Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programma van Eisen deel 1: Introductie

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 juli 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 Doel van het Programma van Eisen

Dit is deel 1 van het Programma van Eisen (PvE) voor de PKI voor de overheid. Het doel van het PvE is om eisen vast te leggen voor het gebruik van de PKI voor de overheid en de bij de PKI voor de overheid betrokken partijen hierover te informeren.

Dit deel geeft een introductie op het PvE. In hoofdstuk 1 wordt allereerst de historie van de PKI voor de overheid beschreven en een korte introductie op PKI (Public Key Infrastructuur) gegeven. Vervolgens wordt in hoofdstuk 2 ingegaan op de inrichting van de PKI voor de overheid, waarin de uitgangspunten en de architectuur aan bod komen. In hoofdstuk 3 wordt beschreven welke eisen er binnen de PKI voor de overheid van toepassing zijn en hoe deze zijn gepositioneerd binnen de PKI voor de overheid. Tevens is aangegeven hoe de betrouwbaarheid van de dienstverlening binnen de PKI voor de overheid wordt gewaarborgd en kan worden gecontroleerd. Tenslotte is in hoofdstuk 4 een leeswijzer opgenomen waarin alle delen uit het PvE worden toegelicht.

1.2 Voorgeschiedenis

De Nederlandse overheid heeft hoge ambities op het gebied van elektronische dienstverlening, zoals vastgelegd in het actieprogramma "Andere Overheid". Hierin is expliciet de doelstelling geformuleerd dat in 2007 65% van de publieke dienstverlening moet worden aangeboden via het internet. Eind 2007 werd vastgesteld dat deze doelstelling is behaald[1]. Een essentiële voorwaarde voor elektronische dienstverlening is de betrouwbaarheid van de elektronische communicatie. Zo vraagt bijvoorbeeld een elektronische subsidieaanvraag in het algemeen om de identiteitsvaststelling van de betrokkenen, de wilsverklaring dat er daadwerkelijk een overheidsdienst wordt gevraagd en om vertrouwelijkheid van de communicatie van de aanvrager met de subsidieverstrekkende instantie.

Dit alles kan mogelijk worden gemaakt door toepassing van generieke mechanismen zoals identificatie en een elektronische handtekening op basis van Public Key Cryptografie. Public Key Cryptografie kan op verschillende manieren worden toegepast om betrouwbare elektronische communicatie te realiseren, waarbij men wel spreekt over een Public Key Infrastructuur (PKI). PKI is een zeer effectieve basis voor het cryptografische deel van de informatiebeveiliging.

Eind 1999 is bij een besluit van de ministerraad de Taskforce PKIoverheid opgericht. De werkzaamheden van de Taskforce PKIoverheid hebben onder andere geleid tot een in 2002 ingerichte topstructuur van de PKI voor de overheid[2]. In 2003 is de eerste Certification Service Provider (CSP) toegetreden tot de PKI voor de overheid en inmiddels zijn er al meerdere organisaties als CSP actief binnen de PKI voor de overheid.

---

[1] Zie rapport "Publieke dienstverlening 65% elektronisch" d.d. 5 december 2007

[2] In paragraaf 2.4 wordt in detail ingegaan op deze topstructuur en de volledige inrichting van de PKI voor de overheid.

Uit de Taskforce PKIoverheid is in 2003 de Policy Authority (PA) van de PKI voor de overheid voortgekomen. De PA is de beheerder van de topstructuur van de PKI voor de overheid en van het normenkader (Programma van Eisen, PvE) dat aan de PKI voor de overheid ten grondslag ligt. In de Certification Practice Statement (CPS) van de PA wordt in detail ingegaan op de activiteiten die de PA uitvoert in het kader van het beheer van de PKI voor de overheid. Dit CPS is te vinden op www.logius.nl/pkioverheid.

1.3 Waarom PKI

1.3.1 Behoefte aan vertrouwen

De behoefte aan PKI kan niet los worden gezien van de groeiende behoefte aan elektronische communicatie en dienstverlening binnen de maatschappij in het algemeen en de overheid in het bijzonder. De vraag naar elektronische afhandeling van transacties neemt toe. De gebruiker hoeft zich niet fysiek te melden bij zijn transactiepartner en kan gebruiksvriendelijk vanaf zijn PC de transactie uitvoeren. Bovendien kan de ontvanger van een transactieaanvraag zijn administratieve organisatie stroomlijnen met de nieuwe technologie en zijn bedrijfsproces daarmee efficiënter inrichten. Hiermee wordt tegemoet gekomen aan de steeds verdergaande vraag naar hoogwaardige dienstverlening in de 24-uurs economie.

Een absolute voorwaarde voor een volwaardige en volledige elektronische dienstverlening is een betrouwbaar mechanisme dat kan zorgen voor dezelfde waarborgen die op dit moment in de "papieren" wereld gelden. Dit geldt voor alle dienstverlening, zowel bij de overheid als in het normale economische verkeer. Elektronische handelingen vragen om identiteitsvaststelling van de betrokkenen, de wilsverklaring van partijen en de vertrouwelijkheid van de communicatie tussen transactiepartners.

1.3.2 Mogelijkheden PKI

De PKI voor de overheid maakt het mogelijk dat communicerende partijen waarborgen krijgen omtrent:

- de identiteit van een persoon die een dienst afneemt of de dienst zelf (identificatie en authenticiteit);
- de (juridische) zekerheid dat een bericht door een bepaalde persoon is verzonden of een document door een bepaalde persoon is ondertekend en dit ook niet achteraf kan worden ontkend (elektronische handtekening, onweerlegbaarheid);
- de mogelijkheid om communicatie te beschermen tegen ongewenste inzage (vertrouwelijkheid, privacy) of wijziging (integriteit) door derden.

1.3.3 Wat is een PKI en hoe werkt het

Een PKI is een infrastructuur bestaande uit organisatorische en technische componenten waarbinnen beveiligde communicatie mogelijk is. De basis van PKI ligt opgesloten in de gebruikte asymmetrische cryptografische algoritmes. Hierbij krijgt de gebruiker een sleutelpaar, bestaande uit een private, alleen bij hem bekende, sleutel en een publieke, voor iedereen toegankelijke, sleutel. De private en publieke sleutel van een gebruiker zijn onlosmakelijk met elkaar verbonden. De publieke sleutel mag worden verspreid (bijvoorbeeld in een database, vgl. een telefoonboek); de private sleutel dient zorgvuldig geheim gehouden te worden door de gebruiker.

Met behulp van dergelijke sleutelparen kan betrouwbare elektronische communicatie plaatsvinden. Voor het aanbrengen van een digitale handtekening en het realiseren van vertrouwelijkheid en authenticatie worden met de sleutels verschillende handelingen uitgevoerd.

Wat is nu de garantie dat een gebruikte sleutel inderdaad bij de verzender/ontvanger behoort? De oplossing voor de koppeling tussen de gebruiker en het sleutelpaar wordt gerealiseerd door middel van PKI. De gebruiker verkrijgt een digitale identiteit, een certificaat, waarin wordt verklaard dat de publieke sleutel bij hem hoort. Een certificaat is een klein bestandje waarin de gegevens van de gebruiker samen met diens publieke sleutel zijn opgenomen. Deze gegevens zijn vervolgens elektronisch ondertekend door een Certification Service Provider. De ontvangende partij, ook wel vertrouwende partij genoemd, kan aan de hand van het certificaat controleren of de verzender ook daadwerkelijk is wie hij zegt te zijn. De vertrouwende partij vertrouwt hierbij op de CSP die de gegevens in het certificaat heeft bekrachtigd met zijn elektronische handtekening. Een verdere uitleg van de werking van PKI treft u aan op www.logius.nl/pkioverheid.

1.3.4 Keuze voor PKI

Naast PKI zijn er ook andere mechanismen om identiteiten langs elektronische weg vast te stellen. Denk aan het gebruik van wachtwoorden, PINcodes en hulpmiddelen die eenmalige codes genereren. Deze mechanismen bieden echter, in tegenstelling tot PKI, geen ondersteuning voor vertrouwelijkheid of juridische gelijkwaardigheid met de handgeschreven handtekening. Wanneer dus de behoefte bestaat om informatie vertrouwelijk te communiceren en/of een elektronische handtekening te zetten die juridisch gelijkwaardig is met de handgeschreven handtekening is PKI de oplossing om dit te realiseren.

De ondersteuning van meervoudige functies door PKI is vaak de reden om PKI in te zetten voor het realiseren van betrouwbare communicatie. PKIoverheid certificaten worden inmiddels gebruikt in diverse processen binnen de overheid en het bedrijfsleven. Op www.logius.nl/pkioverheid is een actueel overzicht te vinden van organisaties die als CSP opereren binnen de PKI voor de overheid.

1.4 Status

Dit is versie 4.0 van deel 1 van het Programma van Eisen. De huidige versie is bijgewerkt tot en met januari 2015.

Alle delen van het PvE staan onder wijzigingenbeheer. Wijzigings-verzoeken worden in behandeling genomen conform de procedure, zoals deze is beschreven in het document "Procedurebeschrijving wijzigingen in PvE". Dit document kan worden geraadpleegd op de website www.logius.nl/pkioverheid.

1.5 Normatieve referenties

De normen en wet- en regelgeving waaraan in dit document wordt gerefereerd, zijn de volgende:

[1] Wet Elektronische Handtekeningen
Wet van 8 mei 2003 tot aanpassing van Boek 3 en Boek 6 van het Burgerlijk Wetboek, de Telecommunicatiewet en de Wet op de economische delicten inzake elektronische handtekeningen ter uitvoering van de richtlijn nr. 1999/93/EG van het Europees Parlement en de Raad van de Europese Unie van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG L 13).

[2] Besluit Elektronische Handtekeningen
Besluit van 8 mei 2003, houdende de vaststelling van eisen voor het verlenen van diensten voor elektronische handtekeningen.

[3] Regeling Elektronische Handtekeningen, 6 mei 2003 nr. WJZ/03/02263 Regeling van de Staatssecretaris van Economische Zaken houdende nadere regels met betrekking tot elektronische handtekeningen.

[4] Beleidsregel aanwijzing certificatieorganisaties elektronische handtekeningen, 6 mei 2003 nr. WJZ/03/02264
Beleidsregel van de Staatssecretaris van Economische Zaken met betrekking tot de aanwijzing van organisaties die certificatiedienst-verleners toetsen op de overeenstemming met de bij of krachtens de Telecommunicatiewet gestelde eisen, op grond van artikel 18.16 van de Telecommunicatiewet.

[5] ETSI EN 319 411-2, "Electronic Signatures and Infrastructures (ESI);Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates ".
Deze Europese Norm bevat de eisen voor CSP's die gekwalificeerde certificaten voor elektronische handtekeningen uitgeven aan het publiek. Binnen de PKI voor de overheid is deze norm specifiek aan CSP's voorgeschreven voor persoonsgebonden certificaten.

[6] ETSI TS 102 042, " Policy requirements for certification authorities issuing public key certificates", ESI.
Deze Technical Specification bevat de eisen voor CSP's die public key certificaten uitgeven aan het publiek. Binnen de PKI voor de overheid is deze norm specifiek aan CSP's voorgeschreven voor niet-persoonsgebonden certificaten.

[7] TTP.NL Scheme for management system certification of Service Providers issuing Qualified Certificates for Electronic Signatures, Public Key Certificates, and / or Time-stamp tokens, version 9.2_final.
Het doel van dit schema is om te voorzien in criteria en procedures voor het uitvoeren van een certificatieonderzoek door onafhankelijke instellingen en het certificeren van Certification Authorities (CAs) die gekwalificeerde certificaten uitgeven.

[8] EN 45012:1998, Algemene eisen voor instellingen die beoordeling en certificatie/registratie van kwaliteitssystemen uitvoeren.

[9] "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures", CEN/ISSS WS/E-Sign (CWA 14167-1).
Dit is een uitwerking van de eisen aan systemen van certificatiedienstverleners, zoals genoemd in Bijlage II (sub f) van de richtlijn.

[10] ETSI TS 102 176-1, "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
In dit document is beschreven welke algoritmes en sleutellengtes binnen de PKI voor de overheid worden toegestaan.

[11] "Security Requirements For Cryptographic Modules", NIST (FIPS PUB 140-2).
Hierin staan eisen van de Amerikaanse overheid voor cryptografische producten.

[12] "Secure Electronic Signature Devices, Version EAL 4+", CEN/ISSS WS/E-Sign (CWA 14169).
Hierin staan eisen voor het veilige middel voor het aanmaken van elektronische handtekeningen, zoals genoemd in Bijlage III van de richtlijn.

[13] "EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes", CEN/ISSS WS/E-Sign (CWA 14172-2).
Hierin staat een toelichting op de eisen voor certificatiedienst-verleners.

[14] "Cryptographic module for CSP Signing Operations" – Protection Profile CEN/ISSS WS/E-Sign (CWA 14167-2).
Hierin staan eisen voor de door een certificatiedienstverlener specifiek gebruikt cryptografisch product.

[15] "EESSI Conformity Assessment Guidance – Part 3: Trustworthy systems managing certificates for electronic signatures", CEN/ISSS WS/E-Sign (CWA 14172-3).
Hierin staat een toelichting op de eisen voor de door een certificatiedienstverlener gebruikte systemen.

[16] "Cryptographic module for CSP Signing Operations" – Protection Profile CEN/ISSS WS/E-Sign (CWA 14167-4).
Hierin staan eisen voor de door een certificatiedienstverlener specifiek gebruikt cryptografisch product.

[17] ETSI EN 319 411-3, "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates ".
Deze Europese Norm bevat de eisen voor CSP's die niet-gekwalificeerde certificaten voor uitgeven aan het publiek.

2 Overzicht PKI voor de overheid

2.1 Inleiding

In dit hoofdstuk wordt allereerst ingegaan op de strategische uitgangspunten die aan de PKI voor de overheid ten grondslag liggen. Vervolgens wordt ingegaan op het certificatenmodel dat wordt gehanteerd en tenslotte wordt een toelichting gegeven op de inrichting van de PKI voor de overheid.

2.2 Strategische uitgangspunten

Voor de realisatie van PKI diensten binnen de PKI voor de overheid zijn de volgende strategische uitgangspunten van toepassing:

- Werkbare infrastructuur. De PKI voor de overheid faciliteert de communicatie tussen overheid en overheid, tussen overheid en bedrijven, tussen bedrijven en bedrijven en tussen overheid en burger (communicatiedomeinen).
- Eén vastgesteld betrouwbaarheidsniveau. Het betrouwbaarheidsniveau van de PKI voor de overheid is gebaseerd op de Wet Elektronische Handtekeningen en internationale standaarden. Hierdoor kunnen gebruikers met één soort handtekening, die dezelfde rechtsgevolgen heeft als een handgeschreven handtekening, gebruik maken van de elektronische dienstverlening van de overheid.
- Organisatorische interoperabiliteit. Aan organisaties die binnen de PKI voor de overheid certificaten willen uitgeven worden hoge eisen gesteld met betrekking tot het registreren, produceren, uitgeven, beheren en controleren van certificaten en sleutelparen. Deze eisen zijn opgenomen in de Certificate Policy (CP)[3], die als deel 3 onderdeel uitmaakt van het PvE. Deze eisen zijn aan alle partijen binnen de PKI voor de overheid opgelegd.
- Technische interoperabiliteit. De PKI voor de overheid is gebaseerd op open standaarden waardoor interoperabiliteit is gerealiseerd. Hierdoor kunnen verschillende leveranciers producten aanbieden binnen de PKI voor de overheid en zijn proceseigenaren niet afhankelijk van één aanbieder.
- Certificaten voor rollen. Binnen de PKI voor de overheid worden certificaten uitgegeven in een aantal domeinen, te weten het domein Overheid/Bedrijven, Organisatie, het domein Burger en het domein Autonome Apparaten. In de domeinen Overheid/Bedrijven en Organisatie worden certificaten uitgegeven aan entiteiten die zijn verbonden aan een organisatie, dan wel handelen uit hoofde van een erkend beroep. In het domein Burger worden certificaten uitgegeven aan individuen. Hierdoor wordt transparantie verkregen over de rol die een persoon vervult in de elektronische communicatie. In het domein Autonome Apparaten worden certificaten uitgegeven aan apparaten die in hun operationele levensfase zelfstandig de integriteit en authenticiteit van (meet)gegevens waarborgen ten behoeve van (een specifiek doel binnen een kerntaak van) een bepaalde overheidsinstantie.
- Centrale deel PKI voor de overheid bepalend voor vertrouwen. De betrouwbaarheid van de PKI voor de overheid wordt bepaald door de

[3] *Een CP beschrijft welke eisen er aan uitgifte en gebruik van een bepaald type certificaat worden gesteld. Een Certification Practice Statement (CPS) beschrijft daarentegen op welke wijze een CSP aan deze eisen tegemoet is gekomen. De CP's zijn opgesteld door de PA en gelden voor alle CSP's in een domein. Het CPS wordt daarentegen door iedere CSP zelf opgesteld.*

betrouwbaarheid van het centrale deel. In het Certification Practice Statement van de PA is beschreven welke procedures en maatregelen de PA heeft getroffen om de betrouwbaarheid van het centrale deel te waarborgen.

2.3 Certificatenmodel

Het certificaat speelt een centrale rol binnen een PKI (zie ook paragraaf 1.3). Door middel van het certificaat verkrijgt de certificaathouder namelijk een digitale identiteit. Binnen de PKI voor de overheid wordt onderscheid gemaakt tussen certificaten voor personen, certificaten voor services (bijvoorbeeld systemen en applicaties), Extended Validation SSL certificaten en certificaten voor Autonome Apparaten. In de navolgende paragrafen wordt een toelichting gegeven op het certificatenmodel dat binnen de PKI voor de overheid wordt gehanteerd.

2.3.1 Persoonsgebonden certificaten

Certificaten voor individuen zijn persoonsgebonden (of identiteitsgebonden). Wel kunnen personen in verschillende hoedanigheden verschillende certificaten krijgen: als burger, als medewerker van een overheidsorganisatie of bedrijf of handelend vanuit een erkend beroep. De PKI voor de overheid maakt gebruik van drie afzonderlijke certificaten en sleutels voor de elektronische handtekening, authenticiteit en vertrouwelijkheid. Dit wordt ook wel het 3-certificatenmodel genoemd.

Het certificaat voor de elektronische handtekening voldoet aan de juridische vereisten, zoals deze in de Europese richtlijn 1999/93/EG zijn gepubliceerd en in de Nederlandse wetgeving[4] zijn opgenomen, van een handtekening in relatie tot gegevens in elektronische vorm, op dezelfde wijze als een handgeschreven handtekening.

Het authenticiteitcertificaat is geschikt voor betrouwbare identificatie en authenticatie van personen langs elektronische weg.

De vertrouwelijkheidcertificaten die binnen de PKI voor de overheid worden uitgegeven zijn geschikt voor het beschermen van de vertrouwelijkheid van gegevens die onderling in elektronische vorm worden uitgewisseld.

De certificaten voor authenticatie en vertrouwelijkheid hebben hetzelfde betrouwbaarheidsniveau als het gekwalificeerde certificaat. Dit betekent dat de eisen zoals gesteld aan het certificaat voor de elektronische handtekening ook van toepassing zijn op het authenticiteitcertificaat en het vertrouwelijkheidcertificaat.

2.3.2 Services certificaten

Het services certificaat is een niet-persoonsgebonden certificaat. Er is hiervan sprake wanneer de certificaathouder een apparaat of een systeem (een niet-natuurlijke persoon) is, bediend door of namens een organisatorische entiteit. Maar hiervan is ook sprake wanneer een certificaat, onder verantwoordelijkheid van een organisatorische entiteit niet aan één certificaathouder is gekoppeld. Een voorbeeld hiervan is een certificaat dat aan een functie is gekoppeld; op het moment dat bij vertrek

[4] *Het betreft de Wet en het Besluit Elektronische Handtekeningen en bijbehorende Regelingen.*

van een medewerker, een andere persoon de functie vervult, kan het certificaat aan deze persoon worden doorgegeven.

De PKI voor de overheid maakt gebruik van drie afzonderlijke services certificaten en sleutels, te weten een authenticiteitcertificaat, een vertrouwelijkheidcertificaat en een servercertificaat. Het authenticiteit- en vertrouwelijkheidcertificaat kunnen in beide hierboven beschreven categorieën worden gebruikt.
Het servercertificaat hoort uitsluitend in de eerste categorie (apparaat of systeem) thuis. Bij services certificaten is vooral van belang dat er zekerheid wordt gegeven over de verbondenheid tussen het apparaat, het systeem of de functie en de organisatie die in het certificaat wordt genoemd.

De drie typen services certificaten hebben hetzelfde betrouwbaarheidsniveau. Dit betrouwbaarheidsniveau is gebaseerd op het niveau van de persoonsgebonden certificaten.

2.3.3 Extended Validation (EV) SSL certificaten

EV SSL certificaten zijn niet persoonsgebonden certificaten. Deze kunnen worden gebruikt voor het beveiligen van een verbinding tussen een bepaalde client en een server, via het TLS/SSL protocol, die behoort bij de organisatorische entiteit die als abonnee wordt genoemd in het betreffende certificaat.

Eén van de belangrijkste eigenschappen van een EV SSL certificaat is dat deze de adresbalk van de browser groen laat kleuren. Dit houdt in dat de identiteit van de eigenaar van de website, welke in het SSL certificaat vermeld staat, is gevalideerd aan de hand van de zeer strenge EV richtlijnen.

2.3.4 Autonome apparatencertificaten

Het autonome apparatencertificaat is een niet-persoonsgebonden certificaat die in het domein Autonome Apparaten wordt uitgegeven. Er is hiervan sprake wanneer de certificaathouder een apparaat is, waarvan de werking en de wijze van produceren aantoonbaar conformeren aan het normenkader van een specifieke soort autonome apparaten en dat in die hoedanigheid door de kadersteller geautoriseerd is gebruik te maken van een aan (bijv. het serienummer van) dat apparaat gekoppeld autonome apparatencertificaat.

De PKI voor de overheid maakt gebruik van drie afzonderlijke autonome apparatencertificaten en sleutels, te weten een authenticiteitcertificaat, een vertrouwelijkheidcertificaat en een combinatiecertificaat.

Authenticiteitcertificaten kunnen worden gebruikt voor het langs elektronische weg betrouwbaar identificeren en authenticeren van het Autonome Apparaat en diens gecertificeerde werking.
Vertrouwelijkheidcertificaten kunnen worden gebruikt voor het beschermen van de vertrouwelijkheid van gegevens, die worden uitgewisseld met het Autonome Apparaat en/of daarin worden opgeslagen in elektronische vorm. Combinatiecertificaten kunnen worden gebruikt voor het beveiligen van een verbinding tussen een bepaalde cliënt en een Autonoom Apparaat.

2.4 Inrichting PKI voor de overheid

De Public Key Infrastructuur (PKI) voor de overheid kent een structuur waarbij een centraal en een uitvoerend c.q. lokaal deel van PKIoverheid is gedefinieerd. Binnen PKIoverheid worden en drie typen stamcertificaten onderscheiden:

- de reguliere root;
- de extended validation root; en
- de private root

Bij de reguliere root is sprake van een structuur c.q. root (Staat der Nederlanden Root CA) gebaseerd op het SHA-1 algoritme, een root (Staat der Nederlanden Root CA – G2) gebaseerd op het SHA-256 algoritme en een root (Staat der Nederlanden Root CA – G3) eveneens gebaseerd op het SHA-256 algoritme.
De root en de domeinen o.b.v. het SHA-1 algoritme worden aangemerkt als G1, waarbij G staat voor generatie. De root en de domeinen o.b.v. het SHA-256 algoritme worden aangemerkt als G2 en G3.

Voor de G1 (SHA-1) root is er sprake van de domeinen Overheid/Bedrijven (deze twee domeinen zijn in de loop van de tijd samengevoegd) en Burger.

De G2 (SHA-256) bevat de volgende domeinen:
- Organisatie
- Burger
- Autonome Apparaten

De G3 (SHA-256) bevat de volgende domeinen:
- Organisatie Persoon
- Burger
- Organisatie Services
- Autonome Apparaten

Voor de EV root is sprake van een aparte structuur c.q. root (Staat der Nederlanden EV Root CA) voor de uitgifte van PKIoverheid EV SSL certificaten met daaronder 1 EV intermediair CA gebaseerd op het SHA-256 algoritme.

Ten slotte kent PKIoverheid een private root gebaseerd op het SHA-256 algoritme, waaronder niet-publiekelijk vertrouwde certificaten worden uitgegeven. De Private root bevat de volgende domeinen:
- Private services
- Private personen

2.4.1 Beschrijving structuur Staat der Nederlanden Root CA structuur

Binnen het centrale deel van de structuur van de Staat der Nederlanden Root CA structuur worden een aantal actoren onderscheiden. Deze actoren zijn:
1. de Overheids (Ov)-PA, op het hoogste niveau verantwoordelijk voor het vaststellen van het beleid en normen van algemene aard die gelden binnen de structuur van de Staat der Nederlanden Root CA en uitgifte van certificaten;
2. de Ov-CA, betreft een technische component die het hoogste (of Root-) certificaat produceert binnen de structuur van de Staat der

Nederlanden Root CA en certificaten produceert voor de onderliggende domein CA's;
3. de Domein (D)-PA, die de domeinspecifieke invulling van de normen van de Ov-PA verzorgt, en de voorwaarden van uitgifte van certificaten binnen een domein vaststelt;
4. de D-CA, betreft een technische component die de feitelijke productie van certificaten voor de CSP's verricht.

Het overkoepelende overheidsniveau en het domeinniveau vormen de beleidsstructuur van de PKI. Binnen deze niveaus worden beleid en normen vastgesteld en wordt het toezicht georganiseerd.

Het CSP-niveau vormt het uitvoerend c.q. lokaal deel van de Staat der Nederlanden Root CA structuur waar de directe interactie met de gebruikers plaatsvindt. Op het CSP-niveau heeft de CSP-organisatie de eindverantwoordelijkheid voor het uitgeven van certificaten.

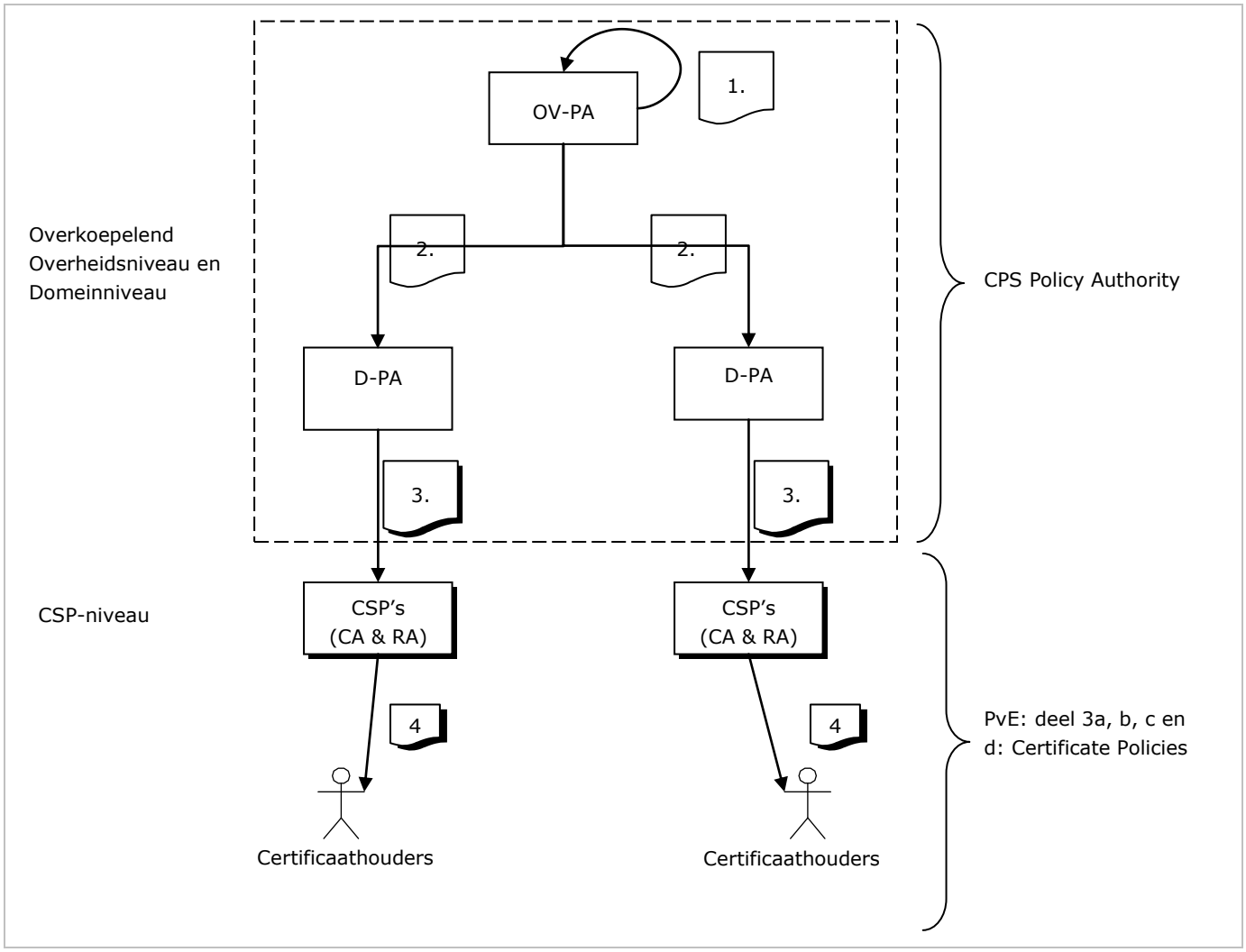
Het CSP-niveau vormt het operationele niveau waar de directe interactie met de gebruikers van de Staat der Nederlanden Root CA structuur plaatsvindt. Op het CSP-niveau heeft de CSP-organisatie de eindverantwoordelijkheid voor het uitgeven van certificaten. De certificaten van de CSP's zijn gegenereerd door de domein-CA's. Een en ander wordt geïllustreerd in onderstaand figuur 1. In deze figuur zijn ook de certificaten uit de centrale infrastructuur weergegeven, te weten het stamcertificaat (1), de domeincertificaten (2) en de CSP-certificaten (3). Zoals in het figuur is aangegeven beschrijft de CPS Policy Authority de procedures die de PA hanteert bij het uitgeven en beheren van de certificaten uit de centrale infrastructuur. In de volgende paragrafen worden de verschillende niveaus en componenten nader beschreven.

2.4.2 Overkoepelende Overheidsniveau en Domeinniveau

Het beheren van het gehele stelsel van afspraken en het regelen van het noodzakelijk toezicht zijn taken en verantwoordelijkheden van wat in PKI termen de PA (Policy Authority) heet. De PA PKIoverheid heeft een aantal taken binnen de de Staat der Nederlanden Root CA structuur, waarvan er hier een aantal belangrijke worden genoemd:

- het beheren van het normenkader (PvE), waarin de eisen voor ieder domein zijn opgenomen;
- het signaleren van consequenties en vereiste aanpassingen voor en van wet- en regelgeving;
- het beheren van de centrale deel van de Staat der Nederlanden Root CA structuur en het zorgen voor opname van partijen binnen de hiërarchie van de Staat der Nederlanden Root CA structuur;
- het handhaven van toezicht op de hiërarchie (CSP's);
- voorbereiding op het gebied van het toelaten van CSP's tot de de Staat der Nederlanden Root CA structuur;
- effectuering van de toelating van CSP's met inbegrip van creatie, uitgifte en beheer van CSP-certificaten;
- periodiek publiceren van de CRL’s voor de stam en domein certificaten van het centrale deel van de hiërarchie van PKIoverheid;
- periodiek publiceren van OCSP signing certificaten voor stam en domein certificaten van het centrale deel van de hiërarchie van PKIoverheid die moeten voldoen aan de Baseline Requirements van het CA/Browserforum;
- het volgen van de internationale standaardisatieontwikkelingen en zo nodig het initiatief nemen in deze ontwikkelingen evenals het

afstemmen met ontwikkelingen ten aanzien van PKI bij buitenlandse overheden.



Figuur 1

2.4.3 Beschrijving structuur Staat der Nederlanden EV Root CA

De structuur van de Staat der Nederlanden EV Root CA komt grotendeels overeen met de structuur van de Staat der Nederlanden Root CA G1 en G2.

Binnen het centrale deel van de structuur van de Staat der Nederlanden EV CA worden een aantal actoren onderscheiden. Deze actoren zijn:

1. de Overheids (Ov)-PA, op het hoogste niveau verantwoordelijk voor het vaststellen van het beleid en normen van algemene aard die gelden binnen de structuur van de Staat der Nederlanden EV Root CA en uitgifte van certificaten;
2. de Ov-CA, betreft een technische component die het hoogste (of Root-) certificaat produceert binnen de Staat der Nederlanden EV CA en certificaten produceert voor de onderliggende domein CA's;
3. de Intermediair I-CA, betreft een technische component die de feitelijke productie van certificaten voor de CSP's verricht.

Het overkoepelende overheidsniveau vormt de beleidsstructuur van de Staat der Nederlanden EV Root CA structuur. Binnen dit niveau worden beleid en normen vastgesteld en wordt het toezicht georganiseerd.

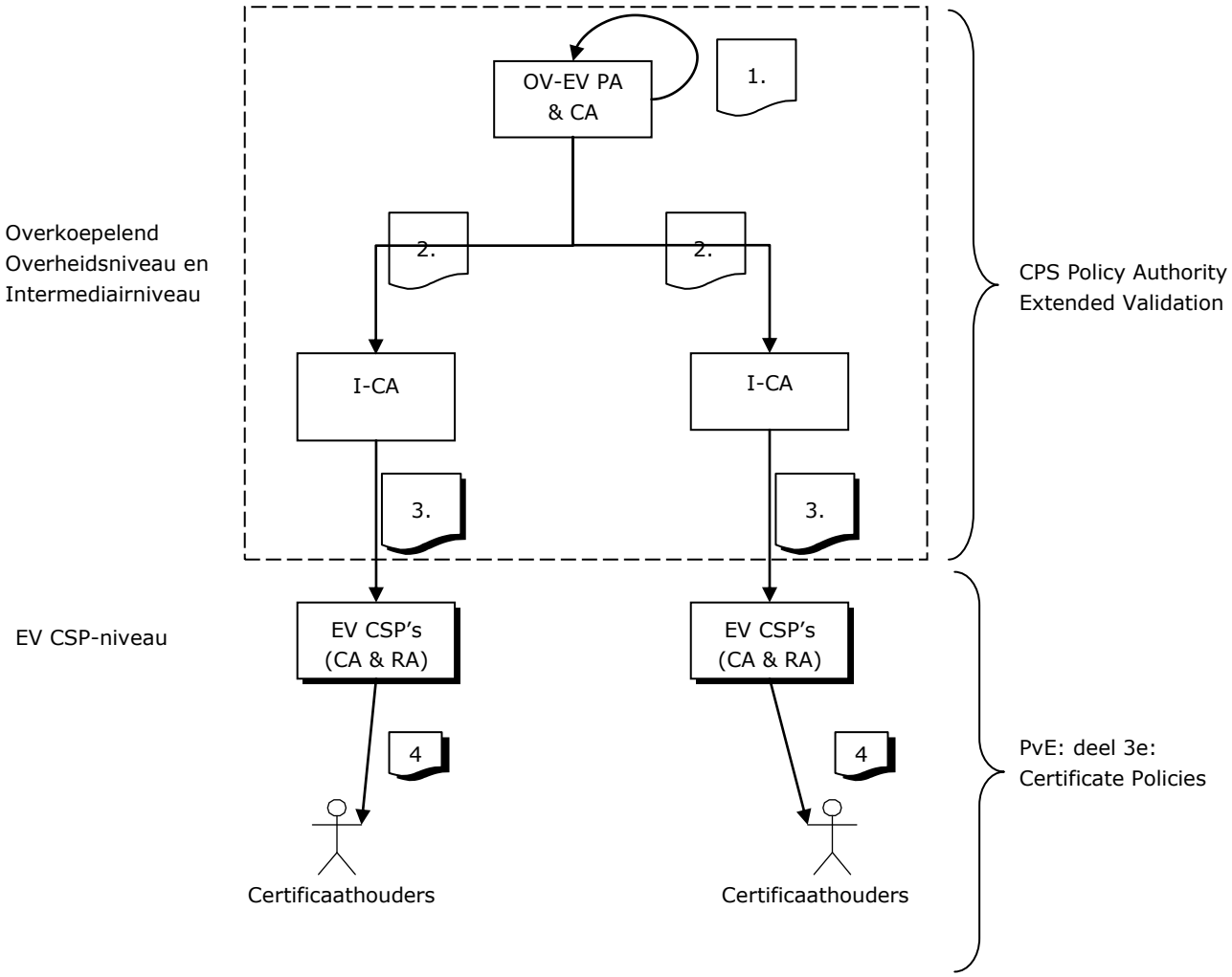
Het CSP-niveau vormt het uitvoerend c.q. lokaal deel binnen de Staat der Nederlanden EV Root CA structuur waar de directe interactie met de gebruikers plaatsvindt. Op het CSP-niveau heeft de CSP-organisatie de eindverantwoordelijkheid voor het uitgeven van EV SSL certificaten.

Het CSP-niveau vormt het operationele niveau waar de directe interactie met de gebruikers plaatsvindt. Op het CSP-niveau heeft de CSP-organisatie de eindverantwoordelijkheid voor het uitgeven van EV SSL certificaten. De certificaten van de CSP's zijn gegenereerd door de Staat der Nederlanden EV Intermediair CA. Een en ander wordt geïllustreerd in onderstaand figuur 2. In dit figuur zijn ook de certificaten uit de centrale infrastructuur weergegeven, te weten het Staat der Nederlanden EV Root CA (1), het Staat der Nederlanden EV Intermediair CA certificaat (2) en de EV CSP-certificaten (3). Zoals in het figuur is aangegeven beschrijft de CPS Policy Authority de procedures die de PA hanteert bij het uitgeven en beheren van de EV certificaten uit de centrale infrastructuur. In de volgende paragrafen worden de verschillende niveaus en componenten nader beschreven.

2.4.4 Overkoepelende Overheids- en Intermediairniveau

Het beheren van het gehele stelsel van afspraken en het regelen van het noodzakelijk toezicht zijn taken en verantwoordelijkheden van wat in PKI termen de PA (Policy Authority) heet. De PA PKIoverheid heeft een aantal taken binnen de structuur van de Staat der Nederlanden EV Root CA, waarvan er hier een aantal belangrijke worden genoemd:

- het beheren van het normenkader PvE deel 3e;
- het signaleren van consequenties en vereiste aanpassingen voor en van wet- en regelgeving;
- het beheren van de centrale deel van de structuur Staat der Nederlanden EV Root CA en het zorgen voor opname van partijen binnen de hiërarchie van de Staat der Nederlanden EV Root CA structuur;
- het handhaven van toezicht op de hiërarchie (CSP's);
- voorbereiding op het gebied van het toelaten van CSP's tot de Staat der Nederlanden EV Root CA structuur;
- effectuering van de toelating van CSP's met inbegrip van creatie, uitgifte en beheer van EV CSP CA certificaten;
- periodieke publicatie van de Staat der Nederlanden EV Root CA en de Staat der Nederlanden EV Intermediair CA CRL's;
- het volgen van de internationale standaardisatieontwikkelingen en zo nodig het initiatief nemen in deze ontwikkelingen alsmede het afstemmen met ontwikkelingen ten aanzien van PKI bij buitenlandse overheden.



Figuur 2

2.4.5 Operationeel niveau

CSP-niveau
Onder de centrale infrastructuur bevindt zich de laag waar, in termen van de Europese Richtlijn en de Nederlandse Wet, sprake is van een certificatiedienstverlener c.q. Certification Service Provider (CSP). De CSP is verantwoordelijk voor de uitgifte van certificaten aan eindgebruikers, zowel in de vorm van natuurlijke personen als overige eindentiteiten. De organisatie die de CSP-functie uitvoert is opgenomen in het certificaat in het veld "uitgever c.q. issuer". Binnen de PKI voor de overheid zijn meerdere CSP's actief op basis van de door de PA gestelde eisen.

RA
De RA is een deelactiviteit die binnen de verantwoordelijkheid van de CSP valt. In het RA-proces wordt de identiteit van de aanvrager van een certificaat gecontroleerd voordat het certificaat wordt uitgegeven. Het RA-proces bestaat uit de registratie van de aanvraag, de verificatie van de identiteit van de aanvrager en de uitgifte van het certificaat. De RA heeft een duidelijke relatie met een of meerdere CA's (bijvoorbeeld voor de verschillende typen certificaten): zij geeft opdracht aan de CA's voor de productie van certificaten.

CA
De CA is een deelactiviteit die onder de verantwoordelijkheid van de CSP wordt uitgevoerd. Na de registratie en de succesvolle verificatie moet het certificaat worden geproduceerd. De RA geeft hiertoe een opdracht aan de CA.

3 Betrouwbaarheid van de dienstverlening

3.1 Positionering eisen PKI voor de overheid

3.1.1 CSP-dienstverlening

Het normenkader van de PKI voor de overheid heeft betrekking op de dienstverlening van CSP's binnen de PKI voor de overheid. Dit normenkader is gebaseerd op:
A. eisen voortvloeiend uit (inter)nationale wetgeving;
B. eisen voortvloeiend uit internationale standaarden; en
C. PKIoverheid eisen.

De positionering van de eisen binnen de PKI voor de overheid is als volgt:

A. Leidend voor wat betreft de eisen waaraan binnen de PKI voor de overheid voldaan dient te worden (door CSP's) is de Wet elektronische handtekeningen (Wet EH) en bijbehorende regelgeving (met name het Besluit EH en de Regeling EH). De wet is alleen van toepassing op het gekwalificeerde certificaat.

B. Onder regie van EESSI is in internationaal verband een uitgebreid stelsel opgebouwd van standaarden met inhoudelijke eisen voor CSP's die PKI certificaten uitgeven. De eisen uit deze standaarden geven nadere specificaties voor artikelen uit het wettelijk kader. Het gaat hier om de standaard ETSI EN 319 411-2 waarin eisen staan voor uitgifte van gekwalificeerde certificaten, ETSI EN 319-411-3 waarin eisen staan voor uitgifte van niet-gekwalificeerde certificaten en ETSI TS 102 042 waarin eisen staan voor uitgifte van server en/of EV SSL certificaten.

C. De op grond van A. en B. geformuleerde eisen zijn op een aantal punten, voor wat betreft de PKI voor de overheid, onvoldoende expliciet geformuleerd. Daarom zijn deze eisen nader ingevuld in de vorm van PKIoverheid eisen. CSP's die PKIoverheid certificaten willen uitreiken dienen daarom ook aan deze eisen te voldoen.

   Hoewel de Wet EH, de standaard ETSI EN 319 411-2 en de PKIo-eisen specifiek zijn ontwikkeld voor het gekwalificeerde certificaat, is er vanuit het uitgangspunt van één betrouwbaarheidsniveau voor alle persoonsgebonden certificaten op één veilig middel, binnen de Staat der Nederlanden Root CA structuur voor gekozen dit betrouwbaarheidsniveau ook van toepassing te verklaren op het persoonsgebonden vertrouwelijkheidcertificaat en het authenticiteitcertificaat.

3.2 Vaststellen betrouwbaarheid

3.2.1 Toetreding en toezicht

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.

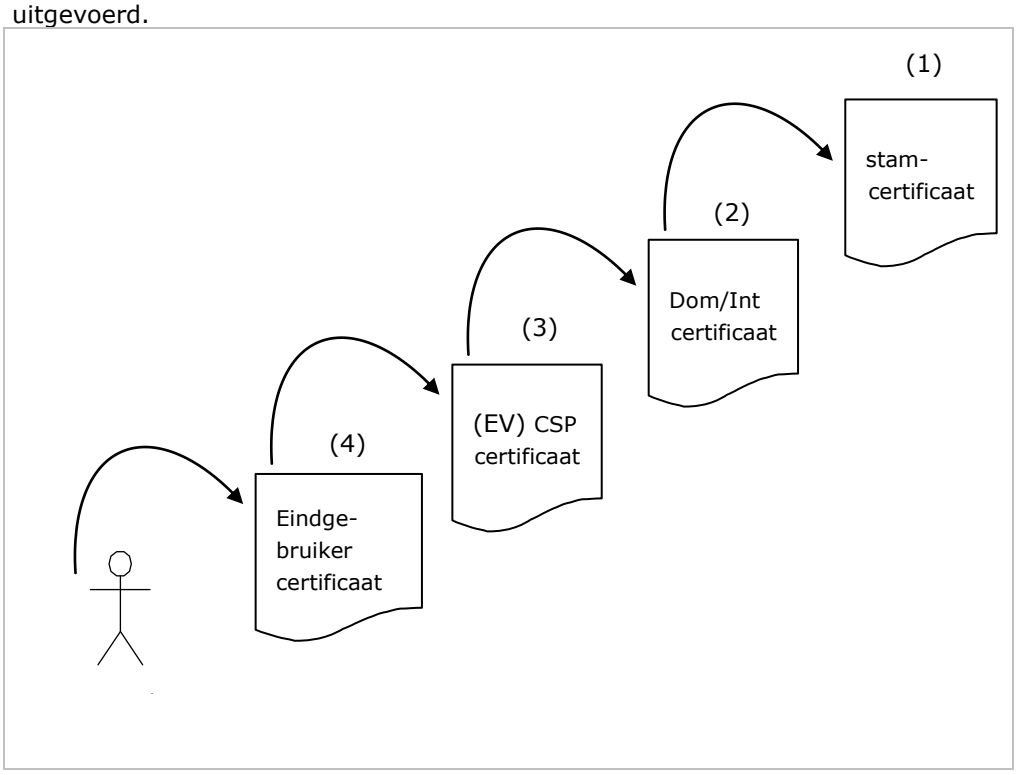
Om vast te stellen of de CSP voldoet aan de gestelde eisen en alle formaliteiten moet een formele toetredingsprocedure worden doorlopen. Hierin is beschreven welke conformiteitbewijzen moeten worden ingeleverd en welke kwaliteitscriteria voor de uitvoerende auditorganisaties van toepassing zijn. Hierbij is aansluiting gezocht bij reeds ontwikkelde, algemeen geaccepteerde normen en certificatieschema's.

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 PA toezicht op de toegetreden CSP's en moeten de CSP's periodiek conformiteitbewijzen inleveren.

De gehele toetredingsprocedure en de wijze waarop de PA toezicht houdt is beschreven in PvE deel 2 "Toetreding tot en Toezicht binnen de PKI voor de overheid".

3.2.2 Vertrouwensketen

Om als vertrouwende partij te kunnen vertrouwen op een eindgebruikercertificaat moeten een aantal controles worden uitgevoerd. De zogenaamde vertrouwensketen moet worden doorlopen. In figuur 3 is de vertrouwensketen van de PKI voor de overheid grafisch weergegeven. Vervolgens wordt aangegeven welke controlestappen dienen te worden uitgevoerd.



Figuur 3

Een vertrouwende partij heeft een certificaat van een ander (de certificaathouder) en wil zekerheid omtrent de betrouwbaarheid van dit certificaat. Een certificaat wordt geverifieerd door de volgende controles uit te voeren[5]:

- Is het bericht tijdens verzending niet gewijzigd, ofwel is de integriteit gewaarborgd?
- Is het gebruikte certificaat ingetrokken en op een zogenaamde "zwarte lijst" geplaatst?
- Is het certificaat nog geldig?

Vervolgens wordt door de software vastgesteld of het eindgebruikerscertificaat door een vertrouwde instantie is uitgegeven. Om deze laatste controle te kunnen uitvoeren, moet de software beschikken over het stamcertificaat van de Staat der Nederlanden. Wanneer het stamcertificaat niet aanwezig is, krijgt de gebruiker een foutmelding. Voor de reguliere root en de EV root heeft de PA ervoor gekozen om het stamcertificaat op te nemen in veelgebruikte besturingsystemen en OpenSource-browsers.

Wanneer software wordt gebruikt waarin het stamcertificaat niet is opgenomen in de truststore van applicaties zoals het geval is bij de private root van PKIoverheid, kan de vertrouwende partij het stamcertificaat op een betrouwbare wijze downloaden op https://cert.pkioverheid.nl.

Het CSP-certificaat is uitgegeven door de PA en kan worden gecontroleerd aan de hand van het domein/intermediaircertificaat. Dit laatste certificaat is ook uitgegeven door de PA en kan worden gecontroleerd aan de hand van het stamcertificaat. Het vertrouwen in een certificaat hangt daarom op elk niveau van de PKI voor de overheid af van het vertrouwen dat men stelt in de partij die het certificaat heeft uitgegeven. Vanuit het gezichtspunt van een vertrouwende partij is dat bij de eerste controlestap de CSP, bij de tweede stap de PA op het niveau van de domeinen of het Intermediair certificaat en ten slotte de PA op het hoogste niveau van de hiërarchie. Het stamcertificaat is dus het ankerpunt van vertrouwen in de hiërarchie van de PKI voor de overheid en bepaalt het vertrouwen dat in alle andere certificaten wordt gesteld die zijn uitgegeven binnen het PKIoverheid stelsel. Door het vertrouwen uit te spreken in het stamcertificaat, worden alle onderliggende domein- of intermediair-, CSP- en eindgebruikercertificaten vertrouwd. De gebruikers hoeven dus slechts één certificaat te vertrouwen. Een belangrijk aspect hierbij is het bepalen van de betrouwbaarheid van de uitgevende instantie van het certificaat.

3.2.3 Betrouwbaarheid uitgevende instantie

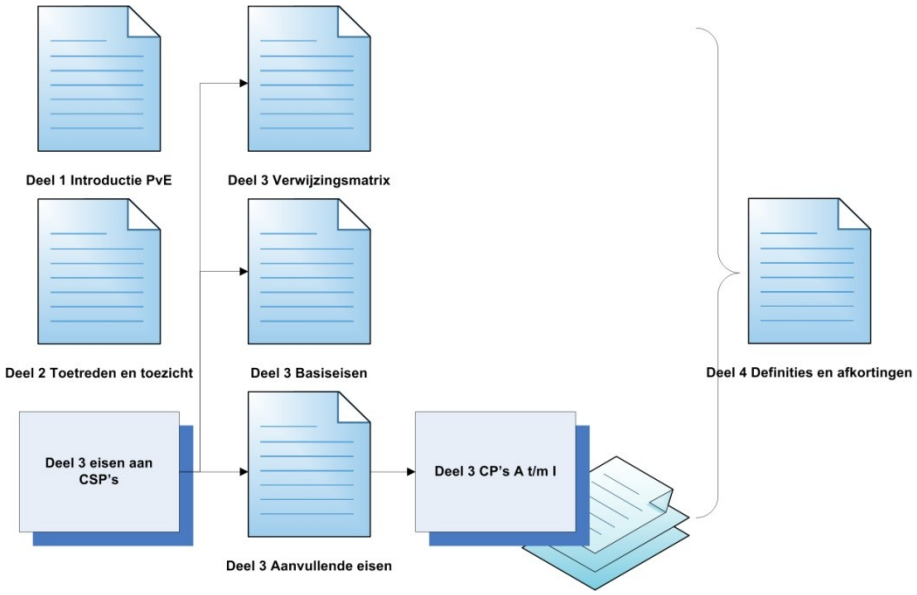
Om van een betrouwbare hiërarchie te kunnen spreken is het van groot belang dat de PA op een betrouwbare wijze functioneert. De PA waarborgt de betrouwbaarheid van de stamcertificaten en de domeincertificaten en het Intermediaircertificaat door adequate beveiligingsmaatregelen toe te passen. Deze beveiligingsmaatregelen evenals de wijze waarop de PA toezicht houdt op de CSP's zijn beschreven in de CPS van de PA. Door de CPS van de PA te beoordelen kan de vertrouwende partij vaststellen of hij/zij vertrouwt op een certificaat dat is uitgegeven binnenhet PKIoverheid stelsel. Door de hiërarchische opbouw wordt voorkomen dat een vertrouwende partij iedere CPS van de CSP's binnen de PKI voor de

[5] *Deze controles worden normaliter automatisch door de gebruikte applicatie uitgevoerd. De genoemde controles dienen voor ieder certificaat uit de vertrouwensketen te worden uitgevoerd.*

overheid in detail moeten gaan beoordelen. Ten slotte wordt het betrouwbaar functioneren van de PA periodiek vastgesteld door het laten uitvoeren van een audit door externe auditors.

4 Leeswijzer Programma van Eisen

In de navolgende figuur is de documentstructuur van het PvE weergegeven. Vervolgens is per deel een korte toelichting opgenomen.



Figuur 4: Documentstructuur Programma van Eisen

Deel 1: Introductie Programma van Eisen
In deel 1 is een introductie opgenomen op het PvE en de PKI voor de overheid in het algemeen. Tevens is aangegeven hoe de binnen de PKI voor de overheid geldende eisen zijn opgebouwd. Dit deel biedt vooral voor vertrouwende partijen, certificaathouders en proceseigenaren belangrijke informatie om inzicht te krijgen in de PKI voor de overheid en bijbehorend normenstelsel zonder dat diepgaande kennis van PKI is vereist.

Deel 2: Toetreding tot en Toezicht binnen de PKI voor de overheid
In het PvE zijn eisen vastgelegd waaraan CSP's moeten voldoen. In deel 2 wordt beschreven op welke wijze een CSP kan toetreden tot de PKI voor de overheid, conformiteit aan de eisen kan aantonen en aan welke formaliteiten moet worden voldaan. Tevens is beschreven op welke wijze de PA toezicht houdt op de toegetreden CSP's.

Deel 3: 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

Onder een Certificate Policy is het mogelijk meerdere typen certificaten uit te geven. Dit staat in het betreffende CP duidelijk aangegeven. Deel 3a maakt bijvoorbeeld onderscheid in authenticiteit-, vertrouwelijkheid- en onweerlegbaarheidcertificaten. Ieder CP bevat een bijlage met daarin het certificaatprofiel.

Deel 4: Definities en afkortingen
In deel 4 zijn de in het PvE gehanteerde definities en afkortingen toegelicht.

5 Revisies

5.1 Wijzigingen van versie 3.7 naar 4.0

5.1.1 Redactioneel

Verwijzing naar de private root en de nieuwe indeling van het PvE deel 3.

5.2 Wijzigingen van versie 3.6 naar 3.7

5.2.1 Redactioneel

Verwijzing naar versie 9.2 van het TTP.NL schema.

5.3 Wijzigingen van versie 3.5 naar 3.6

5.3.1 Aanpassingen

Er zijn wijzigingen doorgevoerd in verband met de introductie van het G3 stamcertificaat en de certificering tegen ETSI EN 319 411-2 binnen de PKI voor de overheid.

5.4 Wijzigingen van versie 3.4 naar 3.5

Geen wijzigingen.

5.5 Wijzigingen van versie 3.3 naar 3.4

Geen wijzigingen.

5.6 Wijzigingen van versie 3.2 naar 3.3

Geen wijzigingen.

5.7 Wijzigingen van versie 3.1 naar 3.2

Geen wijzigingen.

5.8 Wijzigingen van versie 3.0 naar 3.1

Geen wijzigingen.

5.9 Wijzigingen van versie 2.1 naar 3.0

5.9.1 Nieuw

De volgende paragrafen zijn nieuw in verband met de introductie van Extended Validation binnen de PKI voor de overheid:

- Paragraaf 2.3.3;
- Paragraaf 2.4.3;
- Paragraaf 2.4.4.

5.9.2 Aanpassingen

De volgende paragrafen zijn aangepast in verband met de introductie van Extended Validation binnen de PKI voor de overheid:

- Paragraaf 1.5;
- Paragraaf 2.3;
- Paragraaf 2.4, 2.4.1 en 2.4.2;
- Paragraaf 3.1.1;
- Paragraaf 3.2.2;
- Hoofdstuk 4.

5.9.3 Redactioneel

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

5.10 Wijzigingen van versie 2.0 naar 2.1

5.10.1 Redactioneel

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

5.11 Wijzigingen van versie 1.2 naar 2.0

5.11.1 Nieuw

De volgende paragrafen zijn nieuw in verband met de introductie van het Domein Autonome Apparaten binnen de PKI voor de overheid:

- Paragraaf 2.3.3.

5.11.2 Aanpassingen

De volgende paragrafen zijn aangepast in verband met de introductie van het Domein Autonome Apparaten binnen de PKI voor de overheid:

- Paragraaf 2.3;
- Paragraaf 2.5.1;
- Hoofdstuk 3.

5.11.3 Redactioneel

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

5.12 Wijzigingen van versie 1.1 naar 1.2

5.12.1 Nieuw

De volgende paragrafen zijn nieuw in verband met de creatie van de Staat der Nederlanden Root CA – G2 binnen de PKI voor de overheid:

- Paragraaf 2.4.

5.12.2 Aanpassingen

- Paragraaf 2.2;
- Paragraaf 2.4.2;
- Hoofdstuk 4.

5.12.3 Redactioneel

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

5.13 Wijzigingen van versie 1.0 naar versie 1.1

Geen wijzigingen.

5.14 Versie 1.0

Eerste versie.