voldoen aan de X.509v3 standaard voor publieke sleutel certificaten en CRL's.
Een CRL bevat informatie over ingetrokken certificaten die binnen de huidige geldigheidsperiode vallen of waarvan de geldigheidsperiode minder dan 6 maanden geleden is verlopen (conform Wet Elektronische Handtekeningen).

CRL attributen

Veld / Attribuut	Criteria	Beschrijving	Norm referentie1	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. Ten behoeve van maximale interoperabiliteit wordt voor certificaten onder het G1 stamcertificaat alleen sha-1WithRSAEncryption toegestaan. 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

Veld / Attribuut	Criteria	Beschrijving	Norm referentie1	Type	Toelichting
					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 document of basisregistratie.	ETSI TS 102280: 5.2.4	UTF8String	
Issuer.organizationalUnitName	O	Optionele aanduiding van een organisatieonderdeel. Dit veld MAG NIET een functieaanduiding of dergelijke bevatten. Wel eventueel de typen certificaten die worden ondersteund.	ETSI TS 102280: 5.2.4	UTF8String	Meerdere instanties van dit attribuut MOGEN gebruikt worden.
Issuer.localityName	N	Wordt niet gebruikt.	PKIo	UTF8String	-
Issuer.serialNumber	O	MOET worden gebruikt indien eenduidige naamgeving dit vereist	RFC 3739	Printable String	

Veld / Attribuut	Criteria	Beschrijving	Norm refe-rentie1	Type	Toelichting
Issuer.commonName	V	MOET de naam van de CA te bevatten conform geaccepteerd document of basisregistratie, optioneel aangevuld met de Domein aanduiding en/of de typen certificaat die worden ondersteund.	PKIo, RFC 5280	UTF8String	
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 datum en tijdstip van revocatie en serialNumber van de ingetrokken certificaten bevatten.	RFC 5280	SerialNumbers, UTCTime	Als er geen ingetrokken certificaten zijn MAG de revoked certificates list niet aanwezig zijn.

CRL extensies

Veld / Attribuut	Criteria	Critical	Beschrijving	Norm referentie1	Type	Toelichting
authorityKeyIdentifier	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	KeyIdentifier	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	
DeltaCRLIndicator	O	Ja	Indien van 'delta CRLs' gebruik wordt gemaakt MOET een waarde voor dit attribuut worden ingevuld.	RFC 5280	BaseCRLNumber	Bevat het nummer van de basisCRL waarop de Delta-CRL een uitbreiding vormt.

issuingDistributionPoint	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.
authorityInfoAccess	O	Nee	Optionele verwijzing naar het certificaat van de CRL.Issuer.	RFC 5280	id-ad-caIssuers (URI)	MOET conformeren aan § 5.2.7 van RFC 5280.
CRLReason	O	Nee	Indien gebruikt geeft dit de reden aan waarom een certificaat is ingetrokken.	RFC 5280	reasonCode	Als geen reden wordt opgegeven MOET dit veld worden weggelaten.
holdInstructionCode	N	Nee	Wordt niet gebruikt.	RFC 5280	OID	De PKI voor de overheid maakt geen gebruik van de status 'On hold'.
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 de datum en tijdstip waarop de CSP de revocatie heeft verwerkt.	RFC 5280	Generalized-Time	
certificateIssuer	A	Ja	Als gebruik wordt gemaakt van een indirecte CRL	RFC 5280	GeneralNames	

			kan dit attribuut worden gebruikt om de oorspronkelijke uitgever van het certificaat te identificeren.			

Profiel OCSP

Algemene eisen aan OCSP

- Indien de CSP het Online Certificate Status Protocol (OCSP) ondersteunt, MOETEN OCSP responses en OCSPSigning certificates voldoen aan de eisen die hieraan worden gesteld in IETF RFC 2560.
- OCSPSigning certificaten MOETEN in overeenstemming zijn met de X.509v3 norm voor publieke sleutel certificaten. Algemene eisen aan certificaten staan in RFC 5280.
- 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.
- OCSPSigning certificaten moeten voldoen aan het profiel voor services certificaten zoals hierboven gegeven, met de volgende uitzonderingen:

OCSP Signing certificaat attributen

Veld / Attribuut	Criteria	Beschrijving	Norm referentie1	Type	Toelichting
Issuer	V	MOET een Distinguished Name (DN) bevatten.	PKIo		Een OCSPSigning certificaat MOET zijn uitgegeven onder de hiërarchie van de PKI voor de overheid.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
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 OCSPSigning certificaten MOET het digitalSignature bit zijn opgenomen en de extensie als essentieel zijn aangemerkt. Het non-Repudiation bit MAG NIET worden opgenomen.	RFC 5280, RFC 2560	BitString	
CertificatePolicies	V	Nee	MOET de OID bevatten van de PKIoverheid certificate policy (CP) voor authenticiteitscertificaten voor services, de URI van het CPS, en een gebruikersnotitie. Het te gebruiken OID schema in de PKI voor de overheid wordt beschreven in de CP - Services.	RFC 3739	OID, String, String	Voor services authenticatiecertificaten in het domein Overheid/Bedrijven is de OID: 2.16.528.1.1003.1.2.2.4. Voor services authenticatiecertificaten in het domein Organisatie is de OID: 2.16.528.1.1003.1.2.5.4.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
ExtKeyUsage	V	Ja	MOET worden gebruikt met de waarde id-kp-OCSPSigning.	RFC 5280		
ocspNoCheck	O			RFC 2560		

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[8]. De PA heeft er bewust voor gekozen om alle eisen maar eenmalig op te nemen.

[8] *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 2.2-4 2.2-5

		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		3.2.1-1
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 3.2.5-3
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**			4.1-1
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[9] artikel 2 lid 1l	4.9.3-1 4.9.3-2 4.9.3-3 4.9.3-4
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

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

4.9.8	Maximale latentie voor CRL's			
4.9.9	Online intrekking/statuscontrole			4.9.9-1 4.9.9-2 4.9.9-3 4.9.9-4 4.9.9-5 4.9.9-6
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		4.10.1-1
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		5.2.5-1

		7.4.5.b 7.4.5.g 7.4.5.h		5.2.5-2
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		5.3.1-1
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 5.5.1-2
5.5.2	Bewaartermijn archief	*7.4.11.e* 7.3.1.n		5.5.2-1 5.5.2-2
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 6.1.1-4
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 6.2.11-3
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 6.3.2-3
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-, CRL- en OSCP-profielen**			
7.1	**Certificaatprofielen**			7.1-1
7.2	**CRL-profielen**			7.2-1
7.3	**OCSP-profielen**			7.3-1

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		9.17-1 9.17-2 9.17-3 9.17-4

		7.5.c 7.5.e 7.5.g		

10 Revisies

10.1 Wijzigingen van versie 3.3 naar 3.4

10.1.1 Nieuw

- Eis 2.2-5 (uiterlijke ingangsdatum 4 weken na publicatie PVE 3.4);
- Eis 5.2.5-2 (uiterlijke ingangsdatum 4 weken na publicatie PVE 3.4);
- Eis 5.3.1-1 (uiterlijke ingangsdatum 1-7-2013);
- Eis 5.3.2-1 (uiterlijke ingangsdatum 4 weken na publicatie PVE 3.4);

10.1.2 Aanpassingen

- Eis 4.1-1 (uiterlijke ingangsdatum 4 weken na publicatie PVE 3.4);
- Eis 4.9.9-7 (uiterlijke ingangsdatum 4 weken na publicatie PVE 3.4);
- Eis 6.1.1-4 (reeds ingegaan via versnelde wijzigingsprocedure op 1-10-2012);
- Beschrijving en toelichting bij subject.Countryname (reeds ingegaan via versnelde wijzigingsprocedure op 1-10-2012);
- Paragraaf 9.12.1 m.b.t. de wijzigingsprocedure

10.1.3 redactioneel

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

10.2 Wijzigingen van versie 3.2 naar 3.3

10.2.1 Nieuw

- Eis 2.2-4;
- Eis 3.2.5-3;
- Eis 4.1-1;
- Eis 4.10.1-1;
- Eis 5.2.5-1 (uiterlijke ingangsdatum 1-12-2012);
- Eis 5.4.3-1;
- Eis 5.5.1-2;
- Eis 5.5.2-2;
- Eis 5.7.4-1 (uiterlijke ingangsdatum 1-12-2012).

10.2.2 Aanpassingen

- Eis 4.9.1-1;
- Eis 4.9.9-1;
- Eis 4.9.9-3;
- 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 6.1.1-4;
- Eis 6.3.2-2 (uiterlijke ingangsdatum 1-10-2012);
- Eis 6.5.1-3;
- Eis 6.7.1-1;
- Beschrijving bij attributen Subject.stateOrProvinceName en Subject.localityName;
- Toelichting bij attributen Subject.commonName, SubjectAltName.iPAddress, SubjectAltName.dNSName en Extkeyusage.

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 6.1.1-4 (uiterlijke ingangsdatum is 1-7-2012);
- 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 3.2.1-1;
- Eis 4.5.2-1 (uiterlijke ingangsdatum is 1-2-2012);
- Eis 4.9.3-4 (uiterlijke ingangsdatum is 1-4-2012);
- Eis 5.7.1-2;
- Eis 6.2.3-2;
- Beschrijving bij attribuut Subject.serialNumber.

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 3.2.1-1, 4.9.7-1, 4.9.9-6, 6.3.2-2, 6.5.1-1, 6.5.1-2, 9.17-2, 9.17-3 en 9.17-4.

10.4.2 Aanpassingen

- Eis 4.9.1-1 en 6.3.2-1;
- 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

10.5.1 Nieuw

- Attribuut SubjectAltName.dNSName.

10.5.2 Aanpassingen

- Paragraaf 1.3;
- Eis 4.9.2-1 en 6.2.11-3;
- Toelichting bij attribuut Signature.

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

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 Wijziging van versie 1.2 naar 2.0

10.7.1 Nieuw
- Eis 4.9.3-1;
- Attribuut authorityInfoAccess onder CRL extensies.

10.7.2 Aanpassingen
- Toelichting bij attribuut Subject.commonName.

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

10.8 Wijziging van versie 1.1 naar 1.2

10.8.1 Nieuw
Geen wijzigingen.

10.8.2 Aanpassingen
- Paragraaf 1.2 en 1.4;
- Eis 3.3.1-1, 3.3.1-2, 6.1.1-1, 6.1.1-2, 6.1.1-3, 6.1.2-1, 6.1.5-1, 6.1.7-1, 6.2.3-1, 6.2.3-2, 6.2.3-3, 6.2.4.2-1, 6.2.5-1, 6.3.1-1, 9.6.1-1, 9.6.1-2, 9.6.1-3, 9.8-1 en 9.8-2;
- Toelichting bij attribuut Signature en CertificatePolicies;
- Attribuut Subject.serialNumber.

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

10.9 Wijziging van versie 1.0 naar 1.1

10.9.1 Nieuw
Geen wijzigingen.

10.9.2 Aanpassingen
- Eis 4.4.1-1;
- Toelichting bij attribuut Subject.commonName.

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

10.10 Versie 1.0
Eerste versie.