Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programma van Eisen deel 2: Toetreding tot en toezicht binnen de PKI voor de overheid

Datum 5 januari 2015

Colofon

Versienummer 4.0
Contactpersoon Policy Authority PKIoverheid

Organisatie Logius

Bezoekadres
Wilhelmina van Pruisenweg 52

Postadres
Postbus 96810
2509 JE DEN HAAG

T 0900 - 555 4555
servicecentrum@logius.nl

Inhoud

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

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

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

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

Revisiegegevens

Versie	**Datum**	**Omschrijving**
1.0	09-11-2005	Vastgesteld door BZK november 2005
1.1	25-01-2008	Vastgesteld door BZK januari 2008
1.2	13-01-2009	Vastgesteld door BZK januari 2009
2.0	09-10-2009	Vastgesteld door BZK oktober 2009
2.1	11-01-2010	Wijzigingen naar aanleiding van naamswijziging GBO.Overheid in Logius
3.0	25-01-2011	Vastgesteld door BZK januari 2011
3.1	01-07-2011	Vastgesteld door BZK juni 2011
3.2	27-01-2012	Vastgesteld door BZK januari 2012
3.3	01-07-2012	Vastgesteld door BZK juni 2012
3.4	04-02-2013	Vastgesteld door BZK januari 2013
3.5	06-07-2013	Vastgesteld door BZK januari 2013
3.6	01-2014	Vastgesteld door BZK januari 2014
3.7	06-2014	Vastgesteld door BZK juni 2014

4.0	12-2014	Vastgesteld door BZK december 2014

1 Inleiding

1.1 Achtergrond

Dit is deel 2 van het Programma van Eisen (PvE) van de PKI voor de overheid. In het PvE zijn de normen voor de PKI voor de overheid vastgelegd. Dit deel heeft betrekking op de toetreding van een Certification Service Provider (CSP) tot de PKI voor de overheid en op het toezicht dat de PA houdt op CSP's die zijn toegetreden tot de PKI voor de overheid.

Voor een gedetailleerde toelichting op de achtergrond en structuur van de PKI voor de overheid wordt verwezen naar deel 1 van het Programma van Eisen. Hierin wordt tevens ingegaan op de samenhang tussen de verschillende delen uit het Programma van Eisen.

1.2 Doelstelling van dit document

Binnen de PKI voor de overheid worden door CSP's certificaten aan eindgebruikers uitgegeven. Om PKIoverheid-certificaten te kunnen uitgeven moet een CSP in de hiërarchie van de PKI voor de overheid worden opgenomen. Concreet betekent dit dat de publieke sleutel van een CSP wordt ondertekend door een Domein-CA van de PKI voor de overheid.

Om de betrouwbaarheid van de PKI voor de overheid te waarborgen, moeten CSP's binnen de PKI voor de overheid betrouwbare organisaties zijn die voldoen aan hoge eisen voor hun operationele procedures, technische middelen, beveiliging van informatie, deskundigheid en betrouwbaarheid van personeel en informatieverstrekking aan hun doelgroep. De concrete eisen waaraan een CSP moet voldoen om certificaten binnen de PKI voor de overheid te mogen uitgeven, zijn opgenomen in deel 3 van het PvE.

CSP's die willen toetreden tot de PKI voor de overheid moeten aantonen dat zij voldoen aan de in deel 3 gestelde eisen. Om aan te geven op welke wijze een CSP conformiteit aan de gestelde eisen moet aantonen en op welke wijze het toetredingsproces verloopt, wordt in dit document in detail ingegaan op de toetredingsprocedure en de daarmee samenhangende formaliteiten.

Om de betrouwbaarheid van de PKI voor de overheid blijvend te kunnen waarborgen, moeten de CSP's ook na toetreding tot de PKI voor de overheid blijven voldoen aan de in deel 3 gestelde eisen. Om dit vast te stellen, houdt de Policy Authority PKIoverheid (PA) toezicht op de toegetreden CSP's. In dit document wordt derhalve ook inzicht gegeven in de wijze waarop de PA toezicht uitoefent en in de formaliteiten waaraan de CSP moet voldoen om periodiek conformiteit aan de gestelde eisen te kunnen aantonen.

Bij het opstellen van dit document is zoveel mogelijk gebruik gemaakt van reeds ontwikkelde, algemeen geaccepteerde normen en certificatieschema's.

1.3 Status

Dit is versie 4.0 van deel 2 van het Programma van Eisen. De huidige versie is bijgewerkt tot en met januari 2015.

1.4 Structuur van dit document

Hoofdstuk 2 geeft een beschrijving van de toetreding tot de PKI voor de overheid. Hierbij worden achtereenvolgens de van toepassing zijnde eisen, certificatie en de goedkeurende audit verklaring en het toetredingsproces behandeld.

In hoofdstuk 3 wordt ingegaan op het toezicht op CSP's binnen de PKI voor de overheid. Hierbij wordt aangegeven welke stukken periodiek moeten worden ingeleverd en welke planning hierbij wordt gehanteerd.

In bijlage A zijn de eisen opgenomen waaraan een accreditatieschema c.q. certificatieschema moet voldoen indien een CSP tegen een ander schema dan het 'TTP.NL Scheme for management system certification of Service Providers issuing Qualified Certificates for Electronic Signatures, Public Key Certificates, and / or Time-stamp tokens' (TTP.NL schema) is gecertificeerd.

1.5 Normen en wetgeving

De normen en wet- en regelgeving waaraan in document wordt gerefereerd [nr.], zijn opgenomen in deel 1 bij paragraaf 1.5 van het PvE.

2 Toetreding tot de PKI voor de overheid

2.1 Eisen aan CSP-dienstverlening

In deel 3 van het PvE zijn de eisen opgenomen waaraan de CSP-dienstverlening moet voldoen wanneer een CSP wil toetreden tot de PKI voor de overheid. Deel 3 is tevens de zogenaamde Certificate Policy (CP) die van toepassing is op de certificaten die door de CSP worden uitgegeven. In deel 3 wordt een onderscheid gemaakt tussen de volgende categorieën van eisen:

- *CSP-dienstverlening*
  Deze categorie eisen vormt het centrale onderdeel van deel 3. De eisen zijn opgebouwd uit:
  1. de eisen die zijn gesteld in de Wet [1] en Besluit Elektronische Handtekeningen [2] en de bijbehorende regelingen [3 en 4];
  2. ETSI EN 319 411-2 [5] (specifiek voor de gekwalificeerde certificaten);
  3. ETSI EN 319 411-3 [17] (specifiek voor niet-gekwalificeerde certificaten);
  4. ETSI TS 102 042 [6] (specifiek voor server, website en EV SSL certificaten);
  5. Aanvullende PKIoverheid-eisen (hierna: PKIo-eisen);

- *Certificaatprofielen en certificaat statusinformatie*
  De eisen in deze categorie hebben betrekking op de inhoud van de uit te geven certificaten en het formaat waarin de certificaat statusinformatie (bijvoorbeeld een Certification Revocation List of het Online Certificate Status Protocol) wordt gepresenteerd. De eisen zijn ingedeeld naar wettelijke eisen, eisen uit ETSI en aanvullende PKIoverheid-eisen. Deze categorie eisen is in deel 3 als bijlage op de CP gepositioneerd en maakt als zodanig onderdeel uit van de CP.

In PvE deel 3 wordt in detail ingegaan op de van toepassing zijnde eisen. Hierin wordt onder meer een overzicht gepresenteerd waarin is aangegeven hoe de wettelijke eisen, eisen uit ETSI en de PKIo -eisen zich tot elkaar verhouden.

2.2 Aantonen conformiteit aan eisen CSP-dienstverlening

2.2.1 Algemeen

Om vast te kunnen stellen of de dienstverlening van de CSP voldoet aan de gestelde eisen verlangt de Policy Authority PKIoverheid dat:

1.

a. de CSP zich laat certificeren tegen ETSI EN 319 411-2 conform het TTP.NL schema. Hiermee wordt aangetoond dat de CSP voldoet aan ETSI EN 319 411-2. Daarnaast dient in de rapportage te worden vermeld dat de CSP voldoet aan de aanvullende eisen uit het Besluit Elektronische Handtekeningen.

b. de CSP zich laat certificeren tegen ETSI EN 319-411-3 conform het TTP.NL schema en het betreffende Certificate Policy indien de CSP niet gekwalificeerde certificaten uitgeeft. Voor toepassing van specifieke policy identifiers wordt verwezen naar desbetreffend PvE deel.

c. de CSP zich laat certificeren tegen ETSI TS 102 042 conform het TTP.NL schema en het betreffende Certificate Policy indien de CSP server en/of website certificaten uitgeeft. Voor toepassing van specifieke policy identifiers wordt verwezen naar desbetreffend PvE deel.

2. de CSP door middel van een goedkeurende auditverklaring aantoont te voldoen aan de PKIo-eisen. Een goedkeurende audit verklaring is noodzakelijk, aangezien er geen certificatieschema's bestaan voor toetsing tegen de PKIo-eisen;

3. alleen in het geval van PKIoverheid EV SSL certificaten, in afwijking van het gestelde onder 2.2.1-1b de CSP een WebTrust for Certification Authorities – Extended Validation audit mag ondergaan.

4. de CSP geregistreerd is bij de ACM.

De kosten voor het certificatieproces, de goedkeurende audit verklaring en de ACM-registratie komen geheel voor rekening van de toetredende CSP. In de navolgende paragrafen wordt in detail ingegaan op de specifieke eisen en omstandigheden die gelden voor het verkrijgen van het TTP.NL certificaat en de goedkeurende audit verklaring. Voor meer informatie omtrent de registratie bij de ACM wordt verwezen naar www.acm.nl.

2.2.2 TTP.NL certificatie

Waarom TTP.NL certificatie?

Voor toetreding tot de PKI voor de overheid is het verplicht dat een CSP is gecertificeerd tegen het TTP.NL schema [7], het in Nederland van toepassing zijnde schema om gecertificeerd te raken tegen ETSI EN 319 411-2. In de Wet Elektronische Handtekeningen is gesteld dat een CSP niet gecertificeerd hoeft te zijn om aan het publiek gekwalificeerde certificaten in Nederland uit te geven. Binnen de PKI voor de overheid is

er echter voor gekozen om TTP.NL certificatie wel verplicht te stellen voor aangesloten CSP's omdat hiermee meer waarborgen worden verkregen omtrent de betrouwbaarheid van de CSP-dienstverlening.

Eisen aan andere schema's voor certificatie van buitenlandse CSP's
Om gelijkwaardige spelregels te verzekeren voor buitenlandse CSP's die onder een ander certificatieschema dan TTP.NL zijn gecertificeerd, heeft de PKI voor de overheid in bijlage A van dit document eisen opgenomen waaraan accreditatie- en certificatieschema's moeten voldoen. Op basis van een beoordeling tegen die eisen kan de PA, op verzoek van de toetredende CSP, schema's aanwijzen. De PA zal hiertoe in overleg treden met de CSP om onder andere de verschillen van het betreffende schema met het TTP.NL schema te bespreken. CSP's of CSP-organisatieonderdelen die onder een aangewezen schema zijn gecertificeerd tegen de eisen zoals genoemd in dit document, kunnen op deze wijze aan de door de PA gestelde eis van certificatie voldoen.

Wat is het TTP.NL schema?
Het TTP.NL schema is gebaseerd op de norm ETSI EN 319 411-2, ETSI EN 319 411-3 en ETSI TS 102 042 en is bedoeld voor conformiteitcertificatie van CSP's die gekwalificeerde certificaten en overige public key certificaten uitgeven aan het publiek. Het schema voorziet in en beschrijft de proceseisen voor:

- het uitvoeren door de Certificerende Instelling (CI) van een initiële certificatie-audit van de CSP;
- het verlenen van een conformiteitcertificaat aan de CSP bij het voldoen aan de eisen van de norm; het certificaat is geldig voor drie jaar;
- het jaarlijks uitvoeren van een controle-audit;
- het na drie jaar uitvoeren van een herbeoordeling van de CSP; de herbeoordeling is van dezelfde zwaarte als de initiële certificatie-audit.

Het TTP.NL schema voorziet ook in deelcertificatie. Bij deelcertificatie wordt een organisatie tegen een vooraf vast te stellen set van in ETSI gestelde eisen gecertificeerd. Dit is van toepassing wanneer de CSP bijvoorbeeld de certificate generation service heeft uitbesteed. De CSP draagt echter de eindverantwoordelijkheid voor alle aspecten van de dienstverlening. Binnen de PKI voor de overheid is het toegestaan dat een CSP een deel van de dienstverlening uitbesteedt aan een andere organisatie. De CSP moet echter conformiteitbewijzen overhandigen over de complete dienstverlening, inclusief de uitbestede dienstverlening. Voor nadere informatie omtrent deelcertificatie wordt naar het TTP.NL schema verwezen.

Het TTP.NL schema is eigendom van ECP-EPN (www.ecp-epn.nl) en wordt beheerd door het College van Belanghebbenden-TTP.NL.

Wie certificeert?
Conformiteitcertificatie onder TTP.NL is gebaseerd op de beoordeling van de CSP door een CI tegen de toepasselijke norm, ETSI EN 319 411-2, ETSI EN 319 411-3 en ETSI TS 102 042. Een CI is een organisatie die een overeenkomst is aangegaan met ECP-EPN. Hiertoe moet de CI zijn geaccrediteerd door de Raad van Accreditatie. In de navolgende alinea wordt nader ingegaan op de accreditatie van een CI.

Accreditatie van een Certificerende Instelling
Het TTP.NL schema voor certificatie van CSP's stelt de eis dat Certificerende Instellingen moeten zijn geaccrediteerd door de Raad voor Accreditatie (RvA) om te toetsen conform de norm EN 45012 [8]. Dit is de norm die door ISO verplicht is gesteld bij de certificatie van kwaliteitssystemen. De geldigheidsduur van een accreditatie is vier jaar. Om vast te stellen of de CI gedurende de periode van vier jaar voldoet aan de norm EN 45012, voert de RvA jaarlijks controles uit bij de CI. Na vier jaar moet de CI opnieuw worden geaccrediteerd.

Van geaccrediteerde Certificerende Instellingen mag worden verwacht dat zij de certificatie op betrouwbare en deskundige wijze uitvoeren. Om dit te waarborgen zijn in het TTP.NL schema eisen opgenomen waaraan de CI en specifiek het auditteam en de teamleden moeten voldoen. Aangezien een CSP binnen de PKI voor de overheid TTP.NL gecertificeerd moet zijn, moet een CI dus voldoen aan de in het TTP.NL schema gestelde kwaliteitseisen. Binnen de PKI voor de overheid worden geen aanvullende kwaliteitseisen aan Certificerende Instellingen gesteld.

Aanwijzing Certificerende Instelling door Minister van Economische Zaken, Landbouw en Innovatie
In aanvulling op de accreditatie van een CI door de RvA kan een CI ook worden aangewezen door de Minister van EL&I. In de "beleidsregel aanwijzing certificatieorganisaties elektronische handtekeningen" van 6 mei 2003 (WJZ/03/02264), worden de eisen gesteld voor aanwijzing van een CI door de minister van EL&I. Wanneer een geaccrediteerde CI door EL&I is aangewezen, wordt het registratieproces bij ACM vereenvoudigd. In de Wet Elektronische Handtekeningen is gesteld dat in dit geval de CSP kan volstaan met het overleggen van het TTP.NL certificaat. In alle andere gevallen moet de CSP een ingevuld vragenformulier en documenten overleggen waaruit blijkt dat aan de wettelijke eisen wordt voldaan.

2.2.3 Goedkeurende audit verklaring voor PKIo-eisen PKI voor de overheid

Zoals reeds in paragraaf 2.2.1 is gesteld moet de CSP over een goedkeurende audit verklaring beschikken om aan te tonen dat wordt voldaan aan de PKIo-eisen. Vanwege het ontbreken van een certificatieschema voor de PKIo-eisen kan een CI logischerwijs niet door de RvA zijn geaccrediteerd om tegen de PKIo-eisen te toetsen en te certificeren. Om over de PKIo-eisen een goedkeurende verklaring te kunnen afgeven, moet een CI echter wel voldoen aan dezelfde kwaliteitseisen als bij TTP.NL certificatie is vereist. De diepgang en de wijze van uitvoering van de audit voor deze goedkeurende verklaring dient vergelijkbaar te zijn met die van het certificatieonderzoek ten behoeve van de TTP.NL certificatie. In deel 3 van het PvE zijn de PKIo-eisen opgenomen per domein en te herkennen aan de markering [PKIo]. Een CSP die onder een specifiek domein certificaten uitgeeft, zal aan de PKIoverheid eisen van dit domein moeten voldoen.

2.2.4 Uitbreiding CSP-dienstverlening naar uitgifte van services certificaten en/of autonome apparatencertificaten en/of EV SSL certificaten

Afwijkende eisen
Voor het uitgeven van services certificaten en/of autonome apparatencertificaten en/of EV SSL certificaten zijn andere eisen van toepassing dan voor het uitgeven van persoonsgebonden PKIoverheid

certificaten. De specifieke eisen die aan de CSP worden gesteld indien deze services certificaten wil uitgeven, zijn gedefinieerd in de Certificate Policy 'Services', welke in deel 3b van het PvE is opgenomen. De specifieke eisen die aan de CSP worden gesteld indien deze autonome apparatencertificaten wil uitgeven, zijn gedefinieerd in de Certificate Policy 'Autonome Apparaten', welke in deel 3d van het PvE is opgenomen. De specifieke eisen die aan de CSP worden gesteld indien deze EV SSL certificaten wil uitgeven, zijn gedefinieerd in de Certificate Policy 'Extended Validation', welke in deel 3e van het PvE is opgenomen.

2.3 Toetredingsproces

Het volledige proces voor de toetreding bestaat uit een drietal fases:

- *Fase 1: Voorbereiding*
  In deze fase bereidt de CSP zich voor op toetreding tot de PKI voor de overheid. De CSP richt zijn dienstverlening in conform de door de PKI voor de overheid gestelde eisen. Tevens zal in deze fase afstemming plaatsvinden tussen de CSP en de PA.

- *Fase 2: Verzoek tot toetreding en besluitvorming*
  Deze fase eindigt met een besluit van de Minister van BZK.

- *Fase 3: Effectueren toetreding*
  In deze fase worden de technische en organisatorische voorzieningen getroffen waarmee de toetreding wordt geëffectueerd.

In de komende paragrafen worden per fase de relevante aandachtspunten besproken.

2.3.1 Fase 1: Voorbereiding

Wanneer de CSP de intentie heeft om toe te treden tot de PKI voor de overheid, is het aan te raden om contact op te nemen met de PA. Er kan dan worden besloten om een periodiek overleg in te voeren waarin afstemming tussen de CSP en de PA plaats vindt. Tevens zullen vaste contactpersonen bij de CSP en de PA worden aangewezen, opdat de communicatielijnen helder en duidelijk zijn. De PA is in de voorbereidende fase beschikbaar voor vragen in relatie tot de eisen die zijn gesteld in het PvE en het verloop van het toetredingsproces.

In de voorbereidende fase dient de CSP zich tevens te verdiepen in de overeenkomst of het convenant, dat met het Ministerie van BZK zal worden afgesloten. Deze overeenkomst of dit convenant wordt door de CSP ondertekend, voordat de Minister van BZK over de toetreding zal beslissen. De standaardovereenkomst c.q. het standaardconvenant kunnen bij de PA worden opgevraagd.

Het voornoemde onderscheid tussen de ETSI-eisen enerzijds en de wettelijke eisen en PKIo-eisen anderzijds betekent voor een CSP dat hij gelijktijdig het certificatietraject voor ETSI EN 319 411-2 en indien van toepassing ETSI EN 319 411-3 en ETSI TS 102 042 en het toetsingstraject voor de overige binnen de PKI voor de overheid geldende eisen kan doorlopen. De CI kan dan binnen hetzelfde onderzoek aandacht besteden aan zowel de conformiteit met ETSI EN 319 411-2 en indien van toepassing ETSI EN 319 411-3 en ETSI TS 102 042 alsmede de wettelijke eisen en de PKIo-eisen van de PKI voor de overheid. Dit kan de CSP zowel een tijds- als een kostenvoordeel opleveren.

De doorlooptijd van de eerste fase is zeer afhankelijk van de situatie bij de CSP en hiervan is derhalve geen inschatting opgenomen.

2.3.2 *Fase 2: Verzoek om toetreding en besluitvorming door de Minister van BZK*

Voor het verzoek tot toetreding dient gebruik te worden gemaakt van het "Aanvraagformulier toetreding PKI voor de overheid" (PKI00112). Dit formulier is te vinden op www.logius.nl/pkioverheid onder Documentatie, "Modelcontracten en -formulieren" en kan ook worden verkregen bij de PA. De CSP die wil toetreden tot de PKI voor de overheid dient het formulier in te vullen en samen met ondersteunende documentatie aan de PA te retourneren. (Het adres van de PA is vermeld in het aanvraagformulier).

Benodigde documentatie bij verzoek tot toetreding
In navolgend schema is aangegeven welke documentatie moet worden ingeleverd.

Hierbij is ook aangegeven welke documenten aanvullend moeten worden ingeleverd, wanneer de toetredende CSP ook services certificaten en/of autonome apparaten en/of EV SSL certificaten wil gaan uitgeven.

Document	**Toelichting**
Bewijs van registratie bij de ACM.	Hiermee wordt aangetoond dat de CSP gerechtigd is om gekwalificeerde certificaten aan het publiek uit te geven en dat de CSP voldoet aan de WEH. Indien de CSP een vestiging in Nederland heeft dient de CSP te zijn geregistreerd bij de Autoriteit Consument en Markt (ACM) of, indien de CSP geen vestiging in Nederland heeft, als alternatief bij een door een lidstaat van de EG aangewezen ander nationaal orgaan, dat een soortgelijke functie vervult als de ACM. (Deze tekst komt overeen met [WEH II onder B, nr.3])
TTP.NL certificaat (inclusief volledige rapportage van de certificatie)[1].	Dit dient als bewijs van conformiteit met ETSI EN 319 411-2. De PA wil de rapportage ontvangen om inzicht te verkrijgen in de mogelijke non-conformiteiten. In de rapportage en/of TTP.NL certificaat moet zijn aangegeven tegen welke versie van het eisenstellende document is getoetst.
Goedkeurende verklaring voor de PKIo-eisen van de PKI voor de overheid (inclusief volledige rapportage)[2].	Met deze verklaring wordt aangetoond dat de CSP voldoet aan de PKIo-eisen van CP deel 3a en/of 3c. De PA wil de rapportage ontvangen om inzicht te verkrijgen in de mogelijke non-conformiteiten. In de rapportage moet zijn aangegeven tegen welke versie van de eisenstellende documenten is getoetst en welke gepubliceerde wijzigingen op het dan geldende PvE zijn

[1] *Het TTP.NL certificaat dient te zijn afgegeven door een geaccrediteerde CI.*
[2] *Voor de genoemde goedkeurende verklaringen hoeft de CI niet geaccrediteerd te zijn, maar moet deze wel aan de gestelde kwaliteitseisen (zie paragraaf 2.2.2) voldoen.*

Document	**Toelichting**
	meegenomen.

Certificaatprofiel voor eindgebruikers.	Dit is de blauwdruk voor de door de CSP uit te geven certificaten. Omdat bij een non-conformiteit de uitgegeven certificaten dienen te worden ingetrokken, is het gewenst dat de PA dit certificaatprofiel vooraf kan controleren.
Volledig ingevuld aanvraagformulier met het verzoek toe te mogen treden tot de PKI voor de overheid.	Op het formulier dienen de nadere details omtrent de aanvraag te worden opgenomen.
Ingevuld OID-aanvraagformulier.	Iedere CSP en CA binnen de PKI voor de overheid krijgt een eigen OID. Op basis van het ingevulde aanvraagformulier vraagt de PA een OID aan voor de CSP en CA.
Bewijs dat de CSP bevoegd is een organisatorische entiteit te vertegenwoordigen (uitreksel KVK of Staatsalmanak).	Hiermee draagt de PA zorg voor het met zekerheid identificeren van de (vertegenwoordigers van de) CSP.
Ondertekende overeenkomst of convenant met het ministerie van BZK in tweevoud.	Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is de eigenaar van de PKI voor de overheid en met het Ministerie van BZK dient derhalve een formele overeenkomst of convenant te worden gesloten voor de toetreding tot de PKI voor de overheid.

Aanvullend voor niet-gekwalificeerde certificaten waaronder services certificaten en Autonome apparaten-certificaten.

TTP.NL certificaat (inclusief volledige rapportage van de certificatie)[3].	Dit dient als bewijs van conformiteit met ETSI EN 319-411-3. De PA wil de rapportage ontvangen om inzicht te verkrijgen in de mogelijke non-conformiteiten. In de rapportage en/of TTP.NL certificaat moet zijn aangegeven tegen welke versie van het eisenstellende document is getoetst.
Goedkeurende verklaring voor de PKIo-eisen van de PKI voor de overheid (inclusief volledige rapportage)[4].	Met deze verklaring wordt aangetoond dat de CSP voldoet aan de PKIo-eisen van de van toepassing zijnde PvE delen. De PA wil de rapportage ontvangen om inzicht te verkrijgen in de mogelijke non-conformiteiten. In de rapportage moet zijn aangegeven tegen welke versie van de eisenstellende documenten is getoetst en welke gepubliceerde wijzigingen op het dan geldende

[3] Het TTP.NL certificaat dient te zijn afgegeven door een geaccrediteerde CI.
[4] Voor de genoemde goedkeurende verklaringen hoeft de CI niet geaccrediteerd te zijn, maar moet deze wel aan de gestelde kwaliteitseisen (zie paragraaf 2.2.2) voldoen.

	PvE zijn meegenomen.
Certificaatprofiel voor niet-gekwalificeerde certificaten	Zie certificaatprofiel voor eindgebruikers.

Aanvullend voor server, website en EV SSL certificaten.

Document	**Toelichting**
TTP.NL certificaat (inclusief volledige rapportage van de certificatie)[5].	Dit dient als bewijs van conformiteit met ETSI TS 102 042. De PA wil de rapportage ontvangen om inzicht te verkrijgen in de mogelijke non-conformiteiten. In de rapportage en/of TTP.NL certificaat moet zijn aangegeven tegen welke versie van het eisenstellende document is getoetst.
In plaats van een TTP.NL certificaat een verklaring van een gekwalificeerde auditor dat er sprake is van conformiteit aan de WebTrust for CA Extended Validation criteria.	Dit dient als bewijs van conformiteit met de WebTrust for CA Extended Validation criteria. De PA wil de rapportage ontvangen om inzicht te verkrijgen in de mogelijke non-conformiteiten. In de rapportage moet zijn aangegeven tegen welke versie van het eisenstellende document is getoetst.
Goedkeurende verklaring voor de PKIo-eisen van de PKI voor de overheid (inclusief volledige rapportage)[6].	Met deze verklaring wordt aangetoond dat de CSP voldoet aan de PKIo-eisen van CP deel 3f EV. De PA wil de rapportage ontvangen om inzicht te verkrijgen in de mogelijke non-conformiteiten. In de rapportage moet zijn aangegeven tegen welke versie van de eisenstellende documenten is getoetst en welke gepubliceerde wijzigingen op het dan geldende PvE zijn meegenomen.
Certificaatprofiel voor EV SSL certificaten	Zie certificaatprofiel voor eindgebruikers.

Besluitvorming
Na ontvangst van alle benodigde documentatie wordt door de PA beoordeeld in hoeverre het verzoek en de overhandigde documentatie voldoende en adequate informatie verschaffen om het toetredingsverzoek in behandeling te nemen. Indien het verzoek tot toetreding niet volledig of onduidelijk is zal de PA tijd inruimen voor consultatie met de CSP en wordt de documentatie teruggestuurd aan de CSP met het verzoek de documentatieset aan te passen of aan te vullen.

Indien het verzoek volledig en correct is, zal de PA de Minister van BZK adviseren. Vervolgens zal de Minister van BZK beslissen over het al dan niet honoreren van dit verzoek tot toetreding. Het ministerie van BZK zal de CSP informeren over de beslissing van de Minister. In het geval een positief besluit wordt genomen zal het ministerie van BZK aan KPN

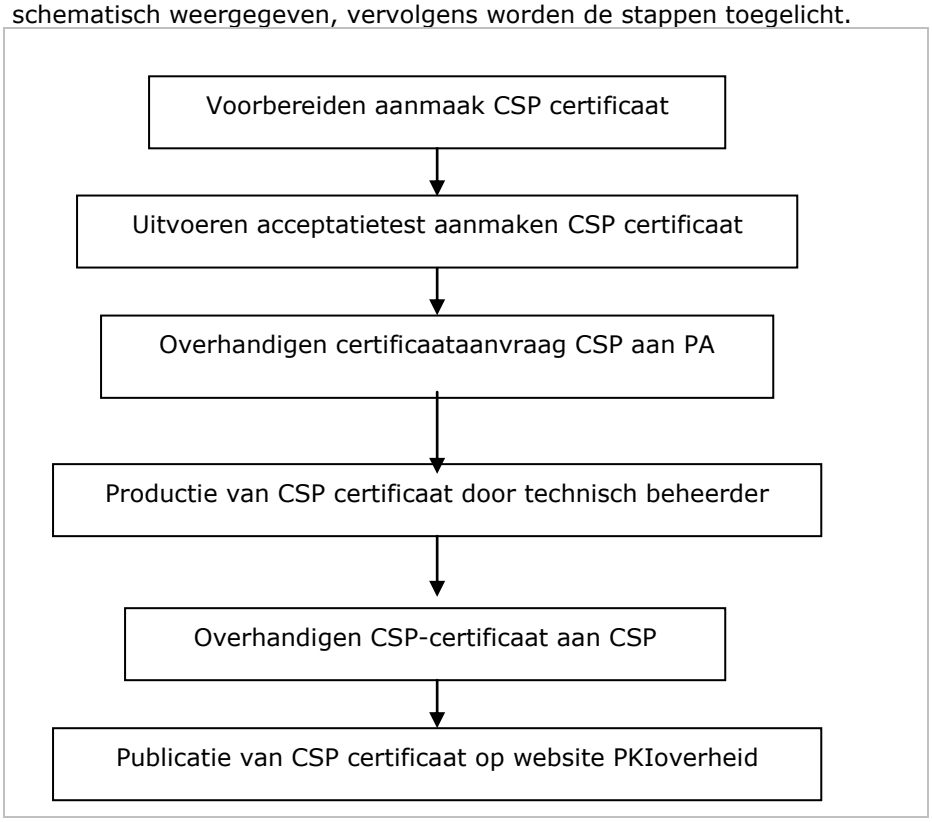
[5] Het TTP.NL certificaat dient te zijn afgegeven door een geaccrediteerde CI.
[6] Voor de genoemde goedkeurende verklaringen hoeft de CI niet geaccrediteerd te zijn, maar moet deze wel aan de gestelde kwaliteitseisen (zie paragraaf 2.2.2) voldoen.

Corporate Market B.V (verder te noemen KPN), de technisch beheerder van de PKI voor de overheid root, de opdracht geven om de CSP op te nemen in de hiërarchie van de PKI voor de overheid.

De doorlooptijd van Fase 2 zal enkele weken bedragen, tenzij er voor de PA reden bestaat om de CSP te consulteren. Deze situatie wordt alleen voorzien als het verzoek tot toetreding niet volledig of onduidelijk is.

2.3.3 *Fase 3: Effectuering*

Bij toetreding tot de PKI voor de overheid dient de CSP zijn publieke sleutel[7] te laten tekenen door de betreffende domeinsleutel van de PKI voor de overheid. Het getekende CSP-certificaat mag alleen worden gebruikt om certificaten uit te geven en CRL's te publiceren, conform het Programma van Eisen van de PKI voor de overheid en om certificaten van eventuele sub-CA's te tekenen. Om te komen tot een door de PKI voor de overheid ondertekend CSP-certificaat dienen een aantal processtappen te worden uitgevoerd. In de navolgende figuur zijn deze stappen schematisch weergegeven, vervolgens worden de stappen toegelicht.



Voorbereiden aanmaak CSP certificaat
De CSP krijgt in deze fase een contactpersoon van de PA toegewezen. Deze contactpersoon voorziet de CSP van de voor de effectuering benodigde informatie. In de afstemmingsfase worden de volgende substappen uitgevoerd:

1. *Bespreken technische en organisatorische randvoorwaarden*
   Hieronder valt de projectplanning van het technische

[7] *Daar waar "sleutel", "CSP-certificaat" en "naming document" staat, kan ook gelezen worden "sleutels", "CSP-certificaten" en "naming documents". Dit hangt af van de door de CSP gekozen inrichting van de CA-structuur.*

certificatietraject, het aanwijzen van de benodigde aanwezigen en de inrichting van de ceremonie.
2. *Afsluiten contract tussen de CSP en KPN*
   Ten behoeve van de uit te voeren acceptatietest dienen de CSP en KPN een contract af te sluiten. Hiertoe geeft de PA onder andere de namen van de contactpersonen bij KPN en andere details (zoals een conceptdatum voor de sleutelceremonie) door.
3. *Verstrekken OID-nummer*
   Het door de CSP aangevraagde OID-nummer wordt door de PA aan de CSP verstuurd.

Op dit moment in de procedure zijn alle gegevens, met uitzondering van de geldigheidsdata, in het naming document bekend. Het naming document dient gebruikt te worden voor de daadwerkelijke productie van het CSP-certificaat[8].

Uitvoeren acceptatietest aanmaken CSP certificaat
Binnen deze stap wordt de acceptatietest uitgevoerd. Deze fase bestaat uit de volgende substappen:
1. *Uitvoeren acceptatietest*
   Tijdens de acceptatietest worden signing script en sleutelceremonie volledig doorlopen als dry-run (proef) voor de productiefase. De acceptatietest wordt door de CSP en KPN gezamenlijk uitgevoerd, zonder betrokkenheid van de PA. Aan het eind van de acceptatietest voeren de CSP en KPN een technische controle uit op het aldus geproduceerde test CSP-certificaat.

2. *Controle door PA*
   Na uitvoering van de acceptatietest verstuurt KPN het test CSP-certificaat naar de PA. De PA controleert vervolgens of de verschillende velden inhoudelijk juist zijn. Vervolgens wordt een definitieve datum vastgesteld voor de productie.

Overhandigen certificaataanvraag CSP aan PA
Deze fase bestaat uit de volgende substappen:

1. *Versturen request aan PA*
   De CSP genereert een certificate request (een PKCS#10 bestand) en overhandigt het request, inclusief een afdruk daarvan, op een betrouwbare wijze aan de PA.

2. *Controle door PA*
   De PA controleert het certificate request om zo meer garanties te hebben dat er tijdens productie geen problemen zullen optreden. Daarnaast moet KPN het volledig ingevulde naming document ter controle versturen aan de PA. Wanneer de controle van het certificate request en van het naming document positief zijn uitgevallen kan de productie van het CSP-certificaat worden uitgevoerd en worden de CSP en KPN hierover ingelicht. Vervolgens overhandigt de PA op een betrouwbare wijze het certificate request aan KPN.

Productie van CSP certificaat door technisch beheerder
Deze fase bestaat uit de volgende substappen:

[8] *Afwijkingen van het naming document kunnen een belemmering vormen, met name wanneer als 'critical' gemerkte velden verschillen van het vereiste certificaatprofiel.*

1. *Overhandigen certificate request aan KPN*
   De PA overhandigt het certficate request op een betrouwbare wijze aan KPN.

2. *Genereren CSP-certificaat*
   De publieke sleutel van de CSP wordt daadwerkelijk getekend door de signing key (van het betreffende domein) van de PKI voor de overheid. Bij dit proces is de PA aanwezig om de juistheid van het proces vast te stellen. De CSP is niet aanwezig bij de generatie van het CSP-certificaat. De output van deze stap is een door de betreffende Domein-CA getekend CSP-certificaat.

Overhandigen CSP-certificaat aan CSP
Deze fase bestaat uit de volgende substappen:

1. *Controle door PA*
   De PA ontvangt van KPN het CSP-certificaat en controleert het CSP-certificaat. Na een positieve controle overhandigt de PA een brief aan KPN waarin de positieve uitslag wordt medegedeeld.

2. *Overhandiging aan CSP*
   De PA overhandigt het CSP-certificaat aan de CSP. De CSP controleert vervolgens het CSP-certificaat en ondertekent een ontvangstbevestiging waarin ook akkoord wordt gegeven voor de inhoud van het CSP-certificaat. De overhandiging vindt direct na de generatie plaats bij KPN te Apeldoorn. De verantwoordelijkheid voor het transport naar de locatie van het CSP-certificaat en de verdere behandeling van het door de Domein-CA getekende CSP-certificaat ligt vanaf dat moment bij de CSP. Het transport van het PKCS#7 bestand naar de locatie van de CSP dient plaats te vinden op een wijze die vergelijkbaar is met het overhandigen van het PKCS#10 bestand om zo een overeenkomstige mate van betrouwbaarheid te verkrijgen.

Publicatie van CSP certificaat op website PKIoverheid
Na overhandiging van het CSP-certificaat zal de PA het CSP-certificaat publiceren op haar website www.logius.nl/pkioverheid.

Doorlooptijd
De geschatte doorlooptijd van de fase effectuering toetreding is twee maanden. Indien de CSP specifieke eisen stelt (uitgebreide key-ceremonies, aanwezigheid / inzet meerdere partijen) of wanneer zich onvoorziene technische complicaties voordoen kan de doorlooptijd toenemen.

Kosten
De kosten voor realisatie van deze fase komen geheel voor rekening van de toetredende CSP en bedragen € 7.000,-. Dit bedrag is vastgelegd in de overeenkomst die het Ministerie van BZK heeft afgesloten met KPN als technisch beheerder van de root.

3 Toezicht

3.1 Inleiding

Om de betrouwbaarheid van de PKI voor de overheid blijvend te kunnen waarborgen, moeten de CSP's ook na toetreding tot de PKI voor de overheid blijven voldoen aan de in deel 3 gestelde eisen. Om dit vast te stellen, houdt de Policy Authority PKIoverheid (PA) toezicht op de toegetreden CSP's. In dit hoofdstuk wordt aangegeven welke stukken periodiek moeten worden ingeleverd en welke planning hierbij wordt gehanteerd.

3.2 Periodiek in te leveren stukken

In het hoofdstuk "Toetreding tot de PKI voor de overheid" is in paragraaf 2.2.2 aangegeven dat een TTP.NL certificatie drie jaar geldig is en dat jaarlijks herhalingsaudits moeten worden uitgevoerd. Deze systematiek is door de PKI voor de overheid overgenomen in relatie tot de goedkeurende auditverklaringen die moeten worden ingeleverd. In deze paragraaf wordt derhalve onderscheid gemaakt tussen de stukken die jaarlijks moeten worden ingeleverd en de stukken die driejaarlijks moeten worden ingeleverd.

3.2.1 Jaarlijks in te leveren

De volgende documenten dient de CSP jaarlijks[9] in te leveren:

- Bewijs van conformiteit aan ETSI EN 319 411-2 c.q. TTP.NL certificatie voor persoonsgebonden certificaten;
- Indien van toepassing, bewijs van conformiteit aan ETSI EN 319 411-3 c.q. TTP.NL certificatie;
- Indien van toepassing, bewijs van conformiteit aan ETSI TS 102 042 c.q. TTP.NL certificatie;
- In plaats van conformiteit aan ETSI TS 102 042 c.q. TTP.NL certificatie: een goedkeurende auditverklaring inzake WebTrust for Certification Authorities – Extended Validation. Alleen in het geval een CSP, PKIoverheid EV SSL certificaten uitgeeft;
- Goedkeurende auditverklaring voor de PKIo-eisen van de PKI voor de overheid;
- Goedkeurende verklaring dat aan de op ETSI TS 102 042 gebaseerde eisen van de CP Services en/of Autonome Apparaten en/of EV SSL is voldaan[10].

Het volledige definitieve auditrapport met detailbevindingen moet worden overhandigd aan de PA PKIoverheid zodra dit door de auditor is opgeleverd. Ook het plan van aanpak voor corrigerende maatregelen (CAP) moet worden overhandigd aan de PA zodra deze door de auditor is goedgekeurd. Waar mogelijk ontvangt de PA tevens de deelcertificering van toeleveranciers. Indien een follow-up audit noodzakelijk blijkt te zijn, wenst de PA PKIoverheid ook de resultaten van deze audit te ontvangen.

Zodra de CSP de goedkeurende verklaring(en) van de CI heeft ontvangen, dient de CSP deze verklaringen per direct via de post of per e-mail toe te zenden aan de Policy Authority PKIoverheid. In de verklaringen en het

---

[9] De termijn start op het moment dat de overeenkomst met BZK, niet zijnde de overeenkomst voor voorlopige toetreding, door beide partijen is ondertekend.

[10] Deze verklaring hoeft uiteraard alleen te worden ingeleverd wanneer de CSP is toegetreden om services certificatenen/of autonome apparatencertificaten en/of EV SSL certificaten uit te geven.

bewijs van conformiteit aan ETSI EN 319 411-2 of ETSI TS 102 042 moet tevens zijn aangegeven tegen welke versie van de eisen stellende documenten is getoetst en welke gepubliceerde wijzigingen op het dan geldende PvE zijn meegenomen.

De bovengenoemde documenten moeten door een CI worden afgegeven, waarbij dezelfde kwaliteitscriteria gelden als bij de toetreding tot de PKI voor de overheid.

3.2.2 Driejaarlijks in te leveren

Driejaarlijks moeten dezelfde documenten worden ingeleverd, zoals benoemd in paragraaf 3.2.1 (m.u.v. auditverklaring inzake WebTrust for Certification Authorities – Extended Validation, deze wordt alleen jaarlijks afgegeven). Hierbij zijn dezelfde vereisten van toepassing zoals deze gelden voor de jaarlijks in te leveren documenten.

3.2.3 Publicatie ETSI-TTP.NL certificaat

De CSP moet het driejarige ETSI-TTP.NL certificaat publiceren op haar website.

3.3 Planning

Vanwege het feit dat de verklaringen (waaronder WebTrust Certification Authorities – Extended Validation) en het conformiteitbewijs aan ETSI EN 319 411-2 en indien van toepassing ETSI EN 319 411-3 en ETSI TS 102 042 jaarlijks worden afgegeven, hebben deze documenten logischerwijs een geldigheidsduur van één jaar. De nieuwe documenten moeten derhalve uiterlijk één jaar na het moment van afgifte door de CI van de voorgaande verklaring en het conformiteitbewijs aan ETSI EN 319 411-2 en indien van toepassing ETSI EN 319 411-3 en ETSI TS 102 042 worden ingeleverd door de CSP bij de PA. De CSP is verantwoordelijk voor het tijdig inleveren van de verklaringen en het conformiteitbewijs aan ETSI EN 319 411-2 en indien van toepassing ETSI EN 319 411-3 en ETSI TS 102 042.

3.4 Wijzigingen in certificatie en ACM-registratie

Omdat het kan voorkomen dat het TTP.NL certificaat wordt ingetrokken of opgeschort of de ACM-registratie wordt beëindigd, heeft de CSP de plicht de PA direct in te lichten wanneer zich één van de volgende situaties voordoet:

- Het TTP.NL certificaat wordt ingetrokken of opgeschort door de CI;
- Het TTP.NL deelcertificaat van de organisatie waaraan de CSP activiteiten heeft uitbesteed wordt ingetrokken of opgeschort door de CI;
- Er is sprake van een negatieve WebTrust for Certification Authorities – Extended Validation verklaring;
- De registratie van de CSP wordt ingetrokken door de ACM.

3.5 Handhaving van afspraken

Overheidsorganisaties die als CSP binnen de PKI voor de overheid opereren zijn een convenant overeengekomen met het Ministerie van BZK. De overige CSP's binnen de PKI voor de overheid hebben een overeenkomst afgesloten met het Ministerie van BZK. In de overeenkomst en het convenant is opgenomen hoe het Ministerie van BZK en de CSP moeten handelen binnen de PKI voor de overheid. Onder andere wordt ingegaan op het blijvend voldoen aan de gestelde eisen en de mogelijkheden tot handhaving van de afspraken door de PA. Dit betreft

onder meer de mogelijkheid om een audit te laten uitvoeren bij de CSP en het ontbinden van de overeenkomst c.q. het convenant.

De overeenkomsten en convenanten hebben een geldigheidsduur van zes jaar. Voorafgaand aan het verlopen van geldigheidsduur neemt de PA contact op met de CSP om de eventuele verlenging van de overeenkomst of het convenant te bespreken.

BIJLAGEN

Bijlage A Eisen aan accreditatieschema's

Inleiding
In hoofdstuk twee is aangegeven dat CSP's die willen toetreden tot de PKI voor de overheid TTP.NL gecertificeerd moeten zijn. Om gelijkwaardige spelregels te verzekeren voor CSP's die onder een ander certificatieschema dan TTP.NL zijn gecertificeerd, zijn in deze bijlage eisen opgenomen waaraan accreditatieschema's moeten voldoen. Op basis van een beoordeling tegen die eisen kan de PA, op verzoek van de toetredende CSP, schema's aanwijzen. CSP's of CSP-organisatieonderdelen die onder een aangewezen schema zijn gecertificeerd tegen de eisen zoals genoemd in dit document, kunnen op deze wijze aan de door de PA gestelde eis van certificatie voldoen.

Eisen
Om in aanmerking te komen voor een aanwijzing door de PA dient aan de volgende eisen te worden voldaan:

- In het accreditatieschema dienen inhoudelijk gelijkwaardige kwaliteitscriteria te zijn opgesteld ten opzichte van het TTP.NL schema, te weten het 'TTP.NL Scheme for management system certification of Service Providers issuing Qualified Certificates for Electronic Signatures, Public Key Certificates, and / or Time-stamp tokens'. Dit schema wordt beheerd door ECP-EPN en de officiële publicatieplaats van het schema is derhalve www.ecp-epn.nl.
- Het in het accreditatieschema gehanteerde toetsingskader moet inhoudelijk gelijkwaardig zijn aan het toetsingskader dat bij TTP.NL wordt gehanteerd.

Om vast te stellen of de schema's gelijkwaardig zijn, zal de PA steunen op de resultaten van een vergelijking tussen het TTP.NL schema en het betreffende schema waaronder de toetredende CSP is gecertificeerd. Deze vergelijking dient de CSP uit te (laten) voeren. Voor het uitvoeren van deze vergelijking heeft de PA een methode ontwikkeld[11], die bij de vergelijking moet worden gehanteerd. De methode is opgesplitst in twee delen, te weten:

- De vergelijking van de kwaliteitscriteria en formaliteiten rondom het certificatieonderzoek;
- De vergelijking van de inhoudelijke eisen van de normenkaders die in de te vergelijken schema's worden gehanteerd.

Alvorens de CSP start met het (laten) uitvoeren van de vergelijking is het raadzaam dat de CSP contact met de PA opneemt om de te hanteren methode te bespreken, zodat voor de betrokken partijen duidelijk is hoe de vergelijking moet worden uitgevoerd en de wederzijdse verwachtingen helder zijn.

[11] *De methode kan bij de PA worden opgevraagd.*

4 Revisies

4.1 Wijzigingen van versie 3.7 naar 4.0

4.1.1 Redactioneel

- Verwijzingen naar ETSI EN 319-411-3.

4.2 Wijzigingen van versie 3.6 naar 3.7

Geen wijzigingen.

4.3 Wijzigingen van versie 3.5 naar 3.6

4.3.1 Aanpassingen

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

4.3.2 Redactioneel

- Verwijzingen naar PKIo-OO, PKIo-Bu, PKIo-Sv etc.

4.4 Wijzigingen van versie 3.4 naar 3.5

4.4.1 Aanpassingen

- Paragraaf 2.2.1 (uiterlijke ingangsdatum 4 weken na publicatie PVE 3.5);
- Paragraaf 3.2.1 (uiterlijke ingangsdatum 4 weken na publicatie PVE 3.5);

4.5 Wijzigingen van versie 3.3 naar 3.4

Geen wijzigingen.

4.6 Wijzigingen van versie 3.2 naar 3.3

Geen wijzigingen.

4.7 Wijzigingen van versie 3.1 naar 3.2

4.7.1 Nieuw

Geen wijzigingen.

4.7.2 Aanpassingen

- Paragraaf 1.4;
- Paragraaf 2.2.1;
- Paragraaf 2.3;
- Paragraaf 2.4;
- Paragraaf 3.2.1;
- Paragraaf 3.2.2;
- Paragraaf 3.3;
- Paragraaf 3.4.

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

4.8 Wijzigingen van versie 3.0 naar 3.1

4.8.1 Nieuw
- Paragraaf 3.2.3.

4.8.2 Aanpassingen
- Paragraaf 3.2.1.

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

4.9 Wijziging van versie 2.1 naar 3.0

4.9.1 Nieuw
Geen wijzigingen.

4.9.2 Aanpassingen
De volgende paragrafen zijn aangepast in verband met de introductie van Extended Validation binnen de PKI voor de overheid:
- Paragraaf 2.1;
- Paragraaf 2.2.1;
- Paragraaf 2.2.3;
- Paragraaf 2.2.4;
- Paragraaf 2.4.2;
- Paragraaf 3.2.1.

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

4.10 Wijziging van versie 2.0 naar 2.1

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

4.11 Wijziging van versie 1.2 naar 2.0

4.11.1 Nieuw
Geen wijzigingen.

4.11.2 Aanpassingen
De volgende paragrafen zijn aangepast in verband met de introductie van het Domein Autonome Apparaten binnen de PKI voor de overheid:
- Paragraaf 2.1;
- Paragraaf 2.2.1;
- Paragraaf 2.2.4;

- Paragraaf 3.2.1.

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

4.12 Wijzigingen van versie 1.1 naar 1.2

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

4.13 Wijzigingen versie 1.0 naar 1.1
Geen wijzigingen.

4.14 Versie 1.0
Eerste versie.