Certification Practice Statement PKIoverheid

KPN Corporate Market B.V.

KPN Corporate Market BV
Fauststraat 1
7323 BA Apeldoorn
Postbus 9105
7300 HN Apeldoorn
T +31 (0) 31 08 86 61 00 00
www.kpn.com/corporatemarket/
K.v.K. Amsterdam nr. 52959597
NL850684481B01

Datum	15 oktober 2011
Plaats	Apeldoorn
Redacteur	Henk Dekker
Functie	Security Process consultant
Versie	versie 4.12

Inhoudsopgave

1 Introductie op het Certification Practice Statement

De PKI voor de overheid, kortweg PKIoverheid, is een afsprakenstelsel voor het mogelijk maken van het generiek en grootschalig gebruik van de Elektronische Handtekening, identificatie op afstand en vertrouwelijke elektronische communicatie . Alle afspraken zijn beschreven in het Programma van Eisen (Logius).

Binnen de PKIoverheid opereert KPN Corporate Market B.V.als Certificatiedienstverlener (of CSP). In navolgende wordt steeds gesproken over KPN. Hiermee wordt bedoeld KPN als Certificatiedienstverlener, als onderscheid met de andere diensten die KPN levert. Als bedoeld wordt KPN Corporate Market B.V., dan wordt die benaming expliciet gebruikt.

Één van de eisen in het Programma van Eisen is dat elke Certificatiedienstverlener binnen de PKIoverheid zijn practices beschrijft in een zogenaamd Certification Practice Statement (verder: CPS).

Het nu voorliggende document is het CPS van KPN. Dit document beschrijft de practices van KPN. Dit hoofdstuk bevat een introductie op dit CPS – document. Het behandelt in het kort een aantal belangrijke aspecten van dit document.

1.1 Overview

De indeling van deze CPS is zoveel mogelijk conform de RFC3647 standaard (voluit: 'Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework') van de Internet Engineering Task Force). Voor meer informatie zie http://www.ietf.org.

1.1.1 Doelgroep en leeswijzer

De primaire doelgroep van dit CPS wordt gevormd door:

- Abonnees van KPN.
- Contactpersonen van de Abonnee.
- Certificaathouders en Certificaatbeheerders van de Abonnee.
- Vertrouwende Partijen.

1.1.2 Doel van het CPS

Het CPS is de beschrijving van de wijze waarop KPN haar certificatiedienstverlening in het domein Overheid/Bedrijven en Organisatie van de PKIoverheid vorm geeft. Het CPS bevat onder meer een beschrijving van de procedures die KPN hanteert bij de aanmaak, de uitgifte en het intrekken van PKIoverheid Certificaten.

1.1.3 Verhouding tussen CP en CPS

De CP beschrijft welke eisen er aan uitgifte en gebruik van een Certificaat binnen het Domein Overheid/Bedrijven en Organisatie van de PKIoverheid worden gesteld. Deze CP, Certificate Policy – Domeinen Overheid/Bedrijven, is opgesteld en wordt onderhouden door de Policy Authority van de PKIoverheid en maakt onderdeel uit (deel 3a en 3b) van het Programma van Eisen van de PKIoverheid (http://www.logius.nl/pkioverheid).

Deel 3a van Programma van Eisen (PvE) heet voluit Certificate Policy – Domein Overheid/Bedrijven en Organisatie. Deel 3b heet voluit Certificate Policy – Services, Bijlage bij CP Domeinen Overheid/Bedrijven en Organisatie.

Ter toelichting: in de titel van beide CP's is sprake van twee domeinen, zijnde het domein Overheid en Bedrijven en het domein Organisatie. Feitelijk zijn dit dezelfde domeinen. Het domein Overheid en Bedrijven, zoals dat wordt genoemd onder de SHA-1 root, is echter door de Overheid Policy Authority met de invoering van de SHA-2 root hernoemd in domein Organisatie. Voor meer details hierover wordt verwezen naar PvE deel 1 Introductie Programma van Eisen, paragraaf 2.4 Inrichting PKIoverheid.
In dit document en op de klantformulieren zal steeds de term 'domein Overheid/Bedrijven en Organisatie' worden gebruikt. Dit gebeurt om aan te geven dat KPN SHA-2 certificaten uitgeeft in het domein Organisatie en nog tot 31 december 2011 SHA-1 (server)certificaten in het domein Overheid/Bedrijven .

Het CPS beschrijft op welke wijze KPN invulling geeft aan deze eisen en daarmee aan deze eisen tegemoet komt.

1.1.4 Positionering van het CPS

Alle typen Certificaten die door de KPN worden uitgegeven, hebben hetzelfde betrouwbaarheidsniveau, conform het Programma van Eisen van PKIoverheid. Om die reden is het CPS op alle Certificaten volledig van toepassing.

1.1.5 Status

De datum, waarop de geldigheid van dit CPS start, staat vermeld op het titelblad van dit CPS. De CPS is geldig voor zolang als de KPN dienstverlening voortduurt, dan wel totdat het CPS wordt vervangen door een nieuwere versie (aan te duiden in het versienummer met +1 bij ingrijpende wijzigingen en +0.1 bij redactionele aanpassingen).

1.2 Documentnaam en Identificatie

Formeel wordt dit document als volgt aangeduid: 'Certification Practice Statement PKIoverheid'. In het kader van dit document wordt ze ook wel aangeduid als 'PKIoverheid CPS' maar meestal kortweg als 'CPS'. Daar waar van die afkorting sprake is, wordt dit document bedoeld.

Dit CPS kan via de volgende Object Identifier (OID) worden geïdentificeerd: 2.16.528.1.1005.1.1.1.2

1.3 Gebruikersgemeenschap

De gebruikersgemeenschap binnen het domein Overheid/Bedrijven en Organisatie bestaat enerzijds uit Certificatiedienstverleners en anderzijds uit Abonnees, organisatorische entiteiten binnen overheid en bedrijfsleven, Certificaathouders, Certificaatbeheerders en Vertrouwende Partijen. Tevens zijn er beroepsbeoefenaars die zowel Abonnee als Certificaathouder zijn. Voor een beschrijving van deze begrippen wordt verwezen naar paragraaf 1.7 Definities en afkortingen.

Het Programma van Eisen van PKIoverheid (deel 3a en 3b) is op deze gebruikersgemeenschap van toepassing. In het verlengde daarvan zijn ook de KPN Bijzondere Voorwaarden PKIoverheid

Certificaten (verder: Bijzondere Voorwaarden) van toepassing. Zie daarvoor de Elektronische Opslagplaats van KPN, http://www.pki.getronics.nl/website.

De Bijzonder Voorwaarden zijn bindend voor alle bij de certificatiedienstverlening betrokken partijen. In geval van strijd tussen het CPS en de Bijzonder Voorwaarden genieten laatstgenoemde voorrang.

1.4 Certificaatgebruik

De certificaten die KPN uitgeeft, worden uitgegeven in overeenstemming met het Programma van Eisen van PKIoverheid (deel 3a en 3b).

1.4.1 Certificaatgebruik (PvE PKIoverheid deel 3a)

Binnen het domein Overheid/Bedrijven en Organisatie, PvE PKIoverheid deel 3a, geeft KPN een drietal soorten Certificaten namens Abonnees uit aan Certificaathouders. Deze certificaten hebben elk een eigen functie, hebben ook elk een eigen policy. Deze policies worden uniek geïdentificeerd door een OID. Het betreft:

1. Handtekeningcertificaten
2. Authenticiteitcertificaten
3. Vertrouwelijkheidcertificaten

Handtekeningcertificaten (ook wel genoemd Gekwalificeerde Certificaten, zoals beschreven in de Weh, en ook wel genoemd Onweerlegbaarheidscertificaten) zijn bedoeld om elektronische documenten te voorzien van een Gekwalificeerde Elektronische Handtekening [domein Overheid/Bedrijven OID 2.16.528.1.1003.1.2.2.2, domein Organisatie OID 2.16.528.1.1003.1.2.5.2]. Deze Gekwalificeerde Elektronische Handtekening, de Elektronisch Handtekening gebaseerd op een Gekwalificeerd Certificaat en die door een Veilig Middel (Secure Signature Creation Device, SSCD) is aangemaakt, voldoet aan alle wettelijke vereisten voor een handtekening en heeft dezelfde rechtskracht als een handgeschreven handtekening heeft voor papieren documenten.

Authenticiteitcertificaten zijn bedoeld voor het langs elektronische weg betrouwbaar identificeren en authenticeren van personen, organisaties en middelen. Dit betreft zowel de identificatie van personen onderling als tussen personen en middelen [domein Overheid/Bedrijven OID 2.16.528.1.1003.1.2.2.1, domein Organisatie OID 2.16.528.1.1003.1.2.5.1]. Authenticiteitcertificaten zijn geen Gekwalificeerde Certificaten.

Vertrouwelijkheidcertificaten zijn bedoeld voor het beschermen van de vertrouwelijkheid van gegevens die in elektronische vorm worden uitgewisseld en/of opgeslagen. Dit betreft zowel de uitwisseling van gegevens tussen personen onderling als tussen personen en geautomatiseerde middelen [domein Overheid/Bedrijven OID 2.16.528.1.1003.1.2.2.3, domein Organisatie OID 2.16.528.1.1003.1.2.5.3]. Ook Vertrouwelijkheidcertificaten zijn geen Gekwalificeerde Certificaten.

Deze 3 soorten certificaten worden uitgegeven als Beroepsgebonden Certificaten en als Persoonsgebonden Certificaten (feitelijk Organisatiegebonden, als onderscheid t.o.v. Beroepsgebonden). Zie voor de definities 1.7 Definities en afkortingen.

1.4.2 Certificaatgebruik (PvE PKIoverheid deel 3b)

Binnen het domein Overheid/Bedrijven en Organisatie, PvE PKIoverheid deel 3b, geeft KPN ook een drietal soorten certificaten uit aan Abonnees. Deze certificaten hebben elk een eigen functie, hebben ook een eigen policy. Deze policy wordt uniek geïdentificeerd door een OID. Het betreft:

1. Authenticiteitcertificaten;

2. Vertrouwelijkheidcertificaten;
3. Servercertificaten.

Authenticiteitcertificaten zijn bedoeld voor het langs elektronische weg betrouwbaar identificeren en authenticeren van een service als behoren bij de organisatorische entiteit, die verantwoordelijk is voor de betreffende service [domein Overheid/Bedrijven OID 2.16.528.1.1003.1.2.2.4, domein Organisatie OID 2.16.528.1.1003.1.2.5.4].

Vertrouwelijkheidcertificaten zijn bedoeld voor het beschermen van de vertrouwelijkheid van gegevens, die worden uitgewisseld in elektronische vorm [domein Overheid/Bedrijven OID 2.16.528.1.1003.1.2.2.5, domein Organisatie OID 2.16.528.1.1003.1.2.5.5].

Servercertificaten zijn bedoeld voor gebruik, waarbij de vertrouwelijkheidsleutel niet wordt gebruikt om de gegevens te versleutelen, maar enkel tot doel heeft om de verbinding te versleutelen tussen een bepaalde client en een server [domein Overheid/Bedrijven OID 2.16.528.1.1003.1.2.2.6, domein Organisatie OID 2.16.528.1.1003.1.2.5.6]. Deze server moet behoren bij de organisatorische entiteit die als Abonnee wordt genoemd in het betreffende certificaat.

Deze 3 soorten certificaten worden uitgegeven als Services Certificaten (feitelijk Organisatiegebonden, als onderscheid t.o.v. Beroepsgebonden). Het Authenticiteitcertificaat en het Vertrouwelijkheidcertificaat worden samen het Groepscertificaat genoemd. Zie voor de definities 1.7 Definities en afkortingen.

1.5 CA-model

In de hierarchie van PKIoverheid is de Staat der Nederlanden Root CA de hoogste CA. Deze CA is eigendom van PKIoverheid en is een self-signed CA. Onder deze SHA-1 Root CA staan twee domein CA's gepositioneerd, dit betreft domein CA's voor het domein Burger en het domein Overheid/Bedrijven. Onder de SHA-2 Root CA staan 3 domein CA's gepositioneerd. Het betreft het domein Burger, domein Organisatie en domein Autonome Apparaten.
De domein CA's zijn getekend door de Root CA en tekenen op hun beurt weer de CA's van de in het betreffende domein opererende CSP, waaronder die van KPN.

Voorgaande staat volledig beschreven in Programma van Eisen van PKIoverheid (deel 1, Introductie Programma van Eisen). Zowel de Root CA's als de domein CA's worden beheerd door PKIoverheid. Een beschrijving van het beheer van deze CA's kan teruggevonden worden in het CPS Policy Authority PKIoverheid voor certificaten uit te geven door de Policy Authority van de PKIoverheid. Beide documenten zijn terug te vinden op http://www.logius.nl/producten/toegang/pkioverheid.

1.6 Beheer van het CPS

Het CPS van KPN wordt beheerd door een specifiek daartoe geïnstalleerde Policy Management Authority (PMA). Informatie met betrekking tot dit CPS en commentaar daarop kan worden gericht aan:

KPN
T.a.v. KPN Trusted Services, Policy Management Authority
Postbus 9105
7300 HN Apeldoorn
pkisupport@kpn.com

Commerciële vragen betreffende PKIoverheid Certificaten en daarmee verwante dienstverlening kunnen worden gericht aan: pkisales@kpn.com.

Overige documenten die verband houden met de dienstverlening rondom PKIoverheid Certificaten van KPN zijn te vinden in de Elektronische Opslagplaats.

De PKIoverheid Certificaten zijn een dienst van KPN. Voor meer informatie over KPN, wordt verwezen naar de Elektronische Opslagplaats. De onderhavige dienst werd voorheen in de markt gezet onder de naam 'Getronics PinkRoccade CPS' door Getronics PinkRoccade een onderdeel van Getronics NV.

1.7 Samenwerking met het Ministerie van Veiligheid en Justitie

KPN heeft met het Ministerie van Veiligheid en Justitie (verder: het Ministerie) een samenwerkingsovereenkomst inzake certificatiedienstverlening gesloten. Binnen die overeenkomst besteedt KPN de RA-werkzaamheden uit aan het Ministerie voor de certificaataanvragen die door of namens het Ministerie worden ingediend. Het Ministerie heeft daartoe een RA-kantoor ingericht. In het kort komt het er op neer dat het Ministerie de certificaataanvragen die door of namens het Ministerie worden ingediend zelf behandeld. Het Ministerie neemt de aanvragen in ontvangst, registreert deze, beoordeelt de juistheid en de volledigheid van de aanvraag en beslist over de aanvraag. KPN blijft de CA-werkzaamheden uitvoeren, KPN maakt de certificaten aan, plaatst deze, indien van toepassing, op SSCD/SUD's en verstuurt de certificaten naar het Ministerie. Het Ministerie verzorgt de uitgifte van de certificaten, inclusief de identificatie van certificaatbeheerders en certificaathouders. KPN verzorgt, na melding van ontvangst van de SSCD/SUD's op het RA-kantoor de verzending van o.a. de intrekkingsgegevens.
De specifieke practices van het Ministerie, specifiek voorzover ze afwijken van de KPN practices, zijn beschreven in bijlage 1 van dit CPS.

1.8 Samenwerking met CreAim b.v.

KPN heeft met CreAim b.v. (verder: CreAim) een samenwerkingsovereenkomst inzake certificatiedienstverlening gesloten. Binnen die overeenkomst besteedt KPN de volgende activiteiten uit aan CreAim.

- identificatie van de aanvragers van beroepsgebonden certificaten (leden van de beroepsgroepen NIvRA en NOVAA) en de overdracht van deze beroepsgebonden certificaten aan die NIvRA en NOvAA-leden; .
- identificatie van aanvragers en de overdracht van deze certificaten aan deze aanvragers van persoonsgebonden certificaten.

De specifieke CreAim-practices, specifiek voorzover ze afwijken van de KPN practices, zijn beschreven in bijlage 2 van dit CPS.

1.9 Definities en afkortingen

Voor een overzicht van de gebruikte definities en afkortingen wordt verwezen naar respectievelijk de bijlagen 1 en 2.

2 Verantwoordelijkheid voor Publicatie en Elektronische Opslagplaats

2.1 Elektronische opslagplaats

KPN zorgt voor de beschikbaarheid van relevante informatie in de Elektronische Opslagplaats (http://www.pki.getronics.nl/website/).

2.2 Publicatie van CSP-informatie

Via de Elektronische Opslagplaats is tenminste het volgende online beschikbaar:

1. Stamcertificaat;
2. certificaatstatusinformatie;
   a. in de CRL;
   b. in de Directory Dienst (zie 7);
   c. met behulp van OCSP;
3. Bijzonder Voorwaarden;
4. CPS;
5. Certificate Policy – Domein Overheid/Bedrijven en Organisatie (PvE deel 3a);
6. Certificate Policy – Services. Bijlage bij CP Domein Overheid/Bedrijven en Organisatie (PvE deel 3b);
7. Directory Dienst;
8. Afschriften van het (volledige) ETSI TS 101 456-certificaat van KPN en de ETSI TS 101 456 deelcertificaten die KPN heeft verworven ten behoeve van en samen met andere Certificatiedienstverleners.

2.3 Publicatie van het Certificaat

Certificaten worden gepubliceerd met behulp van een Directory Dienst. Via de Directory Dienst kan het Certificaat worden geraadpleegd door Abonnees, Certificaatbeheerders, Certificaathouders en Vertrouwende Partijen.

De Directory Dienst is op adequate wijze beveiligd tegen manipulatie en is online toegankelijk. Informatie over de intrekkingstatus is vierentwintig uur per dag en zeven dagen per week te raadplegen.

Het ETSI TS 101 456-certificaat van KPN Corporate Market B.V.wordt, evenals de ETSI TS 101 456 deelcertificaten, gepubliceerd in de elektronische opslagplaats. De betreffende certificaten geven aan dat KPN Corporate Market B.V. voldoet aan ETSI TS 101 456 Policy requirements for certification authorities issuing qualified certificates en daarmee aan de eisen van de Weh. De auditrapportages betrekking hebbende op de normatieve referenties van KPN Corporate Market B.V.zijn ingevolge haar security policy niet in de Elektronische Opslagplaats opgeslagen.

2.4 Tijdstip of frequentie van publicatie

Wijzigingen in CSP-informatie worden, behalve het navolgende in deze paragraaf, gepubliceerd op het moment dat ze zich voordoen of zo spoedig mogelijk daarna en met inachtneming van de bepalingen die daarvoor gelden. Zie bijvoorbeeld daarvoor paragraaf 9.12 Wijzigingen.

De publicatie van Certificaten vindt plaats onmiddelijk na productie. De CRL wordt 1x per 4 uur vernieuwd.

2.5 Toegang tot gepubliceerde informatie

Informatie in de Elektronische Opslagplaats is publiek van aard en vrij toegankelijk. De Elektronische Opslagplaats kan vierentwintig uur per dag en zeven dagen per week worden geraadpleegd.
De Elektronische Opslagplaats is beschermd tegen het aanbrengen van ongeautoriseerde wijzigingen.

Voor het geval van het optreden van systeemdefecten of andere factoren die de beschikbaarheid van de Elektronische Opslagplaats negatief beïnvloeden is er een passende set van continuïteitsmaatregelen gerealiseerd om ervoor te zorgen dat de CRL binnen 4 uur en de overige onderdelen van de Elektronische Opslagplaats binnen 24 uur weer bereikbaar zijn. Een voorbeeld van een dergelijke maatregel is het hebben gerealiseerd van een uitwijklocatie en -scenario in combinatie met het regelmatig testen van de functionaliteit ervan.

KPN is niet verantwoordelijk voor de niet-beschikbaarheid van de Elektronische Opslagplaats vanwege omstandigheden waar KPN niet verantwoordelijk voor kan worden gehouden.

3 Identificatie en authenticatie

Deze paragraaf beschrijft op welke wijze de identificatie en authenticatie van certificaataanvragers plaatsvindt tijdens de initiële registratieprocedure en welke criteria KPN stelt ten aanzien van de naamgeving.

3.1 Naamgeving

3.1.1 Soorten naamformaten

De in Certificaten gebruikte namen voldoen aan de X.501 naam standaard. De namen bestaan uit de volgende onderdelen:

Attribuut	Waarde
Country (C)	NL
Organization (O)	Naam van de Abonnee
Common Name (CN)	Volledige naam van de Certificaathouder
Subjectserienummer (SN)	Subjectserienummer van de Certificaathouder

De in Servercertificaten en Groepscertificaten gebruikte namen voldoen aan de X.501 naam standaard. De namen bestaan uit de volgende onderdelen:

Attribuut	Waarde
Country (C)	NL
Organization (O)	Naam van de Abonnee
Common Name (CN)	Naam van de Certificaathouder
Optioneel:	
Organizational Unit (OU)	Afdeling van de organisatie van Abonnee
State or Province (S)	Provincie waar de Abonnee gevestigd is
Locality (L)	Plaats waar de Abonnee gevestigd is

3.1.2 Noodzaak van betekenisvolle namen

Geen nadere bepalingen.

3.1.3 Anonimiteit of pseudonimiteit van certificaathouders

Het gebruik van pseudoniemen is binnen de PKIoverheid niet toegestaan.

3.1.4 Regels voor interpretatie van verschillende naamformaten

Namen van personen opgenomen in het Certificaat voldoen aan de eisen zoals verwoord in Programma van Eisen, deel 3a Certificate Policy - Domein Overheid/Bedrijven en Organisatie, BIJLAGE A Profielen Certificaten en certificaatstatusinformatie.

Alle namen worden in principe exact overgenomen uit de overlegde identificatiedocumenten. Het kan echter zijn dat in de naamgegevens bijzondere tekens voorkomen die geen deel uitmaken van de standaard tekenset conform ISO8859-1 (Latin-1). Als in de naam tekens voorkomen die geen deel uitmaken van deze tekenset, zal KPN een transitie uitvoeren. KPN behoudt zich het recht voor om bij registratie de aangevraagde naam aan te passen als dit juridisch of technisch noodzakelijk is.

3.1.5 Uniciteit van namen

De gebruikte namen identificeren de Certificaathouder op unieke wijze. Uniciteit van namen binnen de X.501 name space is daarbij het uitgangspunt.

KPN voorziet erin dat de uniciteit van het ‘subjectaltname’-veld wordt gewaarborgd. Dit betekent dat de onderscheidende naam die is gebruikt in een uitgegeven certificaat, nooit kan worden toegewezen aan een ander subject. Dit gebeurt door middel van het opnemen van een uniek subjectserienummer in dat veld.
Voor Persoonsgebonden Certificaten en Groepscertificaten genereert KPN hiertoe zelf een nummer. In het geval van een Servercertificaat wordt hiervoor het CSR-nummer gebruikt.

In specifieke gevallen, indien daartoe expliciete afspraken over zijn gemaakt, kan er een specifiek nummer aan dit subjectserienummer worden toegevoegd.

3.1.6 Geschillenbeslechting inzake naam claims

In gevallen waarin partijen het oneens zijn over het gebruik van namen, beslist KPN na afweging van de betrokken belangen, voorzover hierin niet wordt voorzien door dwingend Nederlands recht of overige toepasselijke regelgeving.

3.1.7 Erkenning, authenticatie en de rol van handelsmerken

Abonnees dragen de volledige verantwoordelijkheid voor eventuele juridische gevolgen van het gebruik van de door hen opgegeven naam.

De naam van een organisatorische entiteit zoals deze wordt genoemd in het uittreksel van een erkend register, dan wel in de wet of het besluit waarbij de organisatorische entiteit is ingesteld, wordt gebruikt in het Certificaat.

KPN is niet gehouden een onderzoek in te stellen naar mogelijke inbreuken op handelsmerken die ontstaan als gevolg van het gebruik van een naam die deel uitmaakt van de in het Certificaat opgenomen gegevens.

KPN heeft het recht wijzigingen aan te brengen in naamattributen wanneer deze in strijd blijken met een handelsmerk of met andere rechten van intellectueel eigendom.

3.2 Initiële identiteitsvalidatie

3.2.1 Methode om bezit van Private Sleutel aan te tonen

Het sleutelpaar, waarvan de Publieke Sleutel wordt gecertificeerd, wordt aangemaakt door KPN.

Dit geldt echter niet voor het Servercertificaat. Het sleutelpaar voor het Servercertificaat wordt door of namens de Abonnee aangemaakt in de Veilige Omgeving van de Abonnee en ingevoerd op de (HTTPS) website van KPN. De Abonnee tekent op de Certificaataanvraag voor het Servercertificaat ervoor dat dat ook inderdaad gebeurd is.

Zie verder 3.2.3.3 Authenticatie ten behoeve van Servercertificaten en 6.2.11 Eisen voor veilige middelen voor opslag en gebruik van certificaten.

3.2.2 Authenticatie van de Abonnee

Als een organisatie Abonnee wil worden van KPN dient het het daartoe bestemde formulier Abonnee Registratie in te vullen. Bij dit formulier is een uitgebreide toelichting gevoegd. Met het formulier dient de Abonnee een aantal bewijsstukken mee te sturen.

De gegevens die opgevraagd worden zijn:

- naam van de abonnee. De Abonnee kan, indien gewenst, gebruik maken van een handelsnaam, mits deze geregistreerd is;
- naam en functie van diens bevoegd vertegenwoordiger;
- indien een organisatie wil deelnemen aan de digitale diensten van de overheid, zoals Digikoppeling en Digipoort: het OverheidsIdentificatieNummer (voor overheidsorganisaties) of Kamer van Koophandel nummer uit het Nieuwe Handelsregister (voor private organisaties);
- bereikbaarheidsgegevens;
- gegevens van de te autoriseren contactpersoon, zoals diens naam en bereikbaarheidsgegevens.

Het formulier Abonnee Registratie moet worden ondertekend door de Bevoegd Vertegenwoordiger van de Abonnee. Met ondertekening geeft de Bevoegd Vertegenwoordiger aan

- de Certificaataanvraag juist, volledig en naar waarheid te hebben ingevuld,
- akkoord te gaan met de Bijzonder Voorwaarden en
- dat de op het formulier genoemde contactpersoon of contactpersonen geautoriseerd, vertrouwd en ter zake kundig zijn om namens de Abonnee certificaten te mogen aanvragen, installeren, beheren en , indien nodig, in te trekken.

Tevens moet de contactpersoon of contactpersonen het formulier Abonnee Registratie voorzien van een handtekening. Deze handtekening dient om de autorisatie van de contactpersoon tot het indienen van aanvragen te kunnen verifiëren.

De handtekening moet een rechtsgeldige handtekening zijn, het moet dus een handgeschreven of een elektronische handtekening zijn. De elektronische handtekening moet voldoen aan de Wet elektronische handtekeningen. Als de elektronische handtekening wordt gezet namens een organisatie (Abonnee) dient het Gekwalificeerde Certificaat waarmee de elektronische handtekening wordt aangemaakt tevens te zijn uitgegeven aan de Certificaathouder namens dezelfde Abonnee binnen het domein Overheid/Bedrijven en Organisatie de PKIoverheid.

In het navolgende wordt de term ‘Abonnee’ gebruikt. Als een Abonnee een activiteit moet uitvoeren, doet de/een contactpersoon dat in zijn algemeenheid namens de Abonnee. Dat wordt echter niet expliciet aangegeven.

De bewijzen die tegelijk met het formulier aangeleverd moeten worden betreffen:

- het bestaan van de organisatie en de juistheid en volledigheid van diens naam;
- indien een overheidsorganisatie gebruik wil maken van Digikopppeling: een uittreksel uit het DigikoppelingServiceregister;
- de bevoegdheid van de Bevoegde Vertegenwoordiger om de Abonnee te vertegenwoordigen;
- kopie van het identiteitsbewijs van de Bevoegd Vertegenwoordiger dat voldoet aan de eisen uit de Wet op de identificatieplicht (verder: Wid) indien de Bevoegde Vertegenwoordiger de aanvraag voorziet van een handgeschreven handtekening;
- kopie van het identiteitsbewijs van elke Contactpersoon die op het formulier wordt geautoriseerd. Ook dit identiteitsbewijs moet voldoen aan de eisen van de Wid.

Voor gemeenten die in het kader van een gemeentelijke herindeling gaan ontstaan, maar op het moment van de abonnee-aanvraag nog niet bestaan, is het nu ook mogelijke een abonnement aan te vragen. Deze (nieuwe) gemeenten dienen bij de aanvraag aan te tonen dat ze gaan bestaan per een bepaalde datum. Dat kan bijvoorbeeld door een kopie van de wet mee te sturen waarin de betreffende gemeentelijke herindeling is geregeld. Deze gemeenten kunnen na goedkeuring van de abonnee-aanvraag Servercertificaten aanvragen. Na goedkeuring van de certificaataanvraag zullen de aangevraagde certificaten worden uitgegeven onder de beperkende voorwaarde dat de Servercertificaten pas gebruikt worden op of na de datum dat de (nieuwe) gemeente is gaan bestaan.

Indien een beoefenaar van een Erkend Beroep Abonnee wil worden van KPN dient hij/zij het daartoe bestemde formulier Aanvraag beroepsgebonden Certificaten in te vullen. In dit formulier is het aanvragen van een abonnement en Certificaten samengevoegd in één formulier. Dit formulier is terug te vinden op http://www.pki.getronics.nl/website/getronics/401/PKIoverheid+formulieren.html. Dit omdat Abonnee en Certificaathouder één en dezelfde persoon is[1]. Bij dit formulier is een uitgebreide toelichting gevoegd.
Bovenstaande geldt niet voor die erkende beroepen zoals vermeld in de Wet van 11 november 1993, houdende regelen inzake beroepen op het gebied van de individuele gezondheidszorg.

De gegevens die ten behoeve van de abonneeregistratie opgevraagd worden zijn:

- naam van de abonnee;
- bereikbaarheidsgegevens.

De aanvraag beroepsgebonden Certificaten moet worden ondertekend door de Abonnee. Met ondertekening geeft de Abonnee aan de Certificaataanvraag juist, volledig en naar waarheid te hebben ingevuld, akkoord te gaan met de Bijzonder Voorwaarden.

De handtekening moet een rechtsgeldige handtekening zijn, het moet dus een handgeschreven of een elektronische handtekening zijn. De elektronische handtekening moet voldoen aan de Wet elektronische handtekeningen.

De Aanvraag beroepsgebonden Certificaten dient voorzien te zijn van het bewijs dat de certificaathouder geautoriseerd is het Erkende Beroep uit te oefenen. Dit bewijs dient authentiek te zijn. Als authentiek bewijs voor het uitoefenen van een Erkend Beroep wordt alleen beschouwd:

- ofwel een geldig bewijs van inschrijving in een door de betreffende beroepsgroep erkend (beroeps)register waarbij een wettelijke geregeld tuchtrecht van toepassing is;

[1] In het vervolg wordt in het geval van Beroepsgebonden Certificaten, ondanks dat Abonnee en Certificaathouder steeds dezelfde persoons zijn, steeds gesproken over Certificaathouder.

- ofwel een geldig (b.v. een vergunning) dat aan de wettelijke eisen voor het uitoefenen van het beroep wordt voldaan.

Onder geldig bewijs wordt verstaan een bewijs dat niet is verlopen of (voorlopig is) ingetrokken.

Daarnaast dient de Aanvraag beroepsgebonden Certificaten vergezeld te gaan van een kopie van het identiteitsbewijs van de Certificaathouder. Dit identiteitsbewijs dient te voldoen aan de eisen van de Wid. Het identiteitsbewijs dient om de gegevens van de Certificaathouder te kunnen vergelijken met de gegevens van het bewijs voor het uitoefenen van het Erkend Beroep. Het dient tevens om de handtekening op de aanvraag er mee te kunnen vergelijken.

KPN zal het betreffende formulier en de bijbehorende bewijsstukken in ontvangst nemen en de volledigheid en de juistheid ervan beoordelen, onder andere door externe bronnen te raadplegen. Hierbij wordt functiescheiding toegepast tussen hij/zij die beoordeelt (controle) en hij/zij die beslist (beschikken). Alleen indien het formulier volledig en juist is, zal KPN het formulier goedkeuren, overgaan tot registratie, een abonneenummer toekennen en de Abonnee hierover informeren. Het abonneenummer dient steeds bij de communicatie tussen Abonnee en KPN worden gebruikt. Alleen indien een organisatie bij KPN is geregistreerd als Abonnee kan het certificaataanvragen indienen bij KPN.

Indien er wijzigingen optreden in de gegevens die de Abonnee aan KPN heeft verstrekt, is de Abonnee verplicht deze wijzigingen vroegtijdig aan KPN door te geven. Vroegtijdig betekent minimaal 10 werkdagen voor het ingaan van de wijziging. Wijzigingen kunnen niet achteraf worden doorgevoerd.

Wijzigingen die dienen te worden doorgegeven betreffen dan bijvoorbeeld het vertrek van de Bevoegde Vertegenwoordiger of Contactpersoon of wijziging in de contactpersoon van de Abonnee. Voor het doorgeven van wijzigingen zijn formulieren beschikbaar op de site (http://www.pki.getronics.nl/website/401/PKIoverheid+formulieren.html). Deze formulieren zijn eveneens voorzien van een uitgebreide toelichting. Ook hiervoor geldt dat KPN de wijzigingen zal beoordelen op volledigheid en juistheid en dat de Abonnee wordt geïnformeerd over het aanbrengen van wijzigingen in de abonneeregistratie.

KPN zal regelmatig de geregistreerde gegevens controleren dan wel de geregistreerde gegevens schriftelijk ter bevestiging aan Abonnee voorleggen. De Abonnee is er aan gehouden binnen de gestelde termijn de correctheid van de geregistreerde gegevens te bevestigen dan wel, indien deze niet meer correct zijn, voor correctie zorg te dragen met behulp van de daartoe beschikbaar gestelde formulieren.

KPN besteedt delen van haar Certificatiediensten uit aan andere organisaties. In een dergelijke situatie is Authenticatie van die andere organisaties onderdeel van het commerciële proces dat uiteindelijk leidt tot het in een overeenkomst vastleggen van de uitbesteding.

3.2.3 Authenticatie van persoonlijke identiteit

Indien een Abonnee een Certificaat wil aanvragen, dient het een daartoe ontwikkeld aanvraagformulier in te vullen en te sturen naar KPN. Het betreft de formulieren:

- Aanvraag PKIoverheid Persoonsgebonden Certificaten;
- Aanvraag PKIoverheid Beroepsgebonden Certificaten;
- Aanvraag PKIoverheid Groepscertificaten;
- Aanvraag PKIoverheid Servercertificaten (via website).

Het aanvraagformulier dient (elektronisch) te worden ondertekend door de Abonnee. Door ondertekening van het formulier wordt o.a. de Certificaathouder of Certificaatbeheerder geautoriseerd

het aangevraagde Certificaat namens de Abonnee in ontvangst te nemen, alsmede om het te gebruiken en/of te beheren.

De Abonnee dient met de Certificaataanvraag een fotokopie mee te sturen van het identiteitsbewijs van elke Certificaathouder en Certificaatbeheerder waarvoor een Certificaat wordt aangevraagd. Dit is niet noodzakelijk voor Certificaatbeheerders waarbij gesteund kan worden op een al eerder door KPN uitgevoerde identificatie. In dat geval dient de Certificaatbeheerder al door KPN geïdentificeerd te zijn, dient het daarbij gebruikte identiteitsbewijs niet als gestolen of vermist geregistreerd te zijn en dient het nog minimaal 6 weken na indiening van de aanvraag (datum ontvangst door KPN is daarbij leidend) geldig te zijn.
Voor een Certificaatbeheerder die meerdere certificaten gaat beheren geldt dat een eenmalige identificatie volstaat. Dit geldt ook als die Certificaatbeheerder Certificaten gaat beheren namens meerdere Abonnees.

Het identiteitsbewijs moet voldoen aan de eisen uit de Wid. De kopie dient afkomstig te zijn van hetzelfde identiteitsbewijs als waarmee de Certificaathouder of Certificaatbeheerder zich, na ontvangst van de smartcard, bij GWK Travelex gaat legitimeren. Op het tijdstip van vaststelling van de identiteit mag de geldigheid van het betreffende identiteitsbewijs bovendien niet zijn verstreken.

De vaststelling van de identiteit van de Certificaathouder en/of de Certificaatbeheerder geschiedt standaard op een vestiging van GWK Travelex, door een medewerker van GWK Travelex. KPN heeft de vaststelling van de identiteit van de certificaathouder uitbesteed aan GWK Travelex. KPN is en blijft eindverantwoordelijk voor de door GWK Travelex uitgevoerde werkzaamheden.

Indien gekozen wordt voor identificatie op lokatie (tegen meerprijs) geschiedt vaststelling van de identiteit op een nader af te spreken plaats en tijdstip in persoonlijke aanwezigheid van die Certificaathouder door een medewerker van KPN.

3.2.3.1 Authenticatie ten behoeve van Certificaten voor natuurlijke personen

Certificaten voor natuurlijke personen betreffen aanvragen voor Beroepsgebonden of Persoonsgebonden Certificaten. Op het aanvraagformulier voor een dergelijk Certificaat dienen de navolgende gegevens ingevuld te worden.

Van de Abonnee:
- abonneenummer en –naam;
- contactgegevens
- naam Contactpersoon (alleen voor Persoonsgebonden Certificaten).

Van de Certificaathouder tenminste:
- volledige namen;
- andere gegevens benodigd voor identificatie als nationaliteit, geslacht, geboortedatum en –plaats;
- e-mail adres;
- zowel het zakelijke als het privé postadres (indien aanwezig), voor toezending van respectievelijk de PIN-mail en de smartcard.

Andere gegevens, zoals:
- of al eens eerder een certificaat aan de certificaathouder is uitgegeven (in dat geval dient het eerder verkregen subjectserienummer op de aanvraag vermeld te worden);

- of de aanvrager gebruik maakt van een aanspraak op garantie. Dat kan als de uitgifte van het certificaat niet langer is geleden dan 3 maanden. Indien het identiteitsbewijs van de Certificaathouder nog minimaal 6 weken na datum indiening aanvraag geldig is en het niet als gestolen of vermist staat geregistreerd hoeft niet een nieuwe identificatie plaats te vinden.
- of identificatie van de Certificaathouder moet plaatsvinden bij GWK Travelex (standaard) of op locatie bij de Abonnee (meerprijs);
- Universal Principal Name (UPN, de algemene Windows login naam).

3.2.3.2 Authenticatie ten behoeve van Services Certificaat

3.2.3.2.1 Authenticatie van Certificaatbeheerder

Voor Services Certificaten geldt dat deze dienen te worden beheerd door een expliciet daartoe door de Abonnee aangewezen en geautoriseerde Certificaatbeheerder. Certificaatbeheerders kunnen in beginsel meerdere Services Certificaten beheren. Omdat dat veelvuldig voorkomt, is de identificatie en Authenticatie van de Certificaatbeheerder losgekoppeld van de Certificaataanvraag van het Services Certificaat zelf. KPN heeft dientenbehoeve de volgende werkwijze geïmplementeerd.

Certificaatbeheerders dienen door de Abonnee, door elke Abonnee waarvoor hij/zij werkzaam is of gaat zijn, apart te worden geregistreerd. Hiervoor is een registratieformulier beschikbaar. Op het registratieformulier voor Certificaatbeheerders dienen de navolgende gegevens ingevuld te worden.
Van de Contactpersoon:

- abonneenummer en –naam;
- naam en contactgegevens.

Van de Certificaatbeheerder:

- volledige namen;
- gegevens benodigd voor identificatie als nationaliteit, geslacht, geboortedatum en –plaats;
- de naam van de organisatie waarvoor de Certificaatbeheerder werkzaam is (alleen indien de Certificaatbeheerder niet werkzaam is voor de Abonnee);
- e-mail adres en telefoonnummer;
- zakelijke en privé postadres.

Andere gegevens, zoals:

- of identificatie van de Certificaatbeheerder moet plaatsvinden bij GWK Travelex (standaard) of op locatie bij de Abonnee (meerprijs);
- of gesteund kan worden op een eerder uitgevoerde identificatie.

KPN zal het registratieformulier in ontvangst nemen en het beoordelen op volledigheid en juistheid, inclusief de ondertekening en het aangeleverde bewijsmateriaal. Hierbij wordt functiescheiding toegepast tussen hij/zij die beoordeelt (controle) en hij/zij die beslist (beschikken). Alleen indien het registratieformulier volledig en juist is zal KPN de Certificaatbeheerder registreren en kan een Services Certificaat worden aangevraagd.

KPN zal de Abonnee over de registratie schriftelijk of per e-mail informeren.

3.2.3.2.2 Authenticatie ten behoeve van Servercertificaat

Op de Certificaataanvraag voor een Servercertificaat dienen de navolgende gegevens ingevuld te worden.
Van de abonneeorganisatie:

- indien een organisatie wil deelnemen aan de digitale diensten van de overheid, zoals Digikoppeling en Digipoort: het OverheidsIdentificatieNummer (voor overheidsorganisaties) of Kamer van Koophandel nummer (voor private organisaties);

Van de Contactpersoon:
- abonneenummer en –naam;
- naam en contactgegevens.

Van de Certificaathouder tenminste:
- Certificate Signing Request-gegevens van de server;
- identifier of naam van de server.

Van de Certificaatbeheerder:
- volledige namen;
- telefoonnummer;
- registratienummer.

Andere gegevens als:
- of sprake is van een initiële aanvraag of een vervanging;
- de gewenste levensduur van het certificaat.

De abonnee moet aantonen dat de organisatie de naam die de server of de service identificeert mag voeren. Als de service een DNS naam heeft MOET deze in de commonName vermeld worden als “fully-qualified domain name”. Een Fully Qualified Domain Name (FQDN) is een domeinnaam die alle hoger gelegen domeinnamen bevat, inclusief de naam van een eventuele service domeinnaam, top level domeinnaam en eventuele subdomeinnamen [RFC1594]. Voorbeelden zijn webzegel.pkioverheid.nl, www.pkioverheid.nl, gbo.overheid.nl en www.gbo.overheid.nl.
Met een FQDN is het mogelijk een server op het Internet uniek te identificeren. Een certificaat wat bijvoorbeeld voor *www*.pkioverheid.nl wordt aangevraagd, is niet geldig voor *secure*.pkioverheid.nl. Het is daarbij niet toegestaan in de domeinnaam wildcards, private IP adressen en/of hostnames, internationalized domain names (IDN’s) en null characters \0 te gebruiken.

Indien een overheidsorganisatie wil deelnemen aan Digikoppeling, dan dient een uittreksel uit het Digikoppeling Serviceregister te worden aangeleverd, als dat tenminste nog niet gebeurd is bij de abonneeregistratie.

KPN zal de Certificaataanvraag in ontvangst nemen en het beoordelen op volledigheid en juistheid, inclusief de ondertekening en het aangeleverde bewijsmateriaal. Hierbij wordt functiescheiding toegepast tussen hij/zij die beoordeelt (controle) en hij/zij die beslist (beschikken). Alleen indien de Certificaataanvraag volledig en juist is zal KPN de Certificaataanvraag goedkeuren.

KPN zal de Abonnee over goedkeuring van de Certificaataanvraag schriftelijk of per e-mail informeren.

3.2.3.2.3 Authenticatie ten behoeve van Groepscertificaat

Op de Certificaataanvraag voor een Groepscertificaat dienen de navolgende gegevens ingevuld te worden.

Van de Contactpersoon:
- abonneenummer en –naam;
- naam en contactgegevens.

Van de Certificaathouder:
- naam van de service;
- e-mail adres.

Van de Certificaatbeheerder:
- volledige namen;
- telefoonnummer;
- registratienummer.

Andere gegevens als:
- indien een organisatie wil deelnemen aan de digitale diensten van de overheid, zoals Digikoppeling en Digipoort: het OverheidsIdentificatieNummer (voor overheidsorganisaties) of Kamer van Koophandel nummer (voor private organisaties);
- Universal Principal Name;
- of al eerder een certificaat aan de betreffende certificaathouder is uitgegeven;
- de gewenste levensduur van het certificaat.

KPN zal de Certificaataanvraag in ontvangst nemen en het beoordelen op volledigheid en juistheid, inclusief de ondertekening en het aangeleverde bewijsmateriaal. Hierbij wordt functiescheiding toegepast tussen hij/zij die beoordeelt (controle) en hij/zij die beslist (beschikken). Alleen indien de Certificaataanvraag volledig en juist is zal KPN de Certificaataanvraag goedkeuren.

KPN zal de Abonnee over goedkeuring van de Certificaataanvraag schriftelijk of per e-mail informeren.

3.2.4 Autorisatie van de Certificaathouder

De autorisatie van de Certificaathouder om een Certificaat van de organisatie te mogen ontvangen en te gebruiken blijkt uit de ondertekening van de Certificaataanvraag door of namens de Abonnee. Indien sprake is van een Servercertificaat, dient door de Abonnee het bewijs te worden geleverd van de identifier van het apparaat of systeem, waardoor er naar kan worden verwezen.

In de Bijzonder Voorwaarden is geregeld dat de Abonnee de verplichting heeft om, als er relevante wijzigingen plaats hebben in de relatie tussen Abonnee en Certificaathouder, het Certificaat onmiddelijk in te trekken. Relevante wijzigingen in dit verband kunnen bijvoorbeeld schorsing of beëindiging van het dienstverband of de beroepsuitoefening zijn.

3.3 Identificatie en Authenticatie bij vernieuwing van het certificaat

3.3.1 Identificatie en Authenticatie bij het vernieuwen van het sleutelmateriaal

KPN biedt momenteel geen mogelijkheid tot vernieuwing van gecertificeerde sleutels.

3.3.2 Identificatie en Authenticatie bij routinematige vernieuwing van het certificaat

Het CA-Certificaat wordt niet routinematig vernieuwd. Het CA-Certificaat wordt (indien gewenst) vernieuwd rond 3 jaar voor het verstrijken van diens levensduur. Dat zal zijn voor 27 juli 2012. Vernieuwen van het CA-Certificaat zal volgens een strikte procedure gaan in afstemming en in samenwerking met de Policy Authority van de PKIoverheid.

KPN biedt geen mogelijkheid tot routinematige vernieuwing van PKIoverheid Certificaten. Een verzoek tot vernieuwing zal worden behandeld als een verzoek voor een nieuw certificaat.

3.3.3 Identificatie en Authenticatie bij vernieuwing van het Certificaat na intrekking

KPN biedt momenteel geen mogelijkheid tot vernieuwing van gecertificeerde sleutels.

3.4 Identificatie en Authenticatie bij verzoeken tot intrekking

In paragraaf 4.9 Intrekking en opschorting van certificaten is beschreven wie een verzoek tot intrekking mogen indienen.

Alleen de Abonnee of de Certificaathouder, of in geval van een Services Certificaat door de Certificaatbeheerder, mag/kan een verzoek tot intrekking van een Certificaat indienen. Dit kan elektronisch/online gebeuren via de website van KPN (https://www.pki.getronics.nl/website/getronics/178/Intrekken+certificaten.html).
Om te kunnen overgaan tot intrekking dient de Certificaathouder/Certificaatbeheerder gebruik te maken van een intrekkingscode.

De intrekkingscode voor Beroepsgebonden, Persoonsgebonden en Groepscertificaten wordt/is alleen verstuurd naar de Certificaathouder of de Certificaatbeheerder (PIN-mail). De intrekkingscode voor servercertificaten wordt tijdens de aanvraagprocedure door de Certificaatbeheerder gegenereerd.
In voorkomende gevallen is de Abonnee verplicht zijn certificaat in te trekken (zie daarvoor de Bijzonder Voorwaarden). Voor het geval de Certificaathouder/Certificaatbeheerder dit nalaat dient de Abonnee dit zelf te (kunnen) doen. Daartoe dient de Certificaathouder/Certificaatbeheerder deze intrekkingscode aan de Abonnee te verstrekken dan wel dient de Abonnee de intrekkingscode direct na uitgifte bij de Certificaathouder/Certificaatbeheerder op te vragen en zorgvuldig te registreren.

Voor niet spoedeisende intrekkingen kan de Abonnee en/of de Certificaathouder/Certificaatbeheerder een intrekkingsverzoek indienen met behulp van het formulier ‘Intrekkingsverzoek Certificaten’.

Op het formulier ‘Intrekkingsverzoek Certificaten’ dienen de navolgende gegevens ingevuld te worden.
Van de Contactpersoon:

- abonneenummer en –naam;
- naam en contactgegevens.

Van het Certificaat:

- naam in het Certificaat;
- subjectserienummer in het Certificaat;
- type Certificaat;
- serienummer(s) van het Certificaat (de Certificaten);
- intrekkingscode;
- reden voor intrekking.

Het formulier ‘Intrekkingsverzoek Certificaten’ wordt door KPN in ontvangst genomen en beoordeeld op volledigheid en juistheid. Indien het verzoek volledig en juist is gaat KPN over tot intrekking. Hierbij wordt functiescheiding toegepast tussen hij/zij die beoordeelt (controle) en hij/zij die beslist (beschikken).

De Abonnee en de Certificaathouder/Certificaatbeheerder worden schriftelijk of per e-mail over het afhandelen van het intrekkingsverzoek geïnformeerd.

Indien KPN gerede aanleiding heeft om te twijfelen over de authenticiteit van een intrekkingsverzoek, kan van diegene die het verzoek heeft ingediend worden verlangd dat hij/zij zich persoonlijk legitimeert tegenover KPN voordat aan de intrekking uitvoering wordt gegeven.

KPN is eveneens gerechtigd zelfstandig tot intrekking over te gaan indien (zie paragraaf 4.9.2):

- de Abonnee handelt in strijd met de aan hem opgelegde voorwaarden voor gebruik, zoals onder meer vastgelegd in deze CPS en in de Bijzonder Voorwaarden of;
- de Private Sleutel van de CA van KPN of van de Staat der Nederlanden verloren raakt, wordt gestolen of anderszins wordt gecompromitteerd of;
- het gebruikte algoritme wordt gecompromitteerd, dreigt te worden gecompromitteerd of in zijn algemeenheid te zwak is geworden voor het doel waarvoor het gebruikt wordt.

KPN is in staat een certificaat in te trekken zonder intrekkingscode.

Een Vertrouwende Partij kan melding maken van een Abonnee die zich niet of niet geheel houdt aan de opgelegde voorwaarden. Dat kan met behulp van het formulier ‘Melding omstandigheden die kunnen leiden tot intrekking’. Op dit formulier kan het volgende worden ingevuld:

- gegevens van de melder als diens naam, organisatienaam en bereikbaarheidsgegevens;
- gegevens van de omstandigheid, zoals een omschrijving en datum en tijdstip van signalering;
- gegevens van het betrokken Certificaat als de naam en subjectserienummer van de Certificaathouder, het type Certificaat en het serienummer.

KPN zal de melding in ontvangst nemen, de melding beoordelen op volledigheid en juistheid, eventueel proberen benodigde aanvullende informatie te verzamelen en een besluit nemen om al dan niet over te gaan tot intrekking. Hierbij wordt functiescheiding toegepast tussen hij/zij die beoordeelt (controle) en hij/zij die beslist (beschikken).
De melder, de betrokken Abonnee en Certificaathouder/Certificaatbeheerder worden schriftelijk of per e-mail over de melding en de afhandeling ervan geïnformeerd.

4 Operationele eisen certificaatlevenscyclus

4.1 Certificaataanvraag

4.1.1 Wie kan een Certificaataanvraag indienen

In beginsel kan alleen de Bevoegd Vertegenwoordiger van de Abonnee een Certificaataanvraag tot abonneeregistratie indienen. Door middel van ondertekening van het abonneeregistratieformulier autoriseert deze Bevoegde Vertegenwoordiger één of meerdere op het formulier vermeld staande Contactpersonen om namens Abonnee Certificaten aan te vragen, te installeren, te beheren en in te trekken, alsmede om andere Contactpersonen en Certificaatbeheerders aan te autoriseren.

4.1.2 Verantwoordelijkheden en verplichtingen

De verplichtingen en verantwoordelijkheden van betrokkenen, KPN, Abonnee, Certificaathouder/Certificaatbeheerder en Vertrouwende Partij zijn beschreven in de Bijzonder Voorwaarden.

4.1.2.1 Verantwoordelijkheden en verplichtingen van de CSP

KPN is eindverantwoordelijk voor de gehele certificatiedienstverlening en garandeert tegenover Abonnees, Certificaathouders en Vertrouwende Partijen dat het zich zal houden aan de Bijzonder Voorwaarden, het CPS en de van toepassing zijnde CP's. KPN is daarbinnen vanzelfsprekend verantwoordelijk voor de uitbesteding van (delen van) diensten aan andere partijen. Een voorbeeld daarvan is de uitbesteding van de identificatie van certificaathouders en certificaatbeheerders aan GWK Travelex. Maar zo heeft KPN meedere diensten uitbesteed. Als eindverantwoordelijke certificatiedienstverlener, als uitbesteder van diensten, zorgt KPN voor de kwaliteit van de uitbestede diensten door het toepassen van (vormen van) aansturing, afstemming, toezicht en wederzijdse kwaliteitsborging. De implementatie daarvan zal afhankelijk zijn van de specifieke situatie.

Indien een uitbesteding enige omvang heeft zal de uitbesteding worden beschreven in een bijlage van deze CPS.

4.1.2.2 Verantwoordelijkheden en verplichtingen van de Abonnee

De Abonnee is verantwoordelijk voor het correct aanleveren van alle gegevens benodigd voor het aanmaken en leveren van certificaten en voor het correcte gebruik van die certificaten. De Abonnee garandeert tegenover KPN en Vertrouwende Partijen dat het zich zal houden aan de Bijzonder Voorwaarden, het CPS en de van toepassing zijnde CP's.

4.1.2.3 Verantwoordelijkheden en verplichtingen van de Certificaathouder

De Certificaathouder (inclusief, in geval van een Servercertificaat of Groepscertificaat, de Certificaatbeheerder), als houder van het Certificaat dat namens de Abonnee voor de Certificaathouder is aangevraagd, is eveneens verantwoordelijk voor het correct aanleveren van alle gegevens benodigd voor het aanmaken en leveren van certificaten en voor het correcte gebruik van die certificaten. De Certificaathouder garandeert tegenover KPN, de Abonnee en Vertrouwende Partijen dat hij/zij zich zal houden aan de Bijzonder Voorwaarden, het CPS en de van toepassing zijnde CP's.

4.1.2.4 Verantwoordelijkheden en verplichtingen van de Vertrouwende Partij

De Vertrouwende Partij is verantwoordelijk voor het op correcte wijze vertrouwen op een Certificaat en garandeert tegenover KPN, de Abonnee en de Certificaathouder dat het zich zal houden aan de Bijzonder Voorwaarden, het CPS en de van toepassing zijnde CP's.

4.1.3 Het proces

De processen die door KPN zijn gedefineerd ter realisatie van haar certificatiedienstverlening bestaan in zijn algemeenheid uit twee delen. Het eerste deel is het behandeldeel en het tweede deel is het afhandeldeel. In het behandeldeel wordt de ontvangst van een formulier geregistreerd, de volledige invulling van het formulier en het volledig bijgevoegd zijn van de bewijsstukken vastgesteld (acceptatie) en de juistheid ervan beoordeeld. Laatste onderdeel van dit deel is het nemen van een besluit over het formulier. Het tweede deel, het afhandelen, behelst het uitvoering geven aan het genomen besluit en het informeren van betrokkenen erover. In de navolgende paragrafen worden de processen meer in detail beschreven.

4.2 Verwerken van certificaataanvragen

4.2.1 Registratie van Abonnee en Certificaatbeheerder

Organisaties dienen zich, alvorens certificaten te kunnen aanvragen, te registreren als Abonnee van de Certificatiedienstverlening van KPN. Dit kan door een daartoe beschikbaar gesteld formulier Abonnee Registratie in te vullen, het gevraagde bewijsmateriaal (zie paragraaf 3.2.2) bij te voegen en het geheel per post te verzenden naar KPN. Nadere instructies voor het gebruik van het formulier zijn bij het formulier gevoegd. Er zijn ook formulieren voor het onderhouden van de aan KPN verstrekte gegevens. Zie hiervoor de website http://www.pki.getronics.nl.

Onderdeel van de registratie van een Abonnee is de autorisatie van één of meer contactpersonen. Deze contactpersonen moeten geautoriseerd worden om certificaataanvragen te mogen indienen, andere contactpersonen te autoriseren en/of certificaten in te mogen trekken. Het autoriseren geschiedt door ondertekening van het formulier Abonnee Registratie door de Bevoegd Vertegenwoordiger van de Abonnee (zie ook paragraaf 3.2.2).

KPN zal de formulieren in ontvangst nemen en de volledigheid en de juistheid van de formulieren beoordelen. Een registratieformulier dient volledig te zijn om te kunnen worden geaccepteerd en om tot beoordeling van de juistheid over te kunnen gaan. Bij onvolkomendheden zal contact opgenomen worden met de Abonnee die de Certificaataanvraag heeft ingediend.

Indien het abonneeregistratieformulier wordt goedgekeurd, wordt de Abonnee geregistreerd en kan de Abonnee aanvragen voor Certificaten gaan indienen. De Abonnee wordt schriftelijk geïnformeerd over goed- of afkeuring.

Naast de registratie van de organisatie als Abonnee, kunnen tevens Certificaatbeheerders van Services Certificaten worden geregistreerd. Certificaatbeheerders kunnen in beginsel meerdere Certificaten beheren, maar dienen daartoe eerst geregistreerd te worden. Dit kan door het formulier Registratie Certificaatbeheerders in te vullen, het gevraagde bewijsmateriaal (zie paragraaf 3.2.3.2) bij te voegen en het geheel per post of electronisch te sturen naar KPN. Nadere instructies voor het gebruik van het formulier zijn bij het formulier gevoegd. Er zijn ook formulieren voor het onderhouden van de aan KPN verstrekte gegevens.

Ook voor het registreren van Certificaatbeheerders geldt dat KPN de Certificaataanvraag voor registratie van een Certificaatbeheerder in ontvangst zal nemen, de volledigheid en de juistheid ervan zal beoordelen en zal komen tot een goed- of afkeuring. De Abonnee wordt schriftelijk geïnformeerd over die beslissing.

Onderdeel van de registratie van de Certificaatbeheerder is diens persoonlijke identificatie. Dit geschiedt op de wijze zoals dat ook voor Certificaathouders geschiedt, via GWK Travelex (standaard werkwijze) of op locatie (meerprijs) (zie verder paragraaf 4.2.2).

Is een Certificaatbeheerder eenmaal geïdentificeerd en geregistreerd, dan kunnen de aanvragen voor Server- en Groepscertificaten worden afgehandeld zoals in paragraaf 4.2 is beschreven.

Indien de gegevens van de Certificaatbeheerder wijzigen dient de Contactpersoon deze gewijzigde gegevens aan KPN door te geven met behulp van het formulier Wijziging gegevens Certificaatbeheerder (zie Elektronische Opslagplaats) en indien een Certificaatbeheerder niet meer in staat is de aan hem/haar toevertrouwde certificaten te beheren dient de Abonnee dit te melden via een daartoe bestemd formulier Verwijdering Certificaatbeheerders. KPN zal dit formulier beoordelen op volledigheid en juistheid. Na een positief besluit verwijdert KPN de Certificaatbeheerder uit de desbetreffende registratie. Voorwaarde voor die verwijdering is wel dat het beheer van de desbetreffende certificaten wordt overgedragen aan een andere, ook geregistreerde, Certificaatbeheerder.

4.2.2 Aanvraag van certificaten

Er zijn verschillende procedures voor verschillende soorten aanvragen:

- aanvragen van Persoonsgebonden Certificaten en Groepscertificaten, waarbij het sleutelpaar wordt aangemaakt door KPN;
- aanvragen van Beroepsgebonden Certificaten waarbij het sleutelpaar ook wordt aangemaakt door KPN. Deze groep wordt apart behandeld omdat voor de Beroepsgebonden Certificaten geldt dat de Abonnee en de Certificaathouder dezelfde persoon zijn;
- aanvragen van Servercertificaten, waarbij het sleutelpaar wordt aangemaakt door de Abonnee in de Veilige Omgeving van de Abonnee.

4.2.2.1 Aanvraag van Persoonsgebonden Certificaten en Groepscertificaten

Voor het aanvragen van een Persoonsgebonden Certificaat of Groepscertificaat dienen standaard de volgende stappen te worden doorlopen.

1. De Abonnee vult een certificaataanvraagformulier in voor een (beoogd) Certificaathouder (of voor deze een Certificaatbeheerder) en verklaart zich daarin onder andere akkoord met de Bijzonder Voorwaarden. Nadere instructies voor het gebruik van het formulier zijn bij het formulier gevoegd.
2. De Abonnee ondertekent het aanvraagformulier, voorziet deze van een kopie van het identiteitsbewijs van de (beoogd) Certificaathouder/Certificaatbeheerder (ingeval van een aanvraag voor een Persoonsgebonden Certificaat) en verstuurt het naar KPN.
3. KPN neemt de Certificaataanvraag in ontvangst, beoordeelt de volledigheid en de juistheid van de Certificaataanvraag en neemt er een beslissing over. Onder andere wordt bij erkende registers als Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA) gecontroleerd of Abonnee eigenaar is van de domeinnaam, zoals die onderdeel uitmaakt van het e-mail adres.
4. Indien KPN de Certificaataanvraag goedkeurt, wordt het sleutelmateriaal in de SSCD/SUD gegenereerd en het Certificaat gegenereerd. Tevens genereert KPN de geheime PIN- en PUK-code voor de SSCD/SUD en de intrekkingscode voor de Certificaten.
5. De smartcard met daarop de certificaten wordt per post verzonden naar het huisadres van de Certificaathouder/Certificaatbeheerder. Bij deze smartcard is een meldverzoek /

ontvangstbevestiging gevoegd. De Certificaathouder/Certificaatbeheerder dient, indien hij/zij nog niet eerder door KPN is geïdentificeerd, zich met dit meldverzoek / ontvangstbevestiging te vervoegen bij een vestiging van GWK Travelex. De Certificaathouder/Certificaatbeheerder dient zich aldaar te identificeren met het identeitsbewijs waarvan eerder een kopie is meegestuurd met de Certificaataanvraag en hij/zij dient daarvoor/daarbij het ontvangstbewijs te ondertekenen.
Indien KPN kan steunen op een eerder door KPN uitgevoerde identificatie behoeft die identificatie niet opnieuw plaats te vinden. De Certificaathouder/Certificaatbeheerder ontvangt dan met de smartcard een ontvangstbevestiging. De Certificaathouder/Certificaatbeheerder dient deze ontvangsbevestiging te ondertekenen en terug te sturen.
KPN kan voor Certificaatbeheerders steunen op een eerder door of namens KPN uitgevoerde identificatie indien het daarbij gebruikte identiteitsbewijs bij de nieuwe aanvraag weer wordt gebruikt, het niet als gestolen of vermist staat geregistreerd en het nog geldig is tot zes weken na indiening van de aanvraag. De datum van ontvangst van de aanvraag door KPN is daarbij leidend.

6. GWK Travelex identificeert de Certificaathouder, maakt een kopie van diens identiteitsbewijs, stuurt deze kopie samen met de getekende ontvangstbevestiging naar KPN. GWK Travelex bevestigt de identificatie naar KPN tevens op elektronische wijze.
7. KPN verstuurt na ontvangst van de elektronische bevestiging van GWK Travelex het document met daarin vermeld de geheime PIN- en PUK-code voor de SSCD/SUD en de intrekkingscode voor de Certificaten per post naar het zakelijk adres van de Certificaathouder.

KPN blijft de mogelijkheid bieden, tegen meerprijs, de identificatie en uitgifte op een nader af te spreken tijdstip/locatie te laten plaatsvinden.

4.2.2.2 Aanvraag Beroepsgebonden Certificaten

Voor het aanvragen van een Beroepsgebonden Certificaat dienen standaard de volgende stappen te worden doorlopen.

1. De Abonnee/Certificaathouder vult een Aanvraag Beroepsgebonden Certificaten in en verklaart zich daarin onder andere akkoord met de Bijzonder Voorwaarden. Nadere instructies voor het gebruik van het formulier zijn bij het formulier gevoegd.
2. De Certificaathouder ondertekent het aanvraagformulier, vergezelt deze van een kopie van zijn/haar identiteitsbewijs en het bewijs van uitoefening van een Erkend Beroep (zie 3.2.2 Authenticatie van de Abonnee) en verstuurt dit gezamenlijk naar KPN.
3. KPN neemt de Certificaataanvraag in ontvangst, beoordeelt de volledigheid en de juistheid van de Certificaataanvraag en neemt er een beslissing over. Onder andere wordt nagegaan of het bewijs van uitoefening van het Erkend Beroep authentiek is.
4. Indien KPN de Certificaataanvraag goedkeurt, wordt het sleutelmateriaal in de SSCD gegenereerd en het Certificaat gegenereerd. Tevens genereert KPN de geheime PIN- en PUK-code voor de SSCD en de intrekkingscode voor de Certificaten.
5. De smartcard met daarop de certificaten wordt per post verzonden naar het huisadres van de Certificaathouder. Bij deze smartcard is een meldverzoek / ontvangstbevestiging gevoegd. De Certificaathouder dient zich met dit meldverzoek / ontvangstbevestiging te vervoegen bij een vestiging van GWK Travelex. De Certificaathouder dient zich aldaar te identificeren met het identeitsbewijs waarvan eerder een kopie is meegestuurd met de Certificaataanvraag en hij/zij dient daarvoor/daarbij het ontvangstbewijs te ondertekenen.
6. GWK Travelex identificeert de Certificaathouder, maakt een kopie van diens identiteitsbewijs, stuurt deze kopie samen met de getekende ontvangstbevestiging naar KPN. GWK Travelex bevestigt de identificatie naar KPN tevens op elektronische wijze.
7. KPN verstuurt na ontvangst van de elektronische bevestiging van GWK Travelex het document met daarin vermeld de geheime PIN- en PUK-code voor de SSCD en de intrekkingscode voor de Certificaten per post naar het zakelijk adres van de Certificaathouder. Indien niet een zakelijk adres is opgegeven wordt dit naar het privé adres van de Certificaathouder gestuurd.

KPN blijft de mogelijkheid bieden, tegen meerprijs, de identificatie op een nader af te spreken tijdstip/locatie te laten plaatsvinden.

4.2.2.3 Aanvraag van Servercertificaten

De Certificaataanvraag voor een Servercertificaat verloopt in grote lijnen hetzelfde als onder 4.2.2.1 genoemd, met inachtneming van het volgende verschil.

1. De Certificaatbeheerder maakt in de Veilige Omgeving van de Abonnee het sleutelpaar (lengte is 2048 bits) aan en stuurt een Certificate Signing Request (CSR) met daarin de Publieke Sleutel, samen met de Certificaataanvraag Servercertificaat naar de Abonnee. De Abonnee vult het certificaataanvraagformulier (verder) in voor een (beoogd) Certificaathouder en verklaart zich daarin onder andere akkoord met de Bijzonder Voorwaarden. Nadere instructies voor het gebruik van het formulier zijn bij het formulier gevoegd.
2. De Abonnee ondertekent het aanvraagformulier en verstuurt het naar KPN.
3. KPN neemt de Certificaataanvraag in ontvangst en beoordeelt de volledigheid en de juistheid van de aanvraag. Onder andere wordt bij erkende registers als Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA) gecontroleerd of Abonnee eigenaar is van de domeinnaam, zoals die onderdeel uitmaakt van het e-mail adres.
4. Indien KPN de Certificaataanvraag goedkeurt, wordt het Certificaat aangemaakt en per e-mail aan de Certificaatbeheerder verstuurd.

Opmerking: vanaf 1 januari 2011 levert KPN standaard SHA-2 Servercertificaten. In uitzonderingsgevallen kunnen tot 31 december 2011 nog SHA-1 Servercertificaten aangevraagd en geleverd worden. Deze Servercertificaten worden echter alleen geleverd met een sleutellengte 2048 bits en hebben een vaste einddatum 31 december 2011.
In de aanvraagprocedure kunnen Abonnees een SHA-2 Servercertificaat aanvragen. Daarnaast kan de Abonnee, in uitzonderingsgevallen, ook een SHA-1 Servercertificaat aanvragen. Alleen een SHA-1 Servercertificaat aanvragen is vanaf 1 januari 2011 niet meer mogelijk.

4.2.3 Certificaataanvraagverwerkingstijd

KPN hanteert voor het verwerken van een Certificaataanvraag in beginsel een termijn van 10 werkdagen. In beginsel omdat deze termijn ook afhankelijk is van de kwaliteit van de ingediende aanvraag.

4.3 Uitgifte van Certificaten

4.3.1 Uitgifte van Persoonsgebonden Certificaten en Groepscertificaten

De uitgifte van de smartcard met daarop de aangemaakte certificaten en de uitgifte van het document met daarop de bij de smartcard behorende toegangscodes (PIN- en PUK-code, ook wel activeringsgegevens) en de intrekkingscode van de certificaten geschiedt op verschillende momenten en langs verschillende wegen. In eerste instantie wordt de smartcard per post verstuurd naar het huisadres van de Certificaathouder. Deze smartcard gaat vergezeld van een ontvangstbevestiging cq. meldverzoek, die door de Certificaathouder ondertekend en meegebracht dient te worden naar de vestiging van GWK Travelex. Aldaar dient na persoonlijke identificatie, de ondertekende ontvangstbevestiging te worden ingeleverd.

GWK Travelex bericht KPN over het resultaat van de identificatie en het inleveren van de ontvangstbevestiging. Na een positief bericht verstuurt KPN het document met daarop de toegangscodes voor de smartcard en de intrekkingscodes van de certificaten.

In het geval de Certificaathouder zich niet laat identificeren, zal deze daaraan na 3 weken worden herinnerd. Heeft na 6 weken de identificatie niet plaats gevonden zal zonder verdere aankondiging worden overgegaan tot intrekking van de aangevraagde Certificaten.

In die gevallen dat de Certificaathouder niet meer geïdentificeerd hoeft te worden en indien sprake is van een Groepscertificaat, waarbij de Certificaatbeheerder geïdentificeerd is tijdens zijn/haar registratie dient de Certificaathouder / Certificaatbeheerder zelf de ontvangstbevestiging na ondertekening retour te zenden. Indien de Certificaathouder / Certificaatbeheerder niet binnen 3 weken de ontvangstbevestiging heeft geretourneerd wordt deze daaraan door KPN aan herinnerd. Indien de Certificaathouder / Certificaatbeheerder niet binnen 6 weken de ontvangstbevestiging heeft geretourneerd gaat KPN zonder verdere aankondiging over tot intrekking van de betrokken Certificaten.

KPN bevestigt de uitgifte van het Certificaat schriftelijk of per e-mail naar de Abonnee.

4.3.2 Uitgifte van Beroepsgebonden Certificaten

De uitgifte van de smartcard met daarop de aangemaakte certificaten en de uitgifte van het document met daarop de bij de smartcard behorende toegangscodes en de intrekkingscode van de certificaten geschiedt op verschillende momenten en, indien mogelijk, langs verschillende wegen. In eerste instantie wordt de smartcard per post verstuurd naar het huisadres van de Certificaathouder. Deze smartcard gaat vergezeld van een ontvangstbevestiging cq. meldverzoek, die door de Certificaathouder ondertekend en meegebracht dient te worden naar de vestiging van GWK Travelex. Daar dient na persoonlijke identificatie, de ondertekende ontvangstbevestiging te worden ingeleverd.

GWK Travelex bericht KPN over het resultaat van de identificatie en het inleveren van de ontvangstbevestiging. Na een positief bericht verstuurt KPN het document met daarop de toegangscodes voor de smartcard en de intrekkingscodes van de certificaten.

In bepaalde gevallen is het mogelijk dat de Certificaathouder niet meer geïdentificeerd hoeft te worden, bijvoorbeeld bij een vervangingsaanvraag. De Certificaathouder dient in die gevallen zelf de ontvangstbevestiging na ondertekening retour te zenden. Indien de Certificaathouder niet binnen 3 weken de ontvangstbevestiging heeft geretourneerd wordt deze daaraan door KPN aan herinnerd. Indien de Certificaathouder niet binnen 6 weken de ontvangstbevestiging heeft geretourneerd gaat KPN zonder verdere aankondiging over tot intrekking van de betrokken Certificaten.

4.3.3 Uitgifte van Servercertificaten

Bij aanvragen voor geregistreerde Certificaatbeheerders verstuurt KPN de aangemaakte Certificaten per e-mail naar het opgegeven adres van de Certificaatbeheerder.

KPN bevestigt de uitgifte van het Certificaat schriftelijk of per e-mail naar de Abonnee.

4.3.4 Melding van certificaatvervaardiging aan de Certificaathouder of –beheerder

Direct na vervaardiging van het Certificaat is vervaardiging te zien via Directory Dienst. Echter, omdat de fysieke overdracht aan Abonnee op een later moment plaats vindt, is de waarde hiervan gering.

De Certificaathouder wordt expliciet op de hoogte gesteld van de vervaardiging door fysieke toezending van het smartcard, met daarop geplaatst o.a. het vervaardigde certificaat. De Certificaatbeheerder wordt expliciet op de hoogte gesteld van de vervaardiging door toezending van het Servercertificaat per e-mail op het opgegeven e-mail adres.
De Abonnee (geldt niet voor Beroepsgebonden Certificaten) wordt per e-mail of per post op de hoogte gesteld van de aanmaak en toezending van het certificaat.

4.4 Acceptatie van certificaten

4.4.1 Acceptatie van Beroepsgebonden, Persoonsgebonden en Groepscertificaten

Het Beroepsgebonden, Persoonsgebonden of Groepscertificaat wordt geacht te zijn uitgereikt en geaccepteerd zodra de (Abonnee/)Certificaathouder of Certificaatbeheerder ze heeft ontvangen. Deze dient de ontvangst te bevestigen door de meegeleverde ontvangstbevestiging te ondertekenen en in te leveren bij GWK Travelex (op het moment van identificatie) dan wel deze naar KPN te versturen. Deze ondertekende ontvangstbevestiging is de formele bevestiging van de acceptatie.

4.4.2 Acceptatie van Servercertificaten

Het Servercertificaat wordt geacht te zijn uitgereikt en geaccepteerd zodra de Certificaatbeheerder het verkregen Servercertificaat in gebruik neemt.
In het specifieke geval van gemeenten die gaan ontstaan (zie paragraaf 3.2.2) dient de Certificaatbeheerder de ontvangst van het Servercertificaat expliciet en zo spoedig mogelijk aan KPN te bevestigen. De Certificaatbeheerder heeft daarvoor uiteindelijk 6 weken de tijd. KPN zal de Certificaatbeheerder na 3 weken, indien binnen die termijn de ontvangstbevestiging niet is ontvangen door KPN, aan zijn verplichting herinneren. Is de ontvangstbevestiging niet binnen 6 weken ontvangen door KPN dan wordt het betreffende Servercertificaat zonder nadere aankondiging ingetrokken. KPN zal de Abonnee over de intrekking van het Servercertificaat berichten. De betalingsverplichting blijft echter onverminderd van kracht.

4.4.3 Publicatie van het Certificaat door de CA

Na aanmaak van het Certificaat wordt deze direct opgenomen in de Directory dienst.

4.5 Verantwoordelijkheden bij sleutelpaar- en certificaatgebruik

De verantwoordelijkheden en met name de bijbehorende verplichtingen van de Abonnee en de Certificaathouder/Certificaatbeheerder zijn beschreven in de Bijzonder Voorwaarden. Door ondertekening van de verschillende formulieren of erop te vertrouwen gaan betrokkenen akkoord met deze Bijzonder Voorwaarden.
Daarnaast is het voor hen van belang kennis te nemen van het Programma van Eisen van PKIoverheid in het algemeen en de van toepassing zijnde CP in het bijzonder. In de CP staan alle eisen verwoord aan welke alle bij de certificatiedienstverlening betrokkenen dienen te voldoen.

Voor vertrouwende partijen is het met name van belang, alvorens op een Certificaat te vertrouwen, eerst de geldigheid te controleren van de volledige keten van het Certificaat tot aan het Stamcertificaat.

Hierbij dient overigens de geldigheid van een Certificaat niet verward te worden met de bevoegdheid van de Certificaathouder een bepaalde actie namens een organisatie c.q. uit hoofde van zijn/haar beroep uit te mogen voeren. De PKIoverheid regelt geen autorisatie. De vertrouwende partij moet zich zelf op een andere wijze overtuigen van de autorisatie van de Certificaathouder.

4.6 Certificaat vernieuwing

KPN biedt geen mogelijkheid tot vernieuwing van PKIoverheid Certificaten. Een verzoek tot vernieuwing zal worden behandeld als een verzoek voor een nieuw certificaat.

4.7 Certificaat rekey

Sleutels van Certificaathouders zullen na het verstrijken van de geldigheidsduur of na het intrekken van de bijbehorende Certificaten niet opnieuw worden gebruikt.

4.8 Aanpassing van Certificaten

KPN biedt geen mogelijkheid tot aanpassing van de inhoud van PKIoverheid Certificaten. Indien de gegevens in het Certificaat niet meer overeenstemmen met de werkelijkheid dan is de Abonnee verplicht het betrokken Certificaat onmiddelijk in te trekken. Indien gewenst kan de Abonnee daarna een nieuw Certificaat aanvragen.

4.9 Intrekking en opschorting van certificaten

4.9.1 Omstandigheden die leiden tot intrekking

In de volgende gevallen is de Abonnee en/of de Certificaathouder gehouden per direct en zonder vertraging een verzoek om intrekking van het Certificaat in te dienen bij KPN:

- verlies, diefstal of compromittering van het Certificaat, de SSCD, de SUD, de PIN-code en/of PUK-code;
- onjuistheden in de inhoud van het Certificaat;
- wijziging van de in het Certificaat vermelde gegevens (naam, e-mail, etc);
- wijziging van de voor de betrouwbaarheid van het Certificaat noodzakelijke gegevens, bijvoorbeeld de beëindiging van het dienstverband of beroepsuitoefening;
- overlijden van de Certificaathouder (bij Persoonsgebonden of Beroepsgebonden Certificaten);
- beëindiging van de organisatorische eenheid (bij Organisatiegebonden Certificaten);
- ontbinding of faillissement van de rechtspersoon van Abonnee (bij Organisatiegebonden Certificaten).

Daarnaast zullen Certificaten in de volgende gevallen worden ingetrokken.

- De abonnee aangeeft dat het oorspronkelijke verzoek voor een certificaat niet was toegestaan en de abonnee ook met terugwerkende kracht ook geen toestemming verleent.
- KPN over voldoende bewijs beschikt over:

- dat de privésleutel van de abonnee (die overeenkomt met de publieke sleutel in het certificaat) is aangetast en/of
- een vermoeden van compromittatie en/of
- een inherente beveiligingszwakheid en/of
- dat het certificaat op een andere wijze is misbruikt.

  Een sleutel wordt als aangetast beschouwd in geval van ongeautoriseerde toegang of vermoede ongeautoriseerde toegang tot de private sleutel, verloren of vermoedelijk verloren private sleutel of SSCD, gestolen of vermoedelijk gestolen sleutel of SSCD of vernietigde sleutel of SSCD.

- Een abonnee niet aan zijn verplichtingen voldoet zoals verwoord in
  - deze CP en/of
  - het bijbehorende CPS van KPN en/of
  - de overeenkomst die KPN met de abonnee heeft afgesloten.
- KPN op de hoogte wordt gesteld of anderzins zich bewust wordt van een wezenlijke verandering in de informatie, die in het certificaat staat. Een voorbeeld daarvan is: verandering van de naam van de certificaathouder.
- KPN bepaalt dat het certificaat niet is uitgegeven in overeenstemming met deze CP of het bijbehorende CPS van KPN of de overeenkomst die KPN met de abonnee heeft gesloten.
- KPN bepaalt dat informatie in het certificaat niet juist of misleidend is.
- KPN haar werkzaamheden staakt en de CRL en OCSP dienstverlening niet wordt overgenomen door een andere certificatiedienstverlener.

Opmerking: Daarnaast kunnen certificaten worden ingetrokken als maatregel om een calamiteit te voorkomen, c.q. te bestrijden. Als calamiteit wordt zeker de aantasting of vermeende aantasting van de private sleutel van KPN waarmee certificaten worden ondertekend beschouwd. Ook als het gebruikte algoritme is gecompromitteerd, dreigt te worden gecompromitteerd of in zijn algemeenheid te zwak wordt voor het doel waarvoor het gebruikt wordt kan in voorkomende gevallen worden overgegaan tot intrekking.

Voor Servercertificaten gelden ook de volgende redenen.

- KPN op de hoogte wordt gesteld of anderzins zich er bewust van wordt dat het gebruik van de domeinnaam in het certificaat niet langer wettelijk toegestaan is (b.v. door een uitspraak van een rechter).
- De Abonnee een “code signing” certificaat gebruikt om “hostile code” (waaronder spyware, malware, trojans etc.) digitaal te ondertekenen..

Die Servercertificaten die uitgegeven zijn aan een gemeente die betrokken is bij een gemeentelijke herindeling hoeven niet direct te worden ingetrokken, zolang de namen van de betrokken certificaathouders niet wijzigen. Hetzelfde geldt voor Ministeries die betrokken zijn bij een herindeling/fusering van ministeries. Indien de naam van de Certificaathouder gaat wijzigen in verband met de gemeentelijke herindeling of fusie zal het betrokken Certificaat ingetrokken dienen te worden.

Certificaten kunnen door KPN zonder nadere tussenkomst worden ingetrokken indien de Abonnee, de Certificaathouder en/of de Certificaatbeheerder zich niet houdt aan de verplichtingen in de Bijzonder Voorwaarden. De beweegreden voor elke door KPN zelfstandig uitgevoerde intrekking wordt door haar geregistreerd.

KPN zorgt ervoor dat datum en tijdstip van intrekking van (Services) Certificaten precies kunnen worden vastgesteld. In geval van twijfel geldt het door KPN vastgestelde tijdstip als moment van intrekking.

Als een (Services) Certificaat is ingetrokken, kan het niet opnieuw geldig worden verklaard.

4.9.2 Wie mag een verzoek tot intrekking doen?

KPN zal een Certificaat intrekken na een verzoek daartoe van de Abonnee, de Certificaathouder of de Certificaatbeheerder. KPN mag ook zelf een verzoek tot intrekking initiëren.
Een Vertrouwende Partij kan geen verzoek tot intrekking doen, maar kan wel melding maken van het vermoeden van een omstandigheid die aanleiding kan zijn tot het intrekken van een Certificaat. KPN zal zo'n melding onderzoeken en zal, als daar aanleiding toe is, het Certificaat intrekken.

4.9.3 Procedure voor een verzoek tot intrekking

Een verzoek tot intrekking, dan wel de melding van een omstandigheid die kan leiden tot de intrekking van een Certificaat, kan geschieden langs de volgende wegen:

Schriftelijk: KPN Corporate Market B.V.
t.a.v. Afdeling Validatie, PKIoverheid Certificaten
Postbus 9105
7300 HN Apeldoorn

Online: https://www.pki.getronics.nl/website/getronics/178/Intrekken+certificaten.html

Nadrukkelijk wordt erop gewezen dat, in geval met de intrekking een spoedeisend belang gediend is, dit via de online / real time intrekkingspagina's dient te geschieden. Deze vorm van intrekking is zeven dagen per week vierentwintig uur per dag beschikbaar.

Voor het schriftelijk indienen van intrekkingsverzoeken is in de repository (http://www.pki.getronics.nl/website/401/PKIoverheid+formulieren.html) een formulier 'Intrekkingsverzoek Certificaten' beschikbaar.

KPN zorgt ervoor dat datum en tijdstip van intrekking van Certificaten precies kunnen worden vastgesteld. In geval van twijfel geldt het door KPN vastgestelde tijdstip als moment van intrekking.

Als een Certificaat is ingetrokken, kan het niet opnieuw geldig worden verklaard.

4.9.4 Tijdsduur voor verwerking intrekkingsverzoek

Zoals aangegeven: indien de intrekking een spoedeisend belang heeft, dient dit elektronisch via de online / real time intrekkingspagina's te geschieden.
Verzoeken tot intrekking per brief worden pas op zijn vroegst de volgende werkdag na ontvangst in behandeling genomen en worden niet gegarandeerd binnen vier uur na ontvangst verwerkt. De verwerkingstermijn hiervoor is 24 uur.

4.9.5 Controlevoorwaarden bij raadplegen certificaat statusinformatie

Vertrouwende Partijen zijn verplicht de actuele status (ingetrokken/niet ingetrokken) van een Certificaat te controleren door naslag van de certificaatstatusinformatie. Certificaatstatusinformatie kan worden verkregen door raadpleging van de CRL, OCSP of Directory Dienst. Tevens zijn Vertrouwende Partijen gehouden om de Elektronische Handtekening waarmee de CRL is getekend, inclusief het bijbehorende certificatiepad, te controleren.

Ingetrokken Certificaten blijven op de CRL staan zolang hun oorspronkelijke geldigheidsdatum niet is verstreken. Nadien is de status van dat Certificaat voor Vertrouwende Partijen enkel nog online te verifiëren via de Directory Dienst van KPN of via OCSP.

4.9.6 CRL-uitgiftefrequentie

De CRL-uitgifte frequentie is eens per vier uur, een CRL heeft een geldigheidsduur van vierentwintig uur.

4.9.7 Maximale vertraging bij CRL-uitgifte

Maximaal vier uur nadat een geautoriseerd online verzoek om intrekking is ontvangen, zal KPN het (Services) Certificaat intrekken.

4.9.8 Online intrekking/statuscontrole

KPN biedt naast de publicatie van CRL's ook certificaatstatusinformatie aan via het zogenaamde OCSP. De inrichting van OCSP is in overeenstemming met IETF RFC 2560.

OCSP validatie is een online validatie methode waarbij KPN aan de vertrouwende partij een elektronisch ondertekend bericht (OCSP response) verstuurt nadat de vertrouwende partij een specifiek verzoek om statusinformatie (OCSP request) heeft verstuurd naar de OCSP dienst (OCSP responder) van KPN. In de OCSP response staat de opgevraagde status van het betreffende certificaat.

De status kan de volgende waarden aannemen: goed, ingetrokken of onbekend. Als een OCSP response om enigerlei reden uitblijft, kan daaruit geen conclusie worden getrokken met betrekking tot de status van het certificaat. De URL van de OCSP responder waarmee de intrekkingstatus van een Certificaat gevalideerd kan worden, staat in het AuthorityInfoAccess.uniformResourceIndicator attribuut van het certificaat.

Een OCSP respons is altijd door de OCSP responder verzonden en ondertekend. Een Vertrouwende Partij dient de handtekening onder de OCSP respons te verifiëren met het systeemcertificaat dat meegestuurd wordt in de OCSP respons. Dit systeemcertificaat is uitgegeven door dezelfde Certification Authority (CA) als de CA die het Certificaat heeft uitgegeven waarvan de status wordt opgevraagd.

4.9.9 Certificate Status Service

De CRL maakt onderdeel uit van een CA-systeem. Dit systeem is 7 dagen per week 24 uur beschikbaar.

Ook in geval van systeemdefecten, service-activiteiten of andere factoren die buiten het bereik van KPN liggen, zorgt KPN ervoor dat voor intrekkingsverzoeken die online worden ingediend binnen vier uur na indiening een nieuwe CRL wordt uitgegeven. Daartoe is onder andere een uitwijklocatie en -scenario ontworpen, dat regelmatig wordt getest, in combinatie met redundante gegevensverwerking en –opslag.

4.9.10 Beëindiging van het abonnement

Indien een Abonnee het abonnement bij KPN wil beëindigen kan het daarvoor gebruik maken van een formulier ‘Opzeggen abonnement’. Voordat KPN het abonnement kan beëindigen dienen alle Certificaten van de Abonnee te zijn ingetrokken.

Die gemeenten die vanwege een gemeentelijke herindeling of die ministeries die vanwege een ministeriële herindeling ophouden te bestaan dienen niet direct maar uiteindelijk wel hun abonnement bij KPN op te zeggen. Niet direct omdat in die gevallen de rechten en plichten van de oude organisatie worden overgenomen door de nieuwe organisatie. Maar uiteindelijk wel omdat formeel de oude organisatie ophoudt te bestaan.

KPN zal het formulier in ontvangst nemen, de volledigheid en juistheid ervan beoordelen en erover beslissen. Onderdeel van deze beoordeling is of de Abonnee alle aan Abonnee uitgegeven Certificaten heeft ingetrokken. KPN informeert de Abonnee over het besluit.

4.9.11 Andere aankondigingen van intrekking

Naast het raadplegen van de certificaatstatus via CRL en OCSP, is het tevens mogelijk dit via de Directory Dienst op te vragen.

4.9.12 Certificaatopschorting

Opschorting van Certificaten (‘suspension’) wordt niet ondersteund door KPN.

4.10 Key Escrow and Recovery

Standaard vindt er geen Escrow van Private Sleutels plaats. Er is geen mogelijkheid tot het in Escrow nemen van Private Sleutels gerelateerd aan Handtekeningcertificaten en Authenticiteitcertificaten.

5 Management, operationele en fysieke beveiligingsmaatregelen

Het bedrijfsonderdeel van KPN dat de certificatiedienstverlening verzorgt is gecertificeerd tegen ISO9001: 2000, ISO27001:2005 en ETSI TS 101 456. Zowel het Quality Management System als het Information Security Management System zijn via de PDCA-cyclus bij voortduring gericht op verbetering van die systemen.

5.1 Fysieke beveiliging

5.1.1 Locatie, constructie en fysieke beveiliging

De certificatiedienstverlening wordt beheerd in en geleverd vanuit een streng beveiligde omgeving binnen het rekencentrum van KPN in Apeldoorn. Deze omgeving voldoet aan de voor de overheid in deze geldende wet- en regelgeving, waaronder onder meer begrepen de Wet Bescherming Staatsgeheimen 1951.

De fysieke toegang tot de beveiligde omgeving wordt gerealiseerd door een combinatie van procedurele en (bouw)technische maatregelen. Toegang tot het gebouw en de beveiligde omgeving wordt bewaakt middels elektronische (biometrische) en visuele middelen. Het toegangssysteem van het gebouw registreert het in- en uitgaan van personeel en bezoekers. Het gebouw wordt 7*24 uur bewaakt door een beveiligingsbedrijf.

De beveiligingssystemen signaleren automatisch pogingen tot (on)geautoriseerde toegang. De technische maatregelen worden ondersteund door verschillende procedures, onder andere door bewegingssensoren die personen en materialen (voor cryptografisch sleutelbeheer) monitoren. De technische infrastructuur inclusief de beveiligingssystemen bevindt zich in beschermde ruimten met een daarvoor benoemde beheerder. Toegang tot deze ruimten wordt geregistreerd o.a. voor audit-doeleinden.

Huishoudelijke regels zijn van kracht voor het registreren en begeleiden van bezoekers en servicepersoneel van derden. Met servicebedrijven zijn afspraken gemaakt voor toegang tot bepaalde ruimten. Daarnaast controleert de gebouwbeheerdienst de in- en uitgaande goederen (op basis van geleidedocumenten).

De beveiligde omgeving van KPN biedt standaard tot minimaal vijf fysieke barrières tot aan de productieomgeving. Voor niet-produktie (offline) opslag van bijvoorbeeld cryptografische hardware en materiaal gelden zes niveaus.

Het oneigenlijke verkrijgen van toegang tot de beveiligde omgeving vereist het compromitteren van meerdere systemen. Afhankelijk van de ruimte kan dit een combinatie zijn van kennis, SSCD/SUD, biometrische data, begeleiding bij toegang en visuele inspectie. Additionele maatregelen zijn onder andere inbraakdetectie en video-opnames. De verschillende toegangscontrolesystemen zijn van elkaar gescheiden en bewaken de toegang tot de beveiligde omgeving. Functiescheiding in combinatie met vijf of zes fysieke barrières zorgen ervoor dat niet één individu toegang kan krijgen tot kritische apparatuur van KPN.

KPN heeft tal van maatregelen getroffen om noodsituaties in de beveiligde omgeving te voorkomen en/of schade te beperken. Voorbeelden daarvan zijn:

- Bliksemafleiding;
- Airco voorzieningen

- Backup van elektricteit met behulp van een eigen elektricteitsvoorziening;
- Bouwkundige maatregelen (brandresistentie, waterafvoer, etc.);
- Brandpreventie door middel van automatisch en handmatige brandalarmvoorzieningen. Zulks in combinatie met gerichte, geautomatiseerde brandblussing.

De maatregelen worden op reguliere basis getest. In geval van uitzonderingssituaties treedt een escalatieplan in werking. Politie en brandweer zijn bekend met de specifieke situatie met betrekking tot de beveiligde omgeving van KPN.

5.1.2 Fysieke beveiliging Certificaathouders

Geen nadere bepalingen indien sprake is van Beroepsgebonden Certificaten, Persoonsgebonden Certificaten of Groepscertificaten.

Indien sprake is van een Servercertificaat, dan geldt dat het sleutelmateriaal moet zijn gegenereerd in een Veilige Omgeving en dat de Private Sleutel daarin blijvend moet zijn/worden ondergebracht. Zie voor een verdere toelichting de definitie van Veilige Omgeving (paragraaf 1.6).

5.1.3 Opslag van media

Opslagmedia van systemen die worden gebruikt voor PKIoverheid Certificaten, worden op een veilige manier behandeld binnen het gebouw om ze te beschermen tegen niet-geautoriseerde toegang, schade en diefstal. Opslagmedia worden zorgvuldig verwijderd wanneer zij niet langer nodig zijn.

5.1.4 Afval verwijdering

KPN heeft een overeenkomst gesloten met een professioneel afvalverwijderbedrijf voor de veilige afvoer van afval, gebruikt papier en dergelijk. Het personeel van KPN is eraan gehouden al het afvalpapier te gooien in de overal in het gebouw aanwezige afgesloten papiercontainers.

5.1.5 Off-site backup

Media met daarop data en programmatuur worden ook opgeslagen in een ander gebouw van KPN, met een minimaal gelijkwaardig beveiligingsniveau.

5.2 Procedurele beveiliging

Beveiligingstaken en –verantwoordelijkheden, waaronder vertrouwelijke functies, zijn gedocumenteerd in functieomschrijvingen. Deze zijn opgesteld op basis van de scheiding van taken en bevoegdheden en waarin de gevoeligheid van de functie is vastgesteld. Waar dat van toepassing is, is in de functieomschrijvingen onderscheid gemaakt tussen algemene functies en specifieke CSP-functies.

Voor alle vertrouwelijke en administratieve taken, die invloed hebben op de levering van Certificatiediensten, zijn procedures opgesteld en geïmplementeerd.

Autorisatie van het CSP personeel vindt plaats op basis van het ‘need-to-know’ principe.

5.2.1 Vertrouwelijke functies

KPN heeft een Trusted Employee Policy geïmplementeerd. In deze policy staat o.a. beschreven voor welke functiecategorieën en rollen de status “vertrouwd” hebben. Het betreft voornamelijk functies die betrokken zijn bij het management van certificaten en sleutelmateriaal, functies die betrokken zijn bij systeemontwikkeling, -beheer en –onderhoud en functies binnen security management, quality management en auditing. Zie ook 5.3.2. Trusted Employee Policy.

5.2.2 Aantal personen benodigd per taak

Voor het uitvoeren van bepaalde, vooraf gedefinieerde, activiteiten op het gebied van sleutel-, certificaatmanagement, systeemontwikkeling, -onderhoud en-beheer zijn meerdere medewerkers nodig. De noodzaak om met meerdere mensen een bepaalde activiteit wordt afgedwongen o.a. met behulp van technische voorzieningen, autorisaties in combinatie met identificatie/authenticatie en aanvullende procedures.

5.2.3 Beheer en beveiliging

KPN draagt zorg voor procedurele beveiliging door de toepassing van ITIL management processen. ITIL is een methodologie voor het standaardiseren van IT beheerprocessen met als doel de kwaliteit van deze processen op een vastgesteld niveau te brengen, te houden en waar mogelijk te verbeteren.

KPN heeft gescheiden systemen voor ontwikkeling, test, acceptatie en productie. Deze systemen worden beheerd met gebruikmaking van eerder genoemde ITIL procedures.
Het overbrengen van programmatuur van de ene omgeving naar de andere vindt gecontroleerd plaats, met gebruikmaking van de procedure voor change management. Deze procedure omvat onder andere het bijhouden en vastleggen van versies, het aanbrengen van wijzigingen en noodreparaties van alle operationele software.

De integriteit van alle systemen en informatie gebruikt voor PKIoverheid Certificaten wordt beschermd tegen virussen, schadelijke software en andere mogelijke verstoringen van de dienstverlening door middel van een passende combinatie van fysieke, logische en organisatorische maatregelen. Deze maatregelen zijn preventief, repressief en correctief van aard. Voorbeelden van getroffen maatregelen zijn: logging, firewalls, intrusion detection en redundantie van systemen.

KPN heeft erin voorzien dat er tijdige en gecoördineerde wijze actie wordt ondernomen om snel te reageren op incidenten en om de invloed van inbreuk op de beveiliging te beperken. Alle incidenten worden zo snel mogelijk gemeld nadat zij zich hebben voorgedaan.

5.2.4 Functiescheiding

KPN hanteert functiescheiding tussen uitvoerende, beslissende en controlerende taken. Daarnaast is er sprake van functiescheiding tussen systeembeheer en bediening van de systemen gebruikt voor PKIoverheid Certificaten, alsmede tussen Security Officer(s), Systeem auditor(s), systeembeheerder(s) en operator(s).

5.3 Personele beveiligingsmiddelen

5.3.1 Vakkennis, ervaring en kwalificaties

Voor de levering van PKIoverheid Certificaten zet KPN personeel in dat beschikt over voldoende vakkennis, ervaring en kwalificaties.

KPN heeft van elke functie vastgesteld welke kennis en ervaring voor een goede invulling benodigd is. Dit wordt onderhouden, omdat de ontwikkelingen in het vakgebied elkaar snel opvolgen. Daarnaast wordt van elke medewerker geregistreerd welke kennis en ervaring hij/zij bezit.
Jaarlijks wordt, als onderdeel van de Planning & Controlcyclus, een opleidingsplan opgesteld en na goedkeuring wordt het voor uitvoering van het plan benodigde budget beschikbaar gesteld. Realisatie van het plan wordt bewaakt en gevolgde opleidingen geregistreerd. Het volgen van vakgerichte opleidingen wordt waar nodig verplicht gesteld en waar mogelijk gestimuleerd. Daarnaast worden medewerkers on the job getraind. Medewerkers worden zo zo breed mogelijk geschoold en getraind, enerzijds om ze zo breed mogelijk te kunnen inzetten, anderzijds om ze zo veel mogelijk variatie in het takenpakket te kunnen bieden.

De medewerkers worden gevolgd m.b.v. een Personeels Performace Management (PPM)-cyclus die o.a. bestaat uit een doelstellingen-, een functionerings- en een beoordelingsgesprek.

5.3.2 Trusted Employee Policy

KPN heeft voor haar certificatiedienstverlening een Trusted Employee Policy opgesteld en geïmplementeerd. Bij het opstellen en onderhouden van deze policy is/wordt goed gekeken naar de mogelijkheden en onmogelijkheden van algemeen geldende wet- en regelgeving als het Burgerlijk Wetboek, de Wbp en de Weh en (klant)specifieke wet- en regelgeving vanuit bijvoorbeeld De Nederlandse Bank, de Pensioen- en Verzekeringskamer en PKIoverheid. In deze Policy is uitgebreid beschreven hoe wordt omgegaan met bijvoorbeeld een pre-employmentscreening (verplicht voor die medewerkers die betrokken zijn bij de certificatiedienstverlening), het opleveren van een Verklaring omtrent het Gedrag (VOG) ingevolge de Wji (eveneens verplicht) en het uitvoeren van veiligheidsonderzoeken door diensten als Algemene Inlichtingen- en Veiligheidsdienst of de Militaire Inlichtingen- en Veiligheidsdienst ter verkrijging van een Verklaring van Geen Bezwaar (VGB). In de policy is ook opgenomen welke mogelijkheden het management heeft indien een (toekomstige) medewerker niet mee wil werken dan wel de uitkomst van het onderzoek niet positief is.

Andere bepalingen uit de TEP zijn:
- Personeel dat geen dienstverband heeft met KPN kan onder geen enkele voorwaarde zonder direct toezicht een functie of rol vervullen met de status “vertrouwd”;
- Een vertrouwde functie/rol mag pas worden uitgevoerd indien het bijbehorende onderzoek is afgerond, er geen bezwaar is gerezen en de medewerker formeel door het management is benoemd.
- Een inschatting maken van de veiligheidsrisico’s gedurende het dienstverband is een verantwoordelijkheid van de directe leidinggevende als onderdeel van de PPM-cyclus.

5.4 Procedures ten behoeve van beveiligingsaudits

5.4.1 Vastlegging van gebeurtenissen

KPN houdt voor audit-doeleinden overzichten bij van:
- aanmaak van accounts;

- installatie van nieuwe software of software updates;
- datum en tijd en andere beschrijvende informatie betreffende backups;
- datum en tijd van alle hardware wijzigingen;
- datum en tijd van auditlog dumps;
- afsluiting en (her)start van systemen.

KPN houdt de volgende gebeurtenissen handmatig of automatisch bij
- Levenscyclus gebeurtenissen ten aanzien van de CA sleutel, waaronder:
    - genereren van sleutels, backup, opslag, herstel, archivering en vernietiging;
    - levenscyclus gebeurtenissen ten aanzien van de cryptografische apparatuur.
- Levenscyclus gebeurtenissen ten aanzien van het beheer van Certificaten, waaronder:
    - certificaataanvragen, uitgifte en intrekking;
    - geslaagde of niet-geslaagde verwerking van aanvragen;
    - genereren en het uitgeven van Certificaten en CRL's.
- Beveiligingsincidenten, waaronder:
    - geslaagde en niet-geslaagde pogingen om toegang tot het systeem te verkrijgen
    - PKI en beveiligingsactiviteiten ondernomen door personeel;
    - lezen, schrijven of verwijderen van beveiligingsgevoelige bestanden of records;
    - veranderingen in het beveiligingsprofiel;
    - systeem crashes, hardware uitval, en andere onregelmatigheden.

De onderdelen van de logs bevatten de volgende elementen:
- datum en tijd;
- volgnummer;
- identiteit invoerder;
- soort.

Audit logs worden regelmatig gereviewed om te bezien of er zich belangrijke security of operationele gebeurtenissen hebben voorgedaan waar eventueel nadere actie op moet worden ondernomen.

5.4.2 Bewaartermijn audit-log

De geconsolideerde (elektronische) auditlogs worden evenals de handmatige registraties tijdens de geldigheidsduur van het Certificaat en bovendien gedurende een periode van ten minste zeven jaar na de datum waarop de geldigheid van het Certificaat is verlopen bewaard.

5.4.3 Bescherming van audit-log

Gebeurtenissen die op elektronische wijze worden geregistreerd, worden opgenomen in audit logfiles. Deze worden door middel van een passende combinatie van verschillende soorten beveiligingsmaatregelen, waaronder onder andere encryptie en functiescheiding, beschermd tegen niet-geautoriseerde inzage, wijziging, verwijdering of andere ongewenste aanpassingen.

Gebeurtenissen die handmatig worden geregistreerd, worden vastgelegd in dossiers. Deze dossiers worden opgeborgen in brandveilige kasten in een van passende toegangsmaatregelen voorziene, fysiek veilige omgeving.

5.4.4 Audit-log back-up procedure

Incrementele backups van audit logs worden op dagelijkse basis, op geautomatiseerde wijze, gecreëerd, volledige backups worden op wekelijkse basis uitgevoerd en worden ook gearchiveerd op een externe locatie.

5.5 Archivering van documenten

5.5.1 Vastlegging van gebeurtenissen

KPN legt alle relevante registratie-informatie vast, waaronder tenminste:
- het certificaataanvraagformulier;
- de gegevens van/over het identiteitsdocument dat door de Certificaathouder of Certificaatbeheerder is getoond;
- de bevindingen en het besluit over de aanvraag;
- de identiteit van van de validatiemedewerker die de Certificaataanvraag heeft behandeld respectievelijk heeft goedgekeurd;
- de methode om identiteitsdocumenten te valideren en identiteiten vast te stellen;
- het bewijs van identificatie en ontvangst.

5.5.2 Bewaartermijn archief

KPN bewaart alle relevante documentatie en informatie van een Certificaat tijdens de geldigheidsduur daarvan, alsmede gedurende een periode van tenminste zeven jaar na de datum waarop de geldigheidsduur van het Certificaat is verlopen.

5.5.3 Bescherming van archieven

KPN verzorgt zelf de archivering. Het zorgt voor de integriteit en toegankelijkheid van de gearchiveerde gegevens gedurende de bewaartermijn.
Alle noodzakelijke apparatuur en programmatuur voor het ontsluiten van de informatie wordt gedurende dezelfde periode bewaard. KPN zorgt voor een zorgvuldige en beveiligde wijze van opslag en archivering.

5.5.4 Archief back-up procedure

Geen nadere bepalingen.

5.5.5 Voorwaarden aan tijdsaanduiding van vastgelegde gebeurtenissen

De preciese datum en tijdstip van relevante gebeurtenissen in de levenscyclus van certificaten en sleutels worden vastgelegd. Dit geldt eveneens voor belangrijke gebeurtenissen in de levenscyclus van de systemen die worden gebruikt voor of ondersteuning bieden aan de certificatiedienstverlening.

5.6 Vernieuwen van sleutels

De sleutels van een CA-Certificaat worden vernieuwd tegelijk met het vernieuwen van dat CA-Certificaat.
Oude sleutels blijven bewaard op het token indien daar ook de nieuwe op geplaatst worden. Oude tokens worden na beëindiging van hun levendsuur en de erbij behorende archiveringsperiode vernietigd (zeroising).

Sleutels van Certificaathouders zullen niet opnieuw worden gebruikt na het verstrijken van de geldigheidsduur of na het intrekken van de bijbehorende (Services) Certificaten.

5.7 Aantasting en continuïteit

5.7.1 Calamiteitmanagement

KPN heeft procedures geïmplementeerd om de gevolgen van eventuele calamiteiten zoveel mogelijk te minimaliseren. Tot deze maatregelen behoren een calamiteitenplan en een uitwijkscenario. Compromittering van de Private Sleutel van KPN wordt beschouwd als een calamiteit. KPN stelt Vertrouwende Partijen, Abonnees, Certificaathouders en Certificaatbeheerders zo spoedig mogelijk op de hoogte van de compromittering van de Private Sleutel van KPN door informatie daaromtrent te publiceren op haar website (zie Elektronische Opslagplaats). Daarnaast zal KPN aan Abonnees, Certificaathouders en Certificaatbeheerders een e-mail sturen en de Overheids-Policy Authority onmiddellijk op de hoogte brengen.

5.7.2 Uitwijk

KPN heeft voor haar CRL en de online intrekkingsfaciliteit een volledige uitwijk ingericht. De uitwijkvoorziening is voor wat betreft programmatuur en gegevens bij voortduring volledig identiek aan de productie-omgeving en er kan, bijvoorbeeld in geval van een calamiteit, van het ene op het andere moment worden overgeschakeld naar de uitwijkvoorziening. Dit overschakelen wordt regelmatig getest. De uitwijklocatie is een andere KPN locatie (Lelystad) en heeft een gelijkwaardig beveiligingsniveau.

Voor de overige onderdelen van het CA-systeem is een uitwijkscenario gerealiseerd. Dit scenario voorziet in het realiseren van een uitwijk binnen 24 uur. Dit scenario wordt onderhouden en jaarlijks getest.

5.8 CSP-beëindiging

In geval KPN de certificatiedienstverlening beëindigt, zal door haar het CA Termination Plan worden uitgevoerd. Onderdelen van het plan zijn onder andere het:

- tenminste drie maanden van tevoren Abonnees, Certificaathouders en Certificaatbeheerders inlichten over de beëindiging en de wijze waarop de beëindiging gerealiseerd gaat worden;
- per direct stoppen met het uitgeven van nieuwe Certificaten;
- waar redelijkerwijs mogelijk maatregelen nemen om schade te beperken die voor Abonnees en Certificaathouders kan ontstaan vanwege de beëindiging van de dienstverlening;
- realiseren van voorzieningen met betrekking tot de overdracht van de verplichtingen aan andere Certificatiedienstverleners, inzoverre dit redelijkerwijs mogelijk is;
- ervoor zorgen dat het bewijs van certificatie, nodig om in rechte bewijs te kunnen leveren, blijft bestaan;
- in stand houden van de revocation status service (inclusief de CRL's) tot 6 maanden nadat de geldigheidsduur van het laatste uitgegeven Certificaat verlopen is of beëindigd is door intrekking. Zodra dit het geval is, zal KPN de voor betreffende dienstverlening gebruikte infrastructuur en alle daarvoor door haar gebruikte Private Sleutels vernietigen of permanent buiten werking stellen.

6 Technische beveiliging

6.1 Genereren en installeren van sleutelparen

6.1.1 Genereren van sleutelparen

Bij het genereren van CA-sleutelparen maakt KPN gebruik van betrouwbare procedures die worden uitgevoerd binnen een beveiligde omgeving die voldoet aan objectieve en internationaal erkende standaards.

De sleutelgeneratie van de voor PKIoverheid Certificaten gebruikte CA's van KPN heeft plaatsgevonden in een EAL4+ gecertificeerde HSM, in overeenstemming met ISO 15408 ('Cryptographic module for CSP Signing Operations'). Hierbij is onder de SHA-1 root (domein Overheid/Bedrijven) gebruik gemaakt van het signature algoritme 'SHA1RSA'. De sleutels van de sleutelparen zijn 2048 bits asymmetrisch RSA en het gebruikte hashing algoritme is 'SHA-1' en hierbij is onder de SHA-2 root (domein Organisatie) gebruik gemaakt van het signature algoritme 'SHA2RSA'. De sleutels van de sleutelparen zijn 4096 bits asymmetrisch RSA en het gebruikte hashing algoritme is 'SHA-2'.

De sleutelgeneratie voor Persoonsgebonden Certificaten vindt plaats in SSCD's. De sleutelgeneratie voor Groepscertificaten vindt plaats in SUD's. Hierbij wordt onder de SHA-2 root (domein Organisatie) gebruik gemaakt van het signature algoritme 'SHA256RSA'. De sleutels van de sleutelparen zijn 2048 bits of hoger asymmetrisch RSA en het gebruikte hashing algoritme is 'SHA-2'.

Bij het behandelen en afhandelen van certificaataanvragen, het genereren van sleutelparen en certificaten voor Eindgebruikers maakt KPN gebruik van veilige middelen en betrouwbare systemen. Deze betrouwbare systemen zijn voorzien van een positieve CWA 14167-1 auditverklaring.

Alle Certificaten, met uitzondering van Servercertificaten, worden door een betrouwbaar systeem in een SSCD (voor persoonsgebonden en beroepsgebonden certificaten) of SUD (voor Groepscertificaten) gegenereerd. Op de SSCD en de SUD kunnen meerdere Certificaten worden opgeslagen. Voor de Servercertificaten geldt dat deze verplicht worden gegenereerd door en onder verantwoording van de Abonnee in een Veilige Omgeving.

6.1.2 Overdracht van Private Sleutel en SSCD aan Abonnee

Persoonsgebonden, Beroepsgebonden Certificaten of Groepscertificaten worden op de volgende wijze overgedragen aan de Certificaathouder: toezending van de SSCD of SUD, met daarop onder andere de door KPN aangemaakte Private Sleutels, via een commercieel postbedrijf, waarbij de benodigde PIN voor de SSCD of SUD gescheiden wordt verstrekt aan de Certificaathouder ('out of band'). De Certificaathouder tekent voor ontvangst van de SSCD of SUD voordat hij/zij zich laat identificeren door GWK Travelex of door KPN zelf en voordat hij/zij de PIN krijgt toegestuurd.

Het sleutelpaar waarvan de Publieke Sleutel door KPN wordt voorzien van een Servercertificaat wordt door de Abonnee gegenereerd in de Veilige Omgeving van de Abonnee. De Private Sleutel blijft in die Veilige Omgeving, wordt dus niet overgedragen.

6.1.3 Overdracht van de Publieke Sleutel van de Abonnee

De sleutelparen van Persoonsgebonden, Beroepsgebonden en Groepscertificaten worden gegenereerd door KPN worden dus niet door de Abonnee aan KPN overgedragen.

De Abonnee stuurt wel de Publieke Sleutel naar KPN om deze te laten voorzien van een Servercertificaat. Deze Publieke Sleutel wordt gevoegd in/bij een elektronisch aanvraagformulier en wordt daarbij gekoppeld aan een uniek Certificate Signing Request-nummer (CSR-nummer). De koppeling van Publieke Sleutel aan CSR-nummer wordt, nadat de Publieke Sleutel is voorzien van een Servercertificaat, gebruikt om de van een Servercertificaat voorziene Publieke Sleutel per e-mail terug te sturen naar het e-mail adres vermeld in de Certificaataanvraag van de Abonnee.

De Abonnee is verplicht de meegestuurde ontvangstbevestiging te ondertekenen en binnen maximaal 6 weken naar KPN te versturen. Indien KPN die ontvangstbevestiging niet tijdig ontvangt wordt het Servercertificaat zonder nadere aankondiging ingetrokken. Indien de ontvangstbevestiging niet binnen 3 weken is terugontvangen stuurt KPN een herinnering.

6.1.4 Overdracht van de Publieke Sleutel van CSP aan Vertrouwende Partijen

De Publieke Sleutels van KPN gebruikt voor PKIoverheid Certificaten worden aan Vertrouwende Partijen beschikbaar gesteld via de Directory Dienst van KPN (zie Elektronische Opslagplaats).

6.1.5 Sleutellengten

De sleutellengte van een Certificaat is minstens 1024 bits RSA. Vanaf 01-01-2011 worden echter alleen nog Certificaten met 2048 bits uitgegeven. De sleutellengte van een SHA-1 CA-Certificaat is 2048 bits RSA en van een SHA-2 CA-Certificaat is dit 4096 bits.

6.1.6 Generatie van Publieke Sleutel-parameters

Geen opmerkingen.

6.1.7 Gebruik van het sleutelpaar

Zie voor het gebruik van key usage extensies paragraaf 7.1.4. Overzicht Certificaatprofielen.

6.1.8 Doelen van sleutelgebruik (zoals bedoeld in X.509 v3)

De Certificaten, inclusief de daarbij behorende sleutelparen, zijn uitsluitend bedoeld voor de doeleinden die beschreven zijn in deze CPS en die zijn opgenomen in (de extensies van) het Certificaat (veld: Key Usage).

6.2 Private sleutelbescherming en cryptografische module engineering beheersmaatregelen

Bij de ontwikkeling en het gebruik van cryptografische onderdelen zorgt KPN er voor dat deze onderdelen voldoen aan alle eisen die kunnen worden gesteld op het gebied van beveiliging, betrouwbaarheid, toepassingsbereik en beperking van de storingsgevoeligheid. Ter beoordeling van de toepasselijke procedures kan worden uitgegaan van internationaal erkende standaards.

6.2.1 Standaarden voor cryptografische module

Voor operationeel gebruik worden de cryptografische gegevens opgeslagen in een HSM. De HSM is EAL4+ gecertificeerd.

De HSM's worden door de leverancier aangeleverd in tamper-evident bags, zijnde verpakking die elke vorm van corruptie daarvan toonbaar maken. Elke zending wordt direct na binnenkomst gecontroleerd aan de hand van de bijbehorende, out-of-band toegestuurde, list.

KPN hanteert Key Management procedures voor het installeren, het activeren, back-up en herstel van de Private Sleutels van de KPN CA's, waarmee (Services) Certificaten en CRL's worden ondertekend. Deze acties worden door tenminste twee werknemers gelijktijdig uitgevoerd.

Private Sleutels van KPN CA's worden vernietigd op het moment dat dit middel buiten gebruik wordt gesteld.

6.2.2 Controle op Private Sleutel door meerdere personen

De Private Sleutels behorende bij de CA-Certificaten van KPN zijn in beginsel niet in één stuk leesbaar. De cryptografische hardware modules waarop ze worden opgeslagen zijn daarnaast zodanig beveiligd, dat meerdere personen nodig zijn om er toegang tot te krijgen, en ze worden opgeborgen in een Veilige Omgeving. Deze Veilige Omgeving is voorzien van meerdere beveiligingslagen, voorzien van beveiligingsmaatregelen van verschillende soort (technisch, fysiek en organisatorisch) en aard (preventief, detectief etc). Om de beveiligingslagen te kunnen passeren zijn meerdere medewerkers nodig van meerdere afdelingen.

6.2.3 Escrow van Private Sleutels van Certificaathouders

Standaard vindt er geen Escrow van Private Sleutels plaats. Desgewenst kan een Abonnee een verzoek indienen tot Escrow van Private Sleutels van Vertrouwelijkheidscertificaten en kunnen daarover afspraken gemaakt worden.

Indien de Private Sleutel van een vertrouwelijkheidscertificaat niet in escrow is genomen, zal verlies, vernietiging of het anderszins onbruikbaar raken van de Private Sleutel tot gevolg hebben dat de hiermee versleutelde gegevens definitief niet meer te ontsleutelen zijn.

Er is geen mogelijkheid tot Escrow van Private Sleutels gerelateerd aan Handtekeningcertificaten en Authenticiteitcertificaten.

6.2.4 Back-up van Private Sleutels

Er wordt een backup gemaakt van de Private Sleutels behorende bij de CA-Certificaten van KPN. De backup wordt in versleutelde vorm bewaard in cryptografische modules en bijbehorende opslagapparatuur.

Van de Private Sleutels behorende bij Certificaten wordt geen backup gemaakt

6.2.5 Archivering van Private Sleutels

Private Sleutels van Certificaten worden niet gearchiveerd.

6.2.6 Toegang tot Private Sleutels in cryptografische module

Voor de Private Sleutels behorende bij CA-Certificaten van KPN, die zijn opgeslagen in een cryptografische hardware module, wordt toegangsbeveiliging gebruikt die garandeert dat de sleutels niet buiten de module kunnen worden gebruikt. Zie 6.2.2.

6.2.7 Opslag van Private Sleutels in cryptografische module

CA-Private Sleutels worden versleuteld opgeslagen in hardware cryptografische modules.

6.2.8 Activering van Private Sleutels

Door middel van een sleutelceremonie, ten overstaan van de daarvoor noodzakelijk aanwezige functionarissen, worden de Private Sleutels behorende bij CA-Certificaten van KPN geactiveerd.

6.2.9 Deactivering van Private Sleutels

Onder specifieke omstandigheden kan KPN bepalen dat de Private Sleutels worden gedeactiveerd, met inachtneming van de daarop van toepassing zijnde waarborgen ten behoeve van zorgvuldigheid.

Indien een SSCD of SUD door de Certificaathouder wordt verloren en door een vinder wordt geretourneerd aan KPN, zal deze SSCD of SUD door haar worden vernietigd, inclusief de daarin opgenomen Private Sleutels. Alsdan zal KPN tevens controleren of de bijbehorende Certificaten zijn ingetrokken en zoniet, dan zal ze daar per direct toe overgaan.

6.2.10 Methode voor het vernietigen van Private Sleutels

De Private Sleutels waarmee Certificaten worden ondertekend, kunnen na het einde van hun levenscyclus niet meer kunnen worden gebruikt. KPN zorgt voor een adequate vernietiging waarbij wordt voorkomen dat het mogelijk is de vernietigde sleutels te herleiden uit de restanten. Als dergelijke sleutels worden vernietigd worden die activiteiten gelogd.

6.2.11 Eisen voor veilige middelen voor opslag en gebruik van Certificaten

Voor die certificaten die worden uitgegeven op smartcards, dat betreft de persoonsgebonden certificaten en de groepscertificaten, geldt dat de smartcards gecertificeerd zijn tegen CWA 14169 op het niveau EAL4+.

In het geval van Servercertificaten wordt gebruik gemaakt van de door PKIoverheid geboden mogelijkheid om de sleutels van een Servercertificaat softwarematig te beschermen. Dit betekent dat de omgeving waarin de sleutels worden gegenereerd en bewaard net zo veilig moet zijn als indien dat gebeurt in een SUD. Datzelfde beveiligingsniveau kan worden bereikt door een samenstel van passende, compenserende maatregelen te treffen in en voor die omgeving.

De compenserende maatregelen moeten van een dusdanige kwaliteit zijn dat het praktisch onmogelijk is de sleutels ongemerkt te stelen of te kopiëren. Bij compenserende maatregelen moet bijvoorbeeld worden gedacht aan een combinatie van fysieke toegangsbeveiliging, logische toegangsbeveiliging, logging en audit en functiescheiding.

Bij de Certificaataanvraag voor een Servercertificaat verklaart de Abonnee dat de omgeving waarin de sleutels zijn gegenereerd en worden bewaard voldoende veilig is, zoals hiervoor beschreven.

In de Bijzonder Voorwaarden opgenomen dat KPN het recht heeft om een controle uit te voeren naar de getroffen maatregelen.

6.3 Andere aspecten van sleutelpaarmanagement

Alle aspecten van sleutelpaarmanagement worden door KPN uitgevoerd met inachtneming van zorgvuldige procedures die in overeenstemming zijn met het beoogde doel.

6.3.1 Archiveren van Publieke Sleutels

Publieke Sleutels worden gearchiveerd door KPN voor tenminste zeven jaar na het verstrijken van de oorspronkelijke geldigheidsduur van een Certificaat. Archivering zal plaatsvinden in een fysiek beveiligde omgeving.

6.3.2 Gebruiksduur voor Certificaten,Publieke Sleutel en Private Sleutels

Voor SHA-1 Certificaten, inclusief het bijbehorende sleutelpaar, geldt een maximale geldigheidsduur van tot 31 december 2011. Voor SHA-2 certificaten kan worden gekozen voor een geldigheidsduur van 3 jaar (standaard) of 5 jaar. Dit geldt echter niet voor Servercertificaten, het PvE van PKIoverheid staat voor Servercertificaten een maximale geldigheidsduur van 3 jaar toe.

KPN zal de Abonnee minimaal twee maanden voor het verstrijken van de geldigheidsduur van de op zijn verzoek uitgegeven Certificaten informeren over het verstrijken van die geldigheidstermijn.

6.4 Activeringsgegevens

6.4.1 Genereren en installeren van activeringsgegevens

De SSCD of SUD, waarin het Sleutelpaar en het bijbehorende Certificaat worden opgeslagen, wordt voorzien van activeringsgegevens. Deze PIN- en PUK-code worden gegenereerd door een betrouwbaar systeem, bestaan uit vijf tekens en worden afgedrukt op een PIN-mail. Na acceptatie van de PIN-mail vernietigt het systeem de PIN- en PUK-code. In de tijd tussen generatie en acceptatie worden de codes geëncrypt opgeslagen door het betrouwbare systeem.

6.4.2 Bescherming activeringsgegevens

De PIN-mail, met daarop onder andere afgedrukt de PIN- en PUK-code, wordt via een andere weg en op een ander tijdstip, gescheiden dus van SSCD of SUD, verstuurt naar de Certificaathouder/Certificaatbeheerder. Na ontvangst van de PIN- en PUK-code is de Certificaathouder/Certificaatbeheerder exclusief verantwoordelijk voor de bescherming en de geheimhouding daarvan.

6.4.3 Werking van de activeringsgegevens

Om toegang te kunnen krijgen tot het Sleutelmateriaal en Certificaat moet de Certificaathouder gebruik maken van de verkregen PIN-code, behorende bij de SSCD of SUD. Indien de PIN-code driemaal onjuist is ingevoerd, wordt de SSCD of SUD automatisch geblokkeerd. Alsdan kan SSCD of SUD enkel worden gedeblokkeerd met de PUK-code.

Indien de PUK-code driemaal onjuist wordt ingevoerd, is de SSCD of SUD definitief geblokkeerd en daardoor onbruikbaar geworden.

6.5 Logische toegangsbeveiliging van CSP-systemen

6.5.1 Specifieke technische vereisten aan computerbeveiliging

KPN beveiligt op passende wijze de voor PKIoverheid Certificaten gebruikte computersystemen tegen ongeautoriseerde toegang en andere bedreigingen, onder andere via multi factor authenticatie.

De integriteit van CSP-systemen en -informatie wordt beschermd tegen virussen, schadelijke en niet-geautoriseerde software en andere mogelijk bronnen die kunnen leiden tot verstoring van de dienstverlening, door middel van een samenstel van passende fysieke, logische en organisatorische maatregelen. Deze maatregelen zijn preventief, dedectief, repressief en correctief van aard. Voorbeelden van maatregelen zijn: logging, firewalls, intrusion detection en redundantie van systemen, systeemonderdelen en netwerkcomponenten.

De Directory Dienst is op adequate wijze beveiligd tegen manipulatie en is online toegankelijk. Informatie over de intrekkings-status is vierentwintig uur per dag en zeven dagen per week te raadplegen.

6.5.2 Beheer en classificatie van middelen

KPN classificeert de gebruikte middelen op basis van een risico-assessment.

6.6 Beheersmaatregelen technische levenscyclus

6.6.1 Beheersmaatregelen ten behoeve van systeemontwikkeling

KPN ontwikkelt daarnaast, gedeeltelijk, haar eigen CardManagementSystem (CMS). Het CMS wordt weliswaar verkregen van een gespecialiseerde leverancier, maar bestaat uit vele, verschillende, kleine modules, die los van elkaar, in verschillende volgorde en in verschillende samenstelling kunnen worden samengevoegd tot een werkend CMS aan de hand van een door de leverancier aangeleverde systematiek. Verschillende ontwikkelaars zijn geschoold in deze systematiek, daar waar nodig worden deze ondersteund door de leverancier.

In het beheer van het CMS is functiescheiding aangebracht tussen de ontwikkel-, de gebruikers- en de beheerorganisatie. Deze functiescheiding is doorgetrokken in de, van elkaar gescheiden, productie-, test- en ontwikkelomgevingen. Overgang van ontwikkel-, naar test- en naar productieomgeving wordt beheerst gerealiseerd m.b.v. de bestaande changemanagement-procedure. Deze changemanagement procedure omvat onder andere het bijhouden en vastleggen van versies, wijzigingen en noodreparaties van alle operationele software.

De andere CA-systemen worden verkregen van betrouwbare leveranciers en zijn, net als het CMS, voorzien van een CWA 14167-1 auditverklaring of gelijkwaardig.

De systemen van KPN maken gebruik van een vertrouwde tijdsbron.

Het capaciteitsgebruik wordt bijgehouden en voorspellingen van de in de toekomst vereiste capaciteit worden gemaakt om te voorzien in voldoende verwerkingsvermogen en opslagcapaciteit in de toekomst.

6.6.2 Security Management beheersmaatregelen

De levering van software door leveranciers is omgeven met beheersmaatregelen waarmee de integriteit en de authenticiteit van de software vastgesteld kan worden. Een maatregel die daarbij gebruikt naast de in 6.6.1. genoemde maatregelen is het gebruik van hashes.

6.7 Netwerkbeveiliging

KPN neemt maatregelen om de stabiliteit, de betrouwbaarheid en de veiligheid van het netwerk te waarborgen. Dit omvat bijvoorbeeld maatregelen om gegevensverkeer te reguleren en ongewenst gegevensverkeer te vinden en onmogelijk te maken, alsmede de plaatsing van firewalls om de integriteit en exclusiviteit van het netwerk te garanderen.

6.8 Time-stamping

KPN verzorgt geen time-stamping services.

7 Certificaat-, CRL- en OCSP-profielen

7.1 Certificaatprofielen

7.1.1 CP OID

De van toepassing zijnde Certificate Policies kunnen via de volgende OID worden geïdentificeerd:

Persoonsgebonden en Beroepsgebonden Certificaten:

Domein Overheid/Bedrijven	
2.16.528.1.1003.1.2.2.1	Authenticiteitcertificaat
2.16.528.1.1003.1.2.2.2	Handtekeningcertificaat
2.16.528.1.1003.1.2.2.3	Vertrouwelijkheidcertificaat
Domein Organisatie	
2.16.528.1.1003.1.2.5.1	Authenticiteitcertificaat
2.16.528.1.1003.1.2.5.2	Handtekeningcertificaat
2.16.528.1.1003.1.2.5.3	Vertrouwelijkheidcertificaat

Servercertificaten:

Domein Overheid/Bedrijven	
2.16.528.1.1003.1.2.2.6	Servercertificaat.
Domein Organisatie	
2.16.528.1.1003.1.2.5.6	Servercertificaat.

Groepscertificaten:

Domein Overheid/Bedrijven	
2.16.528.1.1003.1.2.2.4	Authenticiteitcertificaat.
2.16.528.1.1003.1.2.2.5	Vertrouwelijkheidcertificaat.
Domein Organisatie	
2.16.528.1.1003.1.2.5.4	Authenticiteitcertificaat.
2.16.528.1.1003.1.2.5.5	Vertrouwelijkheidcertificaat.

7.1.2 Overzicht Certificaatprofielen

De PKIoverheid Certificaten zijn opgebouwd volgens de PKIX X.509 v3 standaard, waarbij de mogelijkheid bestaat dat extensies worden gebruikt.
Handtekeningcertificaten worden opgebouwd volgens het Qualified Certificate Profile van EESSI/ETSI. Eventuele extensies in dat kader worden ook in de overige Certificaten opgenomen.
Certificaatprofielen zijn opgemaakt volgens Deel 3 van het Programma van Eisen van de PKIoverheid, conform het Certificaatprofiel van het Certificaat voor het Domein Overheid/Bedrijven en Organisatie.

7.1.2.1 Persoonsgebonden en Beroepsgebonden certificaten

Basis attributen

Veld	Waarde
Version	2 (X.509v3)
SerialNumber	Uniek 128 bits lang serienummer
Signature	Het gebruikte algoritme is onder de SHA-1 root (domein Overheid /Bedrijven) sha1WithRSAEncryption. Het gebruikte algoritme is onder de SHA-2 root (domein Organisatie) sha256WithRSAEncryption.
Issuer	Bevat de naam van de betreffende Getronics PinkRoccade CA wordt weergegeven door de volgende attributen: CommonName, OrganizationName en CountryName. Er zijn meerdere CA certificaten in gebruik (geweest). • In het oude niet meer gebruikte CA-Certificaat is OrganizationName gedefinieerd als 'PinkRoccade Infrastructure Services BV'. De CommonName bevat 'PinkRoccade CSP - Overheid – ' en de aanduiding 'Onweerlegbaarheid CA' of 'Vertrouwelijkheid CA' of 'Authenticiteit CA', afhankelijk van het type certificaat. De CountryName is ingesteld op 'NL'. • In het nieuwe CA-Certificaat is OrganizationName gedefinieerd als 'Getronics PinkRoccade Nederland B.V.'. De CommonName is ingesteld op 'Getronics PinkRoccade PKIoverheid CA – Overheid/Bedrijven en Organisatie'. De CountryName is ingesteld op 'NL'.
Validity	De geldigheidsperiode van het SHA-2 Certificaat is standaard 3 jaar, maar er kan worden gekozen voor een geldigheidsduur van 5 jaar.
Subject	De naam van het subject wordt weergegeven als een Distinguished Name (DN), en wordt weergegeven door tenminste de volgende attributen: • CountryName; • CommonName; • OrganizationName; • Title • SerialNumber (subjectserienummer). De attributen die worden gebruikt om het subject te beschrijven benoemen het subject op unieke wijze. Het CountryName attribuut is ingesteld op de tweeletterige landcode "NL" volgens ISO 3166. Het Title attribuut wordt alleen gevuld met het Erkende Beroep van de Certificaathouder indien een Beroepsgebonden Certificaat is aangevraagd.
subjectPublicKeyInfo	Bevat de PublicKey van de Subject

Standaard extensies

Veld	Essentieel	Waarde
AuthorityKeyIdentifier	Nee	KeyIdentifier is ingesteld op 160 bit SHA-1 hash
SubjectKeyIdentifier	Nee	KeyIdentifier is ingesteld op 160 bit SHA-1 hash
KeyUsage	Ja	In Authenticiteitcertificaten is het digitalSignature bit opgenomen. In Vertrouwelijkheidcertificaten zijn de keyEncipherment, dataEncipherment en de keyAgreement bits opgenomen. In Handtekeningcertificaten is het non-Repudiation bit op unieke wijze zijn opgenomen.
BasicConstraints	Ja	Het CA bit is ingesteld op 'False' en pathLenConstraint op 'none'
CertificatePolicies	Nee	Domein Overheid/Bedrijven Authenticiteitcertificaten bevatten het OID 2.16.528.1.1003.1.2.2.1. Handtekeningcertificaten bevatten het OID: 2.16.528.1.1003.1.2.2.2. Vertrouwelijkheidcertificaten bevatten het OID 2.16.528.1.1003.1.2.2.3. Domein Organisatie Authenticiteitcertificaten bevatten het OID 2.16.528.1.1003.1.2.5.1. Handtekeningcertificaten bevatten het OID: 2.16.528.1.1003.1.2.5.2. Vertrouwelijkheidcertificaten bevatten het OID 2.16.528.1.1003.1.2.5.3. Alle typen Certificaten bevatten een link naar het CPS en een gebruikerstekst. De gebruikersnotitie bevat de melding dat in geval het veld <job_title> gevuld is met een Erkend Beroep sprake is van een Beroepsgebonden Certificaat. De Certificaathouder handelt bij gebruik van diens certificaten uit hoofde van zijn beroep. Zulks onder verwijzing naar dit CPS.
SubjectAltName	Nee	Hierin is opgenomen • het e-mail adres van de Subject; • het OID van de betreffende CA; • het Subjectserienummer van de Certificaathouder. Het OID van de betreffende CA is één van de volgende: • PinkRoccade CSP CA behorend bij het type Certificaat; - authenticiteit 2.16.528.1.1003.1.3.2.2.1, - Onweerlegbaarheid2.16.528.1.1003.1.3.2.2.2, - vertrouwelijkheid 2.16.528.1.1003.1.3.2.2.3 • of de Getronics PinkRoccade PKIoverheid CA – Overheid/Bedrijven en Organisatie CA; 2.16.528.1.1003.1.3.2.2.5 • of de Getronics CSP Organisatie CA – G2; 2.16.528.1.1003.1.3.5.4.1.

		Authenticiteitcertificaten kunnen tevens een UPN bevatten ten behoeve van Windows Smartcard Logon bevatten.
CrlDistributionPoints	Nee	Bevat de URI waarde waar de CRL, die behoort bij het type Certificaat, kan worden opgehaald.
ExtendedKeyUsage	Nee	Authenticiteitcertificaten kunnen deze extensie bevatten. Deze extensie maakt het mogelijk om het Certificaat onder andere voor Windows Smartcard Logon te gebruiken.
AuthorityInfoAccess	Nee	Bevat de URI waarde van de OCSP responder, die behoort bij het type Certificaat. Met de OCSP-responder kan real-time status informatie over het betreffende Certificaat worden opgevraagd.

Private extensies

Veld	Essentieel	Waarde
QCStatements	Nee	Handtekeningcertificaten bevatten de indicatie dat deze zijn uitgegeven in overeenstemming met de Europese Richtlijn 99/93/EG.

7.1.2.2 Server- en Groepscertificaten

Basis attributen

Veld	Waarde
Version	2 (X.509v3)
SerialNumber	Uniek 128 bits lang Certificaatnummer
Signature	Het gebruikte algoritme is onder de SHA-1 root (domein Overheid /Bedrijven) sha1WithRSAEncryption. Het gebruikte algoritme is onder de SHA-2 root (domein Organisatie) sha256WithRSAEncryption.
Issuer	Bevat de naam van de betreffende Getronics PinkRoccade CA behorend bij het type Certificaat en wordt weergegeven door de volgende attributen: CommonName, OrganizationName en CountryName. Er zijn meerdere CA certificaten in gebruik (geweest). • In het oude, niet meer gebruikte CA-Certificaat is OrganizationName gedefinieerd als ‘PinkRoccade Infrastructure Services BV’. De CommonName bevat ‘PinkRoccade CSP - Overheid – Services CA’. De CountryName is ingesteld op ‘NL’.

	• In het daarna volgende CA-Certificaat is OrganizationName gedefinieerd als 'Getronics PinkRoccade Nederland B.V.'. De CommonName is ingesteld op 'Getronics PinkRoccade PKIoverheid CA – Overheid/Bedrijven en Organisatie'. De CountryName is ingesteld op 'NL'. • In het nieuwe SHA-2 CA-Certificaat is de OrganizationName gedefinieerd als 'Getronics Nederland BV'. De CommonName is ingesteld op 'Getronics CSP Organisatie CA – G2. De CountryName is ingesteld op 'NL'.
Validity	De geldigheidsperiode van het SHA-1 Servercertificaat loopt tot 31 december 2011. De geldigheidsperiode van het SHA-2 Servercertificaat is standaard 3 jaar.
Subject	De naam van het subject wordt weergegeven als een Distinguished Name (DN), en wordt weergegeven door tenminste de volgende attributen: • CountryName; • CommonName; • OrganizationName. • SerialNumber (subjectserienummer). Optioneel kunnen tevens de attributen OrganizationUnit, State en Locality worden opgenomen.
	Locality worden gebruikt. De CommonName bevat de naam van de Service, dit kan bijvoorbeeld een DNS- of een groepsnaam zijn. De attributen die worden gebruikt om het subject te beschrijven benoemen het subject op unieke wijze. Het CountryName attribuut is ingesteld op de tweeletterige landcode "NL" volgens ISO 3166.
subjectPublicKeyInfo	Bevat de PublicKey van de Subject

Standaard extensies

Veld	Essentieel	Waarde
AuthorityKeyIdentifier	Nee	KeyIdentifier is ingesteld op 160 bit SHA-1 hash
SubjectKeyIdentifier	Nee	KeyIdentifier is ingesteld op 160 bit SHA-1 hash
KeyUsage	Ja	In Authenticiteitcertificaten is het digitalSignature bit opgenomen. In Vertrouwelijkheidcertificaten zijn de keyEncipherment, dataEncipherment en de keyAgreement bits opgenomen. In servercertificaten zijn de digitalSignature-, keyAgreement en Key Encipherment bits op unieke wijze opgenomen.
BasicConstraints	Ja	Het CA bit is ingesteld op 'False' en pathLenConstraint op 'none'
CertificatePolicies	Nee	Domein Overheid/Bedrijven • Authenticiteitcertificaten bevatten het OID 2.16.528.1.1003.1.2.2.4. • Vertrouwelijkheidcertificaten bevatten het OID 2.16.528.1.1003.1.2.2.5). • Server certificaten bevatten het OID 2.16.528.1.1003.1.2.2.6. Domein Organisatie • Authenticiteitcertificaten bevatten het OID

		2.16.528.1.1003.1.2.4.4. • Vertrouwelijkheidcertificaten bevatten het OID 2.16.528.1.1003.1.2.4.5). • Server certificaten bevatten het OID 2.16.528.1.1003.1.2.4.6. Alle typen certificaten bevatten een link naar het CPS en een gebruikerstekst.
SubjectAltName	Nee	Hierin is het OID van de CA: • PinkRoccade CSP Services CA; 2.16.528.1.1003.1.3.2.2.4; • of de Getronics PinkRoccade PKIoverheid CA – Overheid/Bedrijven en Organisatie CA; 2.16.528.1.1003.1.3.2.2.5; • of de Getronics CSP Organisatie CA – G2; 2.16.528.1.1003.1.3.5.4.1 en het Subjectnummer van de Certificaathouder opgenomen. In Vertrouwelijkheidcertificaten en Authenticiteitcertificaten is tevens het e-mail adres van de Subject opgenomen.
CrlDistributionPoints	Nee	Bevat de URI waarde van de betreffende CRL, die behoort bij het type Certificaat, kan worden opgehaald.
ExtendedKeyUsage	Nee	Groepscertificaten kunnen deze extensie bevatten, dit maakt het mogelijk om het Certificaat onder andere voor Windows Smartcard Logon en Codesigning te gebruiken. Servercertificaten kunnen deze extensie bevatten. Dit maakt het mogelijk om het Certificaat te gebruiken voor systemen die het gebruik van deze extensie vereisen.
AuthorityInfoAccess	Nee	Bevat de URI waarde van de OCSP responder, die behoort bij het type Certificaat. Met de OCSP-responder kan real-time status informatie over het betreffende Certificaat worden opgevraagd.

7.2 CRL-profielen

De CRL (of meer recente statusinformatie) gebruikt voor de PKIoverheid Certificaten is aldus opgebouwd dat ze makkelijk onderwerp kan vormen voor validatieprocessen.

De inrichting van de CRL en het formaat van de CRL, alsmede het aan de CRL ten grondslag liggende principe, kunnen door KPN worden aangepast, zulks in overeenstemming met de belangen van betrokken partijen.

7.2.1 Persoonsgebonden Certificaten

Attributen

Veld	Waarde
Version	1 (X.509 versie 2)
signatureAlgorithm	Het gebruikte algoritme is onder de SHA-1 root (domein Overheid

	/Bedrijven) sha-1 WithRSAEncryption. Het gebruikte algoritme is onder de SHA-2 root (domein Organisatie) sha-2 WithRSAEncryption.
Issuer	Bevat de naam van de betreffende Getronics PinkRoccade CA wordt weergegeven door de volgende attributen: CommonName, OrganizationName en CountryName. Er zijn meerdere CA's in in gebruik (geweest). • In het oude, niet meer gebruikte CA-Certificaat is OrganizationName gedefinieerd als 'PinkRoccade Infrastructure Services BV'. De CommonName bevat 'PinkRoccade CSP - Overheid – ' en de aanduiding 'Onweerlegbaarheid CA' of 'Vertrouwelijkheid CA' of 'Authenticiteit CA', afhankelijk van het type certificaat. De CountryName is ingesteld op 'NL'. • In het daarna volgende CA-Certificaat is OrganizationName gedefinieerd als 'Getronics PinkRoccade Nederland B.V.'. De CommonName is ingesteld op 'Getronics PinkRoccade PKIoverheid CA – Overheid/Bedrijven en Organisatie'. De CountryName is ingesteld op 'NL'. • In het nieuwe SHA-2 CA-certificaat is de OrganizationName gedefinieerd als Getronics Nederland BV. De CommonName is ingesteld op 'Getronics CSP Organisatie CA – G2. De CountryName is ingesteld op 'NL'.
effective date	datum van uitgifte
next update	is datum van uitgifte plus 24 uur
revoked certificates	de ingetrokken Certificaten met certificaatserienummer en datum van intrekking en mogelijk reden van intrekking.

Extensies

Veld	Essentieel	Waarde
AuthorityKeyIdentifier	Nee	Bevat 160 bit SHA-1 hash

7.2.2 Servercertificaten en Groepscertificaten

Attributen

Veld	Waarde
Version	V2
Issuer	Bevat de naam van de betreffende Getronics PinkRoccade CA en wordt weergegeven door de volgende attributen: • Commonname; • OrganizationName; • CountryName.
effective date	Datum van uitgifte
next update	Dit is datum van uitgifte plus 24 uur, effectief wordt een nieuwe CRL 4 uur na de datum van uitgifte gegenereerd en gepubliceerd .
signatureAlgorithm	Het gebruikte algoritme is onder de SHA-1 root (domein Overheid /Bedrijven) sha1WithRSAEncryption.

	Het gebruikte algoritme is onder de SHA-2 root (domein Organisatie) sha256WithRSAEncryption.

CRL extensies

Veld	Waarde
AuthorityKeyIdentifier	Bevat een160 bit sha-1 hash van de Publieke Sleutel van de CA.
CRL Number	Bevat een integer welke het volgnummer van de betreffende CRL aangeeft.

Revocation List entry velden

Veld	Waarde
Serial Number	Bevat het certificaatserienummer van het ingetrokken certificaat.
Revocation Date	Bevat de datum en tijd van intrekking.

7.3 OCSP-profielen

Voor PKIoverheid certificaten zijn geen specifieke OCSP profiel eisen gedefinieerd. De OCSP Responder conformeert zich aan RFC 2560.

7.3.1 OCSP-profielen

Versie 1 van de OCSP specificaties, zoals gedefinieerd in RFC 2560, wordt gebruikt.

7.3.2 OCSP velden

KPN gebruikt geen unieke tijdsindicatie (nonce) in haar OCSP respons waarmee optioneel de versheid van de respons kan worden aangetoond, ook niet indien het OCSP verzoek wel een dergelijke tijdsindicatie bevat.
Het gebruikersysteem kan echter haar lokale systeemklok gebruiken voor controle van de versheid van de OCSP respons.

8 Conformiteitbeoordeling

Sinds 1 november 2002 is KPN Corporate Market B.V. (één van haar rechtsvoorgangers) door KPMG Certification b.v. gecertificeerd tegen het "Scheme for Certification of Certification Authorities against ETSI TS 101 456" en voldoet daarmee aan de eisen zoals gesteld aan Certificatiedienstverleners in de Weh. Het betreffende Certificaat is op dezelfde datum in de jaren 2005 en 2008 verlengd door BSI Management Systems b.v.

In het Scheme is onder andere verwoord met welke frequentie de audit wordt uitgevoerd, aan welke eisen de certificerende instelling moet voldoen en hoe omgegaan wordt met zogenaamde non-conformities. Een certificerende instelling moet alvorens te kunnen certificeren geaccrediteerd zijn door de Raad van Accreditatie.

KPN voldoet tevens aan de relevante onderdelen van het Programma van Eisen van de PKIoverheid zoals gesteld in het Programma van Eisen (zie hiervoor http://www.logius.nl/producten/toegang/pkioverheid/). Dit is aantoonbaar met behulp van een door BSI Management Systems b.v. afgegeven auditverklaring,

Een afschrift van het ETSI TS 101 456-certificaat staat vermeld op de site van KPN (zie Elektronische Opslagplaats). De door de betreffende auditors opgestelde auditrapporten zijn vanuit beveiligingsoogpunt geheim. Ze worden niet beschikbaar gesteld aan derden en zijn alleen op verzoek en onder strikte geheimhouding in te zien.

KPN is als Certificatiedienstverlener geregistreerd bij de OPTA, onder registratienummer 901278, als getoetste uitgever van Gekwalificeerde Certificaten aan het publiek.

9 Algemene en juridische bepalingen

KPN is de eindverantwoordelijke certificatiedienstverlener. KPN is ook verantwoordelijk voor die delen die zijn uitbesteed naar andere organisaties.

KPN heeft het identificeren van certificaathouders en certificaatbeheerders uitbesteed naar GWK Travelex N.V. te Diemen.

9.1 Tarieven

Geen nadere bepalingen.

9.2 Financiële verantwoordelijkheid en aansprakelijkheid

KPN heeft adequate regelingen getroffen, onder andere in de vorm van verzekeringen, om aansprakelijkheden die verband houden met de onderhavige dienstverlening af te dekken. Daarnaast bezit KPN de financiële stabiliteit en middelen die nodig zijn voor een gezonde bedrijfsvoering.

9.3 Vertrouwelijkheid van bedrijfsgevoelige gegevens

De financiële jaarrekening van KPN Corporate Market B.V.is geïntegreerd in de jaarrekening van Koninklijke KPN N.V.. Als beursgenoteerd bedrijf is het Koninklijke KPN N.V. niet toegestaan om, buiten de reguliere verslagen en officiële kanalen, financiële gegevens te verstrekken.

9.3.1 Opsomming van gegevens die als vertrouwelijk worden beschouwd

Het volgende wordt onder andere als vertrouwelijk beschouwd:

- overeenkomsten met onder andere Abonnee's;
- interne procedures voor behandeling en afhandeling van Abonnee-, Certificaataanvragen en intrekkingsverzoeken;
- gegevens over systemen en infrastructuren;
- PIN-, PUK- en intrekkingscodes;
- interne beveiligingsprocedures en –maatregelen;
- audit rapporten;
- private sleutels.

Zie voor persoonsgegevens 9.4.2 Vertrouwelijke persoonsgegevens.

9.3.2 Opsomming van gegevens die als niet-vertrouwelijk worden beschouwd

Geen nadere bepalingen.

9.3.3 Verantwoordelijkheid om geen gegevens te verstrekken

Voor alle informatie betrekking hebbende op beveiligingsonderwerpen (zie o.a. 9.3.1.) heeft KPN beleid geformuleerd. Dit beleid stelt onder andere dat die informatie vertrouwelijk is en alleen ter beschikking wordt gesteld op basis van het 'need-to-know' principe. Dat betekent tevens dat deze informatie in beginsel enkel binnen het KPN-gebouw ter inzage wordt gegeven aan derden, doch slecht voorzover daartoe een duidelijke noodzaak bestaat (bijvoorbeeld een audit) en steeds onder strikte geheimhouding.

9.4 Vertrouwelijkheid van persoonsgegevens

KPN voldoet aan de eisen van de Wbp. KPN heeft zich geregistreerd bij het College Bescherming Persoonsgegevens als zijnde verantwoordelijk voor het verwerken van persoonsgegevens ten behoeve van de certificatiedienstverlening.

9.4.1 Privacy Statement

KPN heeft onder andere ten behoeve van haar certificatiedienstverlening een privacy statement geformuleerd. In de statement is opgeschreven op welke wijze KPN omgaat met persoonsgegevens. Het privacy statement wordt o.a. beschikbaar gesteld via de site van KPN (zie Elektronische Opslagplaats).

9.4.2 Vertrouwelijke persoonsgegevens

De volgende persoonsgegevens worden als vertrouwelijk beschouwd en worden niet aan derden verstrekt:

- Abonneegegevens;
- certificaataanvraaggegevens en certificaataanvraagbehandelgegevens;
- certificaataanvraagafhandelgegevens;
- certificaatintrekkinggegevens;
- meldingen van omstandigheden die kunnen leiden tot intrekking;

9.4.3 Niet-vertrouwelijke gegevens

De gepubliceerde gegevens van certificaten zijn openbaar raadpleegbaar. De informatie die wordt verstrekt met betrekking tot gepubliceerde en ingetrokken certificaten is beperkt tot hetgeen in hoofdstuk 7 'Certificaat-, CRL- en OCSP-profielen' van voorliggend CPS vermeld is.

Informatie met betrekking tot intrekking van certificaten is beschikbaar via de CRL. De daar gegeven informatie betreft slechts het certificaatnummer, het moment van intrekking en de status (geldig/ingetrokken) van het certificaat.

9.4.4 Verantwoordelijkheid om Private Sleutels te beschermen

De verantwoordelijkheid voor de bescherming van private CA-sleutels ligt bij KPN.

De verantwoordelijkheid voor de bescherming van de Private Sleutel van de Certificaathouder en daarmee voor de SSCD/SUD waarop het is opgeslagen ligt tot en met de overdracht van de SSCD/SUD bij KPN en na de overdracht bij de Certificaathouder/Certificaatbeheerder. Dientengevolge ligt de verantwoordelijkheid voor de bescherming van de PIN- en de PUK-code die de

smartcard beveiligen eveneens tot en met de overdracht van de PIN-mail bij KPN en na de overdracht bij de Certificaathouder/Certificaatbeheerder.

De Abonnee maakt zelf het sleutelpaar aan waarvoor het een Servercertificaat aanvraagt. De Abonnee is verantwoordelijk voor het aanmaken en bewaren van de desbetreffende Private Sleutel in zijn Veilige Omgeving, de Abonnee is eveneens verantwoordelijk voor die Veilige Omgeving zelf.

9.4.5 Melding van- en instemming met het gebruik van persoonsgegevens

De Certificaathouder, de Certificaatbeheerder en de Abonnee geven toestemming voor publicatie van certificaatgegevens door instemming met de Bijzonder Voorwaarden. Het voltooien van een aanvraagprocedure door de Certificaathouder wordt door KPN beschouwd als toestemming voor publicatie van de gegevens in het Certificaat.

9.4.6 Overhandiging van gegevens als gevolg van rechtsgeldige sommatie

KPN verstrekt vertrouwelijke gegevens niet aan opsporingsambtenaren, behoudens voor zover Nederlandse wet- en regelgeving KPN daartoe dwingt en enkel na overlegging van een rechtsgeldige sommatie.

9.4.7 Verstrekking in verband met privaatrechterlijke bewijsvoering

Het Certificaat en de bij de Certificaataanvraag verstrekte gegevens zullen blijven opgeslagen gedurende een nader aan de Abonnee en/of Certificaathouder opgegeven periode en voor zover nodig voor het leveren van bewijs van certificatie in de rechtsgang. Vertrouwelijke gegevens zullen slechts ter bewijsvoering aan andere partijen dan de Abonnee en de Certificaathouder worden verstrekt met voorafgaande schriftelijke toestemming van de Abonnee danwel de Certificaathouder.

9.4.8 Verstrekking op verzoek van de eigenaar

KPN verstrekt de Abonnee en/of Certificaatbeheerder of Certificaathouder desgevraagd de hem betreffende persoonsgegevens. KPN verstrekt de Abonnee desgevraagd persoonsgegevens van een Certificaatbeheerder of Certificaathouder die in Certificaataanvraag van de betreffende Abonnee een Certificaat heeft ontvangen.
KPN is gerechtigd per verstrekking een passende vergoeding te vragen.

9.4.9 Openbaarmaking informatie intrekking certificaat

Informatie met betrekking tot intrekking van Certificaten is beschikbaar via de CRL. De daar gegeven informatie betreft slechts het Certificaatnummer en het moment van intrekking. Indien KPN eigenhandig een Certificaat intrekt, zal deze via de CRL worden gepubliceerd.

9.4.10 Andere omstandigheden die kunnen leiden tot informatieverstrekking

Geen nadere bepalingen.

9.5 Intellectuele eigendomsrechten

Het intellectueel eigendomsrecht van deze CPS berust bij KPN.

Eigendomsrechten met betrekking tot het Certificaat, de SSCD en de SUD blijven ook na uitgifte berusten bij KPN en diens licentiegevers, inclusief rechten van intellectueel eigendom. Hetzelfde geldt voor documentatie verstrekt vanwege de dienstverlening van KPN, inclusief deze CPS.

9.6 Verplichtingen en garanties

In de Bijzonder Voorwaarden is de wijze opgenomen waarop KPN en betrokken partijen om dienen te gaan met verplichtingen en garanties.

9.7 Beperkingen van garanties

In de Bijzonder Voorwaarden is de wijze opgenomen waarop KPN en betrokken partijen om dienen te gaan met de beperkingen in garanties.

9.8 Aansprakelijkheid

9.8.1 Aansprakelijkheid van KPN

KPN aanvaardt de aansprakelijkheid voor PKIoverheid Certificaten zoals opgenomen in de Bijzonder Voorwaarden.

9.8.2 Beperkingen van aansprakelijkheid jegens de Vertrouwende Partij

De aansprakelijkheid van KPN jegens Vertrouwende Partijen is beperkt op de wijze zoals beschreven in de Bijzonder Voorwaarden.

9.9 Vertrouwensrelaties

Geen nadere bepalingen.

9.10 Beëindiging

In de Bijzonder Voorwaarden is de wijze opgenomen waarop KPN omgaat met beëindiging.

9.11 Communicatie met betrokkenen

KPN communiceert op verschillende manieren met betrokkenen. Dat gebeurt mondeling/telefonisch, voornamelijk via de medewerkers van de afdeling Validatie, die onder andere de Certificaataanvragen be- en afhandelen. Deze afdeling is bereikbaar via het telefoonnummer +31 (0)88 661 05 00.

Communicatie geschiedt ook schriftelijk via dit CPS en bijvoorbeeld de gebruikte certificaataanvraagformulieren, die allemaal voorzien zijn van een uitgebreide toelichting. Daarbij bestaat de mogelijkheid om via e-mail adres pkivalidation@kpn.com vragen of andere zaken aan de orde te stellen.

De genoemde documenten en ook veel andere informatie zijn beschikbaar in de Elektronische Opslagplaats.

9.12 Wijzigingen

9.12.1 Wijzigingsprocedure

KPN heeft het recht het CPS te wijzigen of aan te vullen. De werking van het geldende CPS wordt ten minste jaarlijks beoordeeld door de PMA van KPN. Abonnees, Certificaathouders, Certificaatbeheerders en Vertrouwende Partijen kunnen opmerkingen plaatsen met betrekking tot de inhoud van het CPS en deze indienen bij het PMA van KPN (pkisupport@kpn.com). Indien op grond hiervan wordt vastgesteld dat wijzigingen in het CPS noodzakelijk zijn, zal het PMA deze wijzigingen conform het daartoe ingerichte proces voor change management doorvoeren.

Wijzigingen van het CPS worden vastgesteld door de PMA van KPN. Wijzigingen van redactionele aard of correcties van kennelijke schrijf- en/of spelfouten kunnen zonder voorafgaande bekendmaking in werking treden en zijn herkenbaar doordat het versienummer met 0.1 wordt opgehoogd (1.1 > 1.2). Bij ingrijpende veranderingen zal een nieuwe versie worden vervaardigd, herkenbaar doordat het versienummer met 1 wordt opgehoogd (1.0 > 2.0).

9.12.2 Notificatie van wijzigingen

Wijzigingen in de CPS worden op de website van KPN (zie Elektronische Opslagplaats) aangekondigd. Dit gebeurt twee weken voorafgaande aan de startdatum van de geldigheid van het CPS. Deze startdatum van geldigheid staat vermeld op het voorblad van dit CPS.

9.13 Geschillenbeslechting

KPN heeft een klachtenprocedure. Klachten kunnen worden gericht aan de directeur van KPN.

Geschillen worden opgelost zoals beschreven in de Bijzonder Voorwaarden.

9.14 Van toepassing zijnde wetgeving

De Weh is van toepassing op de certificatiedienstverlening van KPN binnen de PKIoverheid, voor zover het de Gekwalificeerde Certificaten (onweerlegbaarheid) betreft.

Op de onderhavige diensten van KPN is verder bij uitsluiting Nederlands recht van toepassing.

9.15 Overige juridische voorzieningen

Geen nadere bepalingen.

9.16 Overige bepalingen

Geen nadere bepalingen.

Bijlage 1 Practices Ministerie van Veiligheid en Justitie

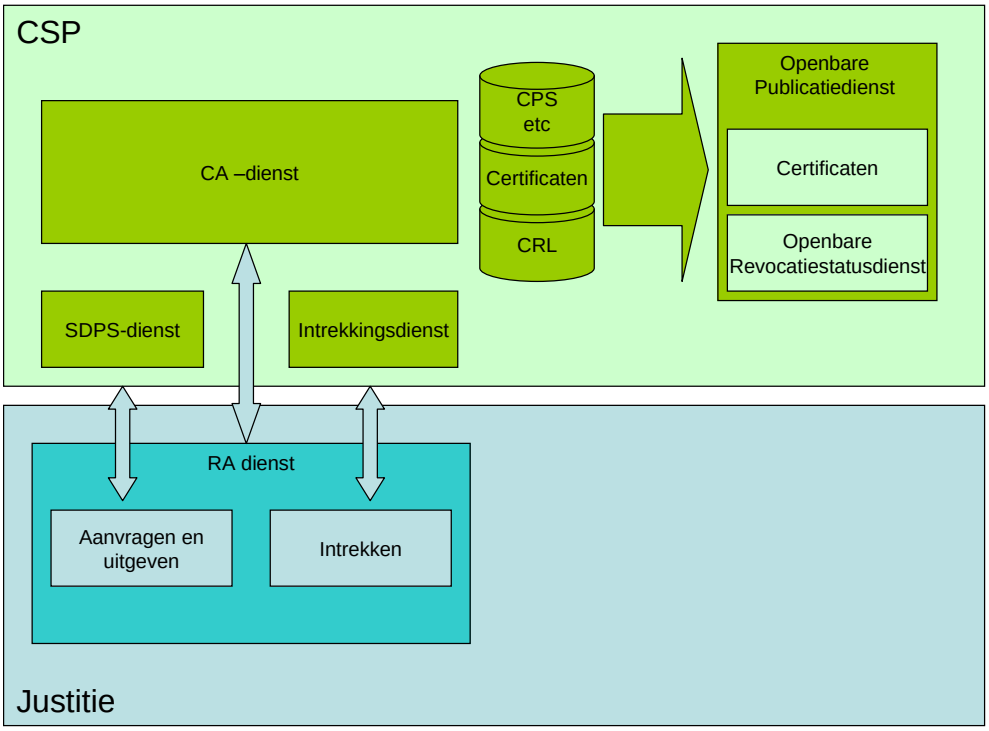
Deze Ministerie van Veiligheid en Justitie (verder: het Ministerie) bijlage is onderdeel van het generiek "Certification Practice Statement" van KPN Corporate Market B.V. [1] (vanaf hier: CPS). Deze bijlage bevat de specifieke aanvulling op het CPS ten behoeve van de PKI dienstverlening voor het Ministerie. De hoofdstukindeling komt volledig overeen met de hoofdstukindeling van het CPS. In geval van strijdigheden tussen het CPS en deze bijlage, prevaleren de aanvullingen van het Ministerie in deze bijlage.

1 Inleiding

Het Ministerie maakt gebruik van een Public Key Infrastructure (PKI) binnen het afsprakenstelsel van PKIoverheid. Het Ministerie gebruikt de PKI dienstverlening voor de informatie-uitwisseling tussen de onderdelen van het Ministerie onderling, tussen het Ministerie en haar ketenpartners en voor de logische toegang tot informatie en applicaties van het Ministerie. Daarnaast worden PKI server certificaten gebruikt om veilige verbindingen op te zetten tussen systemen onderling en om systemen te authenticeren. De PKI dienstverlening zorgt voor het uitgeven van gekwalificeerde certificaten aan medewerkers van het Minsterie. Hierbij treedt KPN op als Certificatiedienstverlener en het Ministerie als Registration Authority (RA) binnen de PKI dienstverlening.

1.1 Overview

De opbouw van de PKI bestaat uit diverse organisatorische onderdelen die zijn weergegeven in Figuur 1.



Figuur 1: PKI organisatieonderdelen

CSP

De Certificaatdienstverlener is de dienstverlener die certificaten onder PKIoverheid uitgeeft. De CSP verstrekt en beheert certificaten en sleutelinformatie met inbegrip van de hiervoor voorziene dragers (tokens: smatcard en USB-token). De CSP heeft tevens de eindverantwoordelijkheid voor het leveren van de certificaatdiensten ook al voert de CSP de feitelijke werkzaamheden niet zelf uit.

CA DIENST
De Certification Authority (CA) tekent op aanvraag van de RA de certificaten en plaatst het persoonsgebonden certificaat op het token. Tevens levert de CA op aanvraag van de RA server- en groepscertificaten. Daarnaast is de CA verantwoordelijk voor het ondertekenen van de certificaatstatusinformatie (CRL – Certificate Revocation List) en de publicatie hiervan.

PUBLICATIEDIENST
De Publicatiedienst is een dienst die certificaten verspreidt onder abonnees en, met toestemming van de abonnees, aan vertrouwende partijen. De dienst verspreidt tevens de Certificate Policies (CP) en Certification Practice Statements (CPS) onder de certificaathouders, abonnees en vertrouwde partijen.

INTREKKINGSDIENST (REVOCATION MANAGEMENT SERVICE)
De Intrekkingsdienst zorgt voor de verwerking van verzoeken die te maken hebben met intrekking van certificaten. Van ingetrokken certificaten wordt de statusinformatie beschikbaar gesteld voor publicatie via de Openbare Publicatiedienst.

OPENBARE REVOCATIESTATUS DIENST (REVOCATION STATUS SERVICE)
De statusinformatie wordt verspreid door middel van de Revocation Status Service. Dit is een dienst die de revocatiestatus levert aan vertrouwde partijen. Deze dienst kan een real-time dienst zijn (OCSP - Online Certificate Status Protocol), maar kan ook zijn gebaseerd op revocatiestatus informatie die wordt bijgewerkt op regelmatige intervallen (CRL publicatie).

SDPS DIENST (SUBJECT DEVICE PROVISIONING SERVICE)
De Subject Device Provisioning Service bereidt de levering van Secure Signature Creation Devices (SSCD's of token) voor, voert die uit en levert de tokens (waarop de private sleutels staan) aan de certificaathouders af. Dit gebeurt op een zodanige wijze dat de vertrouwelijkheid van de private sleutels niet gecompromitteerd wordt en de afgifte aan de beoogde certificaathouders is gegarandeerd. In het geval van persoonlijke of groepscertificaten zal het token moeten voldoen aan de eisen voor een SSCD. Voor de server certificaten worden andere eisen aan het token gesteld: het moet voldoen aan de eisen voor een Secure User Device (SUD). De vereisten voor SSCD en SUD gelden zowel voor de smartcard als voor USB-tokens.

RA DIENST (REGISTRATION AUTHORITY)
Een Registration Authority (RA) zorgt voor de verwerking van certificaataanvragen en alle daarbij behorende taken waarbij de verificatie van de identiteit van de certificaathouder de belangrijkste is. De RA heeft een duidelijke relatie met de CA: De RA geeft – na de verificatie van de volledigheid en juistheid van de aanvraag - opdracht aan de CA voor de productie van tokens met daarop de desbetreffende certificaten. Voor de operationele taken zoals aanvragen en uitreiken kan de RA gebruik maken van één of meerdere Lokale Registratie Autoriteit(en) (LRA). De RA bepaalt daarbij welke taken de LRA daadwerkelijk mag uitvoeren, waarbij geldt dat alle RA processen ook door een LRA moeten kunnen worden uitgevoerd. De RA kan een LRA inrichten, wijzigen of opheffen en is eindverantwoordelijk voor een LRA.

1.3 Gebruikersgemeenschap
Het Ministerie heeft een contract gesloten met KPN voor de PKI dienstverlening. De KPN Bijzondere Voorwaarden PKIoverheid Certificaten (Bijzondere Voorwaarden) zijn niet van toepassing.

1.4.1 Certificaatgebruik (PvE PKIoverheid deel 3a)
Het Ministerie maakt geen gebruik van Beroepsgebonden Certificaten.

Binnen de PKI dienstverlening zijn drie typen certificaten beschikbaar:
- Persoonsgebonden certificaat;
- Server certificaat;
- Groepscertificaat.

De Server en Groepscertificaten worden aangeduid als Services certificaten.

De persoonsgebonden certificaten bestaan uit twee niet gekwalificeerde certificaten waarvan de één de functie van identificatie en authenticatie uitvoert en de ander de functie van vertrouwelijkheid ondersteunt. Daarnaast is er het gekwalificeerd certificaat dat de functie van onweerlegbaarheid ondersteunt. Een persoonsgebonden certificaat wordt uitgegeven aan één persoon (de certificaathouder). Waarbij het de bedoeling is dat alleen die certificaathouder toegang heeft tot het certificaat.

Een server certificaat is een binnen de Veilige Omgeving van het Ministerie opgeslagen niet gekwalificeerde certificaat dat de functies van authenticiteit/vertrouwelijkheid ondersteunt. Het server certificaat wordt uitgegeven aan een server wat deel uitmaakt van de ICT omgeving van het Ministerie.

Een groepscertificaat bestaat uit twee niet gekwalificeerde certificaten die de functies van identificatie/authenticatie en vertrouwelijkheid ondersteunen. Een groepscertificaat wordt uitgegeven aan een afdeling of groep medewerkers van het Ministerie. Het verschil tussen de certificaten is dat met een persoonsgebonden certificaat men elektronische berichten van een gekwalificeerde elektronische handtekening kan voorzien. Dit kan niet met server- of groepscertificaten. Zie voor de bij de certificaten horende plichten de gebruiksvoorwaarden uit de gebruikersovereenkomst.

1.6 Beheer van het CPS
Informatie met betrekking tot de RA dienstverlening kan worden verkregen bij:

Het Ministerie van Veiligheid en Justitie
Justitiële Informatiedienst (JustID)
Loket RA-PKI
Postbus 337
7600 AH Almelo

Voor informatie en/of ondersteuning kan contact worden opgenomen via email: certificatenpki@justid.nl of telefonisch met het Frontoffice van JustID onder nummer: 0546-834100.

3.2.1 Methode om bezit van Private Sleutel aan te tonen
Het sleutelpaar, waarvan de Publieke Sleutel wordt gecertificeerd, wordt voor de Servercertificaten aangemaakt aangemaakt door KPN in de Veilige Omgeving van het Ministerie en ingevoerd in het CMS van het Ministerie.

3.2.2 Authenticatie van de Abonnee
Binnen de PKI dienstverlening is het Ministerie de enige Abonnee. Het Ministerie maakt binnen de PKI dienstverlening geen gebruik van "GWK Travelex" en "DigiKoppeling ".

3.2.3 Authenticatie van persoonlijke identiteit
Binnen de PKI dienstverlening heeft het Ministerie bevoegde aanvragers aangesteld, die gerechtigd zijn om aanvragen van beoogd certificaathouders in te dienen. De bevoegde aanvrager kent vanuit

zijn of haar verantwoordelijkheid de beoogde certificaathouder en is verantwoordelijk voor volledig en juist aanleveren van de certificaataanvraag. De certificaataanvragen worden door de RA-medewerkers gevalideerd en geautoriseerd.

3.2.3.1 Authenticatie ten behoeve van Certificaten voor natuurlijke personen
Medewerkers van het Ministerie moeten een certificaat aanvragen via een bevoegd aanvrager. Een overzicht van de actieve bevoegd aanvragers is aanwezig bij de RA. De bevoegd aanvrager controleert de identiteit van de medewerker a.d.h.v. het identiteitsdocument van de medewerker (face-to-face controle) en stuurt de aanvraag inclusief een kopie van het identiteitsdocument naar de RA.

3.2.3.2 Authenticatie ten behoeve van Services Certificaat
Services certificaten worden aangevraagd door certificaatbeheerders. Bij ontvangst van de aanvraag controleert de RA medewerker of de betreffende certificaatbeheerder nog actief is in het CMS en of de gegevens in de aanvraag correct zijn.

3.2.3.2.1 Authenticatie van Certificaatbeheerder
Medewerkers van het Ministerie die worden aangesteld als certificaatbeheerder moeten hiervoor een aanvraag indienen via een bevoegd aanvrager. De bevoegd aanvrager controleert de identiteit van de medewerker a.d.h.v. het identiteitsdocument van de medewerker (face-to-face controle) en stuurt de aanvraag inclusief een kopie van het identiteitsdocument naar de RA. Een overzicht van de actieve bevoegd aanvragers is aanwezig bij de RA.

3.2.3.2.2 Authenticatie ten behoeve van Servercertificaat
Servercertificaten worden aangevraagd door certificaatbeheerders. Certificaatbeheerders moeten door de bevoegd aanvrager zijn aangevraagd en actief zijn in het CMS. Bij ontvangst van de aanvraag controleert de RA medewerker of de certificaatbeheerder nog actief is in het CMS. Daarnaast controleert de RA medewerker of de gegevens in de aanvraag correct zijn.

3.2.3.2.3 Authenticatie ten behoeve van Groepscertificaat
Groepscertificaten worden aangevraagd door certificaatbeheerders. Certificaatbeheerders moeten door de bevoegd aanvrager zijn aangevraagd en actief zijn in het CMS. Bij ontvangst van de aanvraag controleert de RA medewerker of de certificaatbeheerder nog actief is in het CMS. Daarnaast controleert de RA medewerker of de gegevens in de aanvraag correct zijn.

3.2.4 Autorisatie van de Certificaathouder
Medewerkers van het Ministerie moeten een certificaat aanvragen via een bevoegd aanvrager. Een overzicht van de actieve bevoegd aanvragers is aanwezig bij de RA. De bevoegd aanvrager controleert de identiteit van de medewerker a.d.h.v. het identiteitsdocument van de medewerker (face-to-face controle) en stuurt de aanvraag inclusief een kopie van het identiteitsdocument naar de RA. De RA medewerker controleert of de gegevens in de aanvraag correct zijn.

3.4 Identificatie en Authenticatie bij verzoeken tot intrekking
Binnen de PKI dienstverlening hebben de begrippen PIN-mail en PINmailer dezelfde betekenis.

Een aanvraag voor intrekking kan door de certificaathouder of de bevoegde aanvrager via een "self service portaal" van KPN, de helpdesk van de RA bij JustID (via telefoon of persoonlijke verschijning) of schriftelijk bij de RA van JustID worden ingediend.

In geval van een intrekkingsverzoek direct aan de RA per telefoon worden de gegevens gecontroleerd middels een aantal identificerende vragen en vervolgens teruggebeld voor verificatie. Er wordt gevraagd naar de reden van intrekking certificaat.

In geval van een intrekkingsverzoek direct aan de RA per e-mail worden de gegevens van de certificaathouder vermeld op de e-mail gecontroleerd en gaat er een verzoek via e-mail terug voor noodzakelijke aanvullende gegevens. Vervolgens wordt er teruggebeld voor verificatie. Er wordt gevraagd naar de reden van intrekking certificaat.

In geval van een intrekkingsverzoek in persoon aan de RA: A.d.h.v. de beschikbare kopie van het identiteitsdocument wordt de identiteit van de persoon gecontroleerd. Er wordt gevraagd naar de reden van intrekking certificaat.

KPN kan ook een verzoek tot intrekking initiëren (zie hoofdstuk 4.9.2 van het CPS).

De certificaathouder levert tokens met ingetrokken of verlopen certificaten in bij de bevoegde aanvrager of bij de RA van JustID. De RA houdt het inleveren van de tokens bij in het tokenregister (Excel bestand). Dit register bevat de tokennummers en de bijbehorende certificaatbeheerder voor groepscertificaten. Voor het USB token is dit het graveernummer, voor de smartcard is dit het serie en identificatie nummer. Bij inlevering van het token wordt dit geregistreerd in het register en afgetekend op de gebruikersovereenkomst. Voor de reader wordt geen registratie aangelegd maar deze moet wel ingeleverd worden. Indien het token vermist of gestolen is en dit is doorgegeven aan de RA, dan wordt dit geregistreerd in het tokenregister en aangetekend op de gebruikersovereenkomst

De desbetreffende tokens worden in een afgesloten kist overgedragen aan het gespecialiseerde vernietigingsbedrijf waar JustID een contract mee heeft afgesloten voor het vernietigen van dergelijke materialen.

4.2.1 Registratie van Abonnee en Certificaatbeheerder
Het Ministerie is als Abonnee initieel geregistreerd bij KPN. Het Ministerie heeft Certificaatbeheerders aangesteld die verantwoordelijk zijn voor het beheer van server- en groepscertificaten binnen het Ministerie. Medewerkers van Ministerie die worden aangesteld als certificaatbeheerder moeten hiervoor een aanvraag indienen via een bevoegd aanvrager. Een overzicht van de actieve bevoegd aanvragers is aanwezig bij de RA. De bevoegd aanvrager controleert de identiteit van de medewerker a.d.h.v. het identiteitsdocument van de medewerker (face-to-face controle) en stuurt de aanvraag inclusief een kopie van het identiteitsdocument naar de RA.

4.2.2 Aanvraag van certificaten
Het Ministerie maakt geen gebruik van Beroepsgebonden certificaten.
De verschillende typen certificaten (zie aanvulling van het Ministerie bij hoofdstuk 1.4.1 van deze bijlage) worden aangevraagd door bevoegde aanvragers van het Ministerie en ingediend door de RA medewerkers bij KPN voor het aanmaken van certificaten. Een bevoegd aanvrager kan worden aangesteld door een tekenbevoegd manager. De RA medewerker controleert of de tekenbevoegd manager in de competentietabel voorkomt die beschikbaar is bij de RA en of de bevoegd aanvrager voorkomt op de lijst c.q. in de verzameling van goedgekeurde aanvragen voor de functie bevoegd aanvrager.

4.2.2.1 Aanvraag van Persoonsgebonden Certificaten en Groepscertificaten
De in hoofdstuk 4.2.2.1 van het CPS genoemde werkwijze is niet van toepassing.

De generieke aanvraagprocedure voor persoonsgebonden- en groepscertificaten binnen de PKI dienstverlening verloopt als volgt:

1. De aanvraagprocedure start met het invullen van het "aanvraagformulier persoonsgebonden-respectievelijk groepscertificaat" door (beoogd) certificaathouder/certificaatbeheerder en ingediend bij de bevoegde aanvrager van het Ministerie.
2. De bevoegde aanvrager ondertekent de aanvraag en stuurt de aanvraag naar de RA.

3. De RA medewerker (validator) controleert de aanvraag op volledigheid en juistheid en voert de gegevens van de aanvraag in het Card Management Systeem (CMS) in.
4. De RA medewerker (autorisator) keurt de aanvraag definitief goed of wijst de aanvraag af.

4.2.2.2 Aanvraag Beroepsgebonden Certificaten
Het Ministerie maakt geen gebruik van Beroepsgebonden Certificaten.

4.2.2.3 Aanvraag van Servercertificaten en groepscertificaten
De aanvraagprocedure voor Servercertificaten binnen de PKI dienstverlening verloopt als volgt:
1. De aanvraagprocedure start met het invullen van het "aanvraagformulier servercertificaat" door de certificaatbeheerder en ingediend bij RA.
2. De RA medewerker (validator) controleert de aanvraag op volledigheid en juistheid en voert de gegevens van de aanvraag in het Card Management Systeem (CMS) in.
3. De RA medewerker (autorisator) keurt de aanvraag definitief goed of wijst de aanvraag af.

4.2.3 Certificaataanvraagverwerkingstijd
Het Ministerie maakt geen gebruik van GWK Travelex, maar heeft een eigen RA ingericht binnen de organisatie van het Ministerie.

De verwerking van certificaataanvragen van de RA is één werkdag na ontvangst certificaataanvraag. De totale doorlooptijd van een certificaataanvraag, inclusief de verwerkingstijd van KPN, is maximaal vijf werkdagen.

4.3.1 Uitgifte van Persoonsgebonden Certificaten en Groepscertificaten
Het Ministerie maakt geen gebruik van GWK Travelex, maar heeft een eigen RA ingericht binnen de organisatie van het Ministerie.
Nadat KPN het persoonsgebonden-/groepscertificaat heeft aangemaakt en de gewenste gegevens op het token heeft aangebracht wordt het certificaat uitgeleverd aan de RA locatie van het Ministerie. De RA van het Ministerie reikt de certificaten uit na controle van de identiteit van de certificaatbeheerder/certificaathouder. Bij deze controle moet de certificaatbeheerder/certificaathouder in het bezit zijn van de PINmailer en het identiteitsbewijs waarmee de aanvraag is ingediend. Alleen dan kan het certificaat wordt uitgegeven.

4.3.2 Uitgifte van Beroepsgebonden Certificaten
Het Ministerie maakt geen gebruik van Beroepsgebonden Certificaten.

4.3.3 Uitgifte van Servercertificaten
Bij aanvragen voor geregistreerde Certificaatbeheerders stelt KPN de aangemaakte Certificaten beschikbaar aan de RA van het Ministerie. De RA medewerker stuurt het betreffende certificaat door naar de certificaatbeheerder.

4.3.4 Melding van certificaatvervaardiging aan de Certificaathouder of –beheerder
De Certificaathouder of de Certificaatbeheerder wordt door KPN via email op de hoogte gesteld van de vervaardiging van het certificaat.

4.4.1 Acceptatie van Beroepsgebonden, Persoonsgebonden en Groepscertificaten
Het Ministerie maakt geen gebruik van Beroepsgebonden certificaten. De RA van het Ministerie reikt de certificaten uit, derhalve maakt het Ministerie geen gebruik van GWK Travelex.

4.4.2 Acceptatie van Servercertificaten

Na de definitieve goedkeuring van de aanvraag in het CMS wordt het server certificaat gegenereerd en zet KPN de server certificaten klaar in het CMS zodat deze door de RA kan worden uitgegeven aan de certificaatbeheerder die de aanvraag heeft ingediend.
Bij een server certificaat wordt alleen voor de intrekking een PINmailer met intrekkingscode aangemaakt. KPN stuurt de PINmailer op een beveiligde wijze naar de RA. Dit proces wordt door KPN verzorgd. De certificaatbeheerder wordt door KPN per email geïnformeerd:

- Dat de PINmailer naar de RA wordt gestuurd;
- Dat de certificaatbeheerder een afspraak moet maken om de PINmailer in ontvangst te nemen.

4.9.2 Wie mag een verzoek tot intrekking doen?

De volgende entiteiten zijn bevoegd om een verzoek tot intrekking in te dienen:

- De Certificaathouder;
- De Abonnee;
- De bevoegd aanvrager;
- De Certificaatbeheerder;
- De CSP (KPN Corporate Market B.V.).

De bevoegd aanvragers bij het Ministerie zijn alle tekenbevoegde managers. Deze zijn opgenomen in bestaande competentietabellen bij het Ministerie. Daarnaast mogen tekenbevoegde managers andere medewerkers aanstellen als bevoegd aanvrager. Hiervoor is een proces ingericht waarbij de RA medewerkers de identiteit van de bevoegde aanvrager kunnen controleren en kunnen nagaan of de betreffende bevoegd aanvrager door een tekenbevoegd manager is aangemeld.

4.9.3 Procedure voor een verzoek tot intrekking

Een verzoek tot intrekking, dan wel de melding van een omstandigheid die kan leiden tot de intrekking van een Certificaat, dient binnen de PKI dienstverlening langs de volgende wegen plaats te vinden:

Online:
https://minjus-portal.managedpki.nl/themes/XFClient/ssp.html

Schriftelijk: JustID
Loket RA-PKI
Postbus 337
7600 AH Almelo

De entiteit die een verzoek tot intrekking van een certificaat indient, doet dit door middel van:

- De self service portal van KPN URL: https://minjus-portal.managedpki.nl/themes/XFClient/ssp.html (en met behulp van de intrekkingscode) of
- Het intrekkingsformulier voor het intrekken van certificaten of
- Via de telefoon of in persoon aan/bij de RA van het Ministerie.

De bevoegdheid van de indiener van het verzoek tot intrekken certificaten wordt door de RA gecontroleerd.

In geval van een intrekkingsverzoek direct aan de RA per telefoon worden de gegevens gecontroleerd middels een aantal identificerende vragen en vervolgens teruggebeld voor verificatie. Er wordt gevraagd naar de reden van intrekking certificaat.

In geval van een intrekkingsverzoek direct aan de RA per e-mail worden de gegevens gecontroleerd van de certificaathouder vermeld op de e-mail en gaat er een verzoek via e-mail terug voor

noodzakelijke aanvullende gegevens. Vervolgens wordt er teruggebeld voor verificatie. Er wordt gevraagd naar de reden van intrekking certificaat.

In geval van een intrekkingsverzoek in persoon aan de RA: A.d.h.v. de beschikbare kopie van het identiteitsdocument wordt de identiteit van de persoon gecontroleerd. Er wordt gevraagd naar de reden van intrekking certificaat.

Noodprocedure
KPN kan bij ernstige verstoringen aan het RA station en selfservice portaal handmatig certificaten intrekken op de CA van het Ministerie.
In voorkomende gevallen kan een Certificaathouder en/of een RA-medewerker contact opnemen met een gemachtigd persoon die de noodprocedure richting KPN mag starten. De gemachtigde persoon geeft de opdracht tot intrekking middels een ondertekende Email (juridisch rechtsgeldige digitale handtekening) met opgave van voornamen, achternaam, Emailadres en common name van de pashouder en pasnummer. KPN is geïnformeerd over de personen die aan Ministerie zijde zijn gemachtigd.
Deze noodprocedure is niet bedoeld om toegepast te worden tijdens onderhoudsmomenten aan apparatuur van het Ministerie. Verwacht wordt dat tijdens zo een onderhoud moment back-up systemen beschikbaar zijn om intrekken mogelijk te laten blijven.

4.9.4 Tijdsduur voor verwerking intrekkingsverzoek
De intrekking door de certificaathouder dient bij voorkeur via het self service portal van KPN plaats te vinden. Hiervoor geldt een maximale verwerkingsduur van vier uur.
Andere intrekkingsmogelijkheden zijn:

- Schriftelijk bij RA van het Minsterie;
- Telefonisch bij RA van het Ministerie;
- In persoon bij RA ven het Ministerie.

Deze meldingen worden op basis van "best effort" verwerkt.

5 Management, operationele en fysieke beveiligingsmaatregelen
De fysieke, procedurele en personele beveiligingsmaatregelen van het RA deel bij het Ministerie zijn nader gedetailleerd in het InformatieBeveiligingsplan RA-PKI-DI [3] van het Ministerie.

5.1.1 Locatie, constructie en fysieke beveiliging
Het Ministerie draagt zorg voor een adequate fysieke beveiliging om de risico's op verlies, beschadiging en compromittering van de RA dienstverlening tot een minimum te beperken. Dit geldt in het bijzonder voor de omgeving van de RA, waar de certificaten worden uitgeven en beheerd. De fysieke beveiliging voldoet aan de basisvoorziening informatiebeveiliging 2007 [4] van het Ministerie en zijn op basis van een risicoanalyse op de RA dienstverlening vastgesteld. Deze beveiligingsmaatregelen zijn opgenomen in het InformatieBeveiligingsplan RA-PKI-DI [3].

5.1.4 Afval verwijdering
Het Ministerie heeft maatregelen getroffen om vertrouwelijke gegevens op een veilige wijze te vernietigen conform de algemene procedures van het Ministerie [4].

5.2 Procedurele beveiliging
De procedurele beveiligingsmaatregelen zijn nader gedetailleerd in het InformatieBeveiligingsplan RA-PKI-DI [3] van het Ministerie.

5.2.1 Vertrouwelijke functies
De beveiligingsmaatregelen ten aanzien van het personeel zijn nader gedetailleerd in het InformatieBeveiligingsplan RA-PKI-DI [3] van het Ministerie.

5.2.4 Functiescheiding
De organisatorische beveiligingsmaatregelen zijn nader gedetailleerd in het InformatieBeveiligingsplan RA-PKI-DI [3] en de standaard interne procedures voor aanvragen en uitgeven van certificaten [2] van het Ministerie.

5.2.5 Vakkennis, ervaring en kwalificaties
JustID heeft voor RA medewerkers vastgesteld welke kennis en ervaring voor een goede invulling benodigd is. Dit is vastgelegd in de functiebeschrijvingen van de RA functies.

5.2.6 Trusted Employee Policy
Alle ambtenaren van het Ministerie leggen een eed of belofte af. Daarnaast zijn de RA medewerkers in het bezit van een VOG. Deze VOG is bij aanstelling niet ouder dan zes maanden.

5.4.3 Bescherming van archieven
De RA van het Minsieterie zorgt voor archivering van aanvraag en intrekkingsformulieren, kopieën van Wid documenten en andere relevante informatie. Deze documenten worden veilig opgeslagen in een kluis.
Zie verder het beveiligingsplan [3] en de standaard interne procedures[2] van het Ministerie.

5.8 CSP-beëindiging
Bij het aflopen van de huidige overeenkomst, dan wel bij het tussentijds beëindigen van de overeenkomst zullen beide partijen, in goed onderling overleg, onder eindverantwoordelijkheid van KPN, die activiteiten uitvoeren die nodig zijn om de dienstverlening op een passende wijze te beëindigen, waarbij aan relevante wet- en regelgeving wordt voldaan. Bij de uitvoering van die activiteiten zal het van belang zijn welke partij haar dienstverlening gaat beëindigen en wat dus hun onderlinge rolverdeling zal zijn. Minimaal zullen de volgende activiteiten moeten worden uitgevoerd.

- Het met in achtneming van passende termijnen afstemmen en beoordelen op welke wijze de overeenkomst moet worden aangepast en voortgezet om bijvoorbeeld de dienstverlening voort te zetten dan wel overdracht en gepaste archivering van relevante gegevens te realiseren.
- Het analyseren, afstemmen, plannen en uitvoeren van passende communicatie naar alle betrokkenen, waaronder, maar niet uitsluitend, Certificaathouders, Vertrouwende Partijen en de Certificerende Instellingen.
- Het (mogelijk) intrekken van alle certificaten, met daarbij aandacht voor het moment en de wijze waarop. Het daarna eerst in stand houden van de CRL en de CA-sleutels tot minimaal de wettelijke termijn die daarvoor is gesteld en daarna het ontmantelen ervan, het daarbij archiveren en mogelijk overdragen van certificaataanmaak- en intrekkingsgegevens.
- Het intrekken van autorisaties, het ontmantelen van de bestaande CMS-applicatie (en bijbehorende infrastructuur), het maken van het gewenste aantal kopieën van applicatieprogrammatuur, relevante gegevens en documentatie, het eventueel overdragen hiervan aan de andere partij en het daarna schonen van de gebruikte media. Zulks onder opmaking van een proces-verbaal.
- Het beëindigen van overeenkomsten met leveranciers.
- Het verzamelen, indien nodig, onder opmaak van een proces-verbaal, overdragen en op passende wijze archiveren van aanvraagdossiers.
- Het analyseren, verzamelen, archiveren en zo nodig onder opmaking van een proces-verbaal overdragen van alle documenten die kunnen aantonen dat het management systeem gedurende de jaren van de operatie van de stoppende partij op passende wijze heeft gefunctioneerd.
- Gedurende (en na) de beëindigingsperiode wijzigen en publiceren van het CPS.

6.1.2 Overdracht van Private Sleutel en SSCD aan Abonnee
Certificaathouder gaat akkoord met gebruiksvoorwaarden en tekent de ontvangstbevestiging en gebruikersovereenkomst op datum en tijd. RA medewerker controleert gegevens op token met identiteit van certificaathouder. Indien correct voert RA medewerker <identificatie en uitgifte

succesvol> in CMS in. RA medewerker reikt token uit aan certificaathouder en indien van toepassing de kaartlezer inclusief handleiding / instructie voor het gebruik van de smartcard met de kaartlezer. De RA medewerker registreert de uitgereikte hardware en archiveert de ontvangstbevestiging en gebruikersovereenkomst

6.1.5 Sleutellengten
De sleutellengte van een Certificaat is minstens 2048 bits RSA. De sleutellengte van een CA-Certificaat is 4096 bits RSA.

De gebruikte algoritmes en sleutellengte voldoen aan de eisen zoals gedefinieerd in ETSI TS 102 176-1 standaard [5]. De lengtes van de publieke en private sleutels binnen de PKI Dienstverlening zijn:

Type certificaat	Sleutellengte	Hash methode
CA certificaten	RSA 4096	SHA 256
Persoonsgebonden certificaten	RSA 2048	SHA 256
Groepscertificaten	RSA 2048	SHA 256
Server certificaat	CSR 2048	SHA 256

6.4 Activeringsgegevens

6.4.1 Genereren en installeren van activeringsgegevens
De PINmailer (PIN-mail) wordt gegenereerd door het CMS systeem van KPN.

7 Certificaat-, CRL- en OCSP

7.1 Certificaatprofielen

7.1.1 CP OID
De van toepassing zijnde Certificate Policies kunnen via de volgende OID worden geïdentificeerd:

Persoonsgebonden en Beroepsgebonden Certificaten:

2.16.528.1.1003.1.2.5.1	Authenticiteitcertificaat
2.16.528.1.1003.1.2.5.2	Handtekeningcertificaat
2.16.528.1.1003.1.2.5.3	Vertrouwelijkheidcertificaat

Servercertificaten:

2.16.528.1.1003.1.2.5.6	Servercertificaat.

Groepscertificaten:

2.16.528.1.1003.1.2.5.4	Authenticiteitcertificaat.
2.16.528.1.1003.1.2.5.5	Vertrouwelijkheidcertificaat.

7.1.2 Overzicht Certificaatprofielen

De PKIoverheid Certificaten zijn opgebouwd volgens de PKIX X.509 v3 standaard, waarbij de mogelijkheid bestaat dat extensies worden gebruikt.

Handtekeningcertificaten worden opgebouwd volgens het Qualified Certificate Profile van EESSI/ETSI. Eventuele extensies in dat kader worden ook in de overige Certificaten opgenomen. Certificaatprofielen zijn opgemaakt volgens Deel 3 van het Programma van Eisen van de PKIoverheid, conform het Certificaatprofiel van het Certificaat voor het Domein Organisatie.

7.1.2.1 Persoonsgebonden certificaten

Basis attributen

Veld	Waarde
Version	2 (X.509v3)
SerialNumber	Uniek 128 bits lang serienummer
Signature	Het gebruikte algoritme is sha256WithRSAEncryption
Issuer	Bevat de naam van de betreffende Getronics CSP Justitie CA - G2 en wordt weergegeven door de volgende attributen: CommonName, OrganizationName en CountryName. • De CommonName is ingesteld op ‘Getronics CSP Justitie CA - G2 ‘. De OrganizationName is ingesteld op ‘Getronics Nederland BV’. De CountryName is ingesteld op ‘NL’.
Validity	De geldigheidsperiode van het Certificaat is ingesteld op 5 jaar.
Subject	De naam van het subject wordt weergegeven als een Distinguished Name (DN), en wordt weergegeven door tenminste de volgende attributen: • CountryName; • CommonName; • OrganizationName; • SerialNumber (subjectserienummer). De attributen die worden gebruikt om het subject te beschrijven benoemen het subject op unieke wijze. Het CountryName attribuut is ingesteld op de tweeletterige landcode “NL” volgens ISO 3166. De CommonName wordt ingevuld zoals vermeld in het WID document dat bij de identificatie van het subject wordt overlegd.
subjectPublicKeyInfo	Bevat de PublicKey van de Subject

Standaard extensies

Veld	Essentieel	Waarde
AuthorityKeyIdentifier	Nee	KeyIdentifier is ingesteld op 160 bit SHA-1 hash
SubjectKeyIdentifier	Nee	KeyIdentifier is ingesteld op 160 bit SHA-1 hash
KeyUsage	Ja	In Authenticiteitcertificaten is het digitalSignature bit opgenomen. In Vertrouwelijkheidcertificaten zijn de keyEncipherment, dataEncipherment en de keyAgreement bits opgenomen. In Handtekeningcertificaten is het non-Repudiation bit op unieke wijze zijn opgenomen.
BasicConstraints	Ja	Het CA bit is ingesteld op ‘False’ en pathLenConstraint op

		'none'
CertificatePolicies	Nee	Authenticiteitcertificaten bevatten het OID 2.16.528.1.1003.1.2.5.1. Handtekeningcertificaten bevatten het OID: 2.16.528.1.1003.1.2.5.2. Vertrouwelijkheidcertificaten bevatten het OID 2.16.528.1.1003.1.2.5.3. Alle typen Certificaten bevatten een link naar het CPS en een gebruikerstekst.
SubjectAltName	Nee	Hierin is opgenomen • het e-mail adres van de Subject; • het OID van de betreffende CA; • het Subjectserienummer van de Certificaathouder. Het OID van de betreffende CA is: • 2.16.528.1.1003.1.3.5.4.2 Authenticiteitcertificaten kunnen tevens een UPN bevatten ten behoeve van Windows Smartcard Logon bevatten.
CrlDistributionPoints	Nee	Bevat de URI waarde waar de CRL, die behoort bij het type Certificaat, kan worden opgehaald.
ExtendedKeyUsage	Nee	Authenticiteitcertificaten kunnen deze extensie bevatten. Deze extensie maakt het mogelijk om het Certificaat onder andere voor Windows Smartcard Logon te gebruiken.
AuthorityInfoAccess	Nee	Bevat de URI waarde van de OCSP responder, die behoort bij het type Certificaat. Met de OCSP-responder kan real-time status informatie over het betreffende Certificaat worden opgevraagd.

Private extensies

Veld	Essentieel	Waarde
QCStatements	Nee	Handtekeningcertificaten bevatten de indicatie dat deze zijn uitgegeven in overeenstemming met de Europese Richtlijn 99/93/EG.

7.1.2.2 Server- en Groepscertificaten

Basis attributen

Veld	Waarde
Version	2 (X.509v3)
SerialNumber	Uniek 128 bits lang Certificaatnummer
Signature	Het gebruikte algoritme is sha256WithRSAEncryption

Issuer	Bevat de naam van de betreffende Getronics CSP Justitie CA - G2 en wordt weergegeven door de volgende attributen: CommonName, OrganizationName en CountryName. • De CommonName is ingesteld op 'Getronics CSP Justitie CA - G2 '. De OrganizationName is ingesteld op 'Getronics Nederland BV'. De CountryName is ingesteld op 'NL'.
Validity	De geldigheidsperiode van het Services Certificaat is ingesteld op 5 jaar.
Subject	De naam van het subject wordt weergegeven als een Distinguished Name (DN), en wordt weergegeven door tenminste de volgende attributen: • CountryName; • CommonName; • OrganizationName. • SerialNumber (subjectserienummer). Optioneel kunnen tevens de attributen OrganizationUnit, State en Locality worden opgenomen. De CommonName bevat de naam van de Service, dit kan bijvoorbeeld een DNS- of een groepsnaam zijn. De attributen die worden gebruikt om het subject te beschrijven benoemen het subject op unieke wijze. Het CountryName attribuut is ingesteld op de tweeletterige landcode "NL" volgens ISO 3166.
subjectPublicKeyInfo	Bevat de PublicKey van de Subject

Standaard extensies

Veld	Essentieel	Waarde
AuthorityKeyIdentifier	Nee	KeyIdentifier is ingesteld op 160 bit SHA-1 hash
SubjectKeyIdentifier	Nee	KeyIdentifier is ingesteld op 160 bit SHA-1 hash
KeyUsage	Ja	In Authenticiteitcertificaten is het digitalSignature bit opgenomen. In Vertrouwelijkheidcertificaten zijn de keyEncipherment, dataEncipherment en de keyAgreement bits opgenomen. In servercertificaten zijn de digitalSignature-, keyAgreement en Key Encipherment bits op unieke wijze opgenomen.
BasicConstraints	Ja	Het CA bit is ingesteld op 'False' en pathLenConstraint op 'none'
CertificatePolicies	Nee	• Authenticiteitcertificaten bevatten het OID 2.16.528.1.1003.1.2.5.4. • Vertrouwelijkheidcertificaten bevatten het OID 2.16.528.1.1003.1.2.5.5). • Vertrouwelijkheidcertificaten van server verbindingen bevatten het OID 2.16.528.1.1003.1.2.5.6. Alle typen certificaten bevatten een link naar het CPS en een gebruikerstekst.

SubjectAltName	Nee	Hierin is opgenomen het OID van de CA: • 2.16.528.1.1003.1.3.5.4.2 en het Subjectnummer van de Certificaathouder opgenomen. In Vertrouwelijkheidcertificaten en Authenticiteitcertificaten is tevens het e-mail adres van de Subject opgenomen.
CrlDistributionPoints	Nee	Bevat de URI waarde van de betreffende CRL, die behoort bij het type Certificaat, kan worden opgehaald.
ExtendedKeyUsage	Nee	Groepscertificaten kunnen deze extensie bevatten, dit maakt het mogelijk om het Certificaat onder andere voor Windows Smartcard Logon en Codesigning te gebruiken. Servercertificaten kunnen deze extensie bevatten. Dit maakt het mogelijk om het Certificaat te gebruiken voor systemen die het gebruik van deze extensie vereisen.
AuthorityInfoAccess	Nee	Bevat de URI waarde van de OCSP responder, die behoort bij het type Certificaat. Met de OCSP-responder kan real-time status informatie over het betreffende Certificaat worden opgevraagd.

7.2 CRL-profielen

De CRL (of meer recente statusinformatie) gebruikt voor de PKIoverheid Certificaten is aldus opgebouwd dat ze makkelijk onderwerp kan vormen voor validatieprocessen.

De inrichting van de CRL en het formaat van de CRL, alsmede het aan de CRL ten grondslag liggende principe, kunnen door KPN worden aangepast, zulks in overeenstemming met de belangen van betrokken partijen.

7.2.1 Persoonsgebonden certificaten

Attributen

Veld	Waarde
Version	1 (X.509 versie 2)
signatureAlgorithm	Sha256WithRSAeEncryption
Issuer	Bevat de naam van de betreffende Getronics CSP Justitie CA - G2 en wordt weergegeven door de volgende attributen: CommonName, OrganizationName en CountryName. De CommonName is ingesteld op ‘Getronics CSP Justitie CA - G2 ‘. De OrganizationName is ingesteld op ‘Getronics Nederland BV’. De CountryName is ingesteld op ‘NL’.
effective date	datum van uitgifte
next update	is datum van uitgifte plus 24 uur
revoked certificates	de ingetrokken Certificaten met certificaatserienummer en datum van intrekking en mogelijk reden van intrekking.

CRL extensies

Veld	Waarde
AuthorityKeyIdentifier	Bevat een160 bit sha-1 hash van de Publieke Sleutel van de CA.
CRL Number	Bevat een integer welke het volgnummer van de betreffende CRL aangeeft.

Revocation List entry velden

Veld	Waarde
Serial Number	Bevat het certificaatserienummer van het ingetrokken certificaat.
Revocation Date	Bevat de datum en tijd van intrekking.

7.2.2 Servercertificaten en Groepscertificaten
De inrichting en het formaat van de CRL zijn voor de servercertificaten, en de groepscertificaten hetzelfde als van de persoonsgebonden certificaten.

7.3 OCSP-profielen
Voor PKIoverheid certificaten zijn geen specifieke OCSP profiel eisen gedefinieerd. De OCSP Responder conformeert zich aan RFC 2560.

7.3.1 OCSP-profielen
Versie 2 van de OCSP specificaties, zoals gedefinieerd in RFC 2560, wordt gebruikt.

7.3.2 OCSP velden
KPN gebruikt geen unieke tijdsindicatie (nonce) in haar OCSP respons waarmee optioneel de versheid van de respons kan worden aangetoond, ook niet indien het OCSP verzoek wel een dergelijke tijdsindicatie bevat.
Het gebruikersysteem kan echter haar lokale systeemklok gebruiken voor controle van de versheid van de OCSP respons.

8 Conformiteitbeoordeling
Voor de RA functie van het Minsterie is een deelcertificaat afgegeven door PricewaterhouseCoopers Certification B.V. De scope van deze RA audit betreft de processen die noodzakelijk zijn om de RA functie van de PKI Dienstverlening door het Ministerie te kunnen vervullen en is vastgelegd in de Overview of Applicabillity [6].

9 Algemene en juridische bepalingen
Het Ministerie maakt geen gebruik van GWK Travelex diensten.

9.4 Vertrouwelijkheid van persoonsgegevens
Bij het Ministerie zijn de maatregelen ten aanzien van vertrouwelijkheid persoonsgegevens nader gedetailleerd in het document basisvoorziening informatiebeveiliging 2007 [4].

9.4.1 Privacy Statement
De maatregelen ten aanzien van vertrouwelijkheid persoonsgegevens zijn nader gedetailleerd in het document basisvoorziening informatiebeveiliging 2007 [4].

9.4.6 Overhandiging van gegevens als gevolg van rechtsgeldige sommatie
Voor het Ministerie geldt dat vertrouwelijke informatie niet wordt vrijgegeven, tenzij hiertoe een wettelijke plicht bestaat.

9.4.7 Verstrekking in verband met privaatrechterlijke bewijsvoering
Voor het Ministerie geldt dat vertrouwelijke informatie niet wordt vrijgegeven, tenzij hiertoe een wettelijke plicht bestaat.

9.4.8 Verstrekking op verzoek van de eigenaar

KPN verstrekt geen persoonsgegevens. Binnen de PKI dienstverlening worden de persoonsgegevens door RA van het Ministerie beheerd.

9.13 Geschillenbeslechting
Klachten betreffende de RA dienstverlening kunnen worden ingediend bij de RA dienstverlener zoals beschreven in hoofdstuk 1.6 van deze bijlage.

APPENDIX 1: Lijst met referenties

[1]	KPN Corporate Market B.V., Certification Practice Statement PKIoverheid, versie 4.12, d.d.15 oktober 2011.
[2]	Ministerie van Veiligheid en Justitie, RA-PKI-DI-RA Processen en procedures Certificaten, definitief.
[3]	Ministerie van Veiligheid en Justitie, InformatieBeveiligingsplan RA-PKI-DI, definitief.
[4]	Ministerie van Veiligheid en Justitie, Basisvoorziening Informatiebeveiliging 2007 Ministerie van Veiligheid en Justitie, versie 0.9b, d.d. 23 februari 2007.
[5]	ETSI TS 107-176-1, Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms, V2.0.0., d.d. November 2007.

Bijlage 2 Practices CreAim

3.2.3 Authenticatie van de Abonnee

De leden van de beroepsgroepen NIvRA en NOVAA die een Certificaat aanvragen behoeven niet aan te tonen dat zij in de desbetreffende registers opgenomen zijn. CreAim raadpleegt het desbetreffende register om vast te kunnen stellen dat de aanvragers geregistreerd zijn. CreAim heeft daartoe een overeenkomst gesloten met de NIvRA en NOVAA.

3.2.3 Authenticatie van persoonlijke identiteit

De vaststelling van de identiteit van de persoonsgebonden en beroepsgebonden Certificaathouder (leden van de beroepsgroepen NIvRA en NOVAA) geschiedt door CreAim op een door CreAim en de Certificaathouder te bepalen plaats en tijdstip. Hierbij kunnen alleen Certificaathouders worden geïdentificeerd die zich identificeren met een Nederlands identiteitsbewijs.
Hergebruik van identiteitsbewijzen is voor de Certificaathouder, waarvan de identificatie en overdracht plaats vindt via CreAim, niet voorzien.

4.2.2.2 Aanvraag Beroepsgebonden Certificaten

Stap 5 wijzigt als volgt.
KPN verstuurt de SSCD met daarop de certificaten en met daarbij een formulier Identificatie en Overdracht per post naar CreAim. Creaim organiseert de identificatie en de overdracht.
De aanvragende Certificaathouder dient zich bij de overdracht te identificeren met hetzelfde identeitsbewijs waarvan hij/zij eerder een kopie met de Certificaataanvraag heeft meegestuurd.

Stap 6 wijzigt als volgt.
Op het moment van overdracht identificeert (een medewerker van) CreAim de aanvragende Certificaathouder en regelt daarna de overdracht van de SSCD. Hierbij tekent de Certificaathouder voor ontvangst en worden datum en tijdstip van overdracht geregistreerd op het formulier Identificatie en Overdracht. Creaim verstuurt het ingevulde en getekende formulier Identificatie en Overdracht naar KPN.

Stap 7 wijzigt als volgt.
KPN verstuurt na ontvangst van formulier Identificatie en Overdracht van CreAim de PIN-mail per post naar het opgegeven adres van de Certificaathouder.

4.3.2 Uitgifte van Certificaten

De uitgifte van de SSCD met daarop de aangemaakte certificaten en de uitgifte van de PINmail geschiedt op verschillende momenten en langs verschillende wegen.
In eerste instantie wordt de SSCD per post verstuurd naar CreAim. CreAim regelt de identificatie en daarna de overdracht van de SSCD.
Na ontvangst van het getekende formulier Identificatie en Overdracht verstuurt KPN de PINmail naar het bij de aanvraag opgegeven adres.

CreAim en KPN zorgen er beide voor dat de certificaten tijdig worden uitgegeven. Indien de CreAim niet binnen 3 weken na verzending van de SSCD de overdracht niet heeft uitgevoerd wordt het daaraan door KPN herinnerd. Indien CreAim niet binnen 6 weken na verzending van de SSCD de ontvangstbevestiging heeft geretourneerd gaat KPN zonder verdere aankondiging over tot intrekking van de betrokken Certificaten.

4.4.1 Acceptatie vanCertificaten

De Certificaten worden geacht te zijn uitgereikt en geaccepteerd zodra de Certificaathouder de SSCD waarop ze geplaatst zijn heeft ontvangen. De Certificaathouder dient de ontvangst te bevestigen door bij overdracht het formulier Identificatie en Overdracht te ondertekenen. Deze ondertekende ontvangstbevestiging is de formele bevestiging van de acceptatie.

5.1 Fysieke beveiliging

5.1.1 Locatie, constructie en fysieke beveiliging

De aanvragen Beroepsgebonden Certificaten, de SSCD's en de ontvangsbevestiging worden gedurende een zo kort mogelijke tijd bewaard in de vestiging van CreAim.

Dit gebouw is voorzien van een passende combinatie van fysieke, organisatorsiche en procedurele beveiligingsmaatregelen, zoals zonering en inbraakbeveiliging.

Huishoudelijke regels zijn van kracht, waaronder een clean desk policy.

6.1.2 Overdracht van Private Sleutel en SSCD aan Abonnee

Certificaten worden op de volgende wijze overgedragen aan de Certificaathouder. KPN zendt de SSCD, met daarop onder andere de door KPN aangemaakte Private Sleutels, via een commercieel postbedrijf naar CreAim. CreAim voert de fysieke overdracht van de SSCD aan de aanvragende Certificaathouder uit.

De Certificaathouder tekent tijdens de overdracht door CreAim voor ontvangst van de SSCD.

KPN stuurt, na ontvangst van het getekende formulier Identificatie en Overdracht, de PIN-mail met de benodigde toegangscodes voor de SSCD en de intrekkingscode voor certificaten, gescheiden ('out of band'), via eveneens een commercieel postbedrijf, aan de Certificaathouder.

Bijlage 3 Definities

Aanvrager: een natuurlijke persoon (Beroepsgebonden Certificaten) of rechtspersoon (Organisatiegebonden Certificaten) die een Certificaataanvraag tot uitgifte van een Certificaat indient bij KPN. De Aanvrager hoeft niet dezelfde partij te zijn als de Abonnee of de Certificaathouder, maar is wel één van beide.

Abonnee: de natuurlijke persoon (Beroepsgebonden Certificaten) of rechtspersoon (Organisatiegebonden Certificaten) die een overeenkomst aangaat met KPN om uitgifte van PKIoverheid Certificaten aan door de Abonnee aangewezen Certificaathouders te bewerkstelligen.

Asymmetrisch Sleutelpaar: een Publieke Sleutel en Private Sleutel binnen de public key cryptografie die wiskundig zodanig met elkaar zijn verbonden dat de Publieke Sleutel en de Private Sleutel elkaars tegenhanger zijn. Wordt de ene sleutel gebruikt om te versleutelen, dan móet de andere gebruikt worden om te ontsleutelen en omgekeerd.

Authenticatie: (1) Het controleren van een identiteit voordat informatieoverdracht plaatsvindt; (2) het controleren van de juistheid van een boodschap of afzender.

Authenticiteitcertificaat: Certificaat waarin de Publieke Sleutel wordt gecertificeerd van het sleutelpaar dat voor identificatie- en authenticatiediensten wordt gebruikt.

Authentificatie: zie Authenticatie.

Beroepsgebonden Certificaat: een op een SSCD opgeslagen combinatie van twee Niet-Gekwalificeerde Certificaten die tezamen de functies van authenticiteit en vertrouwelijkheid ondersteunen, alsmede een Gekwalificeerd Certificaat dat de functie van Onweerlegbaarheid ondersteunt, en die uitsluitend worden uitgegeven aan een beoefenaar van een Erkend Beroep.
De Certificaten voldoen aan de volgende vereisten:

a) ze zijn uitgegeven aan een natuurlijke persoon, die het Certificaat gebruikt of gaat gebruiken uit hoofde van zijn/haar beroep, en
b) ze zijn uitgegeven op basis van de binnen de PKIoverheid geldende ‘Certificate Policy Domein Overheid/Bedrijven en Organisatie” (PvE deel 3a).

Bevoegd vertegenwoordiger
Een natuurlijk persoon die bevoegd is een organisatie te vertegen-woordigen. Bevoegdheid tot vertegenwoordiging kan voortvloeien uit de wet of uit een volmacht. Er kan ook sprake zijn van meerdere natuurlijk personen, b.v. een bestuur van een vereniging, die bevoegd zijn een organisatie te vertegenwoordigen.

In onderstaand schema volgt een beschrijving wie *normaliter* bevoegd is om een bepaalde organisatie te vertegenwoordigen:

Organisatie	Vertegenwoordigingsbevoegd
Gemeente	Burgemeester Gemeente secretaris
Provincie	Commissaris van de Koningin
Ministerie	Minister Directeur Generaal

	Secretaris Generaal
School	Directeur/Hoofd Secretaris van het bestuur
Waterschap	Directeur (Dijkgraaf) Bestuurder(s)
Zorginstelling	Directeur Bestuurder(s)
Vereniging	Bestuurder(s)
BV	Bestuurder(s)
NV	Bestuurder(s)
Maatschap	Alle maten of één der maten als vertegenwoordiger van de maatschap (d.w.z. als vertegenwoordiger van alle maten gezamenlijk) als deze door de andere maten hiertoe is gevolmachtigd.
Eenmanszaak	Eigenaar
Vennootschap onder Firma (VOF)	Iedere vennoot, die daarvan niet is uitgesloten, is bevoegd om 'ten name van de vennootschap' (d.w.z. de gezamenlijke vennoten) te handelen
Commanditaire vennootschap	Alleen beherende vennoten: zij zijn bevoegd om namens de commandi-taire vennootschap op te treden en zij zijn hoofdelijk verbonden voor de in naam van de vennootschap aangegane verbintenissen.
Coöperatie	Bestuurder(s)
Baten-lastendienst	Directeur Bestuurder(s)
Zelfstandig bestuursorgaan (ZBO)	Directeur Bestuurder(s)

CA-Certificaat: een Certificaat van een Certification Authority.

CA-Sleutels: het sleutelpaar, de Private en de Publieke Sleutel van een Certification Authority.

Certificaat: de Publieke Sleutel van een Eindgebruiker, samen met aanvullende gegevens. Een Certificaat is vercijferd met de Private Sleutel van de Certification Authority die de Publieke Sleutel heeft uitgegeven, waardoor het Certificaat onvervalsbaar is.
Certificaten zijn op verschillende wijzen te groeperen. Ten eerste is er het onderscheid tussen Organisatiegebonden en Beroepsgebonden Certificaten. Voor Organisatiegebonden Certificaten geldt dat de Certificaten worden aangevraagd door een organisatorische entiteit, die Abonnee is bij KPN, voor een Certificaathouder die onderdeel is van of een relatie onderhoudt met die organisatorische entiteit. De Certificaathouder gebruikt het Certificaat namens de organisatie.

Voor Beroepsgebonden Certificaten geldt dat deze worden aangevraagd door een beoefenaar van een Erkend Beroep, die in die hoedanigheid zelf een Abonnee, maar tegelijk ook Certificaathouder is. De Certificaathouder gebruikt het Certificaat uit hoofde van zijn beroep.
De Organisatiegebonden Certificaten zijn onder te verdelen in Persoonsgebonden Certificaten en Services Certificaten. De Services Certificaten zijn op hun beurt onder te verdelen in Groeps- en Servercertificaten.

Certificaataanvraag: de door een Aanvrager ingediend verzoek om uitgifte van een Certificaat door KPN.

Certificaatbeheerder: een natuurlijke persoon die bevoegd is om namens de Abonnee en ten behoeve van de Certificaathouder een Servercertificaat of Groepscertificaat aan te vragen, te installeren, te beheren en/of in te trekken. De Certificaatbeheerder voert handelingen uit waartoe de Certificaathouder zelf niet in staat is.

Certificaathouder: een entiteit die geïdentificeerd wordt in een Certificaat als de houder van de Private Sleutel behorende bij de Publieke Sleutel die in het Certificaat gegeven wordt.
In beginsel zijn er twee soorten Certificaathouders: de organisatiegebonden Certificaathouder en de beroepsgebonden Certificaathouder. De organisatiegebonden Certificaathouder is onderdeel van een organisatorische entiteit waarbij de organisatorische entiteit de Abonnee is die voor de Certificaathouder Certificaten aanvraagt en waarbij de Certificaathouder deze Certificaten namens de Abonnee mag gebruiken. De beroepsgebonden Certificaathouder is een beoefenaar van een erkend beroep, die in die hoedanigheid Abonnee wordt bij KPN en voor zichzelf Certificaten aanvraagt. Bij de beroepsgebonden Certificaten is de Abonnee de Certificaathouder, de Abonnee en de Certificaathouder zijn dezelfde persoon.

Certificaatprofiel: een beschrijving van de inhoud van een Certificaat. Ieder soort Certificaat (handtekening, vertrouwelijkheid, e.d.) heeft een eigen invulling en daarmee een eigen beschrijving – hierin staan bijvoorbeeld afspraken omtrent naamgeving e.d.

Certificate Policy (CP): een benoemde verzameling regels die de toepasbaarheid van een Certificaat aangeeft voor een bepaalde gemeenschap en/of toepassingsklasse met gemeenschappelijke beveiligingseisen. Met behulp van een CP kunnen Abonnees en Vertrouwende Partijen bepalen hoeveel vertrouwen zij kunnen stellen in het verband tussen de Publieke Sleutel en de identiteit van de houder van de Publieke Sleutel. De van toepassing zijnde CP's zijn opgenomen in het Programma van Eisen van de PKIoverheid (PvE). Het betreft hier het deel 3a Certificate Policy – Domein Overheid/Bedrijven en Organisatie en het deel 3b Certificate Policy – Services, bijlage bij CP Domein Overheid/Bedrijven en Organisatie.

Certificate Revocation List: zie Certificaten Revocatie Lijst.

Certificaten Revocatie Lijst (CRL): een openbaar toegankelijke en te raadplegen lijst van ingetrokken Certificaten, ondertekend en beschikbaar gesteld door de uitgevende CSP.

Certificatie Autoriteit (CA): een organisatie die Certificaten genereert en intrekt. Het functioneren als CA is een deelactiviteit die onder de verantwoordelijkheid van de CSP wordt uitgevoerd. In dit verband opereert KPN derhalve als CA.

Certificatiediensten: het afgeven, beheren en intrekken van Certificaten door Certificatiedienstverleners.

Certification Practice Statement (CPS): een document dat de door een CSP gevolgde procedures en getroffen maatregelen ten aanzien van alle aspecten van de dienstverlening beschrijft. Het CPS

beschrijft daarmee op welke wijze de CSP voldoet aan de eisen zoals gesteld in de van toepassing zijnde CP.

Certification Practice Statement PKIoverheid (CPS PKIoverheid): de onderhavige CPS, zoals van toepassing op de uitgifte door KPN van PKIoverheid Certificaten alsmede het gebruik daarvan.

Certificatiedienstverlener: een natuurlijke persoon of rechtspersoon die als functie heeft het verstrekken en beheren van Certificaten en sleutelinformatie, met inbegrip van de hiervoor voorziene dragers (SSCD, SUD). De Certificatiedienstverlener heeft tevens de eindverantwoordelijkheid voor het leveren van de Certificatiediensten waarbij het niet uit maakt of het de feitelijke werkzaamheden zelf uitvoert of deze uitbesteedt aan anderen.

Certification Service Provider (CSP): zie Certificatiedienstverlener.

Digitale Handtekening: zie Geavanceerde Elektronische Handtekening.

Directory Dienst: een dienst van (of met medewerking van) een CSP die de door de CA uitgegeven Certificaten online beschikbaar en toegankelijk maakt ten behoeve van raadplegende of vertrouwende partijen.

Eindgebruiker: een natuurlijke persoon of rechtspersoon die binnen de PKIoverheid één of meer van de volgende rollen vervult: Abonnee, Certificaathouder of Vertrouwende Partij. Gezien het geringe onderscheidende vermogen van deze term wordt ze in het CPS niet gebezigd, behalve daar waar het de voorgeschreven structuur van het document betreft (d.w.z. headings e.d.)

Elektronische Handtekening: elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie. De Elektronische Handtekening wordt ingezet om ervoor te zorgen dat elektronische correspondentie en transacties op twee belangrijke punten kunnen wedijveren met de aloude “handtekening op papier”. Door het plaatsen van een Elektronische Handtekening staat vast dat iemand die zegt een document te hebben ondertekend, dat ook daadwerkelijk heeft gedaan.

Elektronische Opslagplaats: locatie waar relevante informatie ten aanzien van de dienstverlening van KPN is te vinden.
Zie: http://www.pki.getronics.nl/website/401/PKIoverheid+formulieren.html

Erkend beroep
Voor beroepsgebonden Certificaathouders gelden dat zij een erkend beroep moeten uitoefenen om Certificaten binnen de PKIoverheid te kunnen aanvragen. Een erkend beroep is in dit verband een beroep waarbij sprake is van:

- een door de betreffende beroepsgroep erkend (beroeps)register waarbij een wettelijk geregeld tuchtrecht van toepassing is en waarbij inschrijving in het register verplicht is om het beroep uit te mogen oefenen;
- wettelijke eisen voor het uitoefenen van het beroep, waarbij een geldig bewijs (b.v. een vergunning) moet worden verkregen om het beroep te mogen uitoefenen.

Escrow (Key-Escrow): Een methode om tijdens uitgifte van een Certificaateen kopie te genereren van de Private Sleutel ten behoeve van toegang tot versleutelde gegevens door daartoe bevoegde partijen, alsmede de beveiligde bewaarneming daarvan.

Geavanceerde Elektronische Handtekening: een Elektronische Handtekening die voldoet aan de volgende eisen:

a) het is op unieke wijze aan de ondertekenaar verbonden;

b) het maakt het mogelijk de ondertekenaar te identificeren;
c) het komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
d) het is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord.

Gegevens voor het aanmaken van Elektronische Handtekeningen: zie Signature Creation Data.

Gegevens voor het verifiëren van een Elektronische Handtekening: zie Signature Verification Data.

Gekwalificeerd Certificaat: een Certificaat dat voldoet aan de eisen, gesteld krachtens artikel 18.15, tweede lid van de Telecommunicatiewet, en is afgegeven door een Certificatiedienstverlener die voldoet aan de eisen gesteld krachtens artikel 18.15, eerste lid van de Telecommunicatiewet. Het Certificaat dient tevens te strekken tot toepassing van de Gekwalificeerde Elektronische Handtekening.

Gekwalificeerde Elektronische Handtekening: een Elektronische Handtekening die voldoet aan de volgende eisen:

a) het is op unieke wijze aan de ondertekenaar verbonden;
b) het maakt het mogelijk de ondertekenaar te identificeren;
c) het komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
d) het is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;
e) het is gebaseerd op een Gekwalificeerd Certificaat als bedoeld in artikel 1.1 onderdeel dd van de Telecommunicatiewet;
f) het is gegenereerd door een veilig middel voor het aanmaken van Elektronische Handtekeningen als bedoeld in artikel 1.1 onderdeel gg van de Telecommunicatiewet.

Generiek TopLevelDomein (gTLD)
De gTLD is een generiek topleveldomein (generic Top Level Domain), een domeinnaam extensie die niet aan een bepaald land toebehoort en die in principe door iedereen waar ook ter wereld geregistreerd kan worden. Enkele voorbeelden van gTLD's zijn .com, .edu, .gov, .mil en .org.

KPN Bijzondere Voorwaarden PKIoverheid Certificaten: de Bijzondere Voorwaarden, die van toepassing zijn op alle bij de uitgifte en het gebruik van PKIoverheid Certificaten betrokken partijen.

Groepscertificaat : een op een SUD opgeslagen combinatie van twee Niet-Gekwalificeerde Certificaten die tezamen de functies van vertrouwelijkheid en authenticiteit ondersteunen en die voldoen aan de volgende vereisten:

a) ze zijn uitgegeven aan een dienst of een functie, deel uitmakend van de Abonnee (organisatorische entiteit), en
b) ze zijn uitgegeven op basis van de binnen de PKIoverheid geldende ‘Certificate Policy Services’ (PvE deel 3b)

Hardware Security Module: De randapparatuur dat wordt gebruikt aan de server kant om cryptografische processen te versnellen. Met name dient hierbij gedacht te worden aan het aanmaken van sleutels.

Land code TopLevelDomein (ccTLD)
De ccTLD (country code Top Level Domain) dit is de domeinnaam extensie voor een land of onafhankelijk grondgebied. Een ccTLD bestaat uit de 2-letterige landcode die volgens de ISO 3166-1 norm is vastgelegd. B.v. .nl, .be en .de.
Middel voor het vervaardigen van handtekeningen: zie Signature Creation Device.

Niet-Gekwalificeerd Certificaat: een Certificaat dat niet voldoet aan de voor een Gekwalificeerd Certificaat gestelde eisen.

Object Identifier (OID): een rij van getallen die op unieke wijze en permanent een object aanduidt.

Online Certificate Status Protocol (OCSP): een methode om de geldigheid van Certificaten online (en real time) te controleren. Deze methode kan worden gebruikt als alternatief voor het raadplegen van de CRL.

Onweerlegbaarheid: de eigenschap van een bericht om aan te tonen dat bepaalde gebeurtenissen of handelingen hebben plaatsgevonden, zoals het verzenden en ontvangen van elektronische documenten.

Organisatiegebonden certificaten
Er zijn twee verschillende soorten organisatiegebonden certificaten:
1. voor personen;
2. voor services.

Ad. 1
Bij organisatiegebonden certificaten voor personen is de certificaathouder onderdeel van een organisatorische entiteit. De certificaathouder heeft de bevoegdheid een bepaalde transactie namens die organisatiorische entiteit te doen.

Ad. 2
Bij organisatiegebonden certificaten voor services is de certificaathouder:
- een apparaat of een systeem (een niet-natuurlijke persoon), bediend door of namens een organisatorische entiteit; of
- een functie van een organisatorische entiteit.

Overheid
Binnen de context van PKIoverheid wordt/worden als overheid c.q. als overheidsorganisaties beschouwd:
- het geheel van het Rijk, de provincies, de gemeenten, de samenwerkingsverbanden op grond van de Wet Gemeenschappelijke Regelingen en de waterschappen;
- uitvoerende organisaties en diensten zoals inspecties, baten en lastendiensten en politiediensten;
- rechterlijke macht;
- zelfstandige bestuursorganen zoals vermeldt in het ZBO-register[2]

Overheids-CA: een CA die binnen de hiërarchie van de PKIoverheid de stam-CA is. Ze vormt in technische zin het centrale punt voor het vertrouwen binnen de hiërarchie en wordt aangestuurd door de Overheids-Policy Authority.

OverheidsIdentificatieNummer (OIN): Identificerend nummer uit het Digikoppeling Serviceregister. Dit is een register voor overheidsorganisaties. Indien overheidsorganisaties willen deelnemen in Digikoppeling, een overheidsvoorziening voor verbetering van elektronische communicatie tussen

[2] http://almanak.zboregister.overheid.nl/sites/min_bzk2/index.php

overheidsorganisaties, dan moeten zij, bij de aanvraag van een Servercertificaat, hun bestaan aantonen met een uittreksel uit het Digikoppeling Serviceregister en wordt het OIN opgenomen in hun Servercertificaat.

Overheids-Policy Authority: de hoogste beleidsbepalende autoriteit binnen de hiërarchie van de PKIoverheid die de regie over de Overheids-CA voert.

Persoonsgebonden certificaten
De certificaathouder zal in het geval van persoonsgebonden certificaten een natuurlijke persoon zijn. De certificaathouder is ofwel onderdeel van een organisatorische entiteit waarvoor een abonnee de contracterende partij is (organisatiegebonden certificaathouder), ofwel de beoefenaar van een erkend beroep en in die hoedanigheid zelf een abonnee en daarmee de contracterende partij (beroepsgebonden certificaathouder) ofwel een burger en in die hoedanigheid zelf een abonnee en daarmee de contracterende partij.

PKI voor de overheid, de Public Key Infrastructure van de Staat der Nederlanden (ook wel PKIoverheid): een afsprakenstelsel dat generiek en grootschalig gebruik mogelijk maakt van de Elektronische Handtekening, en faciliteert voorts identificatie op afstand en vertrouwelijke communicatie. Het afsprakenstelsel is eigendom van de Minister van Binnenlandse Zaken en Koninkrijksrelaties en wordt beheerd door de Policy Authority PKIoverheid.

PKIoverheid Certificaat: een onder de PKIoverheid door KPN uitgegeven Certificaat.

Policy Management Authority: de organisatorische entiteit binnen KPN die verantwoordelijk is voor ontwikkelen, onderhouden en formeel vaststellen van aan de dienstverlening verwante documenten, inclusief het CPS.

Private key: zie Private Sleutel.

Private Sleutel: de sleutel van een asymmetrisch sleutelpaar die alleen bekend dient te zijn bij de houder ervan en strikt geheim moet worden gehouden. In het kader van de PKIoverheid wordt de Private Sleutel door de Certificaathouder gebruikt om zich elektronisch te identificeren, zijn Elektronische Handtekening te zetten of om een vercijferd bericht te ontcijferen.

Public key: zie Publieke Sleutel.

Public Key Infrastructure (PKI): het geheel van organisatie, procedures en techniek, benodigd voor het uitgeven, gebruiken en beheer van Certificaten.

Publieke Sleutel: de sleutel van een asymmetrisch sleutelpaar die publiekelijk kan worden bekendgemaakt. De Publieke Sleutel wordt gebruikt voor de controle van de identiteit van de eigenaar van het asymmetrisch sleutelpaar, voor de controle van de Elektronische Handtekening van de eigenaar van het asymmetrisch sleutelpaar en voor het vercijferen van informatie voor een derde.

Root: het centrale gedeelte van een (PKI-)hiërarchie waaraan de gehele hiërarchie en haar betrouwbaarheidsniveau is opgehangen.

Root Certificate: zie Stamcertificaat.

Root Certification Authority (Root-CA): een CA die het centrum van het gemeenschappelijk vertrouwen in een PKI-hiërarchie is. Het Certificaat van de Root-CA (de Root Certificate of Stamcertificaat) is self-signed, waardoor het niet mogelijk is de bron van de handtekening op dit Certificaat te authenticeren, alleen de integriteit van de inhoud van het Certificaat. De Root-CA wordt

echter vertrouwd op basis van bijvoorbeeld de CP en andere documenten. De Root-CA hoeft niet noodzakelijkerwijs aan de top van een hiërarchie te zijn gepositioneerd.

Secure Signature Creation Device (SSCD): een middel voor het aanmaken van Elektronische Handtekeningen dat voldoet aan de eisen gesteld krachtens artikel 18.17, eerste lid van de Telecommunicatiewet. Een SSCD wordt ingezet t.b.v persoonsgebonden en beroepsgebonden certificaten. Een SSCD kan bijvoorbeeld een smartcard of een USB token zijn.

Secure User Device (SUD): een middel dat de gebruikers private sleutel(s) bevat, deze sleutel(s) tegen compromittatie beschermt en authenticatie of ontcijfering uitvoert namens de gebruiker. Een SUD wordt gebruikt voor services certificaten. Ook en SUD kan bijvoorbeeld een smartcard of een USB token zijn. Een smartcard of USB-token wordt SSCD genoemd als er elektronische handtekeningen mee kunnen worden aangemaakt, als er dus gekwalificeerde certificaten op geplaatst zijn. Als een smartcard of USB-token services certificaten bevat wordt het een SUD genoemd.

Servercertificaat: een binnen de Veilige Omgeving van de Abonnee opgeslagen Niet-Gekwalificeerde Certificaat die de functies van authenticiteit en vertrouwelijkheid ondersteunt en die voldoet aan de volgende vereisten:

a) het is uitgegeven aan een server, deel uitmakend van de Abonnee (organisatorische entiteit), en
b) het is uitgegeven op basis van de binnen de PKIoverheid geldende ‘Certificate Policy Services’ (PvE deel 3b).

Services Certificaat: een certificaat waarmee een functie of apparaat, bijvoorbeeld een server, wordt gekoppeld aan een rechtspersoon of andere organisatie. Een Services Certificaat kan zijn een Servercertificaat, indien een apparaat wordt gekoppeld aan een organisatie, of een Groepscertificaat , indien een functie wordt gekoppeld aan een organisatie.

Signature Creation Data: unieke gegevens, zoals codes of private cryptografische sleutels, die door de ondertekenaar worden gebruikt om een Elektronische Handtekening te maken.

Signature Creation Device: geconfigureerde software of hardware die wordt gebruikt voor het implementeren van de gegevens voor het aanmaken van Elektronische Handtekeningen.

Signature Verification Data: gegevens, zoals codes of cryptografische Publieke Sleutels, die worden gebruikt voor het verifiëren van een Elektronische Handtekening.

Stamcertificaat: het Certificaat van de Root-CA. Dit is het Certificaat behorend bij de plek waar het vertrouwen in alle binnen de PKIoverheid uitgegeven Certificaten zijn oorsprong vindt. Er is geen hoger liggende CA waaraan het vertrouwen wordt ontleend. Dit Certificaat wordt door de Certificaathouder (binnen de PKIoverheid is dat de Overheids-CA) zelf ondertekend. Alle onderliggende Certificaten worden uitgegeven door de houder van het Stamcertificaat.

Veilig Middel voor het aanmaken van Elektronische Handtekeningen: zie Secure Signature Creation Device.

Veilige Omgeving: De omgeving van het systeem dat de sleutels van de Servercertificaten bevat. Binnen deze omgeving is het toegestaan de sleutels softwarematig te beschermen, in plaats van in een SUD. De compenserende maatregelen hiervoor moeten van dusdanige kwaliteit zijn dat het praktisch onmogelijk is de sleutels ongemerkt te stelen of te kopiëren. Bij compenserende maatregelen moet bijvoorbeeld worden gedacht aan een combinatie van fysieke toegangsbeveiliging, logische toegangsbeveiliging, logging, audit en functiescheiding.

Vertrouwelijkheidcertificaat: Certificaat waarin de Publieke Sleutel wordt gecertificeerd van het sleutelpaar dat voor vertrouwelijkheidsdiensten wordt gebruikt.

Vertrouwende Partij: de natuurlijke persoon of rechtspersoon die ontvanger is van een Certificaat en die handelt in vertrouwen op dat Certificaat.

X.509: een ISO standaard die een basis voor de elektronische opmaak van Certificaten definieert.

Bijlage 4 Afkortingen

Afkorting	Betekenis
CA	Certificatie Autoriteit (Certification Authority)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificaten Revocatie Lijst
CSP	Certification Service Provider ofwel Certificatiedienstverlener
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunication Standardisation Institute
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OPTA	Onafhankelijke Post- en Telecommunicatie Autoriteit
PIN	Persoonlijk Identificatie Nummer
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PUK	Persoonlijk Unlock Kengetal
PvE	(PKIoverheid) Programma van Eisen
RA	Registratie Autoriteit (Registration Authority)
SSCD	Secure Signature Creation Device
SUD	Secure User Device
Weh	Wet elektronische handtekeningen
Wji	Wet justitiële informatie
Wbp	Wet bescherming persoonsgegevens
Wid	Wet op de identificatieplicht