



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Programma van Eisen deel 3c: Certificate Policy - Domein Burger

Datum 23 juni 2014

Authenticiteit	2.16.528.1.1003.1.2.3.1
Onweerlegbaarheid	2.16.528.1.1003.1.2.3.2
Vertrouwelijkheid	2.16.528.1.1003.1.2.3.3

Colofon

Versienummer 3.7
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

Inhoud	3
1 Introductie op de Certificate Policy	7
1.1 <i>Achtergrond</i>	7
1.1.1 <i>Opzet van de Certificate Policy</i>	7
1.1.2 <i>Status</i>	8
1.2 <i>Verwijzingen naar deze CP</i>	9
1.3 <i>Gebruikersgemeenschap</i>	9
1.4 <i>Certificaatgebruik</i>	10
1.5 <i>Contactgegevens Policy Authority</i>	10
2 Publicatie en verantwoordelijkheid voor elektronische opslagplaats	11
2.1 <i>Elektronische opslagplaats</i>	11
2.2 <i>Publicatie van CSP-informatie</i>	11
2.4 <i>Toegang tot gepubliceerde informatie</i>	12
3 Identificatie en authenticatie	13
3.1 <i>Naamgeving</i>	13
3.2 <i>Initiële identiteitsvalidatie</i>	13
3.3 <i>Identificatie en authenticatie bij vernieuwing van het certificaat</i>	14
4 Operationele eisen certificaatlevenscyclus	16
4.4 <i>Acceptatie van certificaten</i>	16
4.5 <i>Sleutelpaar en certificaatgebruik</i>	16
4.9 <i>Intrekking en opschorting van certificaten</i>	16
4.10 <i>Certificaat statusservice</i>	21
5 Management, operationele en fysieke beveiligingsmaatregelen	22
5.2 <i>Procedurele beveiliging</i>	22
5.3 <i>Personele beveiliging</i>	23
5.4 <i>Procedures ten behoeve van beveiligingsaudits</i>	24
5.5 <i>Archivering van documenten</i>	25
5.7 <i>Aantasting en continuïteit</i>	25
6 Technische beveiliging	28
6.1 <i>Genereren en installeren van sleutelparen</i>	28
6.2 <i>Private sleutelbescherming en cryptografische module engineering beheersmaatregelen</i>	30

6.3	<i>Andere aspecten van sleutelpaarmanagement</i>	32
6.4	<i>Activeringsgegevens</i>	33
6.5	<i>Logische toegangsbeveiliging van CSP-computers</i>	33
6.6	<i>Beheersmaatregelen technische levenscyclus</i>	35
6.7	<i>Netwerkbeveiliging</i>	35
7	Certificaat-, CRL- en OCSP-profielen	37
7.1	<i>Certificaatprofielen</i>	37
7.2	<i>CRL-profielen</i>	37
7.3	<i>OCSP-profielen</i>	37
8	Conformiteitbeoordeling	38
9	Algemene en juridische bepalingen	39
9.2	<i>Financiële verantwoordelijkheid en aansprakelijkheid</i>	39
9.5	<i>Intellectuele eigendomsrechten</i>	39
9.6	<i>Aansprakelijkheid</i>	39
9.8	<i>Beperkingen van aansprakelijkheid</i>	40
9.12	<i>Wijzigingen</i>	41
9.12.1	<i>Wijzigingsprocedure</i>	41
9.13	<i>Geschillenbeslechting</i>	42
9.14	<i>Van toepassing zijnde wetgeving</i>	42
9.17	<i>Overige bepalingen</i>	42
	Bijlage A Profielen certificaten en certificaat statusinformatie	43
	Bijlage B Verwijzingsmatrix	60
10	Revisies	83
10.1	<i>Wijzigingen van versie 3.6 naar 3.7</i>	83
10.1.1	<i>Aanpassingen</i>	83
10.2	<i>Wijzigingen van versie 3.5 naar 3.6</i>	83
10.2.1	<i>Aanpassingen</i>	83
10.2.2	<i>Redactioneel</i>	83
10.3	<i>Wijzigingen van versie 3.4 naar 3.5</i>	83
10.3.1	<i>Aanpassingen</i>	83
10.4	<i>Wijzigingen van versie 3.3 naar 3.4</i>	83
10.4.1	<i>Nieuw</i>	83
10.4.2	<i>Aanpassingen</i>	83
10.4.3	<i>Redactioneel</i>	83
10.5	<i>Wijzigingen van versie 3.2 naar 3.3</i>	83
10.5.1	<i>Nieuw</i>	84
10.5.2	<i>Aanpassingen</i>	84
10.5.3	<i>Redactioneel</i>	84

<i>10.6</i>	<i>Wijzigingen van versie 3.1 naar 3.2</i>	<i>84</i>
10.6.1	Nieuw	84
10.6.2	Aanpassingen	84
10.6.3	Redactioneel	84
<i>10.7</i>	<i>Wijzigingen van versie 3.0 naar 3.1</i>	<i>84</i>
10.7.1	Nieuw	84
10.7.2	Aanpassingen	84
10.7.3	Redactioneel	84
<i>10.8</i>	<i>Wijzigingen van versie 2.1 naar 3.0</i>	<i>84</i>
10.8.1	Nieuw	84
10.8.2	Aanpassingen	85
10.8.3	Redactioneel	85
<i>10.9</i>	<i>Wijzigingen van versie 2.0 naar 2.1</i>	<i>85</i>
10.9.1	Redactioneel	85
<i>10.10</i>	<i>Wijzigingen van versie 1.2 naar 2.0</i>	<i>85</i>
10.10.1	Nieuw	85
10.10.2	Aanpassingen	85
10.10.3	Redactioneel	85
<i>10.11</i>	<i>Wijzigingen van versie 1.1 naar 1.2</i>	<i>85</i>
10.11.1	Nieuw	85
10.11.2	Aanpassingen	85
10.11.3	Redactioneel	85
<i>10.12</i>	<i>Wijzigingen van versie 1.0 naar 1.1</i>	<i>85</i>
10.12.1	Nieuw	85
10.12.2	Aanpassingen	85
10.12.3	Redactioneel	85
<i>10.13</i>	<i>Versie 1.0</i>	<i>86</i>

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	Vastgesteld door BZK januari 2013
3.5	06-07-2013	Vastgesteld door BZK juli 2013
3.6	01-2014	Vastgesteld door BZK januari 2014
3.7	06-2014	Vastgesteld door BZK juni 2014

1 Introductie op de Certificate Policy

1.1 Achtergrond

Dit is deel 3c 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 persoonsgebonden certificaten uitgegeven door een CSP in het domein Burger.

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

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

1.1.1 Opzet van de Certificate Policy

Zoals in deel 1 van het PvE is aangegeven bestaan de eisen die onderdeel uitmaken van de CP uit eisen¹:

- die voortkomen uit het Nederlandse wettelijke kader in relatie tot de elektronische handtekening;
- die voortkomen uit de vigerende versie van de standaard ETSI EN 319 411-2, QCP public + SSCD (ETSI CP OID 0.4.0.1456.1.1);
- die specifiek door en voor de PKIoverheid zijn opgesteld.

In de hoofdstukken 2 t/m 9 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 ² .
Nummer	Uniek nummer van de PKIo-eis. Per paragraaf wordt een doorlopende nummering gehanteerd voor de PKIo-eisen. In combinatie met het RFC 3647 paragraafnummer vormt dit een unieke aanduiding voor de PKIo-eis.
ETSI	Verwijzing naar de eis(en) uit ETSI EN 319 411-2 waarvan de PKIo-eis is afgeleid c.q. een nadere invulling is.
PKIo	De PKIo-eis die binnen dit domein van de PKI voor de overheid van toepassing 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 In de hoofdstukken 2 t/m 9 zijn alleen die paragrafen uit RFC 3647 opgenomen waarvoor een PKIo-eis van toepassing is.

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 eindgebruikercertificaten en certificaat statusinformatie opgenomen.

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

1.1.2

Status

Dit is versie 3.7 van deel 3c van het PvE. De huidige versie is bijgewerkt tot en met juni 2014.

De PA heeft de grootst mogelijke aandacht en zorg besteed aan de gegevens en informatie, die zijn opgenomen in deze CP. Desalniettemin is het mogelijk dat onjuistheden en onvolkomenheden voorkomen. De PA aanvaardt geen enkele aansprakelijkheid voor schade als gevolg van deze onjuistheden of onvolkomenheden, noch voor schade die wordt veroorzaakt door het gebruik of de verspreiding van deze CP, indien deze CP wordt gebruikt buiten het in paragraaf 1.4 van deze CP beschreven certificaatgebruik.

1.2 Verwijzingen naar deze CP

Binnen de PKI voor de overheid is er sprake van een structuur gebaseerd op het SHA-1 algoritme (G1) en op het SHA-256 algoritme (G2 en G3). Verder is er onder de stamcertificaten, een indeling gemaakt in verschillende domeinen.

Voor de G1 root is sprake van de domeinen Overheid/Bedrijven (deze twee domeinen zijn in de loop van de tijd samengevoegd) en Burger. Voor de G2 root is er sprake van een domein Organisatie, een domein Burger en een domein Autonome Apparaten.

Voor de G3 root is sprake van een domein Organisatie Persoon, een domein Organisatie Services, een domein Burger en een domein Autonome Apparaten.

Elke CP wordt uniek geïdentificeerd door een OID, conform het onderstaande schema.

OID	CP
2.16.528.1.1003.1.2.3.1	voor het authenticiteitcertificaat, dat de publieke sleutel bevat ten behoeve van identificatie en authenticatie
2.16.528.1.1003.1.2.3.2	voor het handtekeningcertificaat, dat de publieke sleutel bevat ten behoeve van de gekwalificeerde elektronische handtekening
2.16.528.1.1003.1.2.3.3	voor het vertrouwelijkheidcertificaat, dat de publieke sleutel bevat ten behoeve van vertrouwelijkheid

De OID is als volgt opgebouwd: {joint-iso-itu-t (2). country (16). nederland (528). Nederlandse organisatie (1). nederlandse-overheid (1003). pki voor de overheid (1). cp (2). domein burger (3). authenticiteit (1)/onweerlegbaarheid (2)/vertrouwelijkheid (3). versienummer}.

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

1.3 Gebruikersgemeenschap

In het domein Overheid en Bedrijven, het domein Organisatie en het domein Organisatie Persoon is het onderscheid tussen abonnee en certificaathouder relevant omdat in de praktijk de volgende situatie is voorzien: de CSP heeft een overeenkomst met de abonnee waarin is geregeld dat de CSP certificaten zal uitgeven aan de door de abonnee aan te wijzen certificaathouders (bijvoorbeeld werknemers van de abonnee). In het domein Burger zijn abonnee en certificaathouder dezelfde persoon. Waar in het CP Burger de abonnee wordt vermeld, dient deze te worden gelezen als certificaathouder. De burger neemt daarmee de verplichtingen van zowel abonnee als certificaathouder op zich.

Binnen het domein Burger bestaat de gebruikersgemeenschap uit certificaathouders (de burgers die de certificaten gebruiken) en uit vertrouwende partijen die handelen in vertrouwen op certificaten van de betreffende certificaathouders.

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

- Een abonnee is een natuurlijke persoon die met een CSP een overeenkomst sluit voor het laten certificeren van de publieke sleutels. Een abonnee is tevens certificaathouder.
- 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.
- Een vertrouwende partij is iedere natuurlijke of rechtspersoon die ontvanger is van een certificaat en die handelt in vertrouwen op dat certificaat.

1.4 Certificaatgebruik

Het gebruik van certificaten uitgegeven onder deze CP heeft betrekking op communicatie van certificaathouders op persoonlijke titel.

[OID 2.16.528.1.1003.1.2.3.1] Authenticiteitcertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het betrouwbaar identificeren en authenticeren van personen langs elektronische weg. Dit betreft zowel de identificatie van personen onderling als tussen personen en geautomatiseerde middelen.

[OID 2.16.528.1.1003.1.2.3.1] Authenticiteitcertificaten die onder deze CP worden uitgegeven, kunnen niet worden gebruikt voor het identificeren van personen in gevallen waarbij de wet vereist dat de identiteit van personen alleen met een in de Wet op de identificatieplicht aangewezen document mag worden vastgesteld.

[OID 2.16.528.1.1003.1.2.3.2] Handtekeningcertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt om elektronische handtekeningen te verifiëren, die "dezelfde rechtsgevolgen hebben als een handgeschreven handtekening", zoals wordt aangegeven in artikel 15a, eerste en tweede lid, in Titel 1 van Boek 3 van het Burgerlijk Wetboek onder afdeling 1A en zijn gekwalificeerde certificaten zoals bedoeld in artikel 1.1, lid ss van de Telecomwet.

[OID 2.16.528.1.1003.1.2.3.3] Vertrouwelijkheidcertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het beschermen van de vertrouwelijkheid van gegevens, die worden uitgewisseld en/of opgeslagen in elektronische vorm. Dit betreft zowel de uitwisseling tussen personen onderling als tussen personen en geautomatiseerde middelen.

1.5 Contactgegevens Policy Authority

De PA is verantwoordelijk voor deze CP. Vragen met betrekking tot deze CP kunnen worden gesteld aan de PA, waarvan het adres gevonden kan worden op: <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	7.3.5.e, EN 319 411-2
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	7.3.1.b, EN 319 411-2 6.2, EN 319 401 7.3.5.f, EN 319 411-2
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 EN 319 411-2, QCP public + SSCD. 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	7.3.1.b, EN 319 411-2
PKIo	Het CPS dient in het Nederlands te zijn opgesteld.

RFC 3647	2.2 Publicatie van CSP-informatie
Nummer	2
ETSI	5.2.b, EN 319 411-2
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	7.3.1.b, EN 319 411-2
PKIo	Alle informatie zal in het Nederlands beschikbaar moeten zijn.

RFC 3647	2.2 Publicatie van CSP-informatie
Nummer	4
ETSI	7.3.1.a, EN 319 411-2
PKIo	De CSP dient de burger actief te informeren en in de voorwaarden te vermelden dat het authenticiteitcertificaat niet in de Wet op de identificatieplicht (Wid) als identiteitsdocument is aangewezen en derhalve niet kan worden gebruikt voor het identificeren van personen in gevallen waarbij de wet vereist dat de identiteit van personen met een in de Wet op de identificatieplicht aangewezen document wordt vastgesteld. De CSP moet hiermee tot uitdrukking brengen dat het authenticiteitcertificaat niet kan worden gebruikt bij het afnemen van overheidsdiensten waarbij de wet vereist dat de identiteit van personen met een in de Wid aangewezen document wordt vastgesteld.

2.4 Toegang tot gepubliceerde informatie

RFC 3647	2.4 Toegang tot gepubliceerde informatie
Nummer	1
ETSI	6.1.c, EN 319 401
PKIo	Het CPS van een Certification Service Provider binnen de PKIoverheid dient voor een ieder raadpleegbaar te zijn.
Opmerking	Met een ieder wordt bedoeld dat, naast de abonnees en certificaathouders, 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	7.3.3.a, EN 319 411-2 7.3.6.g, EN 319 411-2
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 en toegestane naamformaten opgenomen.

RFC 3647	3.1.3 Anonimiteit of pseudonimiteit van certificaathouders
Nummer	1
ETSI	7.3.3.a, EN 319 411-2 7.3.6.g, EN 319 411-2
PKIo	Het gebruik van pseudoniemen in certificaten is niet toegestaan.

3.2 Initiële identiteitsvalidatie

RFC 3647	3.2.3 Authenticatie van persoonlijke identiteit
Nummer	1
ETSI	7.3.1.d, EN 319 411-2
PKIo	De CSP dient te verifiëren dat de door de certificaathouder aangemelde volledige naam die in het certificaat wordt opgenomen juist en volledig is, met inbegrip van achternaam, eerste voornaam, initialen of overige voorna(a)m(en) (indien van toepassing) en tussenvoegsels (indien van toepassing).

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	7.3.2.d, EN 319 411-2
PKIo	[OID 2.16.528.1.1003.1.2.3.3] QCP 7.3.2.d is van toepassing.
Opmerking	In QCP 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	7.3.2.d, EN 319 411-2
PKIo	[OID 2.16.528.1.1003.1.2.3.1] en [OID 2.16.528.1.1003.1.2.3.2] QCP 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 handtekeningcertificaat.

RFC 3647	3.3.1 Identificatie en authenticatie bij routinematige vernieuwing van het certificaat
Nummer	3
ETSI	7.3.2.a, EN 319 411-2 7.3.2.c, EN 319 411-2
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	7.3.2.d, EN 319 411-2

PKIo	Na intrekking van het certificaat mogen de desbetreffende sleutels niet opnieuw worden gecertificeerd. QCP 7.3.2.d is niet van toepassing.
-------------	--

4 Operationele eisen certificaatlevenscyclus

4.4 Acceptatie van certificaten

RFC 3647	4.4.1 Activiteiten bij acceptatie van certificaten
Nummer	1
ETSI	7.3.1.i, EN 319 411-2
PKIo	Na uitgifte van een certificaat, dient de certificaathouder expliciet de overhandiging van het sleutelmateriaal behorend bij het certificaat aan de CSP te bevestigen.

4.5 Sleutelbaar en certificaatgebruik

RFC 3647	4.5.2 Gebruik van publieke sleutel en certificaat door vertrouwende partij
Nummer	1
ETSI	6.3.a, EN 319 411-2
PKIo	<p>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.</p> <p>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.</p>
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	7.3.6.a, EN 319 411-2
PKIo	<p>Certificaten zullen worden ingetrokken wanneer:</p> <ul style="list-style-type: none"> 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 priv�sleutel van de

	<p>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 SSCD, gestolen of vermoedelijk gestolen sleutel of SSCD of vernietigde sleutel of SSCD;</p> <ul style="list-style-type: none"> • 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 van een wezenlijke verandering in de informatie, die in het certificaat staat. Voorbeeld daarvan is: verandering van de naam van de certificaathouder; • de CSP bepaald dat het certificaat niet is uitgegeven in overeenstemming met deze CP of het bijbehorende CPS van de CSP of de overeenkomst die de CSP met de abonnee heeft gesloten; • de CSP bepaald dat informatie in het certificaat niet juist of misleidend is; • de CSP haar werkzaamheden staakt en de CRL en OCSP dienstverlening niet wordt overgenomen door een andere CSP. • De PA van PKIoverheid vaststelt dat de technische inhoud van het certificaat een onverantwoord risico met zich meebrengt voor abonnees, vertrouwende partijen en derden (b.v. browserpartijen).
Opmerking	Daarnaast kunnen certificaten worden ingetrokken als maatregel om een calamiteit te voorkomen, c.q. te bestrijden. Als calamiteit wordt zeker de aantasting of vermeende aantasting van de private sleutel van de CSP waarmee certificaten worden ondertekend, beschouwd.

RFC 3647	4.9.2 Wie mag een verzoek tot intrekking doen
Nummer	1
ETSI	7.3.6.a, EN 319 411-2
PKIo	<p>De volgende partijen mogen een verzoek tot intrekking van een eindgebruikercertificaat doen:</p> <ul style="list-style-type: none"> • de certificaathouder; • de CSP; • ieder andere, naar het oordeel van de CSP, belanghebbende partij/persoon.
Opmerking	Aangezien in het domein Burger de certificaathouder ook de abonnee is, is de abonnee niet expliciet opgenomen als partij die een verzoek tot intrekking kan doen.

RFC 3647	4.9.3 Procedure voor een verzoek tot intrekking
Nummer	1
ETSI	7.3.6.a, EN 319 411-2

PKIo	De CSP mag additionele eisen stellen aan een intrekingsverzoek. 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	7.3.6.h, EN 319 411-2
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	7.3.6.a, EN 319 411-2
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	7.3.6.i, EN 319 411-2 (en BEH artikel 2I lid 1)
PKIo	De CSP moet in ieder geval gebruik maken van een CRL om de certificaatstatus informatie beschikbaar te stellen.

RFC 3647	4.9.5 Tijdsduur voor verwerking intrekingsverzoek
Nummer	1
ETSI	7.3.6.a, EN 319 411-2
PKIo	De maximale vertraging tussen de ontvangst van een intrekingsverzoek of intrekingsrapportage 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	6.3.a, EN 319 411-2
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	6.3.a, EN 319 411-2
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	7.3.6, EN 319 411-2
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	7.3.6.i, EN 319 411-2
PKIo	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	7.3.6.i, EN 319 411-2

PKIo	Indien de CSP het Online Certificate Status Protocol (OCSP) ondersteunt, dient dit te gebeuren in overeenstemming met IETF RFC 2560.
-------------	--

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	3
ETSI	7.3.6.i, EN 319 411-2
PKIo	<p>Ter verbijzondering van het in IETF RFC 2560 gestelde dienen OCSP responses digitaal te worden ondertekend door ofwel:</p> <ul style="list-style-type: none"> • de private (CA) sleutel waarmee ook het certificaat is ondertekend waarvan de status wordt gevraagd, of; • een door de CSP aangewezen responder die beschikt over een OCSP-Signing certificaat dat voor dit doel is uitgegeven door de CSP, of; • een responder die beschikt over een OCSP-Signing certificaat dat valt binnen de hiërarchie van de PKI voor de overheid.

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	4
ETSI	7.3.6.i, EN 319 411-2
PKIo	Ter verbijzondering van het in 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	7.3.6.i, EN 319 411-2
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	7.3.6.i, EN 319 411-2

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	4.9.13 Omstandigheden die leiden tot opschorting
Nummer	1
ETSI	7.3.6.d, EN 319 411-2
PKIo	Het is niet toegestaan om certificaatopschorting te ondersteunen.

4.10 Certificaat statusservice

RFC 3647	4.10.2 Beschikbaarheid certificaat statusservice
Nummer	1
ETSI	7.3.6.i, EN 319 411-2
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 Procedurele beveiliging
Nummer	1
ETSI	6.4.1.a, EN 319 401 6.4.5, EN 319 401
PKIo	<p>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.</p> <p>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.</p>

RFC 3647	5.2 Procedurele beveiliging
Nummer	2
ETSI	6.4.1.b, EN 319 401
PKIo	<p>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.</p> <p>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.</p> <p>Ook is de CSP gerechtigd om inzage te verkrijgen in het onderliggende bewijsmateriaal zoals audit dossiers en overige, al dan niet systeem-, documentatie.</p> <p>Uiteraard beperkt zich het bovenstaande tot de bij de leveranciers gehoste CSP-processen, -systemen en -infrastructuur voor PKIo kerndiensten.</p>

RFC 3647	5.2.4 Rollen die functiescheiding behoeven
Nummer	1
ETSI	6.4.3.d en 6.4.3.h, EN 319 401
PKIo	<p>De CSP dient functiescheiding te handhaven tussen tenminste de volgende functies:</p> <ul style="list-style-type: none"> • Security officer De security officer ziet toe op de implementatie en naleving van de vastgestelde beveiligingsrichtlijnen. • Systeem auditor De systeem auditor vervult een toezichhoudende 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	6.4.3.d en 6.4.3.h, EN 319 401
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.

5.3 Personele beveiliging

RFC 3647	5.3 Geheimhoudingsverklaring
Nummer	1
ETSI	6.4.3.e, EN 319 401
PKIo	Omdat het openbaar worden van vertrouwelijke informatie grote gevolgen kan hebben (o.a. voor de betrouwbaarheid) moet de CSP zich inspannen om

	er voor te zorgen dat vertrouwelijke informatie vertrouwelijk behandeld wordt en vertrouwelijk blijft. Eén van de inspanningen die hiervoor geleverd moet worden is het laten tekenen van een geheimhoudingsverklaring door personeelsleden en ingehuurde derden.
--	---

RFC 3647	5.3.2 Antecedentenonderzoek
Nummer	1
ETSI	6.4.3-j, EN 319 401
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	6.4.5.j, EN 319 401
PKIo	<p>Logging dient plaats te vinden op minimaal:</p> <ul style="list-style-type: none"> • Routers, firewalls en netwerk systeem componenten; • Database activiteiten en events; • Transacties; • Operating systemen; • Access control systemen; • Mail servers. <p>De CSP dient minimaal de volgende events te loggen:</p> <ul style="list-style-type: none"> • CA key life cycle management; • Certificate life cycle management; • Bedreigingen en risico's zoals: <ul style="list-style-type: none"> • 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. <p>De log bestanden moeten minimaal het volgende registreren:</p> <ul style="list-style-type: none"> • 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 opslaat.
------------------	--

RFC 3647	5.4.3 Bewaartermijn voor logbestanden
Nummer	1
ETSI	6.4.11.e, EN 319 401
PKIo	<p>De CSP moet logbestanden voor gebeurtenissen met betrekking tot:</p> <ul style="list-style-type: none"> • CA key life cycle management en; • Certificate life cycle management <p>7 jaar bewaren en daarna verwijderen.</p> <p>De CSP moet logbestanden voor gebeurtenissen met betrekking tot:</p> <ul style="list-style-type: none"> • Bedreigingen en risico's; <p>18 maanden bewaren en daarna verwijderen.</p> <p>De logbestanden moeten zodanig worden opgeslagen, dat de integriteit en toegankelijkheid van de data gewaarborgd is.</p>

5.5 Archivering van documenten

RFC 3647	5.5.2 Bewaartermijn archief
Nummer	1
ETSI	6.4.11.e, EN 319 401
PKIo	Geen PKIo-eis van toepassing, alleen een opmerking.
Opmerking	Op verzoek van de rechthebbende kan worden overeengekomen dat de gewenste informatie langer door de CSP wordt bewaard. Dit is echter geen verplichting voor de CSP.

5.7 Aantasting en continuïteit

RFC 3647	5.7.1 Procedures voor afhandeling incidenten en aantasting
Nummer	1
ETSI	7.4.8.d, EN 319 411-2
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

	<p>generation service, subject device provisioning service, dissemination service, revocation management service en revocation status service. Dit is in ieder geval maar niet limitatief:</p> <ul style="list-style-type: none"> • 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	7.4.8.d, EN 319 411-2
PKIo	<p>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.</p>

RFC 3647	5.7.4 Continuïteit van de bedrijfsvoering na calamiteit
Nummer	1
ETSI	6.4.8, EN 319 401
PKIo	<p>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:</p> <ul style="list-style-type: none"> ▪ 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 hoofdvesting 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	7.2.1.c en 7.2.1.d, EN 319 411-2
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	7.2.8.c en 7.3.1.l, EN 319 411-2
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 {12} CWA 14169 "Secure signature-creation devices "EAL 4+"" of gelijkwaardige beveiligingscriteria.

RFC 3647	6.1.1 Genereren van sleutelparen van de certificaathouders
Nummer	3
ETSI	7.2.8.a, EN 319 411-2
PKIo	Het algoritme en de lengte van de cryptografische sleutels dat de CSP gebruikt voor het genereren van de sleutels van certificaathouders dient te voldoen aan de eisen, die daaraan zijn gesteld in de lijst van cryptografische algoritmes en sleutellengtes, zoals gedefinieerd in ETSI TS 102 176-1.
Opmerking	Hoewel in ETSI TS 102 176 over aanbevolen algoritmes en sleutellengtes wordt gesproken, worden deze binnen de PKI voor overheid verplicht gesteld. Verzoeken voor gebruik van andere algoritmes dienen, voorzien van een motivatie te worden gedaan bij de PA van de PKI voor de overheid.

RFC 3647	6.1.2 Overdracht van private sleutel en SSCD aan certificaathouder
Nummer	1
ETSI	7.2.8.d, EN 319 411-2
PKIo	[OID 2.16.528.1.1003.1.2.3.2; OID 2.16.528.1.1003.1.2.3.1] De private sleutel van de certificaathouder dient te worden geleverd aan de certificaathouder, indien van toepassing via de abonnee, op een zodanige wijze dat de vertrouwelijkheid en integriteit van de sleutel niet kan worden aangetast en, eenmaal geleverd aan de certificaathouder, alleen de certificaathouder toegang heeft tot zijn private sleutel.
Opmerking	Deze tekst komt overeen met QCP 7.2.8.d, maar is integraal opgenomen omdat deze eis alleen van toepassing is op handtekening- en authenticiteitscertificaat.

RFC 3647	6.1.5 Sleutellengten van private sleutels van certificaathouders
Nummer	1
ETSI	7.2.8.b, EN 319 411-2
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	7.2.5, EN 319 411-2
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	7.2.4, EN 319 411-2
PKIo	[OID 2.16.528.1.1003.1.2.3.2; OID 2.16.528.1.1003.1.2.3.1] Escrow door de CSP is niet toegestaan voor de private sleutels van het handtekeningcertificaat en het authenticiteitcertificaat.

RFC 3647	6.2.3 Escrow van private sleutels van certificaathouders
Nummer	2
ETSI	7.2.4, EN 319 411-2 (ETSI TS 102 042, 7.2.4.b)
PKIo	[OID 2.16.528.1.1003.1.2.3.3] De geautoriseerde personen, die toegang kunnen krijgen tot de door de CSP in escrow gehouden private sleutel van het vertrouwelijkheidscertificaat (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	7.2.4, EN 319 411-2 (ETSI TS 102 042, 7.2.4.b)
PKIo	[OID 2.16.528.1.1003.1.2.3.3] De CSP dient in de CPS te beschrijven welke partijen en onder welke voorwaarden, toegang tot de in escrow gehouden private sleutel van het vertrouwelijkheidscertificaat kunnen krijgen.

RFC 3647	6.2.3 Escrow van private sleutels van certificaathouders
Nummer	4
ETSI	7.2.4, EN 319 411-2 (ETSI TS 102 042, 7.2.4.b)
PKIo	[OID 2.16.528.1.1003.1.2.3.3] Indien de CSP de private sleutel van het vertrouwelijkheidscertificaat in escrow houdt, dient de CSP te garanderen dat deze private sleutel geheim wordt gehouden en uitsluitend ter beschikking wordt gesteld aan toepasselijk geautoriseerde personen.
Opmerking	Hoewel deze eis overeenkomt met ETSI TS 102 042, 7.2.4.b, is de deze eis

	toch als PKIo-eis gepositioneerd om te waarborgen dat deze onderdeel uitmaakt van de goedkeurende auditverklaring die de CSP moet overleggen.
--	---

RFC 3647	6.2.4 Back-up van private sleutels van certificaathouders
Nummer	1
ETSI	7.2.4 en 7.2.8.e, EN 319 411-2
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	7.2.4 en 7.2.8.e, EN 319 411-2
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 handtekeningen
Nummer	1
ETSI	5.3.1.c, EN 319 411-2
PKIo	Door de CSP uitgegeven of aanbevolen veilige middelen voor het aanmaken van elektronische handtekeningen (SSCD's) moeten voldoen aan de eisen gesteld in document {7} CWA 14169 "Secure signature-creation devices "EAL 4+"" en aan de eisen, gesteld bij of krachtens het Besluit elektronische handtekeningen artikel 5, onderdelen a,b,c en d.
Opmerking	Het gebruik van verschillende veilige middelen zoals een smartcard of een USB-key, zijn toegestaan. Voorwaarde is dat de SSCD aan de inhoudelijke eisen voldoet zoals gespecificeerd in 6.2.11-1, -2 of -3.

RFC 3647	6.2.11 Eisen voor veilige middelen voor het aanmaken van elektronische handtekeningen
Nummer	2
ETSI	5.3.1.c, EN 319 411-2
PKIo	In plaats van conformiteit aan CWA 14169 aan te tonen mogen CSP's SSCD'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 handtekeningen
Nummer	3
ETSI	5.3.1.c, EN 319 411-2
PKIo	De overeenstemming van SSCD's met de eisen zoals genoemd in PKIo-eis nr 6.2.11-1 moet zijn vastgesteld door een volgens de Telecommunicatiewet (TW) artikel 18.17, derde lid, aangewezen instantie voor de keuring van veilige middelen voor het aanmaken van elektronische handtekeningen. Zie hiervoor ook de Regeling elektronische handtekeningen, art. 4 en 5.

6.3 Andere aspecten van sleutelpaarmanagement

RFC 3647	6.3.1 Archiveren van publieke sleutels
Nummer	1
ETSI	6.4.11.e, EN 319 401
PKIo	[OID 2.16.528.1.1003.1.2.3.2] Het handtekeningcertificaat dient tijdens de geldigheidsduur en bovendien gedurende een periode van ten minste zeven jaar na de datum waarop de geldigheid van het certificaat is verlopen te worden bewaard.
Opmerking	De termijn van zeven jaar komt voort uit de BEH artikel 2, lid 1i. Er gelden geen nadere bepalingen voor het authenticiteitcertificaat en het vertrouwelijkheidcertificaat in relatie tot het archiveren van de publieke sleutels.

RFC 3647	6.3.2 Gebruiksduur voor certificaten en publieke en private sleutels
Nummer	1
ETSI	7.2.6, EN 319 411-2
PKIo	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. 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	7.2.6, EN 319 411-2
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	7.2.9.d, EN 319 411-2
PKIo	De CSP verbindt activeringsgegevens aan het gebruik van een SSCD, 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	7.2.9.d, EN 319 411-2
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	7.4.6, EN 319 411-2 6.4.6, EN 319 401
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	7.4.6, EN 319 411-2 6.4.6, EN 319 401
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	6.4.6.a, EN 319 401
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	6.4.7, EN 319 401 7.4.7, EN 319 411-2
PKIo	Bij deze ETSI-eis heeft de PKIoverheid alleen een opmerking geformuleerd en is geen specifieke PKIo-eis van toepassing.
Opmerking	Conformiteit aan QCP 7.4.7. en BEH art. 2 lid 1c kan worden aangetoond door: <ul style="list-style-type: none"> • 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	6.4.6, EN 319 401 7.4.6, EN 319 411-2
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: <ul style="list-style-type: none"> • 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 ³ " 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

³ <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	7.4.6, EN 319 411-2 6.4.6, EN 319 401
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	7.4.6, EN 319 411-2 6.4.6, EN 319 401
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 leveranciersselectie kan de CSP de aanbevelingen in hoofdstuk 4 ("Leveranciersselectie") zoals beschreven in de laatste versie van de whitepaper "Pentesten doe je zo" ⁴ van het NCSC, als guidance gebruiken. Indien noodzakelijk kan de PA een opdracht geven aan de CSP tot het laten uitvoeren van extra pentesten.

⁴ <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	7.3.3.a, EN 319 411-2
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	7.3.6.g, EN 319 411-2
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	6.5.c, EN 319 401
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	6.4 en Annex A, EN 319 411-2
PKIo	[OID 2.16.528.1.1003.1.2.3.1] In de overeenkomst tussen de CSP en de abonnee wordt een beding (een bepaling als bedoeld in artikel 6:253 BW) opgenomen waarin de CSP zich sterk maakt voor een op het certificaat vertrouwende derde. Dit beding strekt tot een aansprakelijkheid van de CSP overeenkomstig artikel 6:196b, eerste tot en met derde lid, van het Burgerlijk Wetboek, met dien verstande dat: <ol style="list-style-type: none"> a. voor "een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss Telecommunicatiewet" gelezen wordt: "een authenticiteitscertificaat"; 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	6.4 en Annex A, EN 319 411-2
PKIo	<p>[OID 2.16.528.1.1003.1.2.3.3] In de overeenkomst tussen de CSP en de abonnee wordt een beding (een bepaling als bedoeld in artikel 6:253 BW) opgenomen waarin de CSP zich sterk maakt voor een op het certificaat vertrouwende derde. Dit beding strekt tot een aansprakelijkheid van de CSP overeenkomstig artikel 6:196b, eerste tot en met derde lid, van het Burgerlijk Wetboek, met dien verstande dat:</p> <ul style="list-style-type: none"> 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 gecijferde data"; d. Voor "verifiëren van elektronische handtekeningen" gelezen wordt: "ontcijferen van gecijferde data".

RFC 3647	9.6.1 Aansprakelijkheid van CSP's
Nummer	3
ETSI	6.4 en Annex A, EN 319 411-2
PKIo	<p>[OID 2.16.528.1.1003.1.2.3.2] De PA kan in een handtekeningcertificaat beperkingen ten aanzien van het gebruik daarvan laten opnemen, mits die beperkingen voor derden duidelijk zijn. De CSP is niet aansprakelijk voor schade die het gevolg is van het gebruik van een handtekeningcertificaat in strijd met daarin overeenkomstig de vorige volzin opgenomen beperkingen.</p>
Opmerking	Dit artikel is gebaseerd op BW art. 196b, lid3

RFC 3647	9.6.1 Aansprakelijkheid van CSP's
Nummer	4
ETSI	6.4 en Annex A, EN 319 411-2
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	6.4, EN 319 411-2
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	6.4, EN 319 411-2
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 wijzigingsprocedure voor het PVE van PKIoverheid is opgenomen in het Certification Practice 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	6.5.e, EN 319 401
PKIo	De door de CSP gehanteerde klachtenafhandeling- en geschillenbeslechtsprocedures 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, aangezien ETSI specifiek voor gekwalificeerde certificaten is opgesteld.
PKIo	De CSP moet in staat zijn om alle onder [1.2] genoemde typen persoonsgebonden certificaten uit te geven.

Als één of meerdere bepalingen van deze CP bij gerechtelijke uitspraak ongeldig of anderszins niet van toepassing wordt verklaard, laat dit de geldigheid en toepasselijkheid van alle overige bepalingen onverlet.

Bijlage A Profielen certificaten en certificaat statusinformatie

Profiel van het certificaat voor het domein Burger

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, specifieke eisen voor gekwalificeerde certificaten staan in RFC 3739.

- 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.
- Het certificaat voor de elektronische handtekening MOET voldoen aan het EESSI Qualified Certificate profiel (ETSI TS 101 862). Daar waar verschillen bestaan tussen TS 101 862 en RFC 3739 heeft TS 101 862 voorrang.
- Persoonsgebonden certificaten MOETEN voldoen aan de standaard ETSI TS 102 280 voor wat betreft het certificaatprofiel. Daar waar verschillen bestaan tussen TS 102280 en TS 101862, RFC3739 of RFC5280 heeft TS 102280 voorrang.

Naamconventie Subject.commonName

De volgende eisen gelden ten aanzien van de CommonName van het Subject veld. Het belangrijkste uitgangspunt is dat de CSP verantwoordelijk is voor een adequate vermelding van de CommonName. Dat betekent dat voor een goede uitvoering hiervan elk onderdeel dat wordt ingevoerd gecontroleerd moet kunnen worden door de CSP. Op onderdelen houdt dit het volgende in:

A. Schrijfwijze:

De schrijfwijze en spelling van de onderdelen van de CommonName dienen conform de GBA-registratie te geschieden. Dit kan door het bij de identificatie getoonde WID-document te raadplegen.

B. Volgorde:

De CSP is in principe vrij om de volgorde tussen de categorieën <Voorna(a)m(en) en/of initialen>, <Tussenvoegsels> en <Achternaam> te kiezen. Uiteraard dient binnen een dergelijke categorie de volgorde te worden gehandhaafd (wegens regel A). Het gebruik van komma's als scheidingstekens tussen de categorieën wordt afgeraden vanwege mogelijke technische conflicten bij verwerking van het certificaat.

C. Voornamen in de CommonName:

De CSP is vrij om ofwel voorna(a)m(en) voluit ofwel initialen te vermelden in de CommonName. De schrijfwijze van voorna(a)m(en) of initialen mag niet in strijd zijn met het gebruikte WID document of de GBA-registratie (zie regel A). Indien bij gebruik van volledige voornamen de CommonName meer karakters bevat dan het veld technisch kan hebben, zal gebruik worden gemaakt van het vervangen van de volledige voornamen door initialen, te beginnen bij de laatste volledige voornaam, net zolang totdat de dan ontstane CommonName wel past.

D. Vermelding naam partner/echtgeno(o)t(e):

1. Een certificaathouder is niet verplicht om de partnernaam te laten vermelden in PKIO-certificaten. In dat geval bestaat <Achternaam> alleen uit de <meisjes-/ jongensnaam uit het getoonde WID-document>.
2. Indien de certificaathouder wel de naam van zijn/haar partner vermeld wil hebben in een PKIO certificaat, dan bestaat <Achternaam> uit <Naam partner/echtgeno(o)t(e) >-<meisjes-/ jongensnaam uit het getoonde WID-document>.

3. Voor de juistheid van <Naam partner/echtgeno(o)t(e)> moet de certificaathouder een bewijs tonen. Hierbij zij opgemerkt dat voor wat betreft de vermelding van de status ('e/v') een WID-document niet synchroon hoeft te lopen met de GBA-registratie (en deze hoeft niet synchroon te lopen met de actuele situatie). Het WID-document zal hiervoor dus niet altijd toereikend zijn.

Indien bij vermelding van de naam van de partner/echtgeno(o)t(e) de namen gezamenlijk meer karakters bevatten dan het CommonName veld kan hebben, zal, na toepassing van regel C, worden teruggevallen op alleen de meisjes-/ jongensnaam zoals vermeld in het WID-document.

Persoonsgebonden certificaten

Basisattributen

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
Version	V	MOET ingesteld worden op 2 (X.509v3).	RFC5280	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.	RFC5280	Integer	Alle eindgebruiker certificaten moeten tenminste 8 bytes aan niet te voorspellen willekeurige data bevatten in het serienummer (SerialNumber) van het certificaat.
Signature	V	MOET worden ingesteld op het algoritme, zoals deze door de PA is bepaald.	RFC5280, 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) bevatten. Veld heeft de onderstaande attributen:	PKIo, RFC3739, ETSI TS 102280		Andere attributen dan hieronder genoemd MOGEN NIET worden gebruikt. De attributen die worden gebruikt MOETEN gelijk zijn aan de gelijknamige attributen in het Subject veld van het CSP certificaat (ten behoeve van validatie).
Issuer.countryName	V	MOET de landcode bevatten van het land waar de uitgevende organisatie van het certificaat is gevestigd.	ETSI TS101862, X520, ISO 3166	Printable String	C = NL voor CSP's gevestigd in Nederland.

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
Issuer.stateOrProvinceName	N	Gebruik is niet toegestaan.	PKIo	UTF8String	-
Issuer.OrganizationName	V	Volledige naam conform geaccepteerd document of basisregistratie	ETSI TS 102280	UTF8String	
Issuer. organizationalUnitName	O	Optionele aanduiding van een organisatieonderdeel. Dit veld MAG NIET een functieaanduiding of dergelijke bevatten. Wel eventueel de typen certificaten die worden ondersteund.	ETSI TS 102280: 5.2.4	UTF8String	Meerdere instanties van dit attribuut MOGEN gebruikt worden.
Issuer.localityName	N	Gebruik is niet toegestaan.	PKIo	UTF8String	-
Issuer.serialNumber	O	MOET, conform RFC 3739, worden gebruikt 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, optioneel aangevuld met de Domein aanduiding en/of de typen certificaat die worden ondersteund	PKIo, RFC 3739	UTF8String	Het commonName attribuut MAG NIET nodig zijn om de uitgevende instantie te identificeren (geen onderdeel van de Distinguished Name, eis uit RFC 3739)
Validity	V	MOET de geldigheidsperiode (validity) van het certificaat definiëren volgens RFC 5280.	RFC 5280	UTCTime	MOET begin- en einddatum bevatten voor geldigheid van het certificaat conform het van toepassing zijnde beleid vastgelegd in het CPS.
Subject	V	De attributen die worden gebruikt om het subject (eindgebruiker) te beschrijven MOETEN het subject op unieke wijze benoemen. Veld heeft de onderstaande	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
		attributen:			
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	Het commonName attribuut MOET te worden ingevoerd conform de paragraaf Naamconventie Subject.commonName hierboven.	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	Inhoud van dit veld MOET in overeenstemming zijn met de naam zoals vermeld in de GBA, het WID document of ander bewijsmateriaal (uittreksel bevolkingsregister) kan worden gebruikt om dit aan te tonen. Het gebruik van komma's als scheidingstekens in de commonName wordt afgeraden vanwege mogelijke technische conflicten bij verwerking van het certificaat.
Subject.Surname	A	Een juiste weergave van de in het CN vastgelegde element van de naam. Gebaseerd op WID document.	RFC 3739	UTF8String	Het gebruik van dit veld wordt afgeraden. Indien dit veld wordt gebruikt MOET het een juiste weergave te zijn van de achternaam van het subject, inclusief tussenvoegsels. De surname MAG NIET in strijd zijn met de informatie in de commonname
Subject.givenName	A	Een juiste weergave van de in het CN vastgelegde element van de naam. Gebaseerd op WID document.	RFC 3739	UTF8String	Het gebruik van dit veld wordt afgeraden. Indien dit veld wordt gebruikt MOET het een juiste weergave te zijn van de voorna(a)m(en) van het subject. De givenName MAG NIET in strijd zijn met de informatie in de commonname, wel mag givenName volledige voorna(a)m(en) bevatten terwijl de commonName initialen bevat.
Subject.pseudonym	N	Het gebruik van pseudoniemen is niet toegestaan.	ETSI TS 102 280, RFC 3739, PKIo		

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
Subject.organizationName	N	Voor certificaten in domein burger wordt gebruik van organizationName niet toegestaan	PKIo	UTF8String	In domein burger zijn certificaathouder en abonnee een en dezelfde en is er dus geen sprake van een abonnee organisatie wiens naam kan worden opgenomen in dit veld
Subject.organizationalUnitName	N	Voor certificaten in domein Burger wordt gebruik van organizationalUnitName niet toegestaan	PKIo		In domein burger zijn certificaathouder en abonnee een en dezelfde en is er dus geen sprake van een abonnee organisatieonderdeel wiens naam kan worden opgenomen in dit veld
Subject.stateOrProvinceName	A	Het gebruik wordt afgeraden. Indien aanwezig MOET dit veld de provincie van vestiging van de certificaathouder conform geaccepteerd document of Basisregistratie te bevatten.	PKIo, RFC 3739	UTF8String	Naam van de provincie MOET in overeenstemming zijn met het adres van de certificaathouder volgens de GBA. De certificaathouder zal een recent bewijs van zijn adres moeten overleggen.
Subject.localityName	A	Het gebruik wordt afgeraden. Indien aanwezig MOET dit veld de woonplaats van de certificaathouder conform geaccepteerd document of Basisregistratie te bevatten.	PKIo, RFC 3739	UTF8String	Naam van de woonplaats MOET in overeenstemming zijn met het adres van de certificaathouder volgens de GBA. De certificaathouder zal een recent bewijs van zijn adres moeten overleggen.
Subject.postalAddress	A	Het gebruik wordt afgeraden. Indien aanwezig MOET dit veld het postadres van de certificaathouder conform geaccepteerd document of Basisregistratie te bevatten.	PKIo, RFC 3739	UTF8String	Adres MOET in overeenstemming zijn met het adres van de certificaathouder volgens de GBA. De certificaathouder zal een recent bewijs van zijn adres moeten overleggen.
Subject.emailAddress	N	Gebruik is niet toegestaan.	RFC 5280	IA5String	Dit veld MAG NIET worden gebruikt in nieuwe certificaten.
Subject.serialNumber	V	Door de CSP te bepalen nummer. De combinatie van CommonName en Serialnumber MOET binnen de context van de	RFC 3739, X 520, PKIo	Printable String	Het serialnumber is bedoeld om onderscheid te kunnen maken tussen subjects met dezelfde commonName. Om gevoeligheden te vermijden MOET aan elk subject een serialNumber attribuut worden toegekend.

Veld / Attribuut	Criteria	Beschrijving	Norm referentie	Type	Toelichting
		CSP uniek zijn.			
Subject.title	N	Voor certificaten in domein Burger is gebruik van het title attribuut niet toegestaan	ETSI TS 102 280, RFC 3739, RFC 5280		Bevat de rol van een subject in de organisatie genoemd in het Organization attribuut (RFC 3739). In domein Burger is Organization attribuut niet toegestaan en dus kan ook title niet gebruikt worden.
subjectPublicKeyInfo	V	Bevat o.a. de publieke sleutel.	ETSI TS 102 280, RFC 3279		Bevat de publieke sleutel, identificeert het algoritme waarmee de sleutel kan worden gebruikt.
IssuerUniqueIdentifier	N	Wordt niet gebruikt.	RFC 5280		Gebruik hiervan is niet toegestaan (RFC 5280)
subjectUniquIdentifier	N	Wordt niet gebruikt.	RFC 5280		Gebruik hiervan is niet toegestaan (RFC 5280)

Standaard extensies

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

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
			In certificaten voor de elektronische handtekening MOET het non-repudiation bit zijn opgenomen en zijn aangemerkt als essentieel. Een ander keyUsage MAG hiermee NIET worden gecombineerd.			
privateKeyUsagePeriod	N		Wordt niet gebruikt.	RFC 5280		
CertificatePolicies	V	Nee	MOET de OID bevatten van de certificate policy (CP), de URI van het certification practice statement (CPS), en een gebruikersnotitie. Het te gebruiken OID schema in de PKI voor de overheid wordt beschreven in de CP.	RFC 3739	OID, String, String	Voor domein Burger zijn de OID's: 2.16.528.1.1003.1.2.3.1, 2.16.528.1.1003.1.2.3.2 en 2.16.528.1.1003.1.2.3.3. Verwijzen naar paragraafnummers van het PVE / CP in de gebruikersnotitie wordt afgeraden omdat persistentie hiervan niet kan worden gegarandeerd (in tegenstelling tot het OID nummer van de CP).
PolicyMappings	N		Wordt niet gebruikt.			Deze extensie wordt niet gebruikt in eindgebruikercertificaten
SubjectAltName	V	Nee	MOET worden gebruikt en voorzien zijn van een persoonlijk wereldwijd uniek nummer.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		MOET een unieke identifier bevatten in het othername attribuut. Andere attributen dan hieronder genoemd MOGEN NIET worden gebruikt.
SubjectAltName.otherName	V		MOET worden gebruikt met daarin een uniek nummer dat de certificaathouder identificeert.	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 identificeert, gescheiden door een punt of liggend streepje ('-'). Het is aan te bevelen een bestaand registratienummer uit backoffice systemen te gebruiken. In combinatie met het CSP OID-nummer is deze identifier wereldwijd

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
						uniek. Dit nummer MOET persistent te zijn.
SubjectAltName.rfc822Name	A		MAG worden gebruikt voor het e-mail adres van de certificaathouder, ten behoeve van applicaties die het e-mail adres nodig hebben om goed te functioneren.	RFC 5280	IA5String	Voor PKIoverheid certificaten wordt het gebruik van e-mail adressen afgeraden, omdat e-mail adressen van certificaathouders vaak wisselen en bovendien privacygevoelig zijn (spam). Als het e-mail adres wel in het certificaat wordt opgenomen MOET de CSP: <ul style="list-style-type: none"> • de abonnee hiervoor akkoord laten tekenen én; • controleren of het mailadres behoort aan de abonnee en deze toegang heeft tot het mailadres (bijvoorbeeld door het uitvoeren van een challenge response).
IssuerAltName	N		Wordt niet gebruikt.	RFC 5280		
subjectDirectoryAttributes	N		Wordt niet gebruikt.	RFC 5280; RFC 3739		Het gebruik van deze extensie is niet toegestaan. Deze attributen bevatten persoonsgegevens die de privacy van het subject kunnen schaden.
BasicConstraints	O	Ja	Het "CA" veld MOET op "FALSE" staan of worden weggelaten (default waarde is dan "FALSE").	RFC 5280		In een (Nederlandstalige) browser zal dan te zien zijn: "Subjecttype = Eidentiteit", "Beperking voor padlengte = Geen"
NameConstraints	N		Wordt niet gebruikt.	RFC 5280		Wordt niet gebruikt in eindgebruiker certificaten.
PolicyConstraints	N		Wordt niet gebruikt.	RFC 5280		Wordt niet gebruikt in eindgebruiker certificaten.
CRLDistributionPoints	V	Nee	MOET de URI van een CRL distributiepunt bevatten.	RFC 5280, ETSI TS 102 280		De aanwezige referentie MOET via http of ldap protocol toegankelijk zijn. Het attribuut Reason MAG NIET worden gebruikt,

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
						er MOET naar 1 CRL worden verwezen voor alle soorten intrekingsredenen. Naast CRL MOGEN ook andere vormen van certificaatstatus informatiediensten worden ondersteund.
ExtKeyUsage	N	Nee	Wordt niet gebruikt.	RFC 5280		Wordt in certificaten in domein Burger niet gebruikt. Dit veld wordt ook wel enhancedKeyUsage genoemd.
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, General-name	Dit veld kan gebruikt worden om te verwijzen naar aanvullende informatie over het subject, mits de aangeboden informatie geen inbreuk maakt op de privacy van het subject.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie	Type	Toelichting
BiometricInfo	O	Nee	Bevat de hash van een biometrische template en optioneel een URI die verwijst naar een bestand met de biometrische template zelf.	RFC 3739		
QcStatement	V / N	Nee	<p>Certificaten voor de elektronische handtekening MOETEN aangeven dat zij zijn uitgegeven als gekwalificeerde certificaten overeenstemmend met annex I en annex II van de Europese Richtlijn. Deze overeenstemming wordt aangegeven door het opnemen van de <i>id-etsi-qcs-QcCompliance</i> statement in deze extensie.</p> <p>Certificaten voor de elektronische handtekening MOGEN aangeven dat de private sleutel behorende bij de publieke sleutel in het certificaat is opgeslagen op een secure signature-creation device (SSCD) overeenstemmend met annex III van de Europese Richtlijn. Deze overeenstemming wordt aangegeven door het (additioneel) opnemen van de <i>id-etsi-qcs-QcSSCD</i> statement in deze extensie.</p>	RFC 3739, ETSI TS 102 280, ETSI TS 101 862	OID	<p>De genoemde QcStatement identifiers betreffen de volgende OIDs:</p> <p>id-etsi-qcs-QcCompliance { id-etsi-qcs 1 } 0.4.0.1862.1.1</p> <p>id-etsi-qcs-QcSSCD { id-etsi-qcs 4 } 0.4.0.1862.1.4</p>

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).	RFC5280	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.	RFC5280	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 validatie).
Issuer.countryName	V	MOET de landcode bevatten van het land waar de uitgevende organisatie van het certificaat is gevestigd.	ISO3166, X.520	Printable String	C = NL voor CSP's gevestigd in Nederland.
Issuer.stateOrProvinceName	N	Wordt niet gebruikt.	PKIo	UTF8String	-
Issuer.OrganizationName	V	Volledige naam conform geaccepteerd	ETSI TS	UTF8String	

Veld / Attribuut	Criteria	Beschrijving	Norm referentie1	Type	Toelichting
		document of basisregistratie	102280: 5.2.4		
Issuer.organizationalUnitName	O	Optionele aanduiding van een organisatieonderdeel. Dit veld MAG NIET een functieaanduiding of dergelijke bevatten. Wel eventueel de typen certificaten die worden ondersteund.	ETSI TS 102280: 5.2.4	UTF8String	Meerdere instanties van dit attribuut MOGEN gebruikt worden.
Issuer.localityName	N	Wordt niet gebruikt.	PKIo	UTF8String	-
Issuer.serialNumber	O	MOET worden gebruikt indien eenduidige naamgeving dit vereist	RFC 3739	Printable String	
Issuer.commonName	V	MOET de naam van de CA bevatten conform geaccepteerd document of basisregistratie, MAG worden aangevuld met de Domein aanduiding en/of de typen certificaat die worden ondersteund	PKIo, RFC 5280	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	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.

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm referentie1	Type	Toelichting
			MOET het de URI van een Delta-CRL distributiepunt bevatten. Het komt nooit voor in een Delta-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 MAG dit attribuut worden gebruikt om de oorspronkelijke uitgever van het certificaat te identificeren.	RFC 5280	GeneralNames	

Profiel OCSP

Het OCSP certificaatprofiel is te vinden in de bijlage bij het CP Servicescertificaten.

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 EN 319 411-2 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 al in PvE deel 1 is aangegeven 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-paragraaf⁵. De PA heeft er bewust voor gekozen om alle eisen maar eenmalig op te nemen.

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.b 7.3.4.b		2.1-1 2.1-2

⁵ Dit wordt mede veroorzaakt door het feit dat ETSI TS 101 456 niet volgens de RFC 3647 structuur is opgebouwd.

		7.3.5.e 7.3.5.f		
2.2	Publicatie van CSP-informatie	5.2.b 7.1.a 7.1.b 7.1.d 7.3.2.b 7.3.4 7.3.4.a 7.3.5 7.3.5.c 7.3.5.d 7.3.6.a		2.2-1 2.2-2 2.2-3 2.2-4
2.3	Frequentie van publicatie			
2.4	Toegang tot gepubliceerde informatie	7.1.c 7.3.6.k		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			3.1.3-1
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.k 7.3.1.l		
3.2.2	Authenticatie van organisatorische entiteit			
3.2.3	Authenticatie van persoonlijke identiteit	6.2 6.2.a 7.3.1 7.3.1.a 7.3.1.c 7.3.1.d 7.3.1.g 7.3.1.h		3.2.3-1

3.2.4	Niet-geverifieerde abonnee informatie			
3.2.5	Autorisatie van de certificaathouder			
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.c		
4	Operationele eisen			
4.1	Aanvraag van certificaten			
4.2	Verwerken van een certificaat aanvraag			
4.3	Uitgifte van certificaten			
4.3.1	CSP taken met betrekking tot certificaat uitgifte	7.3.3		

		7.3.3.a 7.3.3.b 7.3.3.c 7.3.3.d		
4.3.2	CSP notificatie van certificaat uitgifte aan abonnee	7.3.5.a		
4.4	Acceptatie van certificaten			
4.4.1	Activiteiten bij acceptatie van certificaten			4.4.1-1
4.4.2	Publicatie van het certificaat door CSP			
4.4.3	CSP notificatie van certificaat uitgifte aan overige entiteiten			
4.5	Gebruik van sleutelparen en certificaten			
4.5.1	Gebruik van private sleutel en certificaat door abonnee	6.2 6.2.b 6.2.c 6.2.e 6.2.f 6.2.g 6.2.h 6.2.i		

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.f		
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.e 7.3.6.h	BEH6 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 intrekkingverzoek moet indienen			

6 BEH staat voor Besluit Elektronische Handtekeningen.

4.9.5	Tijdsduur voor verwerking intrekkingverzoek	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.g		4.9.7-1
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.d		4.9.13-1
4.10	Certificaat Status service			

4.10.1	Operationele eigenschappen	7.3.6.j 7.3.6.l		
4.10.2	Beschikbaarheid certificaat statusservice	7.3.6.i		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.a 7.4.5.b 7.4.5.g 7.4.5.h		5.2-1 5.2-2
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
5.3	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	Vakkennis, ervaring en kwalificaties	7.4.3.a 7.4.3.f		
5.3.2	Antecedentenonderzoek	7.4.3.j	BEH art.2, lid 1s BEH art.2, lid 2 BEH art.2, lid 3	5.3.2-1
5.3.3	Trainingseisen			

5.3.4	Bijscholing frequentie en eisen			
5.3.5	Baanrotatie frequentie en volgorde			
5.3.6	Sancties voor ongeoorloofde activiteiten	7.4.3.b		
5.3.7	Eisen met betrekking tot externe medewerkers			
5.3.8	Documentatie verstrekking aan personeel			
5.4	Procedures ten behoeve van beveiligingsaudits			
5.4.1	Vastlegging van gebeurtenissen	7.4.5.i 7.4.11.g 7.4.11.h 7.4.11.d 7.4.11.k 7.4.11.l 7.4.11.m 7.4.11.n 7.4.11.o		5.4.1-1
5.4.2	Frequentie van verwerking audit-log	7.4.5.j		
5.4.3	Bewaartermijn audit-log	Zie 5.5.2		5.4.3-1

5.4.4	Bescherming van audit-log	7.4.11.a 7.4.11.f		
5.4.5	Audit-log back-up procedure			
5.4.6	Intern of extern auditsysteem			
5.4.7	Notificatie van entiteit die audit-log veroorzaakt			
5.4.8	Analyse van audit-log			
5.5	Archivering van documenten			
5.5.1	Vastlegging van gebeurtenissen	7.4.11 7.4.11.i 7.3.1.f 7.3.1.i		
5.5.2	Bewaartermijn archief	7.4.11.e 7.3.1.j		5.5.2-1
5.5.3	Bescherming van archieven	7.4.10.a 7.4.11.b		
5.5.4	Archief back-up procedure			

5.5.5	Voorwaarden aan tijdsaanduiding van vastgelegde gebeurtenissen			
5.5.6	Intern of extern archiefsysteem			
5.5.7	Procedures ten behoeve van het verkrijgen en verifiëren van archiefinformatie			
5.6	Vernieuwen van sleutels			
5.7	Aantasting en continuïteit			
5.7.1	Procedures voor afhandeling incidenten en aantasting	7.4.8.e		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.f		
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	BEH art.2, lid 1p BEH art. 2, lid 1q	

		7.4.9.c		
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 7.2.8 7.2.8.a		6.1.1-2 6.1.1-3
6.1.2	Overdracht van private sleutel en SSCD aan certificaathouder	7.2.8.c 7.2.8.d 7.2.8.e 7.2.9 7.2.9.a 7.2.9.b 7.2.9.c		6.1.2-1
6.1.3	Overdracht van de publieke sleutel van de eindgebruiker aan de CSP			
6.1.4	Overdracht van de publieke sleutel van de CSP aan gebruikers	7.2.3		

		7.2.3.a		
6.1.5	Sleutellengten van private sleutels van certificaathouders	7.2.8.b		6.1.5-1
6.1.6	Genereren en controleren van parameters voor publieke sleutels			
6.1.7	Doelen van sleutelgebruik (zoals bedoeld in X.09 v3)	7.2.5 7.2.5.a 7.2.5.b		6.1.7-1
6.2	Private sleutel bescherming en beheersmaatregelen cryptografische modulen			
6.2.1	Standaarden voor cryptografische modulen en beheersmaatregelen	7.2.1.b 7.2.2 7.2.2.a 7.2.2.b		
6.2.2	Private CSP-sleutel controle door meerdere personen			
6.2.3	Escrow van private sleutels van certificaathouders	7.2.4		6.2.3-1 6.2.3-2 6.2.3-3 6.2.3-4
6.2.4	Back-up van private sleutel	7.2.2.c 7.2.2.d		6.2.4-1

		7.2.4 7.2.8.e		
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.a		
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 aspecten van sleutelpaarmanagement			
6.3.1	Archiveren van publieke sleutels			6.3.1-1
6.3.2	Gebruiksduur voor certificaten en publieke en private sleutels	7.2.1.e 7.2.6		6.3.2-1 6.3.2-2

6.4	Activeringsgegevens			
6.4.1	Genereren en installeren van activeringsgegevens	7.2.9.d		6.4.1-1 6.4.1-2
6.4.2	Activeringsgegevens bescherming			
6.4.3	Andere aspecten van activeringsgegevens			
6.5	Logische toegangsbeveiliging van CSP-computers			
6.5.1	Specifieke technische vereisten aan computerbeveiliging	7.4.6 7.4.6.c 7.4.6.d 7.4.6.e 7.4.6.f 7.4.6.j 7.4.6.l		6.5.1-1 6.5.1-2 6.5.1-3
6.5.2	Beheer en classificatie van middelen	7.4.2 7.4.2.a		
6.6	Beheersmaatregelen technische levenscyclus			
6.6.1	Beheersmaatregelen ten behoeve van systeemontwikkeling	7.4.7 7.4.7.a		6.6.1-1

		7.4.7.b		
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 Annex A	[OID 2.16.528.1.1003.1.2.3.2] BW7 art. 196b, lid1 en lid 2	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			

7 BW staat voor Burgerlijk Wetboek

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
9.12.3	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.e 7.1.f 7.1.i 7.5 7.5.a 7.5.b 7.5.c 7.5.e 7.5.g		9.17-1
-------------	---------------------------	--	--	--------

10 Revisies

10.1 Wijzigingen van versie 3.6 naar 3.7

10.1.1 *Aanpassingen*

- Eis 6.1.1-2 (ingangsdatum 4 weken na publicatie PVE 3.7);
- Eis 6.2.11-1 (ingangsdatum 4 weken na publicatie PVE 3.7).

10.2 Wijzigingen van versie 3.5 naar 3.6

10.2.1 *Aanpassingen*

- Certificering tegen ETSI EN 319 411-2 (ingangsdatum 4 weken na publicatie PVE 3.6);
- Aanpassing referentienummers ETSI EN 319 4012 (ingangsdatum 4 weken na publicatie PVE 3.6);

10.2.2 *Redactioneel*

- Eis 4.9.9-3 (ingangsdatum 4 weken na publicatie PVE 3.6);
- Eis 5.2 (ingangsdatum 4 weken na publicatie PVE 3.6);
- Eis 6.1.1-1 (ingangsdatum 4 weken na publicatie PVE 3.6);
- Eis 6.1.1-2 (ingangsdatum 4 weken na publicatie PVE 3.6);
- Eis 6.1.1-3 (ingangsdatum 4 weken na publicatie PVE 3.6);
- Eis 6.2 (ingangsdatum 4 weken na publicatie PVE 3.6);
- Eis 6.3.2-1 (ingangsdatum 4 weken na publicatie PVE 3.6); Eis 9.12 (ingangsdatum 4 weken na publicatie PVE 3.6);
- Bijlage A: CRL profiel

10.3 Wijzigingen van versie 3.4 naar 3.5

10.3.1 *Aanpassingen*

- Beschrijving en toelichting bij het attribuut QcStatement (uiterlijke ingangsdatum 4 weken na publicatie PVE 3);
- Toelichting van het attribuut SerialNumber (uiterlijke ingangsdatum 4 weken na publicatie PVE 3.5);

10.4 Wijzigingen van versie 3.3 naar 3.4

10.4.1 *Nieuw*

- Eis 5.2-2 (uiterlijke ingangsdatum 4 weken na datum publicatie PVE 3.4);
- Eis 5.3.2-1 (uiterlijke ingangsdatum 4 weken na datum publicatie PVE 3.4);

10.4.2 *Aanpassingen*

- Beschrijving en toelichting bij subject.Countryname (uiterlijke ingangsdatum 4 weken na publicatie PVE 3.4);

10.4.3 *Redactioneel*

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

10.5 Wijzigingen van versie 3.2 naar 3.3

10.5.1 *Nieuw*

- Eis 5.2-1 (uiterlijke ingangsdatum 1-12-2012)
- Eis 5.4.3-1
- Eis 5.7.4-1 (uiterlijke ingangsdatum 1-12-2012)

10.5.2 *Aanpassingen*

- Eis 4.9.1-1
- Eis 5.4.1-1
- Eis 5.7.1-1 (uiterlijke ingangsdatum 1-10-2012)
- Eis 5.7.1-2 (uiterlijke ingangsdatum 1-10-2012)
- Eis 6.5.1-3
- Eis 6.7.1-1

10.5.3 *Redactioneel*

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

10.6 Wijzigingen van versie 3.1 naar 3.2

10.6.1 *Nieuw*

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

10.6.2 *Aanpassingen*

- Eis 4.5.2-1 (uiterlijke ingangsdatum is 1-2-2012);
- Eis 5.7.1-2;
- Eis 6.2.3-2;
- Toelichting bij SubjectAltName.rfc822Name.

10.6.3 *Redactioneel*

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

10.7 Wijzigingen van versie 3.0 naar 3.1

10.7.1 *Nieuw*

- Eis 4.9.7-1, 4.9.9-6, 6.5.1-1 en 6.5.1-2.

10.7.2 *Aanpassingen*

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

10.7.3 *Redactioneel*

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

10.8 Wijzigingen van versie 2.1 naar 3.0

10.8.1 *Nieuw*

Geen wijzigingen.

10.8.2

Aanpassingen

- Eis 4.9.2-1;
- Toelichting bij attribuut Signature.

10.8.3

Redactioneel

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

10.9 Wijzigingen van versie 2.0 naar 2.1

10.9.1

Redactioneel

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

10.10 Wijzigingen van versie 1.2 naar 2.0

10.10.1

Nieuw

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

10.10.2

Aanpassingen

Geen wijzigingen.

10.10.3

Redactioneel

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

10.11 Wijzigingen van versie 1.1 naar 1.2

10.11.1

Nieuw

Geen wijzigingen.

10.11.2

Aanpassingen

- Eis 6.1.1-1, 6.1.1-2, 6.1.1-3, 6.1.5-1, 6.1.7-1, 6.2.3-4, 6.2.4.2-1, 6.2.5-1, 9.8-1 en 9.8-2;
- Toelichting bij attribuut Signature.

10.11.3

Redactioneel

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

10.12 Wijzigingen van versie 1.0 naar 1.1

10.12.1

Nieuw

Geen wijzigingen.

10.12.2

Aanpassingen

- Paragraaf 1.4.

10.12.3

Redactioneel

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

10.13

Versie 1.0

Eerste versie.