Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programma van Eisen deel 3: Basiseisen 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

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 Trust 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	Vastgestel door BZK juli 2015
4.2	01-2016	Vastgesteld door BZK januari 2016
4.3	07-2016	Vastgesteld door BZK juni 2016
4.4	02-2017	Vastgesteld door BZK februari 2017
4.5	07-2017	Vastgesteld door BZK juni 2017
4.6	01-2018	Vastgesteld door BZK januari 2018
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 Basiseisen van het Programma van Eisen (PvE) van de PKI voor de overheid en wordt aangeduid als Basiseisen PKIoverheid. In het PvE zijn de normen voor de PKI voor de overheid vastgelegd. Dit onderdeel van deel 3 heeft betrekking op de basiseisen die aan de dienstverlening van een Trust Service Provider (TSP) binnen de PKI voor de overheid worden gesteld. Binnen de PKI voor de overheid is onderscheid gemaakt in verschillende domeinen. Deze basiseisen hebben betrekking op alle typen certificaten die onder deze domeinen worden uitgegeven.

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 opgenomen 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.

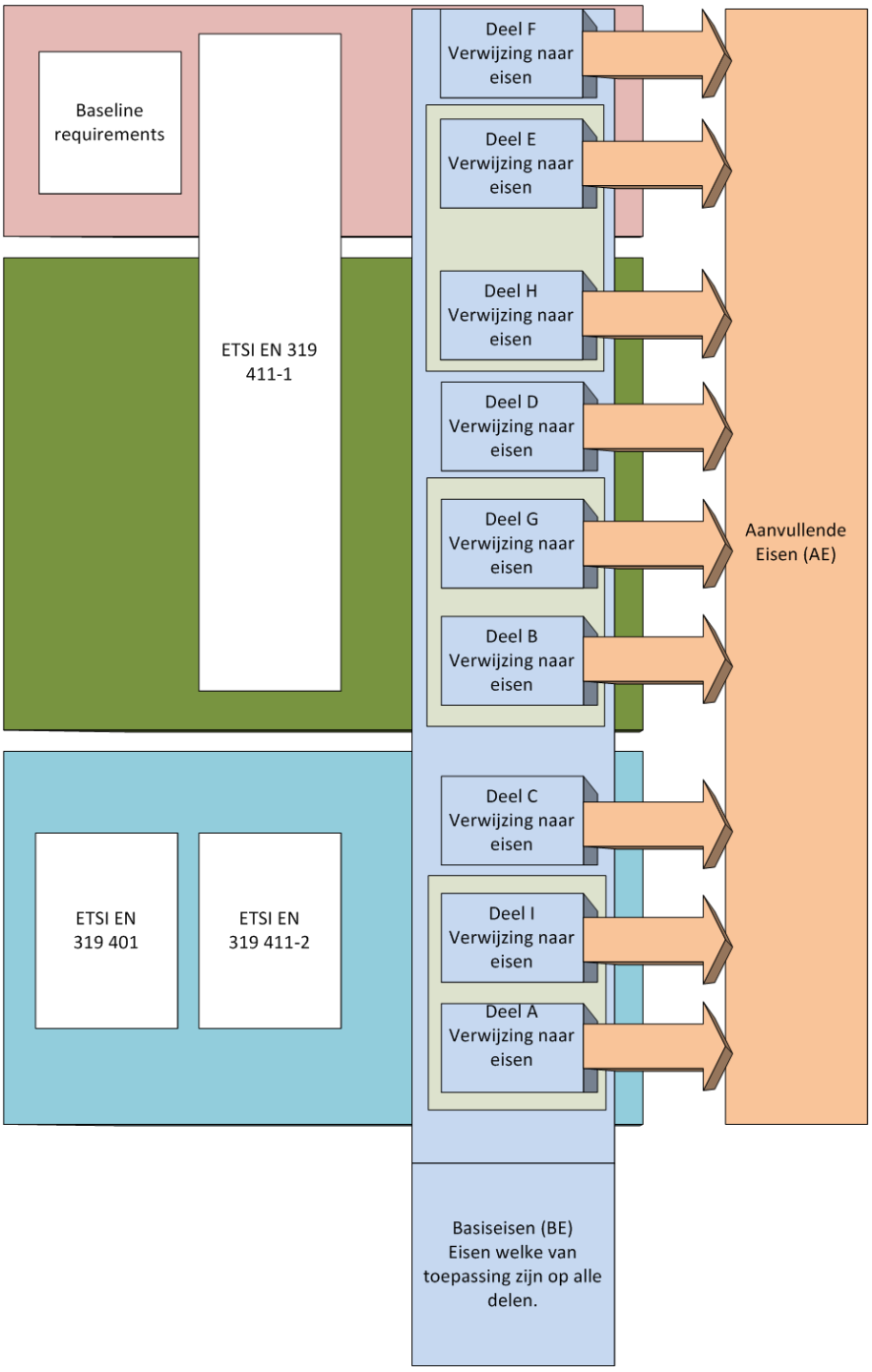
Om te voldoen aan een specifiek CP moet worden voldaan aan het ETSI normenkader dat hierop van toepassing is, de Basiseisen van PKIoverheid en een deel van de Aanvullende eisen van PKIoverheid.

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.*


Baseline requirements
ETSI EN 319 411-1
ETSI EN 319 401
ETSI EN 319 411-2
Deel F Verwijzing naar eisen
Deel E Verwijzing naar eisen
Deel H Verwijzing naar eisen
Deel D Verwijzing naar eisen
Deel G Verwijzing naar eisen
Deel B Verwijzing naar eisen
Deel C Verwijzing naar eisen
Deel I Verwijzing naar eisen
Deel A Verwijzing naar eisen
Aanvullende Eisen (AE)
Basiseisen (BE) Eisen welke van toepassing zijn op alle delen.

1.1.2 Status

Dit is versie 4.8 van deel 3 Basiseisen 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 Basiseisen 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 Basiseisen, indien deze Basiseisen 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 Basiseisen voor uitgifte van PKIoverheid certificaten. Vragen met betrekking tot deel 3 Basiseisen 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	2.1-pkio1
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	2.1-pkio2
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 TSP of door een afzonderlijke organisatie.
Opmerking	De informatie die moet worden gepubliceerd staat beschreven in de relevante ETSI normen. De van toepassing zijnde ETSI norm zijn te vinden in de PvE delen. De relevante artikelen waar de informatie is gespecificeerd zijn te vinden in de verwijzingsmatrix in bijlage B.

2.2 Publicatie van TSP-informatie

RFC 3647	2.2 Publicatie van TSP-informatie
Nummer	2.2-pkio5
PKIo	De TSP dient de OID's van de toegepaste CP's op te nemen in het CPS.

RFC 3647	2.2 Publicatie van TSP-informatie
Nummer	2.2-pkio6
PKIo	Alle informatie zal in het Nederlands beschikbaar moeten zijn.

3 Identificatie en authenticatie

3.1 Naamgeving

RFC 3647	3.1.1 Soorten naamformaten
Nummer	3.1.1-pkio10
PKIo	De TSP dient te voldoen aan de eisen die aan naamformaten zijn gesteld in Certificaat-, CRL- en OCSP-profielen.
Opmerking	In bijlage A van de basiseisen zijn de CRL- en OCSP-profielen opgenomen. Het certificaatprofiel is opgenomen in bijlage A van het op dat type certificaat van toepassing zijnde PvE deel.

3.2 Initiële identiteitsvalidatie

Bevat geen basiseisen.

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	3.3.1-pkio36
PKIo	ETSI EN 319 411-1 GEN-6.3.6-10 is alleen toegestaan op vertrouwelijkheidcertificaten. Voor alle overige typen PKIo certificaattypen MOETEN sleutel paren vernieuwd worden bij uitgifte van een nieuw certificaat.
Opmerking	In ETSI EN 319 411-1 GEN-6.3.6-10 wordt aangegeven onder welke voorwaarden hercertificering van sleutels van vertrouwelijkheidcertificaten is toegestaan. De eis houdt in dat certificaatvernieuwing zonder vernieuwing van de sleutels niet is toegestaan voor het authenticiteit- en handtekeningcertificaat en server certificaten.

RFC 3647	3.3.1 Identificatie en authenticatie bij routinematige vernieuwing van het certificaat
Nummer	3.3.1-pkio45
PKIo	Bij het vernieuwen van certificaten moet altijd worden voldaan aan de eisen die zijn gesteld onder [3.1] en [3.2] van het op dat type certificaat van toepassing zijnde PvE deel en 3.1.1-pkio10 uit dit CP.
Opmerking	De relevante artikelen waarin de eisen zijn gespecificeerd zijn te vinden in deel 3 Verwijzingsmatrix PKIoverheid en ETSI. Ter vervanging van fysieke aanwezigheid van de certificaathouder, kan bij vervanging van een persoonsgebonden certificaat aan het einde van de looptijd bij de registratie en identificatie ook gebruik worden gemaakt van een gekwalificeerde handtekening van een onweerlegbaarheidscertificaat. Hieraan zijn een aantal voorwaarden verbonden: • Het onweerlegbaarheidscertificaat dient geldig te zijn op het moment van vernieuwing; • Het dossier moet actueel en compleet zijn inclusief een kopie van een geldig WID; • Subject details van de aanvrager voor een nieuw persoonsgebonden certificaat komen nog steeds overeen met het geldige onweerlegbaarheidscertificaat zoals het organisatie veld; • Eenmalige vernieuwing van het certificaat zonder fysieke verschijning is alleen mogelijk door de TSP die dit onweerlegbaarheidscertificaat op basis van een fysieke identificatie heeft uitgegeven. Niet alleen het onweerlegbaarheidscertificaat zelf maar ook de overige persoonsgebonden certificaten onder PvE delen 3a, 3c en 3i kunnen op deze wijze eenmalig worden vernieuwd.

RFC 3647	3.3.2 Identificatie en authenticatie bij vernieuwing van het certificaat na intrekking
Nummer	3.3.2-pkio46
PKIo	Na intrekking van het certificaat mogen de desbetreffende sleutels niet opnieuw worden gecertificeerd. ETSI EN 319 411-1 GEN-6.3.6-10 is niet van toepassing.

4 Operationele eisen certificaatlevenscyclus

4.1 Aanvraag van certificaten

Bevat geen basiseisen.

4.2 Verwerking van certificaat aanvraag

Bevat geen basiseisen.

4.3 Uitgifte van certificaten

Bevat geen basiseisen.

4.4 Acceptatie van certificaten

RFC 3647	4.4.1 Activiteiten bij acceptatie van certificaten
Nummer	4.4.1-pkio49
PKIo	Na uitgifte van een certificaat, dient de certificaathouder voor persoonsgebonden certificaten of de certificaatbeheerder voor overige certificaten expliciet de overhandiging van het sleutelmateriaal behorend bij het certificaat aan de TSP te bevestigen.
Opmerking	Indien gebruik wordt gemaakt van softwarematig beschermde sleutels (zie [6.2.11-pkio106 en 6.2.11-pkio107]) waarbij de private sleutel door de certificaatbeheerder wordt gegenereerd en niet door de TSP, is overdracht van het sleutelmateriaal en ontvangstbevestiging niet van toepassing. Wel dienen nog steeds de gegevens te worden vastgelegd die worden vereist in 7.3.1.i en 7.3.1.m. Dit is van toepassing op de CP delen E, F en H.

4.5 Sleutelpaar en certificaatgebruik

RFC 3647	4.5.2 Gebruik van publieke sleutel en certificaat door vertrouwende partij
Nummer	4.5.2-pkio51
PKIo	In de gebruikersvoorwaarden die aan de vertrouwende partijen ter beschikking worden gesteld dient te worden opgenomen dat de vertrouwende partij wordt geacht de geldigheid te controleren van de volledige keten van certificaten tot aan de bron (stamcertificaat) waarop wordt vertrouwd. Daarnaast dient te worden opgenomen dat de abonnee zelf zorg draagt voor een tijdige vervanging in het geval van een naderende afloop geldigheid, en noodvervanging in geval van compromittatie en/of andere soorten van calamiteiten met betrekking tot het certificaat of van bovenliggende certificaten. Van de abonnee wordt verwacht dat hij zelf adequate maatregelen neemt om de continuïteit van het gebruik van certificaten te borgen.
Opmerking	De geldigheid van een certificaat zegt niets over de bevoegdheid van de certificaathouder een bepaalde transactie namens een organisatie c.q. uit hoofde van zijn of haar beroep te doen. De PKI voor de overheid regelt geen autorisatie; daarvan moet een vertrouwende partij zichzelf op andere wijze overtuigen. Het is raadzaam de abonnee te informeren rekening te houden met de "ICT beveiligingsrichtlijnen voor de transport layer security (TLS)" van het NCSC bij het gebruik van PKIoverheid server certificaten. Het advies is online beschikbaar via de website van het NCSC.

4.8 Compliance, audit en assessement

Bevat geen basiseisen.

4.9 Intrekking en opschorting van certificaten

RFC 3647	4.9.2 Wie mag een verzoek tot intrekking doen
Nummer	4.9.2-pkio53
PKIo	De volgende partijen mogen in een verzoek tot intrekking van een eindgebruikercertificaat doen: ▪ de certificaatbeheerder; ▪ de certificaathouder; ▪ de abonnee; ▪ de TSP; ieder andere, naar het oordeel van de TSP, belanghebbende partij/persoon.

RFC 3647	4.9.3 Procedure voor een verzoek tot intrekking
Nummer	4.9.3-pkio54
PKIo	De TSP mag additionele eisen stellen aan een intrekkingsverzoek. Deze additionele eisen moeten in de CPS van de TSP worden opgenomen.

RFC 3647	4.9.3 Procedure voor een verzoek tot intrekking
Nummer	4.9.3-pkio55
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	4.9.3-pkio56
PKIo	De TSP moet de beweegreden voor de intrekking van een certificaat vastleggen, indien de intrekking geïnitieerd is door de TSP.

RFC 3647	4.9.5 Tijdsduur voor verwerking intrekkingsverzoek
Nummer	4.9.5-pkio61
PKIo	De maximale vertraging tussen de ontvangst van een intrekkingsverzoek of intrekkingsrapportage en de wijziging van de revocation status information, die voor alle vertrouwende partijen beschikbaar is, is gesteld op vier uur.
Opmerking	Deze eis is van toepassing op alle typen certificaat statusinformatie (CRL en OCSP)

RFC 3647	4.9.6 Controlevoorwaarden bij raadplegen certificaat statusinformatie
Nummer	4.9.6-pkio63
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	4.9.6-pkio64
PKIo	De in [4.9.6-pkio63] genoemde verplichting dient door de TSP te worden opgenomen in de gebruikersvoorwaarden die ter beschikking worden gesteld aan de vertrouwende partijen.

RFC 3647	4.9.9 Online intrekking/statuscontrole
Nummer	4.9.9-pkio69
PKIo	Ter verbijzondering van het in {16} IETF RFC6960 gestelde is het gebruikt van vooraf berekende OCSP responses (precomputed responses) niet toegestaan.

RFC 3647	4.9.13 Omstandigheden die leiden tot opschorting
Nummer	4.9.13-pkio72
PKIo	Het is niet toegestaan om certificaatopschorting te ondersteunen.

4.10 Certificaat statusservice

RFC 3647	4.10.2 Beschikbaarheid certificaat statusservice
Nummer	4.10.2-pkio73
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	5.2-pkio74
PKIo	De TSP 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 TSP vallen. Op basis van de risicoanalyse moet de TSP 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 TSP de beschikbaarheid, exclusiviteit en integriteit van alle PKIoverheid processen, aanvragen en de gegevens die daarvoor worden gebruikt, waarborgt.

RFC 3647	5.2 Procedurele beveiliging
Nummer	5.2-pkio75
PKIo	Naast een audit uitgevoerd door een geaccrediteerd auditor MAG de TSP 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 TSP en rekening houdend met zijn bedrijfsdoelstellingen, -processen en -infrastructuur hebben geïmplementeerd en geoperationaliseerd. De TSP is vrij in de keuze om zelf een eigen audit uit te (laten) voeren dan wel gebruik te gaan maken van reeds bestaande audit resultaten zoals die van de formele certificeringsaudits, de diverse interne en externe audits, Third party mededelingen (TPM's) en (buitenlandse) compliancy rapportages. Ook is de TSP gerechtigd om inzage te verkrijgen in het onderliggende bewijsmateriaal zoals audit dossiers en overige, al dan niet systeem-, documentatie. Uiteraard beperkt zich het bovenstaande tot de bij de leveranciers gehoste TSP-processen, -systemen en –infrastructuur voor PKIo kerndiensten.

RFC 3647	5.2.4 Rollen die functiescheiding behoeven
Nummer	5.2.4-pkio76
PKIo	De TSP dient functiescheiding te handhaven tussen tenminste de volgende functies: • Security officer De security officer ziet toe op de implementatie en naleving van de vastgestelde beveiligingsrichtlijnen. • Systeem auditor De systeem auditor vervult een toezichthoudende rol en geeft een onafhankelijk oordeel over de wijze waarop de bedrijfsprocessen zijn ingericht en over de wijze waarop aan de eisen ten aanzien van de betrouwbaarheid is voldaan. • Systeembeheerder De systeembeheerder beheert de TSP-systemen, waarbij het installeren, configureren en onderhouden van de systemen is inbegrepen. • TSP-operators De TSP-operators zijn verantwoordelijk voor het dagelijks bedienen van de TSP-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 TSP 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	5.2.4-pkio77
PKIo	De TSP 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	5.3-pkio78
PKIo	Omdat het openbaar worden van vertrouwelijke informatie grote gevolgen kan hebben (o.a. voor de betrouwbaarheid) moet de TSP 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.

5.4 Procedures ten behoeve van beveiligingsaudits

RFC 3647	5.4.3 Bewaartermijn voor logbestanden
Nummer	5.4.3-pkio81
PKIo	De TSP moet logbestanden voor gebeurtenissen met betrekking tot: • CA key life cycle management en; • Certificate life cycle management; 7 jaar bewaren en daarna verwijderen. De TSP moet logbestanden voor gebeurtenissen met betrekking tot: • Bedreigingen en risico's; 18 maanden bewaren en daarna verwijderen. De logbestanden moeten zodanig worden opgeslagen, dat de integriteit en toegankelijkheid van de data gewaarborgd is.

5.5 Archivering van documenten

Bevat geen basiseisen.

5.7 Aantasting en continuïteit

RFC 3647	5.7.1 Procedures voor afhandeling incidenten en aantasting
Nummer	5.7.1-pkio84
PKIo	De TSP dient de PA, het NCSC, het Agentschap Telecom (AT) en de certificerende instantie (CI) onmiddellijk op de hoogte te stellen van een security breach en/of calamiteit. Indien er (daarnaast) ook sprake is van verlies van privacygevoelige informatie dient ook de Autoriteit Persoonsgegevens (AP) te worden geïnformeerd. Na analyse en vaststelling ~~en~~ dient de PA, NCSC, AT en CI van het verdere verloop op de hoogte te worden gehouden.
Opmerking	Onder security breach wordt in de PKIoverheid context verstaan: Een inbreuk op de TSP kerndiensten: registration service, certificate generation service, subject device provisioning service, dissemination service, revocation management service en revocation status service. Dit is in ieder geval maar niet limitatief: • het ongeoorloofd uitschakelen of onbruikbaar maken van een kerndienst; • ongeautoriseerde toegang tot een kerndienst t.b.v. het afluisteren, onderscheppen en of veranderen van berichtenverkeer; • ongeautoriseerde toegang tot een kerndienst t.b.v. het ongeoorloofd verwijderen, wijzigen of aanpassen van computergegevens.

RFC 3647	5.7.1 Procedures voor afhandeling incidenten en aantasting
Nummer	5.7.1-pkio85
PKIo	De TSP 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 TSP uitgevoerde, PKI diensten, niet zijnde PKIoverheid.

RFC 3647	5.7.1 Procedures voor afhandeling incidenten en aantasting
Nummer	5.7.1-pkio181
PKIo	De PA verplicht de TSP zicht te abonneren op de beveiligingsadviezen van het NCSC om 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 af te dekken.

6 Technische beveiliging

6.1 Genereren en installeren van sleutelparen

RFC 3647	6.1.5 Sleutellengten van private sleutels van certificaathouders
Nummer	6.1.5-pkio96
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 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	6.1.7 Doelen van sleutelgebruik (zoals bedoeld in X.509 v3)
Nummer	6.1.7-pkio97
PKIo	De sleutelgebruiksextensie (key usage) in X.509 v3 certificaten (RFC 5280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile) definieert het doel van het gebruik van de sleutel vervat in het certificaat. De TSP dient het gebruik van sleutels in het certificaat aan te geven, conform de eisen, die daaraan zijn gesteld in bijlage A van dit document, te weten "CRL- en OCSP-profielen" en bijlage A van het op dat type certificaat van toepassing zijnde PvE deel, te weten "Certificaatprofielen".

6.2 Private sleutelbescherming en cryptografische module engineering beheersmaatregelen

RFC 3647	6.2.3 Escrow van private sleutels van certificaathouders
Nummer	6.2.3-pkio98
PKIo	Escrow door de TSP is NIET toegestaan voor de private sleutels van PKIoverheid certificaten met uitzondering van vertrouwelijkheidcertificaten.

RFC 3647	6.2.4 Back-up van private sleutels van certificaathouders
Nummer	6.2.4-pkio102
PKIo	Back-up door de TSP van de private sleutels van de certificaathouders, is niet toegestaan.

RFC 3647	6.2.5 Archivering van private sleutels van certificaathouders
Nummer	6.2.5-pkio103
PKIo	Archivering door de TSP van de private sleutels van de certificaathouders, is niet toegestaan.

6.3 Andere aspecten van sleutelpaarmanagement

RFC 3647	6.3.2 Gebruiksduur voor certificaten en publieke en private sleutels
Nummer	6.3.2-pkio110
PKIo	Op het moment van uitgifte van een eindgebruikercertificaat dient de resterende geldigheidsduur van het bovenliggende TSP-certificaat en/of subordinate certificaat langer te zijn dan de beoogde geldigheidsduur van het eindgebruikercertificaat.

6.4 Activeringsgegevens

Bevat geen basiseisen.

6.5 Logische toegangsbeveiliging van TSP-computers

RFC 3647	6.5.1 Specifieke technische vereisten aan computerbeveiliging
Nummer	6.5.1-pkio114
PKIo	De TSP 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 alle gebruikersaccounts waarmee uitgifte of goedkeuring van certificaten kan worden verricht. Dit is tevens verplicht voor systemen of de gebruikersaccounts waarmee gegevensvalidatie plaatsvindt. De TSP mag voor systemen of gebruikersaccounts waarmee gegevensvalidatie plaatsvindt hier vanaf zien, mits zij technische maatregelen heeft geïmplementeerd, waardoor een gebruikersaccount slechts certificaataanvragen kan valideren op basis van een vooraf geaccordeerde lijst van domeinen of e-mailadressen.
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	6.5.1-pkio115
PKIo	Medewerkers van externe Registration Authorities (RA) of Resellers mogen geen toegang hebben tot het systeem of de gebruiker accounts van de TSP waarmee uitgifte of goedkeuring van certificaten kan worden verricht. Dit is alleen voorbehouden aan geautoriseerde medewerkers van de TSP. Als een RA of een Reseller wel deze toegang heeft dan wordt de RA of de Reseller als een onderdeel van de TSP 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	6.5.1-pkio116
PKIo	Voor zowel de de productie omgeving als voor de uitwijk omgeving ZAL de TSP ongeautoriseerde toegang voorkomen tot de volgende kerndiensten: - registration service, - certificate generation service, - subject device provision service, - dissemination service, - revocation management service - revocation status service. Hiertoe worden deze kerndiensten: - fysiek of logisch gescheiden van niet-PKI-netwerkdomeinen, - fysiek of logisch gescheiden van PKI-netwerkdomeinen die niet voldoen aan de Network Security Guidelines van het Cabforum - fysiek of logisch gescheiden van PKI-netwerkdomeinen die niet voldoen aan de netwerk gerelateerde PKIoverheid eisen uit RFC3647 paragraaf 6, "Technische beveiliging". De TSP dwingt een unieke authenticatie voor elke genoemde kerndienst af. Indien de hierboven genoemde fysieke of logische scheiding van netwerkendomeinen niet volledig haalbaar zou zijn, moeten de verschillende kerndiensten op separate netwerkdomeinen uitgevoerd worden waarbij er sprake moet zijn van een unieke authenticatie per genoemde kerndienst. De TSP documenteert de inrichting van de netwerkdomeinen ten minste op grafische wijze. Deze eis is niet van toepassing op de test- of acceptatieomgeving.

6.6 Beheersmaatregelen technische levenscyclus

RFC 3647	6.6.1 Beheersmaatregelen ten behoeve van systeemontwikkeling
Nummer	6.6.1-pkio117
PKIo	Bij ETSI-eisen EN 319 401 7.7, EN 319 411-2 6.5.5 & EN 319 411-1 6.5.5 heeft de PKIoverheid alleen een opmerking geformuleerd en is geen specifieke PKIo-eis van toepassing.
Opmerking	Conformiteit aan 6.4.7 en 7.4.7. en BEH art. 2 lid 1c kan worden aangetoond door: • een auditverklaring van de leverancier van de producten, die een onafhankelijke EDP audit heeft laten uitvoeren voor QSCD's op basis van EN 419 211 of voor SSCD's op basis van CWA 14167-1 (overgangsrecht); • een auditverklaring van een interne auditor van de TSP op basis van QSCD's op basis van EN 419 211 of voor SSCD's op basis van CWA 14167-1 (overgangsrecht); • een auditverklaring van een externe auditor voor QSCD's op basis van EN 419 211 of voor SSCD's op basis van CWA 14167-1 (overgangsrecht);

6.7 Netwerkbeveiliging

RFC 3647	6.7.1 Netwerkbeveiliging
Nummer	6.7.1-pkio118
PKIo	De TSP moet voor wat betreft patchmanagement 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 voldoen aan de volgende eisen: • Indien een update/patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch). • Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd. Minder kritische beveiligingsupdates/-patches moeten worden ingepland bij de eerstvolgende onderhoudsronde. • Uitzonderingen op deze termijnen zijn alleen toegestaan wanneer in een risicoanalyse is vastgelegd dat de security update of patch zou kunnen leiden tot additionele kwetsbaarheden of een verhoogde kans op instabiliteit, welke zwaarder wegen dan de voordelen van het toepassen van de security update of patch. De TSP dient de besluitvorming rond dit proces vast te leggen zodat deze traceerbaar en auditeerbaar is.
Opmerking	

RFC 3647	6.7.1 Netwerkbeveiliging
Nummer	6.7.1-pkio119
PKIo	De TSP voert minimaal maandelijks, met behulp van een audit tool, een security scan uit op haar PKIoverheid infrastructuur. De TSP 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	6.7.1-pkio120
PKIo	De TSP laat minimaal een keer per jaar een pentest uitvoeren op de PKIoverheid internet facing omgeving door een onafhankelijke, ervaren en deskundige externe leverancier. Daarnaast is een TSP verplicht een pentest te laten uitvoeren wanneer substantiële wijzigingen op de internet facing omgeving hebben plaatsgevonden, - Beoordeling of sprake is van substantiële wijzigingen, geschiedt op basis van een gedocumenteerde risicoanalyse. - De pentest moet worden uitgevoerd door een onafhankelijke, ervaren en deskundige pentester. - De pentest moet uiterlijk een maand na de release uitgevoerd zijn maar bij voorkeur voor in productiename. De TSP moet de bevindingen van de bovengenoemde pentesten, en de maatregelen die hierop worden genomen, (laten) documenteren. Indien noodzakelijk kan de PA een opdracht geven aan de TSP tot het laten uitvoeren van extra pentesten.
Opmerking	TOELICHTING Onder substantiële wijzigingen kan worden verstaan: • Nieuwe software; • Nieuwe versie van bestaande software, niet zijnde patches; • Verandering van infrastructuur. Voor de selectie van een pentester kan de TSP de aanbevelingen in hoofdstuk 4 (“Leverancierselectie”) zoals beschreven in de laatste versie van de whitepaper “Pentesten doe je zo2” van het NCSC, als guidance gebruiken.

[2] *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*

RFC 3647	6.7.1 Netwerkbeveiliging
Nummer	6.7.1-pkio185
PKIo	Voor webapplicatie(s) die betrekking hebben op: • de registration service, • certificate generation service, • subject device provision service, • dissemination service, • revocation management service en • revocation status service dient de TSP de volgende zaken te borgen: • Dat de webapplicatie alle invoer van gebruikers controleert en filtert en; • Dat de webapplicatie de dynamische uitvoer codeert en; • Dat de webapplicatie een veilige sessie met de gebruiker onderhoudt en; • Dat de webapplicatie op een veilige manier gebruik maakt van een database.
Opmerking	De TSP kan hiervoor de "ICT-Beveiligingsrichtlijnen voor Webapplicaties" van het NCSC als guidance gebruiken.

7 Certificaat-, CRL- en OCSP-profielen

7.1 Certificaatprofielen

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio121
PKIo	De TSP dient certificaten uit te geven conform de eisen, die daaraan zijn gesteld in bijlage A van het op dat type certificaat van toepassing zijnde PvE deel, te weten "Certificaatprofielen". Alleen die certificaatelementen die zijn opgenomen in het certificaatprofiel mogen worden gebruikt. Alle niet genoemde elementen zijn niet toegestaan.

RFC 3647	7.1 Certificaatprofielen
Nummer	7.1-pkio174
PKIo	Alle elementen binnen het Issuer veld moeten overeenkomen met het corresponderende Subject veld van de uitgevende CA.

7.2 CRL-profielen

RFC 3647	7.2 CRL-profielen
Nummer	7.2-pkio122
PKIo	De TSP dient CRL's uit te geven conform de eisen, die daaraan zijn gesteld in bijlage A van dit document, te weten "CRL- en OCSP-profielen".

7.3 OCSP-profielen

Bevat geen basiseisen.

8 Conformiteitbeoordeling

RFC 3647	8.1 Aantonen conformiteit ETSI/BR
Nummer	8.1-pkio159
PKIo	Een TSP is verplicht om voor elke (jaarlijkse) ETSI audit: - de vigerende versie van de door de PA PKIoverheid ontwikkelde en beschikbaar gestelde Overzicht van Eisen te gebruiken OF; - een door de TSP zelf ontwikkelde overzicht van eisen te gebruiken. Dit overzicht van eisen dient voorafgaand aan de (jaarlijkse) ETSI audit, op het aspect volledigheid, gereviewed en goedgekeurd te worden door de PA. Hiertoe dient de TSP het OvE (inclusief bijbehorende Verklaring van Toepasselijkheid) aan de PA te leveren voorafgaand aan een audit. Als aan een van deze voorwaarden niet wordt voldaan, behoudt de PA zich het recht voor om de audit rapportage niet te accepteren.
Opmerking	- Als onderdeel van deze verklaring dient in de legenda opgenomen te worden welke versies van de van toepassing zijnde normen zijn gebruikt. - De TSP dient rekening te houden met een verwerkingstijd voor het reviewen van de verklaring van toepasselijkheid van maximaal 15 werkdagen. - Een afschrift van de gereviewde verklaring van toepasselijkheid zal naar de ETSI auditor verstuurd worden. - Het overzicht van toepasselijkheid staat ook bekend als OoA, Overview of Applicability

9 Algemene en juridische bepalingen

9.2 Financiële verantwoordelijkheid en aansprakelijkheid

Bevat geen basiseisen.

9.5 Intellectuele eigendomsrechten

RFC 3647	9.5 Intellectuele eigendomsrechten
Nummer	9.5-pkio126
PKIo	De TSP vrijwaart de abonnee ten aanzien van aanspraken door derden vanwege schendingen van intellectuele eigendomsrechten door de TSP.

9.8 Beperkingen van aansprakelijkheid

RFC 3647	9.8 Beperkingen van aansprakelijkheid
Nummer	9.8-pkio135
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 de waarde van de transacties, waarvoor certificaten kunnen worden gebruikt.

9.12 Wijzigingen

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://cps.pkioverheid.nl

RFC 3647	9.12.2 Notificatie van wijzigingen
Nummer	9.12.2-pkio136
PKIo	Indien een gepubliceerde wijziging van het CP consequenties kan hebben voor de eindgebruikers, zullen de TSP'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	9.12.2-pkio137
PKIo	De TSP 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	9.13-pkio138
PKIo	De door de TSP gehanteerde klachtenafhandeling- en geschillenbeslechtingsprocedures mogen het instellen van een procedure bij de gewone rechter niet beletten.

9.14 Van toepassing zijnde wetgeving

Op de CP’s van PKIoverheid (Deel 3a t/m 3i) is het Nederlands recht van toepassing.

9.17 Overige bepalingen

RFC 3647	9.17 Overige bepalingen
Nummer	9.17-pkio184
PKIo	De TSP dient twee maal per jaar de gegevens aan te leveren over het totaal aantal uitgegeven certificaten en uitstaande certificaten in de voorgaande periode. Deze cijfers dienen aangeleverd te worden via het door de PA hiervoor opgestelde en verspreide format.

Bijlage A Profielen CRL en OCSP certificaten t.b.v. de certificaat statusinformatie

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.

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 119 312: "
11. Electronic Signatures and Infrastructures (ESI);
12. Cryptographic Suites", versie 1.1.1 (2014-11).
13. ISO 3166 "English country names and code elements".
14. RFC 6960: “ X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”.

CRL profiel

Algemene eisen

- De CRL's moeten voldoen aan de X.509v2 standaard voor 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.

CRL attributen

Veld / Attribuut	Criteria	Beschrijving	Norm referentie[1]	Type	Toelichting
Version	V	MOET ingesteld worden op 1 (X.509v2 CRL profiel).	RFC 5280	Integer	Beschrijft de versie van het CRL profiel, waarde 1 staat voor X.509 versie 2.
Signature	V	MOET worden ingesteld op het algoritme, zoals deze door de PA is bepaald.	RFC 5280	OID	MOET gelijk zijn aan het veld signatureAlgorithm. 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 TSP certificaat (ten behoeve van validatie).
Issuer.countryName	V	zie eis 7.1-pkio174	ISO3166, X.520	Printable String	
Issuer.stateOrProvinceName	N	Wordt niet gebruikt.	PKIo	UTF8String	-
Issuer.OrganizationName	V	zie eis 7.1-pkio174	ETSI TS 102280: 5.2.4	UTF8String	

Veld / Attribuut	Criteria	Beschrijving	Norm referentie[1]	Type	Toelichting
Issuer.organizationIdentifier	V/N	In het organizationIdentifier veld wordt een identificatie van de uitgevende CA opgenomen. Dit veld is MOET worden opgenomen in CRL's wanneer het veld subject.organizationIdentifier voorkomt in het CSP certificaat waarmee de CRL is ondertekend en MAG NIET worden opgenomen in CRL's wanneer dit veld in het betreffende CSP certificaat niet voorkomt.	EN 319 412-1	UFF8String	De opmaak van de identificatiestring wordt gespecificeerd in paragraaf 5.1.4 van ETSI EN 319 412-1 en bevat: • 3 character legal person identity type reference; • 2 character ISO 3166 [2] country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier (according to country and identity type reference). Toegestane waarden voor dit veld zijn het OIN of een KVK nummer van de CSP. De informatie MOET overeenkomen met de subject.organizationIdentifier zoals opgenomen in het CSP CA certificaat.
Issuer.organizationalUnitName	O	zie eis 7.1-pkio174	ETSI TS 102280: 5.2.4	UTF8String	
Issuer.localityName	N	Wordt niet gebruikt.	PKIo	UTF8String	-
Issuer.serialNumber	O	zie eis 7.1-pkio174	RFC 3739	Printable String	
Issuer.commonName	V	zie eis 7.1-pkio174	PKIo, RFC 5280	UTF8String	Het commonName attribuut MAG NIET nodig zijn om de uitgevende instantie te identificeren (geen onderdeel van de Distinguished Name, eis uit RFC 3739).

Veld / Attribuut	Criteria	Beschrijving	Norm referentie[1]	Type	Toelichting
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	Serial-Numbers, 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 TSP 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 TSP/CA) bevatten.
IssuerAltName	A	Nee	Dit attribuut geeft de mogelijkheid om alternatieve namen voor de TSP (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 TSP 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	RFC 5280		Indien gebruikt MOET dit veld voldoen aan de specificaties in RFC 5280.

Veld / Attribuut	Criteria	Critical	Beschrijving	Norm refe-rentie1	Type	Toelichting
			(zoals een gelimiteerde reden waarom het certificaat is ingetrokken).			
FreshestCRL	O	Nee	Dit attribuut staat ook bekend onder de naam 'Delta CRL Distribution Point'. Indien gebruikt MOET het de URI van een Delta-CRL distributiepunt bevatten. Het komt nooit voor in een Delta-CRL.	RFC 5280		Dit veld wordt gebruikt in volledige CRL's en geeft aan waar Delta-CRL informatie te vinden is die een update vormt op de volledige CRL.
authorityInfoAccess	O	Nee	Optionele verwijzing naar het certificaat van de CRL.Issuer.	RFC 5280	id-ad-caIssuers (URI)	MOET conformeren aan § 5.2.7 van RFC 5280.
CRLReason	O	Nee	Indien gebruikt geeft dit de reden aan waarom een certificaat is ingetrokken.	RFC 5280	reasonCode	Als geen reden wordt opgegeven MOET dit veld worden weggelaten.
holdInstructionCode	N	Nee	Wordt niet gebruikt.	RFC 5280	OID	De PKI voor de overheid maakt geen gebruik van de status 'On hold'.
invalidityDate	O	Nee	Dit attribuut kan gebruikt worden om een datum en tijdstip aan te geven waarop het certificaat gecompromitteerd is geworden indien dit afwijkt van de datum en tijdstip waarop de TSP de revocatie heeft verwerkt.	RFC 5280	Generalized-Time	
certificateIssuer	A	Ja	Als gebruik wordt gemaakt van een indirecte CRL kan dit attribuut worden gebruikt om de oorspronkelijke uitgever van het certificaat te identificeren.	RFC 5280	GeneralNames	

Profiel OCSP

Algemene eisen aan OCSP

- Indien de TSP het Online Certificate Status Protocol (OCSP) ondersteunt, MOETEN OCSP responses en OCSP Signing certificates voldoen aan de eisen die hieraan worden gesteld in IETF RFC 6960.
- OCSP Signing certificaten MOETEN in overeenstemming zijn met de X.509v3 norm voor publieke sleutel certificaten. Algemene eisen aan certificaten staan in RFC 5280.
- De [X.509] standaard staat een onbeperkt uitbreiden van de attributen binnen een certificaat toe. I.v.m. interoperabiliteitseisen is het binnen de PKI voor de overheid niet toegestaan om deze te gebruiken. Alleen attributen die in deze bijlage als Verplicht, Optioneel of Afgeraden worden aangeduid mogen gebruikt worden.
- OCSP Signing certificaten moeten voldoen aan het profiel voor services certificaten zoals *beschreven in deel 3b van het Programma van Eisen PKIoverheid*, met de volgende uitzonderingen:

OCSP Signing certificaat attributen

Veld / Attribuut	Criteria	Beschrijving	Norm refe-rentie1	Type	Toelichting
Issuer	V	MOET een Distinguished Name (DN) bevatten.	PKIo		Een OCSPSigning certificaat MOET zijn uitgegeven onder de hiërarchie van de PKI voor de overheid.

OCSP Signing certificaat extensies

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
KeyUsage	V	Ja	Dit attribuut extensie specificeert het beoogde doel van de in het certificaat opgenomen sleutel. In de PKI voor de overheid zijn per certificaatsoort ver-schillende bits opgenomen in the keyUsage extensie. In OCSPSigning certificaten MOET het digitalSignature bit zijn opgenomen en de extensie als essentieel zijn aangemerkt. Het non-Repudiation bit MAG NIET worden opgenomen.	RFC 5280, RFC 2560	BitString	
CertificatePolicies	V	Nee	MOET het OID bevatten van de PKI-overheid certificate policy (CP)zoals hiernaast beschreven, de URI van het CPS, en een gebruikersnotitie. Het te gebruiken OID schema in de PKI voor de overheid wordt beschreven in de CP - Services.	RFC 3739	OID, String, String	Het te gebruiken OID voor OCSP certificaten (voor alle domeinen) onder de G2 is 2.16.528.1.1003.1.2.5.4 Het te gebruiken OID voor OCSP certificaten onder de G3 is als volgt: - Organisatie Persoon: 2.16.528.1.1003.1.2.5.1 - Organisatie Services: 2.16.528.1.1003.1.2.5.4 - Organisatie Server: 2.16.528.1.1003.1.2.5.6 - Burger: 2.16.528.1.1003.1.2.3.1 - Autonome apparaten: 2.16.528.1.1003.1.2.6.1

Veld / Attribuut	Criteria	Critical?	Beschrijving	Norm refe-rentie	Type	Toelichting
						Het te gebruiken OID voor OCSP certificaten onder de EV is 2.16.528.1.1003.1.2.7 Het te gebruiken OID voor OCSP certificaten onder de Private Root is als volgt: - Private Services/server: 2.16.528.1.1003.1.2.8.4 - Private Personen: 2.16.528.1.1003.1.2.8.1
ExtKeyUsage	V	Ja	MOET worden gebruikt met de waarde id-kp-OCSPSigning.	RFC 5280		
OCSPNoCheck	V/O		De Baseline Requirements verplicht het gebruik van de OCSPnoCheck voor publiekelijk vertrouwde server en EV certificaten. Voor overige PKIoverheid certificaten is gebruik hiervan optioneel.	RFC 2560		De Baseline Requirements verplichten het gebruik van OCSPnoCheck. Het is derhalve niet duidelijk hoe browsers reageren op OCSP responder certificaten zonder een OCSPNoCheck. Browsers zullen zeer waarschijnlijk de status van een OCSP signing certificaat desondanks niet controleren.

10 Revisies

10.1 Wijzigingen van versie 4.7 naar 4.8

10.1.1 Nieuw

- 5.7.1.-pkio181 (ingangsdatum direct na publicatie PVE 4.8)
- 6.7.1-pkio185 beveiliging webapplicaties aparte eis van gemaakt (ingangsdatum direct na publicatie PVE 4.8)
- 9.17-pkio184 opleveren uitgifte cijfers (ingangsdatum direct na publicatie PVE 4.8)

10.1.2 Aanpassingen

- Verwijzing in eis 4.9.9-pkio69 naar IETF RFC 2560 gewijzigd in IETF RFC 6960 (ingangsdatum direct na publicatie PVE 4.8)
- 6.7.1-pkio118 wijziging patchmanagement afspraken (ingangsdatum direct na publicatie PVE 4.8)
- 5.5.2-pkio83 (ingangsdatum direct na publicatie PVE 4.8)

10.1.3 *Redactioneel*

- 6.5.1-pkio116 (ingangsdatum direct na publicatie PVE 4.8)
- 5.7.1-pkio85 eis gesplitst naar deze eis en nwe eis 5.7.1-pkio 181 (ingangsdatum direct na publicatie PVE 4.8)
- 4.9.9-pkio69 verwijzing (ingangsdatum direct na publicatie PVE 4.8)
- 2.2-pkio156 "én" vervangen door "of" (ingangsdatum direct na publicatie PVE 4.8)

10.2 Wijzigingen van versie 4.6 naar 4.7

10.2.1 Nieuw

- Eis 7.1-pkio174 (uiterlijke ingangsdatum 8 weken na publicatie van het PvE)

10.2.2 Aanpassingen

- Eis 4.8-pkio159 overgeheveld naar eis 8.1-pkio159 (uiterlijke ingangsdatum direct na publicatie van het PvE)
- Aanpassing verwijzing naar ETSI eisen, van toepassing voor eis 3.3.1-pkio36 en eis 3.3.2-pkio46 (uiterlijke ingangsdatum direct na publicatie van het PvE)
- Eis 6.6.1-pkio117 verwijzing naar EN 419 211 voor QSCD's. (uiterlijke ingangsdatum direct na publicatie van het PvE)

10.2.3 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.

10.3 Wijzigingen van versie 4.5 naar 4.6

10.3.1 Nieuw

- Eis 4.8-pkio159 (uiterlijke ingangsdatum 1-9-2017, spoedchange)

10.3.2 Aanpassingen

- Eis 5.7.1-pkio85 (uiterlijke ingangsdatum direct na publicatie van het PvE)
- Eis 5.7.1-pkio84 (uiterlijke ingangsdatum direct na publicatie van het PvE)
- Eis 6.5.1-pkio114 (uiterlijke ingangsdatum 1-5-2018)

•

10.4 Wijzigingen van versie 4.4 naar 4.5

10.4.1 Aanpassingen

- Verwijzing naar RFC6960 i.p.v. RFC2560 (uiterlijke ingangsdatum 31-12-2017)
- Aanpassing Policy ID in OCSP certificaat profiel (uiterlijke ingangsdatum 1-7-2017)
- Eis 2.2-pkio3 is een aanvullende eis geworden vanwege splitsing verplichting Nederlands/Engels tussen de verschillende CP delen (uiterlijke ingangsdatum 1-10-2017)

10.4.2 Redactioneel

- Aanpassing Certification Service Provider → Trust Service Provider in paragraaf 1.1
- Vermelding X509v3 aangepast naar X509v2 voor CRL's in het CRL profiel
- Vermelding Wet Elektronische Handtekeningen verwijderd (vervallen)

10.5 Wijzigingen van versie 4.3 naar 4.4

10.5.1 Aanpassingen

- CRL profiel bijgewerkt om overeen te komen met de gewijzigde velden in het certificaatprofiel inzake OrganizationalIdentifier (uiterlijke ingangsdatum 1-2-2017)

10.5.2 Redactioneel

- Verwijzing naar het CPS aangepast (oude URL bestaat niet meer) onder kop 9.12
- Verwijziging naar OCSP profiel aangepast naar correcte PvE deel
- Term TSP (Certificate service provider) vervangen door TSP (Trust Service Provider) n.a.v. eIDAS verordening

10.6 Wijzigingen van versie 4.2 naar 4.3

10.6.1 Aanpassingen

- Alle verwijzingen van ETSI TS 102 042 aangepast naar ETSI EN 319 411-1. Tevens alle verwijzingen naar paragraafnummer in de relevante ETSI normen bijgewerkt.
- Alle verwijzingen naar ETSI TS 102 176-1 aangepast naar ETSI TS 119 312 (uiterste ingangsdatum 4 weken na publicatie PvE)

10.7 Wijzigingen van versie 4.1 naar 4.2

10.7.1 Nieuw

Niet van toepassing

10.7.2 Aanpassingen

- Eis 7.1-pkio121 (uiterlijke ingangsdatum direct na publicatie van het PvE)

10.7.3 Redactioneel

Niet van toepassing

10.8 Wijzigingen van versie 4.0 naar 4.1

10.8.1 Nieuw
Niet van toepassing

10.8.2 Aanpassingen
- Eis 6.7.1-pkio120 (uiterlijke ingangsdatum 01-09-2015)

10.8.3 Redactioneel
- Kleine redactionele wijzigingen aan de volgende eisen:
    - 2.2-pkio5;
    - 5.3-pkio78;
    - 6.2.5-pkio103;
    - 6.7.1-pkio118;
    - 6.7.1-pkio119;
    - 6.7.1-pkio120;
    - 9.12.2-pkio136;

10.9 Wijzigingen van versie 3.7 naar 4.0

10.9.1 Nieuw
Niet van toepassing

10.9.2 Aanpassingen
- PvE eisen zijn omgenummerd volgens een nieuwe naming convention;
- De creatie van een baseline en een aanvullende eisen document;
- Eis 3.3.1-pkio45;
- Eis 6.5.1-pkio116;
- Eis 4.5.2-pkio52.

10.9.3 Redactioneel
Niet van toepassing