Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

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

Datum 8 februari 2019

Colofon

Versienummer	4.7
Contactpersoon	Policy Authority PKIoverheid
Organisatie	Logius
	Bezoekadres Wilhelmina van Pruisenweg 52
	Postadres Postbus 96810 2509 JE DEN HAAG
	T 0900 - 555 4555 servicecentrum@logius.nl

Inhoud

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	Vastgesteld 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

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 (TSP) tot de PKI voor de overheid en op het toezicht dat de PA houdt op TSP'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 TSP's certificaten aan eindgebruikers uitgegeven. Om PKIoverheid-certificaten te kunnen uitgeven moet een TSP in de hiërarchie van de PKI voor de overheid worden opgenomen. Concreet betekent dit dat de publieke sleutel van een TSP wordt ondertekend door een Domein-CA van de PKI voor de overheid.

Om de betrouwbaarheid van de PKI voor de overheid te waarborgen, moeten TSP'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 TSP moet voldoen om certificaten binnen de PKI voor de overheid te mogen uitgeven, zijn opgenomen in deel 3 van het PvE.

TSP'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 TSP 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 TSP'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 TSP's. In dit document wordt derhalve ook inzicht gegeven in de wijze waarop de PA toezicht uitoefent en in de formaliteiten waaraan de TSP 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 4.7 van deel 2 van het Programma van Eisen. De huidige versie is bijgewerkt tot en met 8 februari 2019.

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 TSP's binnen de PKI voor de overheid. Hierbij wordt aangegeven welke stukken periodiek moeten worden ingeleverd en welke planning hierbij wordt gehanteerd.

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 TSP-dienstverlening

In deel 3 van het PvE zijn de eisen opgenomen waaraan de TSP-dienstverlening moet voldoen wanneer een TSP 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 TSP worden uitgegeven. In deel 3 wordt een onderscheid gemaakt tussen de volgende categorieën van eisen:

- *TSP-dienstverlening*
  Deze categorie eisen vormt het centrale onderdeel van deel 3. De eisen zijn opgebouwd uit:
  1. de eisen die zijn gesteld in het Besluit Vertrouwensdiensten en de Europese verordening 910/2014 (eIDAS);
  2. ETSI EN 319 411-2 (specifiek voor de gekwalificeerde certificaten);
  3. ETSI EN 319 411-1 (specifiek voor niet-gekwalificeerde certificaten en server, website en EV SSL certificaten);
  4. Aanvullende PKIoverheid-eisen (hierna: PKIo-eisen);
  5. CA/Browser Forum: "Network and Certificate System Security Requirements" (Netsec).

- *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 TSP-dienstverlening

2.2.1 Algemeen

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

1. De TSP zich laat certificeren tegen ETSI EN 319 411-1 conform het ETSI EN 319 403 schema en het betreffende Certificate Policy indien de TSP niet gekwalificeerde certificaten server en/of website certificaten uitgeeft. Voor toepassing van specifieke policy identifiers wordt verwezen naar desbetreffend PvE deel.

2. de TSP door middel van een goedkeurende auditverklaring aantoont te voldoen aan de PKIo-eisen en eisen gesteld in verordening 910/2014 (eIDAS). Een goedkeurende audit verklaring is noodzakelijk, aangezien er geen certificatieschema's bestaan voor toetsing tegen de PKIo-eisen en wettelijke eisen;

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

Indien de TSP onder PKIoverheid gekwalificeerde certificaten uit wil gaan geven gelden de volgende additionele vereisten:

4. De TSP laat zich certificeren tegen ETSI EN 319 411-2 conform het ETSI EN 319 403 schema. Hiermee wordt aangetoond dat de TSP voldoet aan het ETSI EN 319 411-2. Daarnaast dient in de rapportage te worden vermeld dat de TSP voldoet aan de eIDAS verordening.

5. De TSP is geregistreerd bij AT. De CA waarmee de TSP gekwalificeerde certificaten uit wil geven MOET op de TSL staan bij AT voordat uitgifte van gekwalificeerde certificaten kan aanvangen.

De kosten voor het certificatieproces, de goedkeurende audit verklaring en de AT-registratie komen geheel voor rekening van de toetredende TSP. In de navolgende paragrafen wordt in detail ingegaan op de specifieke eisen en omstandigheden die gelden voor het verkrijgen van het ETSI EN 319 403 certificaat en de goedkeurende audit verklaring. Voor meer informatie omtrent de registratie bij de AT wordt verwezen naar www.agentschaptelecom.nl.

Wat is het ETSI EN 319 403 schema?

Het schema voorziet in en beschrijft de proceseisen voor:

- het uitvoeren door de Certificerende Instelling (CI) van een initiële certificatie-audit van de TSP;
- het verlenen van een conformiteitcertificaat aan de TSP 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 twee jaar uitvoeren van een herbeoordeling van de TSP; de herbeoordeling is van dezelfde zwaarte als de initiële certificatie-audit.
- Door eisen van browserpartijen is bovenstaande door PKIoverheid verzwaard en dient een toegetreden TSP jaarlijks een volledige audit te ondergaan (zie ook 3.2)

Het ETSI EN 319 403 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 TSP bijvoorbeeld de certificate generation service heeft uitbesteed. De TSP draagt echter de eindverantwoordelijkheid voor alle aspecten van de dienstverlening. Binnen de PKI voor de overheid is het toegestaan dat een TSP een deel van de dienstverlening uitbesteedt aan een andere organisatie. De TSP moet echter conformiteitbewijzen overhandigen over de complete dienstverlening, inclusief de uitbestede dienstverlening. Voor nadere informatie omtrent deelcertificatie wordt naar het ETSI EN 319 403 schema verwezen.

Wie certificeert?
Conformiteitcertificatie onder ETSI EN 319 403 is gebaseerd op de beoordeling van de TSP door een CI tegen de toepasselijke norm, ETSI EN 319 411-2 en ETSI EN 319 411-1. Hiertoe moet de CI zijn geaccrediteerd door de Raad van Accreditatie of een andere accreditatie-instantie in de zin van artikel 4 van verordening (EG) nr. 765/2008. In de navolgende alinea wordt nader ingegaan op de accreditatie van een CI.

Accreditatie van een Certificerende Instelling
Het ETSI EN 319 403 schema voor certificatie van TSP's stelt de eis dat Certificerende Instellingen moeten zijn geaccrediteerd door de Raad voor Accreditatie (RvA) of een andere accreditatie-instantie (zie hierboven) om te toetsen conform de norm ISO 17065. Dit is de norm die door ISO verplicht is gesteld bij de certificatie van product/dienstcertificering. 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 ISO 17065, 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 ETSI EN 319 403 schema eisen opgenomen waaraan de CI en specifiek het auditteam en de teamleden moeten voldoen. Binnen de PKI voor de overheid worden geen aanvullende kwaliteitseisen aan Certificerende Instellingen gesteld.

2.2.2 *Goedkeurende audit verklaring voor PKIo-eisen PKI voor de overheid*

Zoals reeds in paragraaf 2.2.1 is gesteld moet de TSP 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 ETSI EN 319 403 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 ETSI EN 319 403 certificatie. In deel 3 van het PvE zijn de PKIo-eisen opgenomen per domein en te herkennen aan de markering [PKIo]. Een TSP die onder een specifiek domein certificaten uitgeeft, zal aan de PKIoverheid eisen van dit domein moeten voldoen.

2.2.3 Uitbreiding TSP-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 TSP 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 TSP 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 TSP 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 TSP zich voor op toetreding tot de PKI voor de overheid. De TSP richt zijn dienstverlening in conform de door de PKI voor de overheid gestelde eisen. Tevens zal in deze fase afstemming plaatsvinden tussen de TSP 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 TSP 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 TSP en de PA plaats vindt. Tevens zullen vaste contactpersonen bij de TSP 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 TSP 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 TSP 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 TSP dat hij gelijktijdig het certificatietraject voor ETSI EN 319 411-2 en indien van

toepassing ETSI EN 319 411-1 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 319 411-1 alsmede de wettelijke eisen en de PKIo-eisen van de PKI voor de overheid. Dit kan de TSP zowel een tijds- als een kostenvoordeel opleveren.

De doorlooptijd van de eerste fase is zeer afhankelijk van de situatie bij de TSP 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 TSP 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 TSP ook services certificaten en/of autonome apparaten en/of EV SSL certificaten wil gaan uitgeven.

Voor gekwalificeerde certificaten

Document	**Toelichting**
Bewijs van registratie bij de AT.	Hiermee wordt aangetoond dat de TSP gerechtigd is om gekwalificeerde certificaten aan het publiek uit te geven. Indien de TSP een vestiging in Nederland heeft dient de TSP te zijn geregistreerd bij het Agentschap Telecom (AT) of, indien de TSP 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 AT.
ETSI EN 319 411-2 certificaat (inclusief volledige rapportage van de certificatie)[1].	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)[2].	Met deze verklaring wordt aangetoond dat de TSP 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 meegenomen.
Certificaatprofiel voor eindgebruikers.	Dit is de blauwdruk voor de door de TSP 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 TSP 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 TSP en CA.
Bewijs dat de TSP 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) TSP.
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.

[1] Het ETSI EN 319 403 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.

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

ETSI EN 319 411-1 certificaat (inclusief volledige rapportage van de certificatie).	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)[3].	Met deze verklaring wordt aangetoond dat de TSP 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 PvE zijn meegenomen.
Certificaatprofiel voor niet-gekwalificeerde certificaten	Zie certificaatprofiel voor eindgebruikers.

Aanvullend voor server, website en EV SSL certificaten.

Document	**Toelichting**
ETSI EN 319 411-1 certificaat (inclusief volledige rapportage van de certificatie).	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.
In plaats van een ETSI EN 319 411-1 certificaat een verklaring van een gekwalificeerde auditor dat er sprake is van conformiteit aan 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)[4].	Met deze verklaring wordt aangetoond dat de TSP 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.

[3] 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.
[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.

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 TSP en wordt de documentatie teruggestuurd aan de TSP met het verzoek de documentatieset aan te passen of aan te vullen.

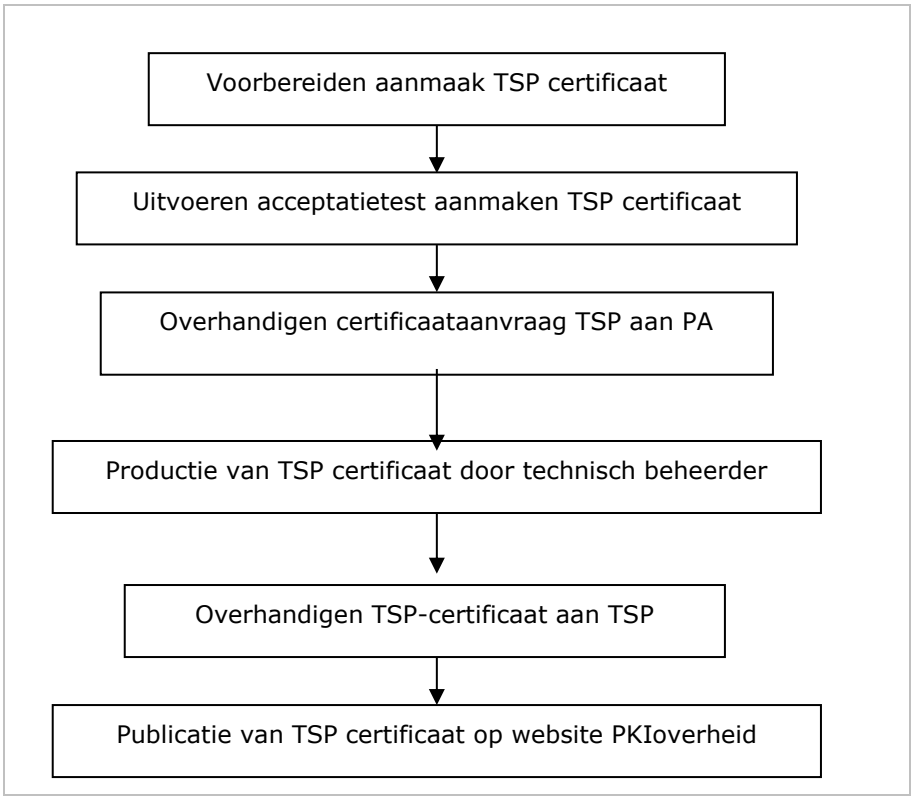
Indien het verzoek volledig en correct is, zal de PA de Minister van BZK adviseren. Vervolgens zal de Minister van BZK beslissen over het al dan niet honoreren van dit verzoek tot toetreding. Het ministerie van BZK zal de TSP informeren over de beslissing van de Minister. In het geval een positief besluit wordt genomen zal het ministerie van BZK aan KPN Corporate Market B.V (verder te noemen KPN), de technisch beheerder van de PKI voor de overheid root, de opdracht geven om de TSP 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 TSP 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 TSP zijn publieke sleutel[5] te laten tekenen door de betreffende domeinsleutel van de PKI voor de overheid. Het getekende TSP-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 TSP-certificaat dienen een aantal processtappen te worden uitgevoerd. In de navolgende figuur zijn deze stappen schematisch weergegeven, vervolgens worden de stappen toegelicht.

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



Voorbereiden aanmaak TSP certificaat
De TSP krijgt in deze fase een contactpersoon van de PA toegewezen. Deze contactpersoon voorziet de TSP 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 certificatietraject, het aanwijzen van de benodigde aanwezigen en de inrichting van de ceremonie.
2. *Afsluiten contract tussen de TSP en KPN*
   Ten behoeve van de uit te voeren acceptatietest dienen de TSP 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 TSP aangevraagde OID-nummer wordt door de PA aan de TSP 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 TSP-certificaat[6].

Uitvoeren acceptatietest aanmaken TSP certificaat
Binnen deze stap wordt de acceptatietest uitgevoerd. Deze fase bestaat uit de volgende substappen:

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

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 TSP en KPN gezamenlijk uitgevoerd, zonder betrokkenheid van de PA. Aan het eind van de acceptatietest voeren de TSP en KPN een technische controle uit op het aldus geproduceerde test TSP-certificaat.

2. *Controle door PA*
   Na uitvoering van de acceptatietest verstuurt KPN het test TSP-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 TSP aan PA
Deze fase bestaat uit de volgende substappen:

1. *Versturen request aan PA*
   De TSP 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 TSP-certificaat worden uitgevoerd en worden de TSP en KPN hierover ingelicht. Vervolgens overhandigt de PA op een betrouwbare wijze het certificate request aan KPN.

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

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

2. *Genereren TSP-certificaat*
   De publieke sleutel van de TSP 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 TSP is niet aanwezig bij de generatie van het TSP-certificaat. De output van deze stap is een door de betreffende Domein-CA getekend TSP-certificaat.

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

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

2. *Overhandiging aan TSP*
   De PA overhandigt het TSP-certificaat aan de TSP. De TSP controleert vervolgens het TSP-certificaat en ondertekent een ontvangstbevestiging waarin ook akkoord wordt gegeven voor de inhoud van het TSP-certificaat. De overhandiging vindt direct na de generatie plaats bij KPN te Apeldoorn. De verantwoordelijkheid voor het transport naar de locatie van het TSP-certificaat en de verdere behandeling van het door de Domein-CA getekende TSP-certificaat ligt vanaf dat moment bij de TSP. Het transport van het PKCS#7 bestand naar de locatie van de TSP 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 TSP certificaat op website PKIoverheid
Na overhandiging van het TSP-certificaat zal de PA het TSP-certificaat publiceren op haar website www.logius.nl/pkioverheid.

Doorlooptijd
De geschatte doorlooptijd van de fase effectuering toetreding is twee maanden. Indien de TSP 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 TSP en bedragen € 7.000,-.voor één TSP CA. Voor elke bijkomende TSP CA geldt een meertarief van € 1.000,- per CA met een maximum van 6 CA’s. Wil een TSP meer dan 6 TSP CA certificaten laten tekenen dan dient de TSP contact op te nemen met de PA. 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 TSP'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 TSP'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 ETSI EN 319 403 certificatie twee jaar geldig is en dat jaarlijks herhalingsaudits moeten worden uitgevoerd. Door eisen van browserpartijen heeft PKIoverheid deze eis verzwaard en dient er jaarlijks een volledige audit te worden uitgevoerd. Deze systematiek is door de PKI voor de overheid overgenomen in relatie tot de goedkeurende auditverklaringen die moeten worden ingeleverd.

3.2.1 Jaarlijks in te leveren

De volgende documenten dient de TSP jaarlijks[7] in te leveren:

- Bewijs van conformiteit aan ETSI EN 319 411-2 c.q. ETSI EN 319 403 certificatie voor persoonsgebonden certificaten;
- Indien van toepassing, bewijs van conformiteit aan ETSI EN 319 411-1 c.q. ETSI EN 319 403 certificatie;
- In plaats van conformiteit aan ETSI EN 319 411-1 c.q. ETSI EN 319 403 certificatie: een goedkeurende auditverklaring inzake WebTrust for Certification Authorities – Extended Validation. Alleen in het geval een TSP, PKIoverheid EV SSL certificaten uitgeeft;
- Goedkeurende auditverklaring voor de PKIo-eisen van de PKI voor de overheid;
- Goedkeurende verklaring dat aan de op ETSI EN 319 411-1 gebaseerde eisen van de CP Services en/of Autonome Apparaten en/of EV SSL is voldaan[8].

Het volledige en definitieve auditrapport met detailbevindingen moet worden overhandigd aan AT en de PA PKIoverheid zodra dit door de auditor is opgeleverd. Dit dient te gebeuren binnen 3 werkdagen na oplevering. Ook het plan van aanpak voor corrigerende maatregelen (CAP) moet worden overhandigd aan AT en de PA zodra deze door de auditor is goedgekeurd. Waar mogelijk ontvangen AT en de PA tevens de deelcertificering van toeleveranciers. Indien een follow-up audit noodzakelijk blijkt te zijn, wensen AT en de PA PKIoverheid ook de resultaten van deze audit te ontvangen waarover de hierboven aangegeven termijnen ook van toepassing zijn.

Voor de de bovengenoemde documenten geldt dat deze in een aantal talen opgeleverd mogen of moeten worden. Onderstaande tabel geeft hier inzicht in.

---

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

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

Document	Nederlands	Engels	Andere taal
Auditrapport	Mogelijk	Mogelijk	Niet toegestaan
CAP	Mogelijk	Mogelijk	Niet toegestaan
Conformiteitsbeoordeling	Mogelijk	Verplicht	Niet toegestaan

Zodra de TSP de goedkeurende verklaring(en) van de CI heeft ontvangen, dient de TSP deze verklaringen per direct via de post of per e-mail toe te zenden aan de Policy Authority PKIoverheid. In de verklaringen en het bewijs van conformiteit aan ETSI EN 319 411-2 of ETSI EN 319 411-1 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 Publicatie ETSI EN 319 403 certificaat

De TSP moet het driejarige ETSI EN 319 403 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 319 411-1 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 319 411-1 worden ingeleverd door de TSP bij de PA. De TSP is verantwoordelijk voor het tijdig inleveren van de verklaringen en het conformiteitbewijs aan ETSI EN 319 411-2 en indien van toepassing ETSI EN 319 411-1.

3.4 Wijzigingen in certificatie en AT-registratie

Omdat het kan voorkomen dat het ETSI EN 319 411-1 of ETSI 319 411-2 certificaat wordt ingetrokken of opgeschort of de AT-registratie wordt beëindigd, heeft de TSP de plicht de PA direct in te lichten wanneer zich één van de volgende situaties voordoet:

- Het ETSI EN 319 411-1 of ETSI 319 411-2 certificaat wordt ingetrokken of opgeschort door de CI;
- Het ETSI EN 319 411-1 of ETSI 319 411-2 deelcertificaat van de organisatie waaraan de TSP 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 TSP wordt ingetrokken door de AT.

3.5 Handhaving van afspraken

Overheidsorganisaties die als TSP binnen de PKI voor de overheid opereren zijn een convenant overeengekomen met het Ministerie van BZK. De overige TSP'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 TSP

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 TSP 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 TSP om de eventuele verlenging van de overeenkomst of het convenant te bespreken.

4 Revisies

4.1 Wijzigingen van versie 4.6 naar 4.7

4.1.1 Aanpassingen

- Schrappen verplichting om een ETSI en 319 403 certificering te overhandigen.

4.2 Wijzigingen van versie 4.5 naar 4.6

Geen wijzigingen.

4.3 Wijzigingen van versie 4.4 naar 4.5

4.3.1 Aanpassingen

- Het normatief houden van de Netsec (als referentie opgenomen in ETSI EN 319 411-1 en nu normatief in het PvE)
- Normatieve referenties aangepast door het vervallen van de WEH en de wijziging van de diverse wetten en de introductie van de eIDAS verordening.

4.4 Wijzigingen van versie 4.3 naar 4.4

4.4.1 Aanpassingen

- Scope van toegestane certificerende instellingen (CI's) aangepast n.a.v. eIDAS verordening (uiterlijke ingangsdatum 1-2-2017)

4.4.2 Redactioneel

- Begrip CSP (Certification Service Provider) vervangen door TSP (Trust Service Provider) t.g.v. eIDAS verordening

4.5 Wijzigingen van versie 4.2 naar 4.3

4.5.1 Aanpassingen

- TTP.NL schema is vervallen ten gunste van Europees schema ETSI EN 319 403 (per 1-7-2016)
- ETSI TS 102 042 is vervangen door ETSI EN 319 411-1 (per 1-7-2016)

4.6 Wijzigingen van versie 4.1 naar 4.2

Geen wijzigingen.

4.7 Wijzigingen van versie 4.0 naar 4.1

4.7.1 Aanpassingen

- Verwijdering van de normatieve verwijzing van ETSI EN 319 411-3 naar ETSI TS 102 042.

4.8 Wijzigingen van versie 3.7 naar 4.0

4.8.1 Redactioneel

- Verwijzingen naar ETSI EN 319-411-3.

4.9 Wijzigingen van versie 3.6 naar 3.7

Geen wijzigingen.

4.10 Wijzigingen van versie 3.5 naar 3.6

4.10.1 Aanpassingen

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

4.10.2 Redactioneel

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

4.11 Wijzigingen van versie 3.4 naar 3.5

4.11.1 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);

4.12 Wijzigingen van versie 3.3 naar 3.4

Geen wijzigingen.

4.13 Wijzigingen van versie 3.2 naar 3.3

Geen wijzigingen.

4.14 Wijzigingen van versie 3.1 naar 3.2

4.14.1 Nieuw

Geen wijzigingen.

4.14.2 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.

4.14.3 Redactioneel

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

4.15 Wijzigingen van versie 3.0 naar 3.1

4.15.1 Nieuw
- Paragraaf 3.2.3.

4.15.2 Aanpassingen
- Paragraaf 3.2.1.

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

4.16 Wijziging van versie 2.1 naar 3.0

4.16.1 Nieuw
Geen wijzigingen.

4.16.2 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.

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

4.17 Wijziging van versie 2.0 naar 2.1

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

4.18 Wijziging van versie 1.2 naar 2.0

4.18.1 Nieuw
Geen wijzigingen.

4.18.2 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.

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

4.19 Wijzigingen van versie 1.1 naar 1.2

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

4.20 Wijzigingen versie 1.0 naar 1.1
Geen wijzigingen.

4.21 Versie 1.0
Eerste versie.