



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Programma van Eisen deel 3: Aanvullende eisen PKIoverheid

Datum 3 februari 2020

Colofon

Versienummer 4.8
Contactpersoon Policy Authority PKIoverheid

Organisatie Logius

Bezoekadres
Wilhelmina van Pruisenweg 52

Postadres
Postbus 96810
2509 JE DEN HAAG

T 0900 - 555 4555
servicecentrum@logius.nl

Inhoud

Colofon	2
Inhoud	3
1 Introductie	6
1.1 <i>Achtergrond</i>	6
1.1.1 <i>Opzet van de Certificate Policies</i>	6
1.1.2 <i>Status</i>	9
1.2 <i>Contactgegevens Policy Authority</i>	9
2 Publicatie en verantwoordelijkheid voor elektronische opslagplaats	10
2.1 <i>Elektronische opslagplaats</i>	10
2.2 <i>Publicatie van TSP-informatie</i>	11
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>	25
4 Operationele eisen certificaatlevenscyclus	26
4.1 <i>Aanvraag van certificaten</i>	26
4.2 <i>Verwerking van certificaat aanvraag</i>	26
4.3 <i>Uitgifte van certificaten</i>	27
4.4 <i>Acceptatie van certificaten</i>	28
4.5 <i>Sleutelpaar en certificaatgebruik</i>	28
4.8 <i>Compliance, audit en assessesment</i>	28
4.9 <i>Intrekking en opschorting van certificaten</i>	28
4.10 <i>Certificaat statusservice</i>	32
5 Management, operationele en fysieke beveiligingsmaatregelen	33
5.2 <i>Procedurele beveiliging</i>	33
5.3 <i>Personele beveiliging</i>	33
5.4 <i>Procedures ten behoeve van beveiligingsaudits</i>	33
5.5 <i>Archivering van documenten</i>	33
5.7 <i>Aantasting en continuïteit</i>	34
6 Technische beveiliging	35
6.1 <i>Genereren en installeren van sleutelparen</i>	35
6.2 <i>Private sleutelbescherming en cryptografische module engineering beheersmaatregelen</i>	39

6.3	<i>Andere aspecten van sleutelpaarmanagement</i>	41
6.4	<i>Activeringsgegevens</i>	43
6.5	<i>Logische toegangsbeveiliging van TSP-computers</i>	43
6.6	<i>Beheersmaatregelen technische levenscyclus</i>	43
6.7	<i>Netwerkbeveiliging</i>	43
7	Certificaat-, CRL- en OCSP-profielen	44
7.1	<i>Certificaatprofielen</i>	44
7.2	<i>CRL-profielen</i>	50
7.3	<i>OCSP-profielen</i>	50
8	Conformiteitbeoordeling	51
9	Algemene en juridische bepalingen	52
9.2	<i>Financiële verantwoordelijkheid en aansprakelijkheid</i>	52
9.5	<i>Intellectuele eigendomsrechten</i>	52
9.6	<i>Aansprakelijkheid</i>	52
9.8	<i>Beperkingen van aansprakelijkheid</i>	54
9.12	<i>Wijzigingen</i>	55
9.13	<i>Geschillenbeslechting</i>	55
9.14	<i>Van toepassing zijnde wetgeving</i>	55
9.17	<i>Overige bepalingen</i>	55
10	Revisies	57
10.1	<i>Wijzigingen</i>	57
10.2	<i>Wijzigingen van versie 4.7 naar versie 4.8</i>	57
10.3	<i>Wijzigingen van versie 4.5 naar versie 4.7</i>	57
10.3.1	<i>Redactioneel</i>	57
10.4	<i>Wijzigingen van versie 4.0 naar versie 4.5</i>	57
10.4.1	<i>Redactioneel</i>	57
10.5	<i>Wijzigingen van versie 3.7 naar 4.0</i>	57
10.5.1	<i>Nieuw</i>	57
10.5.2	<i>Aanpassingen</i>	57
10.5.3	<i>Redactioneel</i>	57

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 (TSP's) tot de PKI voor de overheid begeleiden en voorbereiden van de afhandeling;
- het toezicht houden op en controleren van de werkzaamheden van TSP's die onder de root van de PKI voor de overheid certificaten uitgeven.

De doelstelling van de Policy Authority is:

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

Revisiegegevens

Versie	Datum	Omschrijving
4.0	12-2014	Vastgesteld door BZK december 2014
4.1	07-2015	Vastgesteld door BZK juli 2015
4.1	08-2015	Correctie aan foutief doorgevoerde wijziging aan eis 3.2.2-pkio147
4.2	01-2016	Vastgesteld door BZK januari 2016
4.3	07-2016	Vastgesteld door BZK juni 2016
4.4	02-2017	Vastgesteld door BZK februari 2017
4.5	07-2017	Vastgesteld door BZK juni 2017
4.6	01-2018	Vastgesteld door BZK januari 2017
4.7	02-2019	Vastgesteld door BZK februari 2019
4.8	02-2020	Vastgesteld door BZK februari 2020

1 Introductie

1.1 Achtergrond

Dit is deel 3 Aanvullende eisen van het Programma van Eisen (PvE) van de PKI voor de overheid en wordt aangeduid als Aanvullende eisen PKIoverheid. In het PvE zijn de normen voor de PKI voor de overheid vastgelegd. Dit onderdeel van deel 3 heeft betrekking op de aanvullende eisen die aan de dienstverlening van een Certification Service Provider (TSP) binnen de PKI voor de overheid worden gesteld. Binnen de PKI voor de overheid is onderscheid gemaakt in verschillende domeinen. Deze aanvullende eisen hebben betrekking op alle typen certificaten die onder deze domeinen worden uitgegeven, het onderscheid wordt echter gemaakt in de betreffende PvE's.

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 Policies

Deel 3 van het Programma van Eisen van PKIoverheid bestaat uit de volgende onderdelen:

- *Deel 3 Basiseisen.* De basiseisen zijn van toepassing op alle Certificaten Policies in deel 3 van het Programma van Eisen;
- *Deel 3 Aanvullende eisen.* Hierin zijn alle overige eisen opgenomen die van toepassing zijn op 1 of meerdere CP's maar niet op alle CP's;
- *Deel 3 Verwijzingsmatrix PKIoverheid en ETSI.* Een overzicht van PKIoverheid eisen met verwijzing naar ETSI norm(en) waarop de eis een aanvulling is; en
- Deel 3a t/m i: de Certificate Policies voor de verschillende PKIoverheid certificaten. Het gaat hier om CP's voor de uitgifte van eindgebruikercertificaten voor de reguliere root, de private root en de EV root. Deze stamcertificaten kennen verschillende versies of generaties.

De CP's in deel 3 van het PvE zijn als volgt opgebouwd:

- Deel 3a persoonsgebonden certificaten in het domein organisatie
- Deel 3b services authenticiteits- en vertrouwelijkheidcertificaten in het domein organisatie
- Deel 3c persoonsgebonden certificaten in het domein burger
- Deel 3d services certificaten in het domein autonome apparaten
- Deel 3e website en server certificaten in het domein organisatie
- Deel 3f Extended Validation certificaten onder het EV stamcertificaat
- Deel 3g services authenticiteit- en vertrouwelijkheidcertificaten in het domein private services
- Deel 3h server certificaten in het domein private services
- Deel 3i persoonsgebonden certificaten in het domein private personen

Alle PKIoverheid eisen hebben een uniek en persistent nummer dat tevens een verwijzing naar RFC 3647 bevat. Elke PKIoverheid eis kan bovendien een relatie hebben met een of meerdere ETSI normen voor uitgifte van PKI certificaten. In een aparte Excel tabblad in het OoA template genaamd *Referentiematrix PKIoverheid en ETSI is dit opgenomen zodat de PKIoverheid eisen in de context van de ETSI normen kan worden geplaatst*

Elke PKIoverheid eis is een keer opgenomen in de Basiseisen of Aanvullende Eisen. Voor de Aanvullende eisen is in elk CP deel een verwijzing opgenomen naar de van toepassing zijnde norm in deel 3 Aanvullende Eisen. Naar de Basiseisen wordt niet verwezen omdat deze automatisch van toepassing zijn. Hetzelfde geldt voor de ETSI normen die van toepassing zijn op een CP.

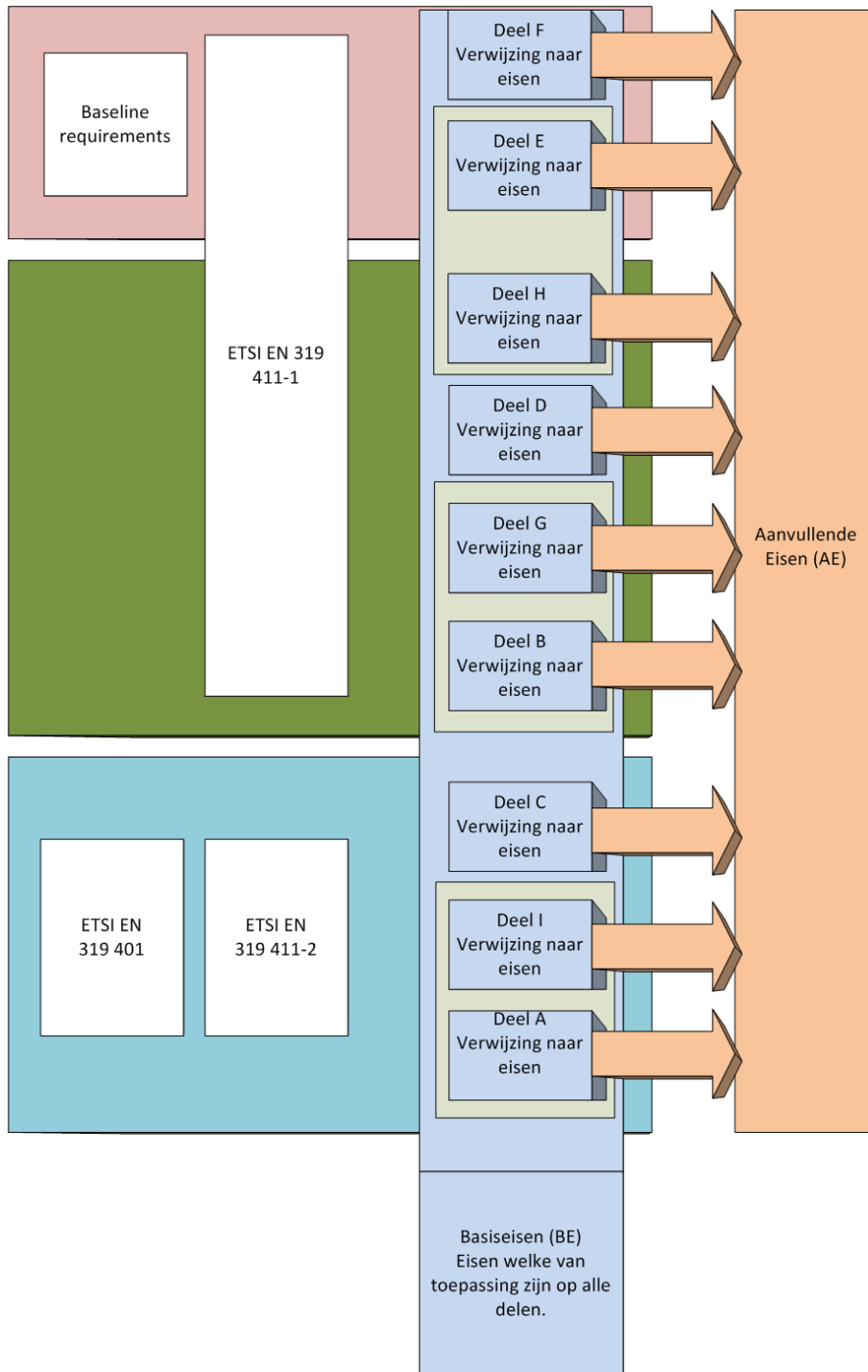
Om te voldoen aan een specifiek CP moet worden voldaan aan het ETSI normenkader dat hierop van toepassing is, de Basiseisen van PKIoverheid en een deel van de Aanvullende eisen van PKIoverheid.

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 ¹ .
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.
PKIo	De PKIo-eis die binnen dit domein van de PKI voor de overheid 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.

Hieronder is schematisch weergegeven hoe deel 3 van het Programma van Eisen is opgebouwd:

¹ In de hoofdstukken 2 t/m 9 zijn alleen die paragrafen uit RFC 3647 opgenomen waarvoor een PKIo-eis van toepassing is.



1.1.2 Status

Dit is versie 4.8 van deel 3 Aanvullende eisen van het PvE. De huidige versie is bijgewerkt tot en met 3 februari 2020.

De PA heeft de grootst mogelijke aandacht en zorg besteed aan de gegevens en informatie, die zijn opgenomen in deze Aanvullende eisen van het Programma van Eisen van PKIoverheid. Toch 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 Aanvullende eisen, indien deze Aanvullende eisen wordt gebruikt buiten het in paragraaf 1.4 van de afzonderlijke PvE delen beschreven certificaatgebruik.

1.2 Contactgegevens Policy Authority

De PA is verantwoordelijk voor deze Aanvullende eisen voor de uitgifte van PKIoverheid certificaten. Vragen met betrekking tot deze Aanvullende eisen kunnen worden gesteld aan de PA, waarvan het adres gevonden kan worden op: <http://www.logius.nl/pkioverheid>.

2 Publicatie en verantwoordelijkheid voor elektronische opslagplaats

2.1 Elektronische opslagplaats

Bevat geen aanvullende eisen.

2.2 Publicatie van TSP-informatie

RFC 3647	2.2 Publicatie van TSP-informatie
Nummer	2.2-pkio3
PKIo	Het CPS zal beschikbaar worden gesteld in het Engels. Daarnaast mag een TSP ook een CPS publiceren in het Nederlands. Hierbij mag er geen sprake mag zijn van een wezenlijk inhoudelijk verschil tussen beide versies.

RFC 3647	2.2 Publicatie van TSP-informatie
Nummer	2.2-pkio7
PKIo	De TSP 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 TSP 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.

RFC 3647	2.2 Publicatie van TSP-informatie
Nummer	2.2-pkio8
PKIo	De certification practice statement van de TSP moet worden gestructureerd volgens RFC 2527, RFC 3647 of het Programma van Eisen van PKIoverheid dat is gebaseerd op RFC 3647 en moet alle relevante hoofdstukken bevatten zoals beschreven in RFC 2527, RFC 3647 of het PVE PKIoverheid.

RFC 3647	2.2 Publicatie van TSP-informatie
Nummer	2.2-pkio155
PKIo	De TSP MOET in haar CPS beschrijven welke validatiemethodes voor het valideren van FQDN's zij hanteert voor opname in het Subject.CommonName veld en/of het SubjectAltName.dNSName veld met daarbij een verwijzing naar het juiste hoofdstuknummer van de Baseline Requirements

RFC 3647	2.2 Publicatie van TSP-informatie
Nummer	2.2-pkio156
PKIo	Het CPS (of de CPS's) van een TSP MOETEN minimaal eenmaal per jaar worden vernieuwd of herzien.

	CA's MOETEN aangeven dat dit is gebeurd door het versienummer te verhogen en een ingevoerde datum met wijzigingslogboek toe te voegen, zelfs als er geen andere wijzigingen in het document zijn aangebracht.
--	---

RFC 3647	2.2 Publicatie van TSP-informatie
Nummer	2.2-pkio157
PKIo	Het CPS zal beschikbaar worden gesteld in het Nederlands en/of Engels. Hierbij mag er geen sprake zijn van een wezenlijk inhoudelijk verschil tussen beide versies.

RFC 3647	2.2 Publicatie van TSP-informatie
Nummer	2.2-pkio166
PKIo	De TSP MOET in haar CPS beschrijven welke validatiemethodes voor het valideren van IP-adressen en/of FQDN's zij hanteert voor opname in het Subject.CommonName veld, het SubjectAltName.dNSName veld en/of het SubjectAltName.iPAdress veld met daarbij een verwijzing naar het juiste hoofdstuknummer van de Baseline Requirements.

RFC 3647	2.2 Publicatie van TSP-informatie
Nummer	2.2pkio167
PKIo	De TSP MOET in haar CPS beschrijven welke validatiemethodes voor het valideren van FQDN's zij hanteert voor opname in het Subject.CommonName veld en het SubjectAltName.dNSName veld met daarbij een verwijzing naar het juiste hoofdstuknummer van de Baseline Requirements.

RFC 3647	2.2 Publicatie van TSP-informatie
Nummer	2.2-pkio168
PKIo	De TSP MOET in haar CPS beschrijven welke validatiemethodes voor het valideren van IP-adressen en/of FQDN's zij hanteert voor opname in het Subject.CommonName veld, het SubjectAltName.dNSName veld en/of het SubjectAltName.iPAdress veld met daarbij een verwijzing naar het juiste hoofdstuknummer van de Baseline Requirements OF een verwijzing naar het door de PA verstrekte nummer in geval van afwijkende validatiemethoden zoals beschreven in eis 3.2.5-pkio162.

3 Identificatie en authenticatie

3.1 Naamgeving

RFC 3647	3.1.3 Anonimiteit of pseudonimiteit van certificaathouders
Nummer	3.1.3-pkio11
PKIo	Het gebruik van pseudoniemen in certificaten is niet toegestaan.

3.2 Initiële identiteitsvalidatie

RFC 3647	3.2.1. Methode om bezit van de private sleutel aan te tonen
Nummer	3.2.1-pkio13
PKIo	<p>De TSP waarborgt dat de abonnee het certificate signing request (CSR) op een veilige manier aanlevert. Het op een veilige manier aanleveren moet als volgt plaatsvinden:</p> <ul style="list-style-type: none"> • het invoeren van het CSR op de daartoe speciaal ontwikkelde applicatie van de TSP waarbij gebruik wordt gemaakt van een SSL verbinding, die gebruikt maakt van een PKIoverheid SSL certificaat of gelijkwaardig of; • het invoeren van het CSR op de HTTPS website van de TSP die gebruikt maakt van een PKIoverheid SSL certificaat of gelijkwaardig of; • het via e-mail verzenden van het CSR voorzien van een gekwalificeerde elektronische handtekening van de certificaatbeheerder die gebruik maakt van een PKIoverheid gekwalificeerd certificaat of gelijkwaardig of; • het invoeren of verzenden van een CSR op een wijze minimaal gelijkwaardig aan bovenstaande manieren.

RFC 3647	3.2.2 Authenticatie van organisatorische entiteit
Nummer	3.2.2-pkio14
PKIo	De TSP dient – bij organisatiegebonden certificaten – te verifiëren dat de abonnee een bestaande organisatie is.

RFC 3647	3.2.2 Authenticatie van organisatorische entiteit
Nummer	3.2.2-pkio4
PKIo	De TSP dient te verifiëren dat de abonnee een bestaande organisatie is.

RFC 3647	3.2.2 Authenticatie van organisatorische entiteit
Nummer	3.2.2-pkio147

PKIo	<p>De TSP dient te verifiëren dat de abonnee een bestaande en legale organisatie is en wie de Bevoegde Vertegenwoordiger (of Vertegenwoordiging) van de abonnee is.</p> <p>Als bewijs dat het om een bestaande en legale organisatie en de juistheid en het bestaan van de door de abonnee opgegeven Bevoegde Vertegenwoordiger (of Vertegenwoordiging) gaat moet de TSP tenminste de volgende bewijsstukken opvragen en verifiëren:</p> <ul style="list-style-type: none"> • Voor organisatorische entiteiten binnen de overheid een recent gewaarmerkt uittreksel (maximaal 1 maand oud) uit het Handelsregister van de Kamer van Koophandel of een wet, oprichtingsakte of een algemene maatregel van bestuur. Indien inschrijving in het Handelsregister nog niet heeft plaatsgevonden, een kopie van de betreffende pagina uit de meest recente versie van de Staatsalmanak waarin de Bevoegde Vertegenwoordiger (of Vertegenwoordiging) staat vermeldt; • Voor privaatrechtelijke organisaties met en zonder rechtspersoonlijkheid een recent gewaarmerkt uittreksel (maximaal 1 maand oud) uit het Handelsregister van de Kamer van Koophandel waarin de Bevoegde Vertegenwoordiger (of Vertegenwoordiging) staat vermeldt. <p>De TSP moet tevens nagaan of de Organisatie en Bevoegde Vertegenwoordiger op de meest recente EU lijst van verboden terroristische organisaties en personen voorkomt, gepubliceerd door de Europese Raad. Deze lijsten zijn te vinden via de webpagina:</p> <p>http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:028:0057:0059:EN:PDF</p> <p>Het gaat hier om de besluiten inzake de actualisering van de lijst van personen, groepen en entiteiten bedoeld in de artikelen 2, 3 en 4 van Gemeenschappelijk Standpunt 2001/931/GBVB betreffende de toepassing van specifieke maatregelen ter bestrijding van het terrorisme.</p> <p>De TSP mag geen EV SSL certificaat uitgeven aan een organisatie of haar Bevoegde Vertegenwoordiger die op deze lijst staat.</p>
-------------	--

RFC 3647	3.2.2 Authenticatie van organisatorische entiteit
Nummer	3.2.2-pkio16
PKIo	De TSP dient – bij organisatiegebonden certificaten – te verifiëren dat de door de abonnee aangemelde organisatiennaam die in het certificaat wordt opgenomen juist en volledig is.

RFC 3647	3.2.2 Authenticatie van organisatorische entiteit
Nummer	3.2.2-pkio144
PKIo	De TSP dient te verifiëren dat de door de abonnee aangemelde organisatiennaam die in het certificaat wordt opgenomen juist en volledig is.

RFC 3647	3.2.2 Authenticatie van organisatorische entiteit
Nummer	3.2.2-pkio186
PKIo	Indien een organisatie van naam wijzigt maar het onderliggende registratienummer (bijv. HRN) blijft gelijk, dan HOEFT de abonnee de abonneeregistratie NIET opnieuw te doorlopen, Indien de organisatiennaam gelijk blijft maar het onderliggende registratienummer wijzigt, dan MOET de TSP de abonneeregistratie opnieuw uitvoeren.
Opmerking	In beide gevallen geldt dat het bestaande certificaat MOET worden ingetrokken omdat de gegevens in het certificaat niet meer conform de oorspronkelijk gevalideerde gegevens zijn.

RFC 3647	3.2.3 Authenticatie van persoonlijke identiteit
Nummer	3.2.3-pkio21
PKIo	Bij uitgifte van certificaten aan natuurlijke personen dient de TSP 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).

RFC 3647	3.2.3 Authenticatie van persoonlijke identiteit
Nummer	3.2.3-pkio22
PKIo	De TSP dient overeenkomstig Nederlandse wet- en regelgeving de identiteit en, indien van toepassing, specifieke eigenschappen te controleren van de certificaatbeheerder. Bewijs van de identiteit dient te worden gecontroleerd aan de hand van fysieke verschijning van de persoon zelf, hetzij direct hetzij indirect, met behulp van middelen waarmee dezelfde zekerheid kan worden verkregen als bij persoonlijke aanwezigheid. Het bewijs van identiteit kan op papier dan wel langs elektronische weg worden aangeleverd.

RFC 3647	3.2.3 Authenticatie van persoonlijke identiteit
Nummer	3.2.3-pkio24

PKIo	Bij identiteitsvastelling, geldt dat de identiteit van de certificaatbeheerder slechts kan worden vastgesteld met de bij artikel 1 van de Wet op de identificatieplicht aangewezen geldige documenten. De TSP dient de geldigheid en echtheid hiervan te controleren.
Opmerking	Indien de controle van de persoonlijke identiteit van de certificaatbeheerder is uitgevoerd bij de aanvraag van een certificaat in een ander domein van PKIoverheid, dan wordt de controle van de identiteit van de certificaatbeheerder onder deze CP vermeend plaats te hebben gevonden.

RFC 3647	3.2.3 Authenticatie van persoonlijke identiteit
Nummer	3.2.3-pkio26
PKIo	<p>De certificaatbeheerder is een persoon van wie de identiteit dient vastgesteld te worden in samenhang met een organisatorische entiteit. Er dient bewijs te worden overlegd van:</p> <ul style="list-style-type: none"> • volledige naam, met inbegrip van achternaam, eerste voornaam, initialen of overige voorna(a)m(en) (indien van toepassing) en tussenvoegsels (indien van toepassing); • geboortedatum en -plaats, een nationaal passend registratienummer, of andere eigenschappen van de certificaatbeheerder die kunnen worden gebruikt om, voor zover mogelijk, de persoon van andere personen met dezelfde naam te kunnen onderscheiden; • bewijs dat de certificaatbeheerder gerechtigd is voor een certificaathouder een certificaat te ontvangen namens de rechtspersoon of andere organisatorische entiteit.

RFC 3647	3.2.3 Authenticatie van persoonlijke identiteit
Nummer	3.2.3-pkio27
PKIo	<p>Ter verbijszondering van het in 3.2.3-pkio22 gestelde, geldt dat de identiteit van de certificaatbeheerder slechts kan worden vastgesteld met de bij artikel 1 van de Wet op de identificatieplicht aangewezen geldige documenten. De TSP dient de geldigheid en echtheid hiervan te controleren.</p> <p>De TSP moet tevens nagaan of de certificaatbeheerder op de meest recente EU lijst van verboden terroristische personen en organisaties voorkomt: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:028:0057:0059:EN:PDF</p> <p>De TSP mag geen EV SSL certificaat uitgeven aan een organisatie of haar certificaatbeheerder die op deze lijst staat</p>

RFC 3647	3.2.3 Authenticatie van persoonlijke identiteit
Nummer	3.2.3-pkio169
PKIo	<p>Voor certificaten die geschikt zijn voor het ondertekenen en/of beveiligen van e-mailberichten en waarin het e-mailadres van de certificaathouder is opgenomen zal de TSP passende maatregelen treffen om zeker te kunnen stellen dat de aanvrager zeggenschap heeft over het e-mailadres in kwestie OF dat hij/zij is gemachtigd door de houder van het e-mailadres om dit e-mail adres op te laten nemen in een certificaat.</p> <p>De TSP moet in haar CPS duidelijk aangeven welke procedures er worden uitgevoerd om bovenstaande te kunnen bevestigen.</p>

RFC 3647	3.2.5 Autorisatie van de certificaathouder
Nummer	3.2.5-pkio29

PKIo	<p>Bij organisatiegebonden certificaathouders dient de TSP te controleren dat:</p> <ul style="list-style-type: none"> • het bewijs, dat de certificaathouder geautoriseerd is namens de abonnee om een certificaat te ontvangen, authentiek is; • de in dit bewijs genoemde naam en identiteitskenmerken overeenkomen met de onder 3.2.3-pkio21 vastgestelde identiteit van de certificaathouder. <p>Bij beroepsgebonden certificaathouders dient de TSP te controleren dat:</p> <ul style="list-style-type: none"> • het bewijs, dat de certificaathouder geautoriseerd is het erkende beroep uit te oefenen, authentiek is; • de in dit bewijs genoemde naam en identiteitskenmerken overeenkomen met de onder 3.2.3-pkio21 vastgestelde identiteit van de certificaathouder.
Opmerking	<p>Als authentiek bewijs voor het uitoefenen van een erkend beroep wordt alleen beschouwd:</p> <ol style="list-style-type: none"> a. ofwel een geldig bewijs van inschrijving in een door de betreffende beroepsgroep erkend (beroeps)register waarbij een wettelijk geregeld tuchtrecht van toepassing is; b. ofwel een benoeming door een Minister; c. ofwel een geldig bewijs (b.v. een vergunning) dat aan de wettelijke eisen voor het uitoefenen van het beroep wordt voldaan; d. ofwel benoeming door een gemeente functionaris of burgemeester (geldt alleen voor Gemeentelijke Belastingdeurwaarders). <p>Onder geldig bewijs wordt verstaan een bewijs dat niet is verlopen of (tijdelijk of voorlopig is) ingetrokken.</p> <p>In eis 3.2.5-pkio160 staat een limitatieve lijst met onder a, b en c bedoelde beroepen.</p>

RFC 3647	3.2.5 Autorisatie van de certificaathouder
Nummer	3.2.5-pkio30
PKIo	<p>De TSP dient te controleren dat:</p> <ul style="list-style-type: none"> • het bewijs, dat de certificaathouder geautoriseerd is namens de abonnee om een certificaat te ontvangen, authentiek is; • of de certificaatbeheerder toestemming heeft verkregen van de abonnee om aan hem opgedragen handelingen uit te voeren (ingeval de certificaatbeheerder het registratieproces uitvoert).
Opmerking	<p>De "certificaatbeheerder" die handelingen overneemt van de certificaathouder hoeft niet noodzakelijkerwijs dezelfde persoon te zijn als de systeembeheerder of personeelsfunctionaris. Tevens is het toegestaan dat de kennis van de activeringsgegevens van het sleutelmateriaal (bijvoorbeeld PIN) door verschillende personen wordt gedeeld als de inrichting van het beheer dat vereist. Echter, aangeraden wordt het aantal personen dat kennis heeft van de PIN zo beperkt mogelijk te houden. Ook is het verstandig maatregelen te treffen die de toegang tot de PIN beperken. Een voorbeeld hiervan is het plaatsen van de PIN in een kluis waartoe slechts geautoriseerde personen in bepaalde situaties toegang kunnen krijgen.</p>

RFC 3647	3.2.5 Autorisatie van de certificaathouder
-----------------	--

Nummer	3.2.5-pkio31
PKIo	<p>De TSP dient te controleren dat:</p> <ul style="list-style-type: none"> • het bewijs, dat de certificaathouder geautoriseerd is via de abonnee om een certificaat te ontvangen, authentiek is; • de certificaatbeheerder toestemming heeft verkregen van de abonnee om aan hem opgedragen handelingen uit te voeren (ingeval de certificaatbeheerder het registratieproces uitvoert); • het aangevraagde certificaat in combinatie met de in de certificaathouder (apparaat) permanent opgeslagen gegevens voldoende informatie bevatten om het volgende eenduidig te kunnen achterhalen: <ul style="list-style-type: none"> ○ de identiteit van het apparaat (bijv. fabrikant en serienummer); ○ het bewijs dat het apparaat en diens productieproces conformeren aan het door de kadersteller vastgelegde normenkader.
Opmerking	<p>De "certificaatbeheerder" die handelingen overneemt van de certificaathouder hoeft niet noodzakelijkerwijs dezelfde persoon te zijn als degene die de certificaathouder (het apparaat) produceert of gebruikt. Tevens is het toegestaan dat de kennis van de activeringsgegevens van het sleutelmateriaal (bijvoorbeeld PIN) door verschillende personen wordt gedeeld als de inrichting van het beheer dat vereist. Echter, aangeraden wordt het aantal personen dat kennis heeft van de PIN zo beperkt mogelijk te houden. Ook is het verstandig maatregelen te treffen die de toegang tot de PIN beperken. Een voorbeeld hiervan is het plaatsen van de PIN in een kluis waartoe slechts geautoriseerde personen in bepaalde situaties toegang kunnen krijgen.</p>

RFC 3647	3.2.5 Autorisatie van de certificaathouder
Nummer	3.2.5-pkio32
PKIo	<p>Abonnee is een rechtspersoon (organisatiegebonden certificaten): In de overeenkomst die de TSP sluit met de abonnee dient te zijn opgenomen dat de abonnee de verantwoordelijkheid heeft om, als er relevante wijzigingen plaats hebben in de relatie tussen abonnee en certificaathouder, deze onmiddellijk aan de TSP kenbaar te maken door middel van een intrekkingverzoek. Relevante wijzigingen kunnen in dit verband bijvoorbeeld beëindiging van het dienstverband en schorsing zijn.</p> <p>Abonnee is een natuurlijk persoon (beroepsgebonden certificaten): In de overeenkomst die de TSP sluit met de abonnee dient te zijn opgenomen dat de abonnee de verantwoordelijkheid heeft om, als er relevante wijzigingen plaats hebben gevonden, deze onmiddellijk aan de TSP kenbaar te maken door middel van een intrekkingverzoek. Een relevante wijziging in dit verband is in ieder geval het niet langer beschikken over een geldig bewijs zoals aangegeven bij 3.2.5-pkio29.</p>

RFC 3647	3.2.5 Autorisatie van de certificaathouder
Nummer	3.2.5-pkio33
PKIo	In de overeenkomst die de TSP sluit met de abonnee dient te zijn opgenomen dat de abonnee de verantwoordelijkheid heeft om, als er relevante wijzigingen plaats hebben in de relatie tussen abonnee en certificaatbeheerder en/of service, deze onmiddellijk aan de TSP door te geven. Wanneer de service ophoudt te bestaan, dient dit door middel van een intrekkingverzoek te geschieden.

RFC 3647	3.2.5 Autorisatie van de certificaathouder
Nummer	3.2.5-pkio34
PKIo	In de overeenkomst die de TSP sluit met de abonnee dient te zijn opgenomen dat de abonnee de verantwoordelijkheid heeft om, als er relevante wijzigingen plaats hebben in de relatie tussen abonnee en certificaatbeheerder en/of certificaathouder (autonoom apparaat), deze onmiddellijk aan de TSP door te geven. Wanneer het apparaat uitvalt, dient dit door middel van een intrekkingverzoek te geschieden.

RFC 3647	3.2.5 Autorisatie van de certificaathouder
Nummer	3.2.5-pkio146
PKIo	<p>Een TSP dient te controleren of de abonnee de eigenaar is van de FQDN die wordt opgenomen in het server en of EV certificaat. De Baseline Requirements schrijven voor onder 4.2.1 dat bijzonder aandacht moet worden besteed aan High Risk Requests. PKIoverheid verstaat hieronder ten minste het volgende:</p> <ul style="list-style-type: none"> • Een domeinaam van een Fortune Global 500 company • Een domeinnaam met een second level domain gelijk aan een second level domain van de top 500 domeinnamen wereldwijd en Nederland specifiek. Een domeinnaam die voorkomt op een bekende spam- en/of phishing blacklist <p>Indien blijkt dat de houder een bedrijf is behorend tot de global 500 of de second level domainname gelijk is aan de top 500 domeinnamen mag de TSP hier alleen een certificaat voor uitgeven na uitdrukkelijke toestemming van een eindverantwoordelijke manager van de TSP die geen onderdeel is van het standaard goedkeuringsproces.</p> <p>Indien de domeinnaam voorkomt op een phishing blacklist mag hiervoor geen certificaat worden uitgegeven.</p>
Opmerking	<p>Grootste bedrijven: http://fortune.com/global500/ Meest gebruikte domeinnamen: http://www.alex.com/topsites Phishing: http://www.phishtank.com.</p> <p>Voorbeelden van high risk requests zoals hierboven gedefinieerd zijn twitter.nl, account.twitter.com.</p> <p>In het geval van het gebruik van een domain authorization letter, dient bij deze verzoeken extra veel zorg te worden besteed aan de verificatie en authenticiteit van de domain authorization letter.</p>

RFC 3647	3.2.5 Autorisatie van de certificaathouder
Nummer	3.2.5-pkio160
PKIo	<p>De limitatieve lijst van erkende beroepen waarvoor beroepsgebonden certificaten kunnen worden uitgegeven is als volgt:</p> <ol style="list-style-type: none"> 1. Accountant-Administratieconsulent; 2. Advocaat; 3. Octrooigemachtigde; 4. Registerloods; 5a. Degenen die zijn ingeschreven in een register als bedoeld in artikel 3 van de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG). 5b. Degenen die een beroep uitoefenen waarvan de opleiding krachtens artikel 34, eerste lid en artikel 36a van de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG) is geregeld of aangewezen. 6. Notaris; 7. Kandidaat notaris 8. Toegevoegd notaris; 9. Gerechtsdeurwaarder; 10. Waarnemend gerechtsdeurwaarder; 11. Toegevoegd gerechtsdeurwaarder; 12. Kandidaat gerechtsdeurwaarder; 13. Registeraccountant; 14. Dierenarts; 15. Zeevarende; 16. (Hoofd) Bewaarder; 17. Gemandateerd bewaarder; 18. Technisch medewerker schepen; 19. Inspecteur Scheepsregistratie; 20. Belastingdeurwaarder; 21. Rijksdeurwaarder. 22. Gemeentelijke Belastingdeurwaarder

RFC 3647	3.2.5 Autorisatie van certificaathouder
Nummer	3.2.5-pkio161
PKIo	<p>De TSP MOET controleren of de door de abonnee aangeleverde FQDN's (zie definitie in deel 4) die in een certificaat worden opgenomen:</p> <ul style="list-style-type: none"> - Daadwerkelijk op naam staan van de abonnee OF; - Deze gemachtigd is door de geregistreerde domeinnaam eigenaar OF; - Dat de abonnee aan kan tonen dat hij (technische) controle uitoefent over de FQDN in kwestie. <p>Dit dient gedaan te worden voor elke FQDN die opgenomen wordt in een certificaat. De TSP dient zich hierbij te beperken tot de methodes zoals deze zijn voorgeschreven in de geldende versie van de Baseline Requirements van het CABForum (hoofdstuk 3.2.2.4). De TSP moet zich hierbij ook houden aan de vereisten in de EV Guidelines (EVCG) hoofdstuk 11.</p> <p>De geverifieerde gegevens mogen worden hergebruikt bij een volgende aanvraag, mits deze niet ouder zijn dan 13 maanden. Indien de gegevens ouder zijn dan 13 maanden dient bovengenoemde controle opnieuw plaats te vinden.</p> <p>Tevens dient de TSP per certificaat bij te houden welke validatiemethode(s) is/zijn gebruikt voor de opgenomen FQDN's.</p> <p>Deze verificatie mag door de TSP niet worden uitbesteed aan externe (onder)leveranciers</p>

RFC 3647	3.2.5 Autorisatie van certificaathouder
Nummer	3.2.5-pkio162
PKIo	<p>Indien een FQDN in het certificaat wordt opgenomen MOET de TSP controleren of de door de abonnee aangeleverde FQDN's (zie definitie in deel 4) die in een certificaat worden opgenomen:</p> <ul style="list-style-type: none"> - Daadwerkelijk op naam staan van de abonnee OF; - Deze gemachtigd is door de geregistreerde domeinnaam eigenaar OF; - Dat de abonnee aan kan tonen dat hij (technische) controle uitoefent over de FQDN in kwestie. <p>De geverifieerde gegevens mogen worden hergebruikt bij een volgende aanvraag, mits deze niet ouder zijn dan 39 maanden. Indien de gegevens ouder zijn dan 39 maanden dient bovengenoemde controle opnieuw plaats te vinden</p> <p>Dit dient gedaan te worden voor elke FQDN die opgenomen wordt in een certificaat. De TSP dient zich hierbij te beperken tot:</p> <ul style="list-style-type: none"> - de methodes zoals deze zijn voorgeschreven in de geldende versie van de Baseline Requirements van het CABForum (hoofdstuk 3.2.2.4) OF; een vooraf door de PA goedgekeurde alternatieve methode. <p>Tevens dient de TSP per certificaat bij te houden welke validatiemethode(s) is/zijn gebruikt voor de opgenomen FQDN's.</p> <p>Deze verificatie mag door de TSP niet worden uitbesteed aan externe (onder)leveranciers</p>

RFC 3647	3.2.5 Autorisatie van certificaathouder
Nummer	3.2.5-pkio170
PKIo	<p>De TSP MOET controleren of de door de abonnee aangeleverde FQDN's (zie definitie in deel 4) of IP-adressen die in een certificaat worden opgenomen:</p> <ul style="list-style-type: none"> - Daadwerkelijk op naam staan van de abonnee OF; - Deze gemachtigd is door de geregistreerde domeinnaam eigenaar OF; - Dat de abonnee aan kan tonen dat hij (technische) controle uitoefent over de FQDN in kwestie. <p>Dit dient gedaan te worden voor elke FQDN die opgenomen wordt in een certificaat. De TSP dient zich hierbij te beperken tot de methodes zoals deze zijn voorgeschreven in de geldende versie van de Baseline Requirements van het CABForum (hoofdstuk 3.2.2.4 voor FQDN's en 3.2.55 voor IP_adressen).</p> <p>Hierbij geldt dat "Any Other Method" uit 3.2.2.5 niet gebruikt mag worden (voor zowel 3.2.2.4.8 als voor IP-adressen direct).</p> <p>De geverifieerde gegevens mogen worden hergebruikt bij een volgende aanvraag, mits deze niet ouder zijn dan 825 dagen. Indien de gegevens ouder zijn dan 825 dagen dient bovengenoemde controle opnieuw plaats te vinden.</p>

	<p>Tevens dient de TSP per certificaat bij te houden welke validatiemethode(s) is/zijn gebruikt voor de opgenomen FQDN's. Deze verificatie mag door de TSP niet worden uitbesteed aan externe (onder)leveranciers</p>
--	---

3.3 Identificatie en authenticatie bij vernieuwing van het certificaat

Bevat geen aanvullende eisen.

4

Operationele eisen certificaatlevenscyclus

4.1 Aanvraag van certificaten

RFC 3647	4.1 Aanvraag van certificaten
Nummer	4.1-pkio47
PKIo	De TSP dient, voorafgaand aan de uitgifte van een services certificaat, een overeenkomst af te sluiten met de abonnee en een, door de certificaatbeheerder ondertekende, certificaataanvraag te ontvangen. De overeenkomst moet ondertekend worden door de Bevoegde Vertegenwoordiger of Vertegenwoordiging van de abonnee

RFC 3647	4.1 Aanvraag van certificaten
Nummer	4.1-pkio48
PKIo	<p>Voorafgaand aan de uitgifte van een EV SSL certificaat moet de TSP een volledig ingevuld en door de certificaatbeheerder, namens de abonnee, ondertekende aanvraag hebben ontvangen. De aanvraag moet de volgende informatie bevatten:</p> <ul style="list-style-type: none"> ▪ De naam van de organisatie; ▪ De domeinnaam (FQDN); ▪ Kamer van Koophandel nummer of Overheid Identificatie Nummer (OIN); ▪ Adres van de abonnee bestaande uit: <ul style="list-style-type: none"> ○ Straatnaam en huisnummer; ○ Plaatsnaam; ○ Provincie; ○ Land; ○ Postcode ○ Algemeen telefoonnummer. ▪ Naam van de certificaatbeheerder.

4.2 Verwerking van certificaat aanvraag

RFC 3647	4.2 Verwerking van certificaat aanvraag
Nummer	4.2-pkio179
PKIo	Een CA moet in staat zijn, zijn totale populatie uitstaande, nog geldige certificaten, binnen 5 dagen te kunnen vervangen, mits de abonnee tijdig medewerking verleent.

Opmerking	<p>Om te zorgen dat een abonnee dergelijke gegevens tijdig kan aanleveren kan de TSP bijvoorbeeld de volgende maatregelen treffen:</p> <ul style="list-style-type: none">• Inrichting van klantportaal die het proces faciliteert en versnelt• Het periodiek controleren van (domein)validatie zodat data "vers" is op het moment dat het benodigd is• Het (deels) automatiseren van het certificaatuitgifteproces via een API (bijv. RFC8555)
------------------	--

4.3 Uitgifte van certificaten

Bevat geen aanvullende eisen.

4.4 Acceptatie van certificaten

RFC 3647	4.4.3 Kennisgeving van het certificaat uitgifte door de CA aan andere entiteiten										
Nummer	4.4.3-pkio154										
PKIo	<p>Het certificaat bevat ten minste het volgende aantal SCT's:</p> <table border="1"> <thead> <tr> <th>Geldigheidsduur certificaat</th> <th>Aantal SCT's</th> </tr> </thead> <tbody> <tr> <td><15 maanden</td> <td>2</td> </tr> <tr> <td>>= 15, <= 27 maanden</td> <td>3</td> </tr> <tr> <td>> 27, <= 39 maanden</td> <td>4</td> </tr> <tr> <td>> 39 maanden</td> <td>5</td> </tr> </tbody> </table> <p>De SCT's zijn afkomstig van een log dat of gekwalificeerd is, of in afwachting van kwalificatie is op het moment van certificaat uitgifte. Onder een gekwalificeerd log wordt verstaan een CT log dat voldoet aan de Certificate Transparency Log Policy van Chromium en is opgenomen door Chromium.</p> <p>Ten minste één SCT is afkomstig van een door Google onderhouden log en één SCT van een niet door Google onderhouden log. Bij het opnemen van meer dan 2 SCT's (zie tabel) blijft de vereiste dat minimaal 1 van de logs waar het certificaat wordt aangemeld van Google is.</p>	Geldigheidsduur certificaat	Aantal SCT's	<15 maanden	2	>= 15, <= 27 maanden	3	> 27, <= 39 maanden	4	> 39 maanden	5
Geldigheidsduur certificaat	Aantal SCT's										
<15 maanden	2										
>= 15, <= 27 maanden	3										
> 27, <= 39 maanden	4										
> 39 maanden	5										
Opmerking	De bovenstaande eis is in lijn met de door Google geadopteerde CT Policy voor gebruik in de Chrome applicatie.										

4.5 Sleutelbaar en certificaatgebruik

Bevat geen aanvullende eisen.

4.8 Compliance, audit en assesement

Bevat geen aanvullende eisen.

4.9 Intrekking en opschorting van certificaten

RFC 3647	4.9.1 Omstandigheden die leiden tot intrekking
Nummer	4.9.1-pkio52
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 TSP beschikt over voldoende bewijs dat de privésleutel van de abonnee, die geassocieerd is met de publieke sleutel in een certificaat, is aangetast of

	<p>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, SSCD, SUD of QSCD, gestolen of vermoedelijk gestolen sleutel, SSCD, SUD of QSCD of vernietigde sleutel, SSCD, SUD of QSCD indien van toepassing;</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 TSP of de overeenkomst die de TSP met de abonnee heeft afgesloten; • de TSP op de hoogte wordt gesteld of anderszins zich bewust wordt van een wezenlijke verandering in de informatie, die in het certificaat staat. Voorbeeld daarvan is: verandering van de naam van de certificaathouder (service); • de TSP bepaald dat het certificaat niet is uitgegeven in overeenstemming met deze CP of het bijbehorende CPS van de TSP of de overeenkomst die de TSP met de abonnee heeft gesloten; • de TSP bepaald dat informatie in het certificaat niet juist of misleidend is; • de TSP haar werkzaamheden staakt en de CRL en OCSP dienstverlening niet wordt overgenomen door een andere TSP; • 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).
<p>Opmerking</p>	<p>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 TSP waarmee certificaten worden ondertekend, beschouwd.</p>

<p>RFC 3647</p>	<p>4.9.3 Procedure voor een verzoek tot intrekking</p>
<p>Nummer</p>	<p>4.9.3-pkio57</p>
<p>PKIo</p>	<p>De TSP moet in ieder geval gebruik maken van een CRL om de certificaatstatus informatie beschikbaar te stellen.</p>

RFC 3647	4.9.3 Procedure voor een verzoek tot intrekking
Nummer	4.9.3-pkio58
PKIo	<p>De TSP moet de procedure voor intrekking publiceren en in die publicatie eenduidige definities geven van de volgende – in chronologische volgorde opgesomde – deelprocessen:</p> <ul style="list-style-type: none"> • De ontvangst van een verzoek tot intrekking; • De identificatie en authenticatie van degene die het verzoek tot intrekking indient; • Het betrouwbaarheidsonderzoek met betrekking tot het verzoek tot intrekking; • De verwerking van (het betrouwbare verzoek tot) de intrekking; • De publicatie van de (verwerkte) intrekking. <p>De definitie van elk deelproces dient minimaal de voorwaarden voor het doorlopen van het deelproces en de in dat deelproces te registreren gegevens te bevatten.</p>

RFC 3647	4.9.3 Procedure voor een verzoek tot intrekking
Nummer	4.9.3-pkio60
PKIo	<p>Als er sprake is van een issuing subordinate CA onder een TSP CA dan:</p> <ul style="list-style-type: none"> ▪ moet de TSP gebruik maken van een OCSP en een CRL om de certificaatstatus informatie, met betrekking tot de issuing subordinate CA, beschikbaar te stellen; ▪ moet de TSP de beweegreden voor de intrekking van het issuing subordinate CA certificaat vastleggen; ▪ de geldigheid van de CRL, met betrekking tot de certificaatstatus informatie van het issuing subordinate CA, is maximaal 7 dagen.

RFC 3647	4.9.5 Tijdsduur voor verwerking intrekkingverzoek
Nummer	4.9.5-pkio62
PKIo	<p>In het geval van een issuing subordinate CA geldt dat de maximale vertraging, tussen het beslismoment om een issuing subordinate CA in te trekken (vastgelegd in een rapportage) en de wijziging van de revocation status information, die voor alle vertrouwende partijen beschikbaar is, is gesteld op 72 uur.</p>

RFC 3647	4.9.7 CRL-uitgiftefrequentie
Nummer	4.9.7-pkio65
PKIo	De TSP 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	4.9.9-pkio66
PKIo	De revocation management services van de TSP 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.
Opmerking	<p>Indien gebruik wordt gemaakt van OCSP zijn de volgende eisen van toepassing:</p> <ul style="list-style-type: none"> • 3.1.1-pkio10 (basiseis) • 4.9.5-pkio61 (basiseis) • 4.9.9-pkio67 • 4.9.9-pkio68 • 4.9.5-pkio69 (basiseis) • 4.9.9-pkio70 • 4.9.9-pkio71 • 4.10.2-pkio73 (basiseis) <p>Nota bene: (EV) server certificaten MOETEN gebruik maken van OCSP dienstverlening volgens ETSI EN 319 411-1 en de Baseline Requirements.</p>

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	4.9.9-pkio67
PKIo	Indien de TSP het Online Certificate Status Protocol (OCSP) ondersteunt, dient dit te gebeuren in overeenstemming met IETF RFC 6960.

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	4.9.9-pkio68
PKIo	<p>Ter verbijzondering van het in IETF RFC 6960 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 TSP aangewezen responder die beschikt over een OCSP-Signing certificaat dat voor dit doel is uitgegeven door de TSP, 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	4.9.9-pkio70
PKIo	<p>Indien de TSP 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.</p>

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	4.9.9-pkio71
PKIo	<p>Indien de TSP OCSP ondersteunt, moet de TSP de OCSP service tenminste een keer in de 4 kalenderdagen bijwerken. De maximale vervaltermijn van de OCSP responses is 10 kalenderdagen. Tevens dienen OCSP responses voorzien te zijn van het "nextUpdate" veld conform RFC6960.</p>

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	4.9.9-pkio152
PKIo	<p>Indien de TSP OCSP ondersteunt, moet de OCSP response een minimale geldigheidsduur hebben van 8 uur en een maximale geldigheidsduur van 7 kalenderdagen. De next update dient tenminste op de helft van de geldigheid van een OCSP response beschikbaar te zijn.</p>

4.10 Certificaat statusservice

Bevat geen aanvullende eisen.

5 Management, operationele en fysieke beveiligingsmaatregelen

5.2 Procedurele beveiliging

Bevat geen aanvullende eisen.

5.3 Personele beveiliging

Bevat geen aanvullende eisen.

5.4 Procedures ten behoeve van beveiligingsaudits

RFC 3647	5.4.1 Vastlegging van gebeurtenissen
Nummer	5.4.1-pkio80
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 TSP 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 TSP zelf welke gegevens zij opslaat.

5.5 Archivering van documenten

RFC 3647	5.5.1 Vastlegging van gebeurtenissen
-----------------	--------------------------------------

Nummer	5.5.1-pkio82
PKIo	De TSP dient alle informatie op te slaan die is gebruikt voor het verifiëren van de identiteit van de abonnee, certificaatbeheerder en indieners van verzoeken tot intrekking, met inbegrip van referentienummers van de documentatie die is gebruikt voor verificatie, evenals beperkingen ten aanzien van de geldigheid.

5.7 Aantasting en continuïteit

RFC 3647	5.7.4 Continuïteit van de bedrijfsvoering na calamiteit
Nummer	5.7.4-pkio86
PKIo	<p>De TSP 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 TSP dienstverlening ten behoeve van abonnees, vertrouwende partijen en derden (waaronder browserpartijen). De TSP 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 TSP dienstverlening; ▪ Onderhoudsschema en testplan dat voorziet in het jaarlijks testen, beoordelen en actualiseren van het BCP; ▪ Bepalingen over het onder de aandacht brengen van het belang van business continuity; ▪ Taken, verantwoordelijkheden en bevoegdheden van betrokken actoren; ▪ Beoogde hersteltijd c.q. Recovery Time Objective (RTO); ▪ Vastleggen van de frequentie van back-ups van kritische bedrijfsinformatie en software; ▪ Vastleggen van de afstand van de uitwijkfaciliteit tot de hoofdvestiging van de TSP; 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 TSP sub CA
Nummer	6.1.1-pkio87
PKIo	Het algoritme en de lengte van de cryptografische sleutels die worden gebruikt voor het genereren van de sleutels voor de TSP 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 119 312.
Opmerking	Hoewel in ETSI TS 119 312 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	6.1.1-pkio88
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 EN 419 211 voor QSCD's of CWA 14169 voor SSCD's (overgangsrecht) "Secure signature-creation devices "EAL 4+"" of gelijkwaardige beveiligingscriteria.

RFC 3647	6.1.1 Genereren van sleutelparen van de certificaathouders
Nummer	6.1.1-pkio89
PKIo	Het algoritme en de lengte van de cryptografische sleutels dat de TSP 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 119 312.
Opmerking	Hoewel in ETSI TS 119 312 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	6.1.1-pkio90
PKIo	Het genereren van sleutelparen van de certificaathouder door de TSP is niet toegestaan.

RFC 3647	6.1.1 Genereren van sleutelparen van de certificaathouders
Nummer	6.1.1-pkio91
PKIo	<p>Indien de TSP de private sleutel genereert ten behoeve van de abonnee MOET deze versleuteld worden aangeleverd aan de abonnee zodat integriteit en vertrouwelijkheid van de private sleutel geborgd is. De volgende maatregelen moeten daarbij in acht worden genomen:</p> <ol style="list-style-type: none"> a. De TSP MOET de private sleutel ten behoeve van de abonnee generen in de beveiligde omgeving waarop de PKIoverheid PvE en de bijbehorende audit van toepassing is; b. Nadat de private sleutel ten behoeve van de abonnee is gegeneerd MOET deze met behulp van een sterk algoritme (conform eisen ETSI TS 119 312) versleuteld worden opgeslagen binnen de beveiligde omgeving van de TSP; c. De TSP MOET daarbij de PKCS#12 (P12) standaard toepassen waarbij gebruik wordt gemaakt van de privacy mode en de integrity mode. Hiertoe MAG de TSP het P12 bestand versleutelen met een persoonsgebonden PKI certificaat van de abonnee / certificaatbeheerder. Indien deze niet beschikbaar is MOET de TSP een wachtwoord gebruiken die door de abonnee is aangeleverd. Dit wachtwoord MOET door de abonnee zijn aangeleverd via de website van de TSP waarbij gebruik wordt gemaakt van een SSL/TLS verbinding of via een gelijkwaardige procedure waarmee dezelfde betrouwbaarheid en veiligheid wordt gewaarborgd; d. Indien een wachtwoord wordt gebruikt om de P12 te versleutelen moet dit wachtwoord minimaal 8 posities bevatten waaronder minimaal één getal en twee bijzondere tekens; e. De TSP MAG het wachtwoord dat wordt gebruikt om de P12 te versleutelen / ontsleutelen NOOIT in cleartext over een netwerk verzenden of op een server opslaan. Het wachtwoord MOET worden versleuteld met behulp van sterk algoritme (conform eisen ETSI TS 119 312); f. Het P12 bestand MOET over een met SSL/TLS beveiligd netwerk aan de abonnee worden gezonden of out-of-band op een informatiedrager (b.v. USB-stick of CD-rom) worden aangeleverd. g. Als de P12 out-of-band wordt aangeleverd moet deze additioneel versleuteld zijn met een andere sleutel dan het P12 bestand. Daarnaast MOET de P12 via een door de gecertificeerde koerier of door een vertegenwoordiger van de TSP in een sealbag worden afgeleverd bij de abonnee. De koerier dient een gecertificeerd te

	<p>zijn conform de normen die voorgeschreven worden in deel 2 onder hoofdstuk 2.2 voor de specifieke dienstverlening die hier van toepassing is.</p> <p>h. Als het P12 bestand over een met SSL/TLS beveiligd netwerk wordt aangeboden MOET de TSP waarborgen dat het P12 bestand maximaal één keer succesvol wordt gedownload. Toegang tot het P12 bestand bij de overdracht via SSL/TLS moet na drie pogingen worden geblokkeerd.</p>
Opmerking	<p>Best practice is dat de abonnee zelf de private sleutel behorend bij de publieke sleutel genereert. Wanneer de TSP ten behoeve van de abonnee de private sleutel behorend bij de publieke sleutel genereert moet deze voldoen aan bovenstaande eisen. Het is hierbij van belang te onderkennen dat niet alleen het P12 bestand wordt versleuteld, maar ook de toegang tot het P12 bestand bij de overdracht wordt beveiligd.</p>

RFC 3647	6.1.1 Genereren van sleutelparen van de certificaathouders
Nummer	6.1.1-pkio92
PKIo	Het is een TSP binnen de PKIoverheid niet toegestaan code signing certificaten uit te geven.

RFC 3647	6.1.1 Genereren van sleutelparen van de certificaathouders
Nummer	6.1.1-pkio93
PKIo	<p>In plaats van de sleutels te laten genereren door de TSP mogen de sleutels van services authenticiteits- en vertrouwelijkheidscertificaten worden gegenereerd in een SUD door de certificaatbeheerder, waarbij gebruik wordt gemaakt van PKCS#10 om de CSR ter ondertekening aan te bieden aan de TSP,</p> <ul style="list-style-type: none"> - Indien in de overeenkomst die wordt gesloten tussen TSP en abonnee, is opgenomen dat de certificaatbeheerder de private sleutel genereert, opslaat en gebruikt op een veilig middel dat voldoet aan de eisen genoemd in CWA 14169 voor een Secure signature-creation devices of EN 419 211 voor Qualified signature-creation devices "EAL 4+" of gelijkwaardige beveiligingscriteria. Hierbij dient de abonnee bij de aanvraag aan te tonen dat de voor sleutelgeneratie gebruikte veilig middel voldoet aan CWA 14169 voor een Secure signature-creation devices of EN 419 211 voor Qualified signature-creation devices "EAL 4+" of gelijkwaardige beveiligingscriteria. De TSP dient daaropvolgend vast te stellen dat de gebruikte SUD inderdaad voldoet (vergelijkbaar met "De abonnee MOET aantonen dat de organisatie deze naam mag voeren.") - Indien de certificaatbeheerder bij registratie ten minste een schriftelijke verklaring overlegt dat maatregelen zijn getroffen in de omgeving van het systeem dat de sleutels genereert / bevat. De maatregelen moeten van een dusdanige kwaliteit zijn dat het praktisch onmogelijk is de sleutels ongemerkt te stelen of te kopiëren.

	<p>Hierbij dient in de overeenkomst tussen abonnee en TSP te worden opgenomen dat de TSP het recht heeft om een controle uit te voeren naar de getroffen maatregelen (conform 6.2.11-pkio107)</p> <ul style="list-style-type: none"> - Indien een bepaling wordt opgenomen in de overeenkomst tussen de TSP en de Abonnee waarin staat dat de abonnee moet verklaren dat de private sleutel (en de daarbij behorende toegangsinformatie b.v. een PINcode), behorend bij de publieke sleutel in het betreffende SUD, op passende wijze, onder controle van de certificaatbeheerder is gegenereerd en in de toekomst geheim wordt gehouden en beschermd.
--	---

RFC 3647	6.1.1 Genereren van sleutelparen van de certificaathouders
Nummer	6.1.1-pkio153
PKIo	<p>Subject key generation van een gekwalificeerd digitaal zegel certificaat voor het in grote hoeveelheid, geautomatiseerd tekenen van gestandaardiseerde data is toegestaan in ETSI 319 411-2. De beveiligingseisen die hieraan worden gesteld zijn niet verder uitgewerkt in ETSI. Subject key generation is binnen PKIoverheid mogelijk onder de volgende voorwaarden:</p> <ul style="list-style-type: none"> - In de overeenkomst die wordt gesloten tussen TSP en abonnee, is een verklaring opgenomen dat de abonnee de private sleutel genereert, opslaat en gebruikt op een gekwalificeerd middel voor elektronische handtekeningen zoals een HSM dat voldoet aan de eisen genoemd in {7} CWA 14169 Secure signature-creation devices of EN 419 211 voor Qualified signature-creation devices "EAL 4+" of gelijkwaardige beveiligingscriteria zoals FIPS 140-2 level 3. <p>Hiervan dient de abonnee bij de aanvraag bewijs te overhandigen door middel van het overleggen van de certificering van het veilig middel en indien nodig een screenshot van de instelling van het veilige middel op FIPS140-2 level 3.</p> <ul style="list-style-type: none"> - Een bepaling wordt opgenomen in de overeenkomst tussen de TSP en de abonnee waarin staat dat de abonnee verklaart dat de private sleutel (en de daarbij behorende toegangsinformatie b.v. een PINcode), behorend bij de publieke sleutel in het betreffende gekwalificeerde middel is gegenereerd en in de toekomst geheim wordt gehouden en beschermd. <p>Hierbij dient de abonnee bewijs te overhandigen van het PKI ceremoniescript dat wordt gehanteerd bij de implementatie van het gekwalificeerde middel voor elektronische handtekeningen en het genereren van het sleutelpaar.</p> <ul style="list-style-type: none"> - de TSP aanwezig is bij de PKI ceremonie voor in gebruik name van het gekwalificeerde middel voor elektronische handtekeningen en het genereren van het sleutelpaar. Hiermee kan de TSP zich ook vergewissen van de effectiviteit van getroffen beveiligingsmaatregelen. - de Abonnee bij registratie ten minste een schriftelijke verklaring overlegt, aantoonbaar te voldoen aan de eisen en/of de voorwaarden die het gekwalificeerde middel voor elektronische handtekeningen stelt aan het gebruik ervan dan wel de certificering van het middel stelt aan de omgeving waarbinnen het geheel wordt beheerd en het beheer zelf. - De abonnee een schriftelijke verklaring overlegt dat de certificaathouder, systeembeheerders van het gekwalificeerd middel voor elektronische handtekeningen expliciet heeft gemandateerd voor het beheer en dat altijd sprake is van dual control voor toegang tot dit middel.
Opmerking	Indien de TSP het sleutelpaar en het certificaat genereert en deze uitlevert op een veilig middel aan de abonnee is het niet noodzakelijk aanwezig te zijn bij de ceremonie

RFC 3647	6.1.2 Overdracht van private sleutel en SSCD of QSCD aan certificaathouder
-----------------	--

Nummer	6.1.2-pkio94
PKIo	<p>[OID 2.16.528.1.1003.1.2.5.2], [OID 2.16.528.1.1003.1.2.5.1] en [OID 2.16.528.1.1003.1.2.3.1]</p> <p>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.</p>
Opmerking	Deze tekst komt overeen met ETSI EN 319 411-1 SDP 6.3.3-09, maar is integraal opgenomen omdat deze eis alleen van toepassing is op handtekening- en authenticiteitcertificaat.

6.2 Private sleutelbescherming en cryptografische module engineering beheersmaatregelen

RFC 3647	6.2.3 Escrow van private sleutels van certificaathouders
Nummer	6.2.3-pkio99
PKIo	De geautoriseerde personen, die toegang kunnen krijgen tot de door de TSP in escrow gehouden private sleutel van het vertrouwelijkheidcertificaat (indien van toepassing), moeten zich identificeren aan de hand van de bij artikel 1 van de Wet op de identificatieplicht aangewezen geldige documenten of een geldig gekwalificeerd certificaat (beperkt tot het PKIoverheid handtekeningcertificaat of gelijkwaardig).

RFC 3647	6.2.3 Escrow van private sleutels van certificaathouders
Nummer	6.2.3-pkio100
PKIo	De TSP dient in de CPS te beschrijven welke partijen en onder welke voorwaarden, toegang tot de in escrow gehouden private sleutel van het vertrouwelijkheids-certificaat kunnen krijgen.

RFC 3647	6.2.3 Escrow van private sleutels van certificaathouders
Nummer	6.2.3-pkio101
PKIo	Indien de TSP de private sleutel van het vertrouwelijkheids-certificaat in escrow houdt, dient de TSP 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 EN 319 411-1, 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 TSP moet overleggen.

RFC 3647	6.2.11 Eisen voor veilige middelen voor het aanmaken van elektronische handtekeningen
Nummer	6.2.11-pkio104
PKIo	Door de TSP uitgegeven of aanbevolen veilige middelen voor het aanmaken van elektronische handtekeningen (SSCD's of QSCD's) moeten voldoen aan de eisen gesteld in document [12] CWA 14169 "Secure signature-creation devices of EN 419 211 voor Qualified 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 of QSCD aan de inhoudelijke eisen voldoet zoals gespecificeerd in 6.2.11-pkio104, 6.2.11-pkio105 en 6.2.11-pkio106.

RFC 3647	6.2.11 Eisen voor veilige middelen voor het aanmaken van elektronische handtekeningen
Nummer	6.2.11-pkio105
PKIo	In plaats van conformiteit aan CWA 14169 (voor SSCD's of SUD's) of EN 419 211 (voor QSCD's) aan te tonen mogen TSP's SSCD's, SUD's of QSCD'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	6.2.11-pkio106
PKIo	De overeenstemming van SSCD's of QSCD's met de eisen zoals genoemd in PKIo-eis nr 6.2.11-pkio104 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.

RFC 3647	6.2.11 Eisen voor veilige middelen voor het aanmaken van elektronische handtekeningen
Nummer	6.2.11-pkio107
PKIo	<p>In plaats van gebruik te maken van een hardwarematige SUD mogen de sleutels van een server certificaat softwarematig worden beschermd indien compenserende maatregelen worden getroffen in de omgeving van het systeem dat de sleutels bevat. De compenserende maatregelen moeten van een dusdanige kwaliteit zijn dat het praktisch onmogelijk is de sleutels ongemerkt te stelen of te kopiëren.</p> <p>De beheerder van de server certificaten die gebruik maakt van deze mogelijkheid voor softwarematige opslag dient bij registratie ten minste een schriftelijke verklaring te overleggen dat compenserende maatregelen zijn getroffen die voldoen aan de hiervoor gestelde voorwaarde. In de overeenkomst tussen abonnee en TSP dient te worden opgenomen dat de TSP het recht heeft om een controle uit te voeren naar de getroffen maatregelen.</p>
Opmerking	Bij compenserende maatregelen moet bijvoorbeeld worden gedacht aan een combinatie van fysieke toegangsbeveiliging, logische toegangsbeveiliging, logging en audit en functiescheiding.

RFC 3647	6.2.11 Eisen voor veilige middelen voor het aanmaken van elektronische handtekeningen
Nummer	6.2.11-pkio125
PKIo	Door de TSP uitgegeven of aanbevolen veilige middelen voor opslag van sleutels (SUD's) moeten voldoen aan de eisen gesteld in document CWA 14169 Secure signature-creation devices "EAL 4+".

6.3 Andere aspecten van sleutelpaarmanagement

RFC 3647	6.3.1 Archiveren van publieke sleutels
Nummer	6.3.1-pkio108

PKIo	[OID 2.16.528.1.1003.1.2.2.2, 2.16.528.1.1003.1.2.5.2 en 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	6.3.2-pkio109
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.

RFC 3647	6.3.2 Gebruiksduur voor certificaten en publieke en private sleutels
Nummer	6.3.2-pkio111
PKIo	Private sleutels die door een certificaathouder worden gebruikt en die zijn uitgegeven onder verantwoordelijkheid van deze CP dienen niet langer dan tien jaar te worden gebruikt. De certificaten, die zijn uitgegeven onder de verantwoordelijkheid van deze CP, dienen een geldigheid te hebben van niet meer dan tien jaar.
Opmerking	De TSP's binnen het domein Autonome Apparaten van de PKI voor de overheid mogen pas certificaten uitgeven met een maximale geldigheidsduur van tien jaar nadat de PA hiervoor expliciet toestemming heeft gegeven.

RFC 3647	6.3.2 Gebruiksduur voor certificaten en publieke en private sleutels
Nummer	6.3.2-pkio178
PKIo	Private sleutels die door een certificaathouder worden gebruikt en die zijn uitgegeven onder verantwoordelijkheid van deze CP, MOGEN NIET langer dan twee (2) jaar te worden gebruikt. De certificaten, die zijn uitgegeven onder de verantwoordelijkheid van deze CP, MOGEN NIET een geldigheid te hebben van meer dan 397 dagen. In het geval dat een certificaat vervangen wordt na intrekking onder sectie 4.9.1.1 van de Baseline Requirements geldt dat de private sleutel van een certificaat NIET mag worden hergebruikt, tenzij dit intrekking betreft onder punt 7 (certificaat niet uitgegeven conform BR of CP/CPS van TSP)
Opmerking	

6.4 Activeringsgegevens

RFC 3647	6.4.1 Genereren en installeren van activeringsgegevens
Nummer	6.4.1-pkio112
PKIo	De TSP verbindt activeringsgegevens aan het gebruik van een SUD, SSCD of QSCD, ter bescherming van de private sleutels van de certificaathouders.
Opmerking	De eisen waaraan de activeringsgegevens (bijvoorbeeld de PIN-code) moet voldoen, kunnen door de TSP'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	6.4.1-pkio113
PKIo	Het is alleen toegestaan om gebruik te maken van een deblokkeringscode als de TSP kan garanderen dat daarbij tenminste wordt voldaan aan de betrouwbaarheidseisen, die aan het gebruik van de activeringsgegevens zijn gesteld.

6.5 Logische toegangsbeveiliging van TSP-computers

Bevat geen aanvullende eisen.

6.6 Beheersmaatregelen technische levenscyclus

Bevat geen aanvullende eisen.

6.7 Netwerkbeveiliging

Bevat geen aanvullende eisen.

7 Certificaat-, CRL- en OCSP-profielen

7.1 Certificaatprofielen

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio149
PKIo	<p>De certificaat extensie Extended Key Usage moet worden opgenomen, MAG NIET als "critical" worden aangemerkt, en MOET ten minste de volgende KeyPurposId's bevatten:</p> <p>Voor een authenticiteitscertificaat: client Authentication =1.3.6.1.5.5.7.3.2 document Signing =1.3.6.1.4.1.311.10.3.12 emailProtection = 1.3.6.1.5.5.7.3.4</p> <p>Voor een onweerlegbaarheidscertificaat: document Signing =1.3.6.1.4.1.311.10.3.12 emailProtection = 1.3.6.1.5.5.7.3.4 (verplicht voor G3, optioneel voor G2)</p> <p>Voor een vertrouwelijkheidscertificaat: emailProtection =1.3.6.1.5.5.7.3.4 Encrypting File System =1.3.6.1.4.1.311.10.3.4</p> <p>Hierbij geldt dat de id-kp-serverAuth NIET MAG worden opgenomen, dat de KeyPurposeId id-kp-codeSigning NIET MAG worden opgenomen.</p> <p>Specifiek voor de G2 certificaten geldt dat er wel elke andere, in een open of geaccepteerde standaard gedefinieerde, KeyPurposeId die correspondeert met het sleutelgebruik zoals aangeduid in de KeyUsage extensie MAG worden opgenomen. Bij de G3 en latere generaties MAG dit NIET.</p> <p>Bij bovenstaande dient rekening gehouden te worden met de opgenomen EKU's in de uitgevende TSP CA. Indien de uitgevende TSP CA niet voorzien is van de hierboven gestelde verplichte EKU's MOGEN deze NIET worden opgenomen in het eindgebruikerscertificaat.</p>

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio150
PKIo	<p>De certificaat extensie Extended Key Usage moet worden opgenomen, MAG NIET als "critical" worden aangemerkt, en MOET ten minste de volgende KeyPurposId's bevatten:</p> <p>Voor een services authenticiteitscertificaat: client Authentication =1.3.6.1.5.5.7.3.2 document Signing =1.3.6.1.4.1.311.10.3.12 EmailProtection = 1.3.6.1.5.5.7.3.4</p> <p>Voor een services vertrouwelijkheidscertificaat: emailProtection =1.3.6.1.5.5.7.3.4</p>

	<p>Encrypting File System =1.3.6.1.4.1.311.10.3.4</p> <p>Voor een zegelcertificaat document Signing =1.3.6.1.4.1.311.10.3.12 EmailProtection = 1.3.6.1.5.5.7.3.4</p> <p>Hierbij geldt dat id-kp-serverAuth NIET MAG worden opgenomen, dat de KeyPurposeId id-kp-codeSigning NIET MAG worden opgenomen, dat de KeyPurposeId AnyextendedKeyusage NIET MAG worden opgenomen, dat elke KeyPurposeId die uitsluitend bedoeld is voor het identificeren van een service op basis van zijn FDQN NIET MAG worden opgenomen.</p> <p>Specifiek voor de G2 certificaten geldt dat er wel elke andere, in een open of geaccepteerde standaard gedefinieerde, KeyPurposeId die correspondeert met het sleutelgebruik zoals aangeduid in de KeyUsage extensie MAG worden opgenomen. Bij de G3 en latere generaties MAG dit NIET.</p> <p>Bij bovenstaande dient rekening gehouden te worden met de opgenomen EKU's in de uitgevende TSP CA. Indien de uitgevende TSP CA niet voorzien is van de hierboven gestelde verplichte EKU's MOGEN deze NIET worden opgenomen in het eindgebruikerscertificaat.</p>
--	---

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio151
PKIo	<p>De certificaat extensie Extended Key Usage moet worden opgenomen, MAG NIET als "critical" worden aangemerkt, en MOET ten minste de volgende KeyPurposId's bevatten:</p> <p>Voor een Autonome Apparaten – authenticiteitscertificaat: Client Authentication =1.3.6.1.5.5.7.3.2</p> <p>Voor een Autonome Apparaten – vertrouwelijkheidscertificaat: emailProtection =1.3.6.1.5.5.7.3.4 Encrypting File System =1.3.6.1.4.1.311.10.3.4</p> <p>Voor een Autonome Apparaten – combinatiecertificaat: client Authentication =1.3.6.1.5.5.7.3.2 document Signing =1.3.6.1.4.1.311.10.3.12 emailProtection =1.3.6.1.5.5.7.3.4 Encrypting File System =1.3.6.1.4.1.311.10.3.4</p> <p>Hierbij geldt dat id-kp-serverAuth NIET MAG worden opgenomen, dat de KeyPurposeId id-kp-codeSigning NIET MAG worden opgenomen, dat de KeyPurposeId AnyextendedKeyusage NIET MAG worden opgenomen, dat elke KeyPurposeId die uitsluitend bedoeld is voor het identificeren van een service op basis van zijn FDQN NIET MAG worden opgenomen.</p> <p>Specifiek voor de G2 certificaten geldt dat er wel elke andere, in een open of geaccepteerde standaard gedefinieerde, KeyPurposeId die correspondeert met het sleutelgebruik zoals aangeduid in de KeyUsage extensie MAG worden opgenomen. Bij de G3 en latere generaties MAG dit NIET.</p> <p>Bij bovenstaande dient rekening gehouden te worden met de opgenomen EKU's in de uitgevende TSP CA. Indien de uitgevende TSP CA niet voorzien is</p>

	van de hierboven gestelde verplichte EKU's MOGEN deze NIET worden opgenomen in het eindgebruikerscertificaat.
--	---

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio163
PKIo	<p>Het Subject.CommonName (indien opgenomen) MOET een FQDN (Fully Qualified Domain Name) bevatten. Een FQDN MOET ook terugkomen in het SubjectAltName.DNsName veld. Een IP-adres MOET ook terugkomen in SubjectAltName.iPAdress veld.</p> <p>Een server certificaat MAG meerdere FQDN's bevatten van verschillende domeinen op voorwaarde dat deze domeinen geregistreerd zijn op naam van dezelfde abonnee of een machtiging van dezelfde abonnee afkomstig is.</p> <p>Dat betekent dat een TSP NIET FQDN's in één certificaat MAG combineren die én afkomstig zijn uit verschillende domeinen én geregistreerd staan op naam van verschillende eigenaren.</p> <p>Onderstaande is NIET toegestaan om op te nemen in het Subject.Commonname veld, SubjectAltName.iPAdress of het SubjectAltName.DNname veld</p> <ul style="list-style-type: none"> - wildcard FQDN's - lokale domeinnamen, - private IP adressen - internationalized domain names (IDN's) - null characters \0 - generiek TopLevelDomein (gTLD) - Land code TopLevelDomein (ccTLD)

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio164
PKIo	<p>Het Subject.CommonName MOET een FQDN (Fully Qualified Domain Name) bevatten. Een FQDN MOET ook terugkomen in het SubjectAltName.DNsName veld.</p> <p>Een Extended Validation certificaat MAG meerdere FQDN's bevatten. Elke FQDN MOET vallen onder hetzelfde hoofddomein. (b.v. www.logius.nl, applicatie.logius.nl, secure.logius.nl etc.).</p> <p>Onderstaande is NIET toegestaan om op te nemen in het Subject.Commonname veld of het SubjectAltName.DNname veld</p> <ul style="list-style-type: none"> - wildcard FQDN's - lokale domeinnamen, - private IP adressen - internationalized domain names (IDN's) - null characters \0 - generiek TopLevelDomein (gTLD) - Land code TopLevelDomein (ccTLD)

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio165
PKIo	<p>Het Subject.CommonName dient bij voorkeur een FQDN (Fully Qualified Domain Name) of een IP-adres te bevatten. Een FQDN moet in dat geval ook terugkomen in het SubjectAltName.DNsName veld. Een IP-adres moet ook terugkomen in SubjectAltName.iPAdress veld.</p> <p>Een server certificaat mag meerdere FQDN's bevatten van verschillende domeinen op voorwaarde dat deze domeinen geregistreerd zijn op naam van dezelfde abonnee of een machtiging van dezelfde abonnee afkomstig is.</p> <p>Dat betekent dat een TSP NIET FQDN's in één certificaat MAG combineren die én afkomstig zijn uit verschillende domeinen én geregistreerd staan op naam van verschillende eigenaren.</p> <p>Indien het niet mogelijk of wenselijk is om een FQDN in het subject.commonName veld op te nemen, maar het veld wel nodig is voor een goede werking van de server, kan ook de functie van een organisatorische entiteit of de naam waarmee de service,apparaat of systeem wordt aangeduid worden opgenomen.</p> <p>Onderstaande is niet toegestaan om op te nemen in het Subject.Commonname veld, SubjectAltName.iPadres of het SubjectAltName.DNname veld</p> <ul style="list-style-type: none"> - wildcard FQDN's - lokale domeinnamen, - private IP adressen - internationalized domain names (IDN's) - null characters \0

	<ul style="list-style-type: none"> - generiek TopLevelDomein (gTLD) - Land code TopLevelDomein (ccTLD)
--	--

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio171
PKIo	<p>In aanvulling op ETSI TS 119 312 MOET de TSP kiezen uit 1 van de volgende opties voor het Signature veld in een certificaat:</p> <ul style="list-style-type: none"> • sha256WithRSAEncryption: 1.2.840.113549.1.1.11 { OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }} • ecdsa-with-SHA256: 1.2.840.10045.4.3.2 { OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }} • sha384WithRSAEncryption : 1.2.840.113549.1.1.12 { OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 }} • ecdsa-with-SHA384:1.2.840.10045.4.3.3 { OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }}

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio172
PKIo	<p>Het veld Authority Information Access dient de volgende subvelden te bevatten:</p> <p>Access Method= - Id-ad-ocsp (On-line Certificate Status Protocol - 1.3.6.1.5.5.7.48.1). Dit veld dient de URI te bevatten waarop de OCSP responder te vinden is die geautoriseerd is door de uitgevende CA van het te controleren certificaat;</p> <p>Access Method= Certification Authority Issuer (1.3.6.1.5.5.7.48.2). Dit veld dient de URI te bevatten waarop het certificaat van de uitgevende CA te vinden is.</p>

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio173
PKIo	<p>Het serienummer van alle eindgebruikerscertificaten dient aan de volgende eisen te voldoen:</p> <p>a) De waarde van het serienummer MAG NIET 0 (nul) zijn b) De waarde van het serienummer MAG NIET negatief zijn c) De waarde van het serienummer MOET uniek zijn binnen de populatie uitgegeven eindgebruikerscertificaten onder een uitgevende TSP CA. d) Het serienummer MOET een minimale lengte hebben van 96 bits (12 octetten) e) De waarde van het serienummer MOET minimaal 64 bits aan niet te voorspellen willekeurige data te bevatten f) Genoemde willekeurige data MOET worden gegenereerd door een CSPRNG (Cryptographically Secure Pseudorandom Number Generator). g) Het serienummer MAG NIET langer zijn dan 160 bit (20 octets).</p>

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio177
PKIo	<p>Het serienummer van alle eindgebruikerscertificaten dient aan de volgende eisen te voldoen:</p> <p>a) De waarde van het serienummer MAG NIET 0 (nul) zijn b) De waarde van het serienummer MAG NIET negatief zijn c) De waarde van het serienummer MOET uniek zijn binnen de populatie uitgegeven eindgebruikerscertificaten onder een uitgevende TSP CA. d) Het serienummer MOET een minimale lengte hebben van 96 bits (12 octetten) e) De waarde van het serienummer MOET minimaal 64 bits aan niet te voorspellen willekeurige data te bevatten f) Genoemde willekeurige data ZOU MOETEN worden gegenereerd door een CSPRNG (Cryptographically Secure Pseudorandom Number Generator). g) Het serienummer MAG NIET langer zijn dan 160 bit (20 octets).</p>

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio182
PKIo	<p>Het veld CertificatePolicies veld MOET volgende velden bevatten:</p> <ul style="list-style-type: none"> • OID van PvE (CP) deel 3e: 2.16.528.1.1003.1.2.5.6 • OV OID van het CA/Browser Forum: 2.23.140.1.2.2 • de URI van het certification practice statement (CPS) • een gebruikersnotitie. <p>Het te gebruiken OID schema in de PKI voor de overheid wordt beschreven in de CP. Voor de gebruikersnotitie ZAL de TSP gebruik maken van UTF8String maar MAG er ook gebruik gemaakt worden van IA5String.</p>
Opmerking	<p>Verwijzen naar paragraafnummers van het PvE / CP in de gebruikersnotitie wordt afgeraden omdat persistentie hiervan niet kan worden gegarandeerd (in tegenstelling tot het OID nummer van de CP).</p>

7.2 CRL-profielen

Bevat geen aanvullende eisen.

7.3 OCSP-profielen

RFC 3647	7.3 OCSP-profielen
Nummer	7.3-pkio123
PKIo	Indien de TSP het Online Certificate Status Protocol (OCSP) ondersteunt, dient de TSP OCSP certificaten en responses te hanteren conform de eisen, die daaraan zijn gesteld in bijlage A van de Basiseisen, te weten " Profielen CRL- en OCSP certificaten".

8 Conformiteitbeoordeling

RFC 3647	8.1 Aantonen conformiteit ETSI/BR
Nummer	8.1-pkio183
	Een TSP MOET, wanneer dit wordt verzocht door de PA, een zelfbeoordeling tegen de Baseline Requirements uitvoeren op basis van een door de PA vooraf vastgesteld sjabloon..
Opmerking	Mozilla vereist dat CA's een vergelijking van hun processen (via CP- en CPS-documenten) met de BR's maken met behulp van een door Mozilla vastgelegd sjabloon om ervoor te zorgen dat hun processen (en praktijken) blijven voldoen aan de Baseline Requirements van het CA / Browser Forum.

RFC 3647	8.6 Aantonen conformiteit BR
Nummer	8.6-pkio158
	<p>De PA informeert TSP's over relevante wijzigingen in de Baseline Requirements en/of de Extended Validation Guidelines. TSP's dienen te bewijzen dat zij voldoen aan gestelde wijzigingen door middel van een getekende verklaring van of namens de bevoegde bestuurder, in te leveren bij de PA voor de ingangsdatum van de wijziging in kwestie. De PA stelt een sjabloon hiervoor ter beschikking.</p> <p>Indien een TSP niet tijdig kan voldoen of niet tijdig een getekende verklaring inlevert behoudt de PA zich het recht voor om de certificaatuitgifte bij desbetreffende TSP (tijdelijk) stil te leggen totdat de TSP wel (aantoonbaar) kan voldoen aan gestelde wijziging.</p>

9 Algemene en juridische bepalingen

9.2 Financiële verantwoordelijkheid en aansprakelijkheid

RFC 3647	9.2. Financiële verantwoordelijkheid en aansprakelijkheid
Nummer	9.2-pkio124
PKIo	De TSP 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 TSP, hetgeen past bij de huidige situatie. Wanneer TSP's meer certificaten gaan uitgeven zal worden bepaald of een passende, hogere, verhaalbaarheid zal worden gevorderd.

9.5 Intellectuele eigendomsrechten

Bevat geen aanvullende eisen.

9.6 Aansprakelijkheid

RFC 3647	9.6.1 Aansprakelijkheid van TSP's
Nummer	9.6.1-pkio127
PKIo	<p>In de overeenkomst tussen de TSP en de abonnee wordt voor een authenticiteits certificaat een beding (een bepaling als bedoeld in artikel 6:253 BW) opgenomen waarin de TSP zich sterk maakt voor een op het certificaat vertrouwende derde. Dit beding strekt tot een aansprakelijkheid van de TSP 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 authenticiteitcertificaat"; b. voor "ondertekenaar" gelezen wordt: "certificaathouder"; c. voor "elektronische handtekeningen" gelezen wordt: "authenticiteitskenmerken".

RFC 3647	9.6.1 Aansprakelijkheid van TSP's
Nummer	9.6.1-pkio128
PKIo	<p>In de overeenkomst tussen de TSP en de abonnee wordt een beding (een bepaling als bedoeld in artikel 6:253 BW) opgenomen waarin de TSP zich sterk maakt voor een op het certificaat vertrouwende derde. Dit beding strekt tot een aansprakelijkheid van de TSP overeenkomstig artikel 6:196b, eerste tot en met derde lid, van het Burgerlijk Wetboek, met dien verstande dat:</p> <p>a. voor "een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss Telecommunicatiewet" gelezen wordt: "een servercertificaat" voor deel 3e, een "combinatiecertificaat uit het PKIoverheid-domein Autonome Apparaten" voor deel 3d of een "EV SSL certificaat" voor deel 3f;</p> <p>b. voor "ondertekenaar" gelezen wordt: "certificaathouder";</p> <p>c. voor "aanmaken van elektronische handtekeningen" gelezen wordt: "verifiëren van authenticiteitskenmerken en aanmaken van gecijferde data";</p> <p>d. Voor "verifiëren van elektronische handtekeningen" gelezen wordt: "ontcijferen van authenticiteitskenmerken en gecijferde data".</p>

RFC 3647	9.6.1 Aansprakelijkheid van TSP's
Nummer	9.6.1-pkio129
PKIo	<p>In de overeenkomst tussen de TSP en de abonnee wordt voor een versleutelingscertificaat een beding (een bepaling als bedoeld in artikel 6:253 BW) opgenomen waarin de TSP zich sterk maakt voor een op het certificaat vertrouwende derde. Dit beding strekt tot een aansprakelijkheid van de TSP overeenkomstig artikel 6:196b, eerste tot en met derde lid, van het Burgerlijk Wetboek, met dien verstande dat:</p> <p>a. voor "een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss Telecommunicatiewet" gelezen wordt: "een vertrouwelijkheidcertificaat";</p> <p>b. voor "ondertekenaar" gelezen wordt: "certificaathouder";</p> <p>c. voor "aanmaken van elektronische handtekeningen" gelezen wordt: "aanmaken van gecijferde data";</p> <p>d. voor "verifiëren van elektronische handtekeningen" gelezen wordt: "ontcijferen van gecijferde data".</p>

RFC 3647	9.6.1 Aansprakelijkheid van TSP's
Nummer	9.6.1-pkio142
PKIo	<p>In de overeenkomst tussen de TSP en de abonnee wordt een beding (een bepaling als bedoeld in artikel 6:253 BW) opgenomen waarin de TSP zich sterk maakt voor een op het certificaat vertrouwende derde. Dit beding strekt tot een aansprakelijkheid van de TSP overeenkomstig artikel 6:196b, eerste tot en met derde lid, van het Burgerlijk Wetboek, met dien verstande dat:</p> <p>a. voor "een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss Telecommunicatiewet" gelezen wordt: "een vertrouwelijkheidcertificaat uit het PKIoverheid-domein Autonome Apparaten";</p> <p>b. voor "ondertekenaar" gelezen wordt: "certificaathouder";</p> <p>c. voor "aanmaken van elektronische handtekeningen" gelezen wordt: "aanmaken van gecijferde data";</p>

	d. voor "verifiëren van elektronische handtekeningen" gelezen wordt: "ontcijferen van gecijferde data".

RFC 3647	9.6.1 Aansprakelijkheid van TSP's
Nummer	9.6.1-pkio131
PKIo	De TSP kan in een onweerlegbaarheidscertificaat beperkingen ten aanzien van het gebruik daarvan laten opnemen, mits die beperkingen voor derden duidelijk zijn. De TSP 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.
Opmerking	Dit artikel is gebaseerd op BW art. 196b, lid3

RFC 3647	9.6.1 Aansprakelijkheid van TSP's
Nummer	9.6.1-pkio132
PKIo	De TSP sluit alle aansprakelijkheid uit voor schade indien het certificaat niet conform het in paragraaf 1.4 beschreven certificaatgebruik van het op dat type certificaat van toepassing zijnde PvE deel wordt gebruikt.

9.8 Beperkingen van aansprakelijkheid

RFC 3647	9.8 Beperkingen van aansprakelijkheid
Nummer	9.8-pkio133
PKIo	Het is de TSP 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	9.8-pkio134
PKIo	Het is de TSP niet toegestaan om binnen het toepassingsgebied van certificaten, zoals benoemd in paragraaf 1.4 van het op dat type certificaat van toepassing zijnde PvE deel, beperkingen te stellen aan het gebruik van EV SSL certificaten.

RFC 3647	9.8 Beperkingen van aansprakelijkheid
Nummer	9.8-pkio143
PKIo	Het is de TSP toegestaan om binnen het toepassingsgebied van certificaten, zoals benoemd in paragraaf 1.4 van het op dat type certificaat van toepassing zijnde PvE deel, beperkingen te stellen aan het gebruik van certificaten.

9.12 Wijzigingen

Bevat geen aanvullende eisen.

9.13 Geschillenbeslechting

Bevat geen aanvullende eisen.

9.14 Van toepassing zijnde wetgeving

Bevat geen aanvullende eisen.

9.17 Overige bepalingen

RFC 3647	9.17 Overige bepalingen
Nummer	9.17-pkio180
PKIo	CA's moeten hun abonnees minstens één (1) keer per halfjaar actief informeren dat, conform de gebruiksvoorwaarden, certificaten worden ingetrokken onder de voorwaarden van - en binnen de in 4.9.1.1 genoemde termijnen van de BRG.

10 Revisies

10.1 Wijzigingen

Wijzigingenbeheer wordt in principe niet toegepast op dit document, deze worden bijgehouden in het van toepassing zijnde CP deel.

10.2 Wijzigingen van versie 4.7 naar versie 4.8

Geen redactionele wijzigingen

10.3 Wijzigingen van versie 4.5 naar versie 4.7

10.3.1 *Redactioneel*

- De referentie naar de ETSI eisen die over hetzelfde onderwerp gaan als de PKIoverheid eis is verplaatst naar een additioneel tabblad in het OoA template.

10.4 Wijzigingen van versie 4.0 naar versie 4.5

10.4.1 *Redactioneel*

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

10.5 Wijzigingen van versie 3.7 naar 4.0

10.5.1 *Nieuw*

Niet van toepassing

10.5.2 *Aanpassingen*

- PvE eisen zijn omgenummerd volgens een nieuwe naming convention;
- De creatie van een baseline en een aanvullende eisen document.

10.5.3 *Redactioneel*

Niet van toepassing