Certification Practice Statement PKIoverheid Private Services Server certificaten

KPN B.V.

KPN BV
Fauststraat 1
7323 BA Apeldoorn
Postbus 9105
7300 HN Apeldoorn
T +31 (0) 8 86 61 00 00
www.kpn.com
K.v.K. ‘s Gravenhage nr. 27124701
NL009292056B01

Datum 17 oktober 2017
Versie versie 1.0.2.

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 B.V. als Trust Service Provider (TSP). In navolgende wordt steeds gesproken over KPN. Hiermee wordt bedoeld KPN als Trust Service Provider, als onderscheid met de andere diensten die KPN levert.

Eén 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 voorliggend document is het CPS van KPN specifiek voor PKIoverheid **Private** Services Server certificaten. Dit document beschrijft de practices voor de Private Services Private Services Server certificaten van KPN. Dit hoofdstuk bevat een introductie op dit CPS. Het behandelt in het kort een aantal belangrijke aspecten van dit document.

Voor het CPS van de **publieke** PKIoverheid certificaten zie de betreffende CPS 'en op de Elektronische Opslagplaats van KPN, https://certificaat.kpn.com/elektronische-opslagplaats/:

- KPN PKIoverheid Certification Practice Statement
- KPN PKIoverheid Extended Validation (EV SSL) Certification Practice Statement

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.
- 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 Private Services 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

Het CP PvE deel 3h beschrijft de minimumeisen die zijn gesteld aan de dienstverlening van KPN binnen PKIoverheid Private Services. Dit voorliggende CPS geeft aan op welke wijze door KPN invulling wordt gegeven aan de PKIoverheid Private Services dienstverlening, voor zover dit valt onder directe verantwoordelijkheid van de PA.

1.1.4 Status

De datum, waarop de geldigheid van dit CPS start, staat vermeld op het titelblad van dit CPS. Het 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 Private Services Server Certificaten’. In het kader van dit document wordt ze ook wel aangeduid als ‘PKIoverheid CPS Private Services Server certificaten’, 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: 2.16.528.1.1005.1.1.1.6

1.3 Gebruikersgemeenschap

De gebruikersgemeenschap binnen het domein Private Services bestaat enerzijds uit Certificatiedienstverleners en anderzijds uit Abonnees, organisatorische entiteiten binnen overheid en bedrijfsleven en Certificaathouders die bij deze abonnees behoren, Certificaatbeheerders en Vertrouwende Partijen. Voor een beschrijving van deze begrippen wordt verwezen naar Bijlage 1 Definities en Bijlage 2 Afkortingen.

Het Programma van Eisen van PKIoverheid (deel 3h) 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, https://certificaat.kpn.com/elektronische-opslagplaats/

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 Private Services Server certificaten die KPN uitgeeft, worden uitgegeven in overeenstemming met het Programma van Eisen van PKIoverheid (deel 3h).
Binnen PKIoverheid Private Services worden Private Services Server certificaten gebruikt voor het beveiligen van een verbinding tussen een bepaalde client en een server via het TLS/SSL-protocol. De PKIoverheid Private Services-certificaten zijn te herkennen aan de specifieke unieke PKIoverheid Private Services Policy Object Identifier (OID) 2.16.528.1.1003.1.2.8.6. Deze OID verwijst naar de CP PvE deel 3h en staat vermeldt in het veld Certificaatbeleid (certificatePolicies) van het certificaat Staat

der Nederlanden Private Services CA, de KPN PKIoverheid Private Services CAcertificaten en de eindgebruiker Private Services Private Services Server certificaten.

1.4.1 Primaire doeleinden

De primaire doelen van een PKIoverheid Private Services Server certificaat zijn om:

1. De organisatie te identificeren die de controle heeft over de website: een PKIoverheid Private Services Server certificaat zorgt voor een redelijke mate van zekerheid dat de website, die door de gebruiker van een internetbrowser c.q. een vertrouwende partij wordt bezocht, onder de controle staat van de organisatie, die staat vermeldt in het PKIoverheid Private Services Server certificaat.
2. Het mogelijk te maken versleuteld te communiceren met een website: een PKIoverheid Private Services Server certificaat maakt het mogelijk om sleutels uit te wisselen. Hiermee is het mogelijk dat, via het internet, de gebruiker van een internetbrowser versleutelde informatie uitwisselt met een website.
3. Certificaten uitgegeven onder het private stamcertificaat worden niet publiekelijk vertrouwd door browsers of andere applicaties. Het toepassingsgebied van deze certificaten is primair een besloten gebruikersgroep waarbinnen afspraken zijn gemaaakt over het gebruik van de private root van PKIoverheid.

1.4.2 Secundaire doeleinden

Een PKIoverheid Private Services Server certificaat:

1. Maakt het moeilijker om phishing- en andere on-line identiteitsfraudeaanvallen uit te voeren waarbij gebruik wordt gemaakt van certificaten.
2. Helpt organisaties die het doelwit zijn van phishing- of andere on-line identiteitsfraudeaanvallen, door hen een voorziening te geven waarmee zij zich beter kunnen identificeren ten opzichte van gebruikers.
3. Helpt Justitie bij een onderzoek naar phishing- en andere on-line identiteitsfraude. In voorkomende gevallen zal PKIoverheid hiertoe contact opnemen met Justitie, zelf nader onderzoek verrichten of juridische stappen nemen tegen de betreffende organisatie.

1.4.3 Uitgesloten doeleinden

Een PKIoverheid Private Services Server certificaat geeft alleen meer zekerheid over de identiteit van de eigenaar van de website. Een PKIoverheid Private Services Server certificaat geeft geen uitsluitsel over de reputatie van een organisatie of de service die zij bieden. Als zodanig is een PKIoverheid Private Services Server certificaat niet bedoeld om enige zekerheid te bieden, of anderszins te garanderen dat:

1. De organisatie vermeld in het PKIoverheid Private Services Servercertificaat er een actieve bedrijfsvoering op nahoudt.
2. De organisatie vermeld in het PKIoverheid Private Services Server certificaat zich houdt aan de Nederlandse wetgeving.
3. De organisatie vermeld in het PKIoverheid Private Services Server -certificaat betrouwbaar, eerlijk of een goede reputatie heeft op het gebied van zaken doen.
4. Dat het “vertrouwd” is om zaken te doen met de organisatie zoals vermeldt in het PKIoverheid Private Services Server certificaat.

1.5 CA-model

1.5.1 Policy Authority voor de PKI voor de overheid

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

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

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

De Policy Authority (PA) is verantwoordelijk voor het beheer van de gehele infrastructuur. De PKI voor de overheid is zo opgezet dat externe organisaties, de Certification Service Providers (CSP's), onder voorwaarden toe kunnen treden tot de PKI voor de overheid. Deelnemende CSP's zijn verantwoordelijk voor de dienstverlening binnen de PKI voor de overheid. De PA ziet toe op de betrouwbaarheid van de gehele PKI voor de overheid.

In algemene zin is de PA in het kader van PKIoverheid Private Services verantwoordelijk voor:

1. Beheer van het normenstelsel van de PKI voor de overheid, het Programma van Eisen deel 3h.
2. Beheer van Object Identifiers, de unieke nummers voor CSP's en hun CPS's.
3. Creatie en beheer van sleutelpaar en het bijbehorende Staat der Nederlanden Private Root CA – G1 stamcertificaat.
4. Intrekken van het Staat der Nederlanden Private Root CA – G1 stamcertificaat en ad hoc publicatie van de CRL.
5. Periodieke publicatie van de Staat der Nederlanden Private Root CA – G1 CRL.
6. Creatie en beheer van sleutelparen en het bijbehorende Domein Private Services certificaat.
7. Intrekken van het Domein Private Services certificaat en ad hoc publicatie van de bijbehorende CRL.
8. Voorbereiding inzake het toelaten van CSP's tot de PKIoverheid Private Root.
9. Effectuering van de toelating van CSP's met inbegrip van creatie, uitgifte en beheer van Domein Private Services CSP CA-certificaten.
10. Voorbereiding inzake het intrekken van Domein Private Services CSP CA-certificaten.
11. Effectuering van het intrekken van Domein Private Services CSP CA-certificaten.
12. Houden van toezicht op toegelaten CSP's.
13. Voorbereiding inzake het vernieuwen van Domein Private Services CSP CA-certificaten.
14. Effectuering van het vernieuwen van EV CSP CA-certificaten met inbegrip van creatie, uitgifte en beheer van nieuwe Domein Private Services CSP CA-certifcaten.
15. Registreren en beoordelen van meldingen omtrent aantasting van de PKIoverheid Domein Private Services.

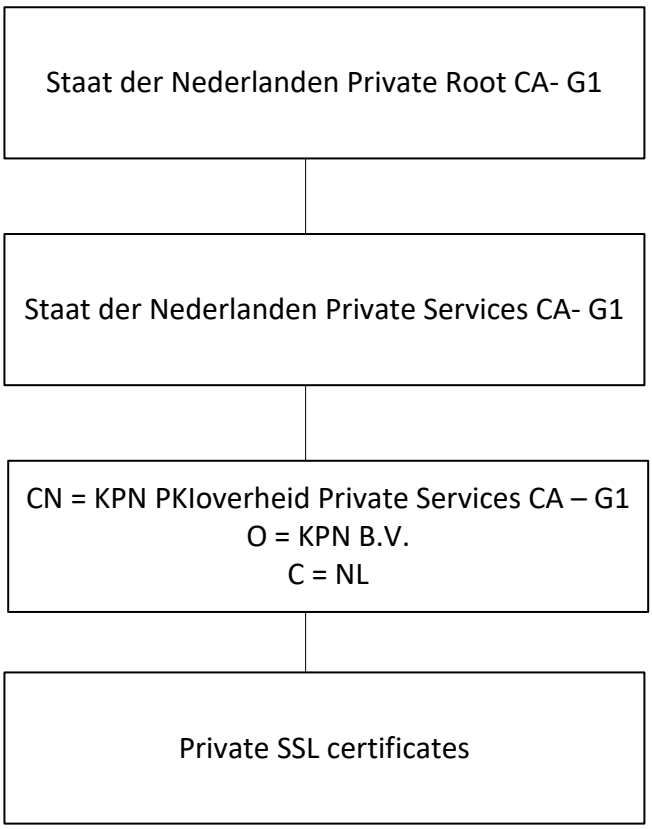
Het technisch beheer van de Staat der Nederlanden Private Root CA G1, de Staat der Nederlanden Private Services Intermediair CA – G1 en de bijbehorende Certificate Revocation Lists (CRL's) vindt plaats door KPN BV.

Het beheer van het stamcertificaat is opgedragen aan de Policy Authority van de PKI voor de overheid. Deze organisatie is ondergebracht bij Logius (http://www.logius.nl), dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

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

1.5.2 CA-model PKIoverheid Private Root

Om duidelijk te maken dat het gaat om Private hiërarchie-certificaten wordt bij de naamformatie het woord ”Private” gebruikt. Dit geldt voor alle CA-certificaten in de PKIoverheid Private hiërarchie. Binnen PKIoverheid Private Hièrachie is de naamformatie van de commonName (CN) als volgt:



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 Security Operations, Policy Management Authority
Postbus 9105

7300 HN Apeldoorn
pkisupport@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 CPS PKIoverheid’ door Getronics Nederland BV.

1.7 Samenwerking met AMP Logistics B.V.

KPN heeft met AMP Logistics B.V. (verder: AMP) een samenwerkingsovereenkomst inzake de certificatiedienstverlening gesloten. Binnen die overeenkomst besteedt KPN de vaststelling van de identiteit van de Certificaatbeheerder en Certificaathouder uit aan AMP. Identiteitsvaststelling geschiedt op een met de Certificaatbeheerder afgesproken plaats en tijdstip door een medewerker van AMP**.**

1.8 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 (https://certificaat.kpn.com/elektronische-opslagplaats/).

2.2 Publicatie van TSP-informatie

Via de Elektronische Opslagplaats is tenminste het volgende online beschikbaar:
1. Stamcertificaat.
2. Bijzondere Voorwaarden:
3. CPS.
4. Certificate Policy – Server Certificaten Domein Private (PvE deel 3h).
5. Directory Dienst.
6. Het BSI Kitemark certificaat wat aangeeft dat KPN voldoet aan de normen uit ETSI EN 319 411-1.

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, 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 EN 319 411-1 certificaat van KPN B.V. wordt gepubliceerd in de elektronische opslagplaats. De betreffende certificaten geven aan dat KPN B.V. voldoet aan ETSI EN 319 411-1 ‘ Electronic Signatures and Infrastructures (ESI);Policy and security requirements for Trust Service Providers issuing certificates;Part 1: General requirements’. De auditrapportages betrekking hebbende op de normatieve referenties van KPN 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 met ingetrokken eindgebruiker Private Services-certificaten wordt standaard elke 15 minuten opnieuw gepubliceerd en ieder CRL-bestand heeft een geldigheidsduur van 24 uur. Daarnaast maakt elke CSP gebruik van een Online Certificate Status Protocol (OCSP) om de certificaatstatusinformatie van eindgebruiker Domein Private Services-certificaten beschikbaar te stellen.

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 Private Services Server certificaten gebruikte namen voldoen aan de X.501 naamstandaard. De namen bestaan uit de volgende onderdelen:

Attribuut	Waarde
Subject	Certificaat
BusinessCategory	MOET een van de volgende waarden Bevatten • Private Organization • Government Entity • Business Entity
Common Name (CN)	FQDN
CountryName (C)	NL
Organization (O)	Naam van de Abonnee
State or Province (S)	Provincie waar de Abonnee gevestigd is
Locality (L)	Plaats waar de Abonnee gevestigd is
SerialNumber	KvK-nummer
PublicKeyInfo	Publieke sleutel
Optioneel:	
Organizational UnitName (OU)	Afdeling van de organisatie van Abonnee
StreetAddress	Adres waar de Abonnee gevestigd is
PostalCode	Postcode waar de Abonnee gevestigd is
JurisdictionOfIncorporationCountryName (Jur)	NL

3.1.2 Noodzaak van betekenisvolle namen

Geen nadere bepalingen.

3.1.3 Anonimiteit of pseudonimiteit

Het gebruik van pseudoniemen is binnen de PKIoverheid niet toegestaan.

3.1.4 Regels voor interpretatie van verschillende naamformaten

De naam van de CSP CA wordt overgenomen van het uittreksel uit het Nederlands Handelsregister.

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 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 de naam

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, voor zover 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 door of namens de Abonnee aangemaakt in de Veilige Omgeving van de Abonnee en ingevoerd op de (HTTPS) website van KPN. Op de Certificaataanvraag voor het Private Services Server certificaat tekent de Abonnee ervoor dat het sleutelspaar ook inderdaad in een Veilige Omgeving is aangemaakt.

Zie verder 3.2.3.3 Authenticatie ten behoeve van Private Services Server certificaten 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 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.

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

- de Certificaataanvraag juist, volledig en naar waarheid is ingevuld,
- hij/zij akkoord gaat met de Bijzondere Voorwaarden en
- 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 in voorkomende gevallen 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 Europese verordening (VERORDENING (EU) Nr. 910/2014 VAN HET EUROPEES PARLEMENT EN DE RAAD van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt .

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.

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 (https://certificaat.kpn.com/formulieren/). 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.

Een organisatie die als abonnee van een andere KPN PKIoverheid hiërarchie geregisteerd is, is tevens abonnee van de Private hiërarchie. Er is geen nieuwe registratie nodig.

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.

3.2.2.1 Verifiëren status organisatie

Bij het verifiëren van de status van de organisatie verifieert KPN dat de abonnee een bestaande en legale organisatie is.

Als bewijs dat het om een bestaande en legale organisatie gaat zal KPN tenminste de volgende bewijsstukken opvragen en verifiëren:

- Voor organisaties binnen de overheid: een recent gewaarmerkt uittreksel (maximaal 1 maand oud) uit het Handelsregister van de Kamer van Koophandel of een wet, oprichtingsakte of een algemene maatregel van bestuur.
- Voor privaatrechtelijke organisaties met en zonder rechtspersoonlijkheid: een recent gewaarmerkt uittreksel (maximaal 1 maand oud) uit het Handelsregister van de Kamer van Koophandel.

3.2.2.2 Verifiëren naam organisatie

Voor het verifiëren van de naam van de organisatie verifieert KPN dat de organisatienaam die in het certificaat wordt opgenomen, juist en volledig is en overeenkomt met de door de abonnee aangemelde organisatienaam.

Als bewijs van de juistheid van de opgegeven officiële organisatienaam zal KPN de volgende bewijsstukken opvragen en verifiëren:

- Voor organisaties binnen de overheid: een recent gewaarmerkt uittreksel (maximaal 1 maand oud) uit het Handelsregister van de Kamer van Koophandel of, indien inschrijving in het Handelsregister nog niet heeft plaatsgevonden, een kopie van de betreffende pagina uit de meest recente versie van de Staatsalmanak waar het adres van de betreffende overheidsorganisatie staat vermeldt.
- Voor privaatrechtelijke organisaties met en zonder rechtspersoonlijkheid: een recent gewaarmerkt uittreksel (maximaal 1 maand oud) uit het Handelsregister van de Kamer van Koophandel. Verder geldt dat het aangeleverde bewijsstuk de organisatorische entiteit dient te onderscheiden van eventuele andere organisaties met dezelfde naam. In het algemeen geldt dat in een uittreksel uit het Handelsregister van de Kamer van Koophandel de officiële naam van de organisatie ook vermeld staat.

3.2.2.3 Verifiëren adres organisatie

Voor het verifiëren van het adres van de organisatie verifieert KPN dat het door de abonnee opgegeven adres van de organisatie juist en volledig is en dat het ook het adres betreft waar de organisatie haar werkzaamheden uitvoert.
Onder adres wordt alleen verstaan:

- straatnaam;
- huisnummer (inclusief toevoeging(en));
- postcode; en
- woonplaats.

Als bewijs van de juistheid en het bestaan van het opgegeven adres en dat het ook het adres is waar de organisatie haar werkzaamheden uitvoert, zal KPN tenminste de volgende bewijsstukken opvragen en verifiëren:

- Voor organisaties binnen de overheid: een recent gewaarmerkt uittreksel (maximaal 1 maand oud) uit het Handelsregister van de Kamer van Koophandel of, indien inschrijving in het Handelsregister nog niet heeft plaatsgevonden, een kopie van de betreffende pagina uit de meest recente versie van de Staatsalmanak waar het adres van de betreffende overheidsorganisatie staat vermeldt.
- Voor privaatrechtelijke organisaties met en zonder rechtspersoonlijkheid: een recent gewaarmerkt uittreksel (maximaal 1 maand oud) uit het Handelsregister van de Kamer van Koophandel.

Alleen als het adres in de bewijsstukken overeenkomt met het adres op de aanvraag, dan zal KPN dit als voldoende bewijs beschouwen.

3.2.2.4 Verifiëren telefoonnummer organisatie

Voor het verifiëren van het telefoonnummer verifieert KPN dat het door de abonnee opgegeven algemene telefoonnummer van de organisatie, juist en volledig is.
Om de juistheid en het bestaan van het opgegeven algemene telefoonnummer van de organisatie vast te stellen zal KPN:

- bellen met het betreffende telefoonnummer en verifiëren dat de abonnee inderdaad te bereiken is op het opgegeven telefoonnummer; en
- het algemene telefoonnummer van de organisatie verifiëren in de meest recente versie van de (online) Telefoongids of door middel van een gewaarmerkt uittreksel (maximaal 1 maand oud) uit het Handelsregister van de Kamer van Koophandel; of
- een verklaring van een externe accountant of notaris ontvangen waarin het opgegeven algemene telefoonnummer van de abonnee wordt bevestigd

3.2.2.5 Verifiëren leeftijd organisatie

Als op basis van de opgevraagde gegevens blijkt dat de organisatie van de abonnee korter dan drie jaar bestaat (gerekend vanaf datum inschrijving Handelsregister of datum publicatie wet- of, algemene maatregel van bestuur tot datum ondertekening aanvraag Private Services Server certificaat), dan zal KPN verifiëren dat de abonnee in staat is om deel te nemen aan het zakelijk verkeer.

Als bewijs van juistheid en het bestaan van de opgegeven betaalrekening zal KPN tenminste één van de volgende bewijsstukken bij de Abonnee opvragen en verifiëren:

- een verklaring van een financiële instelling die in Nederland een vergunning heeft van DNB en valt onder het Nederlandse depositogarantiestelsel waaruit blijkt dat de abonnee over een actieve betaalrekening beschikt;
- een verklaring van een externe accountant dat de abonnee over een actieve betaalrekening beschikt bij een financiële instelling die in Nederland een vergunning heeft van DNB en valt onder het Nederlandse depositogarantiestelsel.

3.2.3 Authenticatie van persoonlijke identiteit

Indien een Abonnee een Certificaat wil aanvragen, dan dient de Abonnee een daartoe ontwikkeld papieren dan wel elektronisch aanvraagformulier in te vullen en te sturen naar KPN. Het betreft het volgende formulier:

- Aanvraag PKIoverheid Private Services SSL Certificaten

Het aanvraagformulier dient (elektronisch) te worden ondertekend door de Abonnee. Door ondertekening van het formulier wordt o.a. Certificaatbeheerder geautoriseerd het aangevraagde Private Services Server certificaat namens de Abonnee in ontvangst te nemen, alsmede om het te gebruiken en/of te beheren.

De Abonnee dient met de Certificaataanvraag, indien daar naar wordt gevraagd, een fotokopie mee te sturen van het identiteitsbewijs van elke 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 Certificaatbeheerder zich bij AMP laat legitimeren. Op het tijdstip van vaststelling van de identiteit mag de geldigheid van het betreffende identiteitsbewijs bovendien niet zijn verstreken.

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

3.2.3.1 Authenticatie van Certificaatbeheerder

Voor Private Services Server certificaten geldt dat deze dienen te worden beheerd door een expliciet daartoe door de Abonnee aangewezen en geautoriseerde Certificaatbeheerder. Certificaatbeheerders kunnen in beginsel meerdere Private Services Server certificaten beheren. Omdat dat veelvuldig voorkomt, is de identificatie en authenticatie van de Certificaatbeheerder losgekoppeld van de certificaataanvraag van het Private Services Server certificaat zelf. KPN heeft 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.

Dit bewijs mag niet ouder zijn dan 13 maanden anders moeten de gegevens opnieuw worden opgevraagd en geverifieerd tenzij in de overeenkomst met de abonnee uitdrukkelijk wordt vastgelegd dat de certificaatbeheerder zijn of haar autorisatie behoudt tot het moment dat dit door de abonnee wordt herzien of tot het moment dat de overeenkomst verloopt of wordt beëindigd. 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 Private Services Server certificaat worden aangevraagd.

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

3.2.3.2 Authenticatie ten behoeve van Private Services Server certificaat

Op de Certificaataanvraag voor een Private Services Server certificaat dienen de navolgende gegevens ingevuld te worden.

Van de abonneeorganisatie:
- Het abonneenummer.

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

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

Andere gegevens als:
- of sprake is van een initiële aanvraag of een vervanging;
- provincienaam;
- landnaam en landcode conform ISO 3166.

De abonnee moet aantonen dat de organisatie de primaire en additionele namen die de server of de service identificeren, mag voeren. De primaire en additionele namen van de server MOETEN vermeld worden als “fully-qualified domain name” (FQDN, zie definities). In dit veld MOGEN meerdere

FQDN"s worden gebruikt. Deze FQDN"s MOETEN uit dezelfde domeinnaam range komen. (b.v. www.logius.nl, applicatie.logius.nl, secure.logius.nl etc.).

In uitzonderlijke situaties is het mogelijk om als naam van de service een 'non-FQDN' (zie definities) op te geven als primaire of additionele naam van de server. Het gebruik van non-FQDN's wordt echter afgeraden. Indien een certificaat is uitgegeven zonder een FQDN, dan zal deze uiterlijk met ingang van 1 oktober 2016 worden ingetrokken.

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. Identificatie en Authenticatie bij vernieuwing van het certificaat.

3.3 Identificatie en authenticatie bij vernieuwen van het Certificaat

3.3.1 Identificatie en Authenticatie bij het vernieuwen van het sleutelmateriaal

De aanvraag tot vernieuwing van een certificaat gebeurt conform de procedures voor een initiële aanvraag.

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 12 november 2028. 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 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 Certificaatbeheerder, mag/kan een verzoek tot intrekking van een Certificaat indienen. Dit kan elektronisch/online gebeuren via de website van KPN (https://certificaat.kpn.com/pkioverheidcertificaten/intrekken/).

Om te kunnen overgaan tot intrekking dient de Certificaatbeheerder gebruik te maken van een intrekkingscode.

De intrekkingscode voor Private Services Server certificaten wordt tijdens de aanvraagprocedure door de KPN gegenereerd. Deze intrekkingcode wordt vervolgens door middel van een pinmailer aan Certificaatbeheerder verstuurd, waarmee het certificaat kan worden ingetrokken.

In voorkomende gevallen is de Abonnee verplicht zijn certificaat in te trekken (zie daarvoor de Bijzonder Voorwaarden). Voor het geval de Certificaatbeheerder dit nalaat dient de Abonnee dit zelf te (kunnen) doen. Daartoe dient de Certificaatbeheerder deze intrekkingscode aan de Abonnee te verstrekken dan wel dient de Abonnee de intrekkingscode direct na uitgifte bij de Certificaatbeheerder op te vragen en zorgvuldig te registreren.

Voor niet spoedeisende intrekkingen kan de Abonnee en/of de 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 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 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, 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, Certificaatbeheerders 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 Certificaatbeheerders en aan AMP. Maar zo heeft KPN meerdere 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 dit 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 Bijzondere Voorwaarden PKIoverheid certificaten, het CPS en de van toepassing zijnde CP's.

Voor verdere details, zoals de benodigde installatie handleidingen zie: https://certificaat.kpn.com .

.

4.1.2.3 Verantwoordelijkheden en verplichtingen van de Certificaatbeheerder

De de Certificaatbeheerder als houder van het Certificaat dat namens de Abonnee 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 Certificaatbeheerder 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 Certificaatbeheerder 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 gedefinieerd 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 de aanvraag 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 de aanvraag. 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 op de website beschikbaar gesteld formulier Abonnee Registratie in te vullen,uit te printen en te ondertekenen, 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 https://certificaat.kpn.com/formulieren/.

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 onvolkomenheden 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 Private Services Server certificaten worden geregistreerd. Certificaatbeheerders kunnen in beginsel meerdere Certificaten beheren, maar dienen daartoe eerst geregistreerd te worden. Dit kan door het web-formulier Registratie Certificaatbeheerders in te vullen, het gevraagde bewijsmateriaal (zie paragraaf 3.2.3.2) bij te voegen en het geheel per post of elektronisch 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 via AMP (zie verder paragraaf 4.2.2).

Is een Certificaatbeheerder eenmaal geïdentificeerd en geregistreerd, dan kunnen de aanvragen voor Private Services Server certificaten worden afgehandeld zoals in paragraaf 4.2.2 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 Private Services Server certificaten

Alvorens voor de eerste keer een Private Services certificaat kan worden aangevraagd dient er een specifieke aanvraag omgeving te worden aangemaakt in de aanvraag portal van KPN. In overleg met de opdrachtgever voor deze specifieke private omgeving en KPN worden dan de eisen die aan het certificaat worden gesteld vastgelegd en zal op basis hiervan aanvraagprocedure ter beschikking worden gesteld.

De Certificaataanvraag voor een Private Services Server certificaat verloopt in hoofdlijnen als volgt:

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 Private Services Server certificaat naar de Abonnee. De Abonnee vult het certificaataanvraagformulier in voor een (beoogde) server. Deze is te vinden op de website van KPN (https://certificaat.kpn.com/toepassingen). Op deze site staan ook nadere instructies voor het gebruik van het formulier.
2. De Abonnee drukt dit aanvraagformulier af, verklaart zich onder andere akkoord met de KPN PKIoverheid Bijzondere Voorwaarden door ondertekening en verstuurt het aanvraagformulier 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. Daarnaast wordt beoordeeld of sprake is van url-spoofing of phishing. En zo wordt ook http://www.phishtank.com of vergelijkbaar geraadpleegd om te bezien of de domeinnaam niet voorkomt op een spam- en/of phishing blacklist. Als KPN een verdenking heeft van phishing of ander mogelijk misbruik zal het die verdenking melden bij http://www.phishtank.com.
   Ook kan er nog een verificatie plaatsvinden van specifieke certificaateisen, zoals bijvoorbeeld het opnemen van een EAN 13 code bij EDSN certificaten.

4. Indien KPN de Certificaataanvraag goedkeurt zal deze voor identificatie van de certificaatbeheerder worden aangeboden aan AMP (identificerende partij voor KPN)

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 Private Services Server certificaten

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

4.3.2 Melding van certificaatvervaardiging aan de Certificaatbeheerder

Direct na vervaardiging van het Certificaat is vervaardiging te zien via Directory Dienst. De Certificaatbeheerder wordt expliciet op de hoogte gesteld van de vervaardiging door toezending van het Private Services Server certificaat per e-mail op het opgegeven e-mail adres.De Abonnee 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 Private Services Server certificaten

Het Private Services Server certificaat wordt geacht te zijn uitgereikt en geaccepteerd zodra de Certificaatbeheerder het verkregen Private Services Server certificaat in gebruik neemt. De Certificaatbeheerder dient na ontvangst de inhoud van het Certificaat op volledigheid en juistheid te controleren, alvorens over te gaan tot installatie en gebruik.

4.4.2 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 Certificaatbeheerder zijn beschreven in de Bijzondere Voorwaarden. Door ondertekening van de verschillende formulieren of erop te vertrouwen gaan betrokkenen akkoord met deze Bijzondere 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.

4.6 Certificaat vernieuwing

KPN biedt geen mogelijkheid tot vernieuwing van het Private Services Server certificaat. Een verzoek tot vernieuwing zal worden behandeld als een verzoek voor een nieuw certificaat.

4.7 Aanpassing van Certificaten

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

4.8 Intrekking en opschorting van certificaten

4.8.1 Omstandigheden die leiden tot intrekking

In de volgende gevallen is de Abonnee en/of de Certificaatbeheerder 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 private sleutel, en/of de intrekkingscode
- 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;
- wijziging van een domeineigenaar;
- beëindiging van de organisatorische eenheid;
- ontbinding of faillissement van de rechtspersoon van Abonnee.

Daarnaast zullen Private Services Server certificaten in de volgende gevallen worden ingetrokken, namelijk indien:

- 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 vernietigde private sleutel.
- 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 anderszins zich bewust wordt van een wezenlijke verandering in de informatie, die in het certificaat staat.
- 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.
- KPN op de hoogte wordt gesteld of anderszins 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).
- Abonnee een “code signing” certificaat gebruikt om “hostile code” (waaronder spyware, malware, trojans etc.) digitaal te ondertekenen.
- Policy Authority van PKIoverheid vaststelt dat de technische inhoud van het certificaat een onverantwoord risico met zich meebrengt voor abonnees, vertrouwende partijen en derden (zoals browserpartijen) en KPN verzoekt tot intrekking over te gaan.

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.

Indien een Private Services Server certificaten is ingetrokken of als de geldigheid van het Private Services Server certificaat is verlopen, is het niet meer toegestaan gebruik te maken van de private sleutel, behorend bij de publieke sleutel van het betreffende Private Services Server certificaat.

Die Private Services Server certificaten die uitgegeven zijn aan een gemeente die betrokken is bij een gemeentelijke herindeling hoeven niet direct te worden ingetrokken.. Hetzelfde geldt voor Ministeries die betrokken zijn bij een herindeling/fusering van ministeries.

Certificaten kunnen door KPN zonder nadere tussenkomst worden ingetrokken indien de Abonnee, 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 Private Services Server certificaten precies kunnen worden vastgesteld. In geval van twijfel geldt het door KPN vastgestelde tijdstip als moment van intrekking.

Als een Private Services Server certificaat is ingetrokken, kan het niet opnieuw geldig worden verklaard.

4.8.2 Wie mag een verzoek tot intrekking doen?

KPN zal een Certificaat intrekken na een verzoek daartoe van de Abonnee, de Certificaatbeheerder of de Policy Authority van PKIoverheid. 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.

4.8.3 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 B.V.
t.a.v. Afdeling Validatie, PKIoverheid Certificaten
Postbus 9105
7300 HN Apeldoorn

Online: https://certificaat.kpn.com/pkioverheidcertificaten/intrekken/.

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 (https://certificaat.kpn.com/files/formulieren/PKIO%20Intrekkingsverzoek%20Certificaten.pdf) 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.

4.8.4 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.

4.8.5 Verzoeken tot intrekking per brief worden pas op zijn vroegst de volgende werkdag na ontvangst in behandeling genomen en worden binnen vier uur na ontvangst verwerkt. Controlevoorwaarden bij raadplegen certificaat statusinformatie

Vertrouwende Partijen zijn verplicht de actuele status (ingetrokken/niet ingetrokken) van een Certificaat te controleren aan de hand van de in het certificaat genoemde datum einde geldigheid en door naslag van de certificaatstatusinformatie, gekoppeld aan het moment waarop het certificaat is c.q. wordt gebruikt. 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.

4.8.6 CRL-uitgiftefrequentie

De update van de CRLwordt om de 15 minuten geïnitieerd, nadat de CRL is gegenereerd wordt de CRL gepubliceerd.Een CRL heeft een geldigheidsduur van vierentwintig uur.

4.8.7 Maximale vertraging bij CRL-uitgifte

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

4.8.8 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.

4.8.9 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 uitwijk-locatie en -scenario ontworpen, dat regelmatig wordt getest, in combinatie met redundante gegevensverwerking en –opslag.

4.8.10 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.

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.

4.8.11 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.

4.8.12 Certificaatopschorting

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

4.9 Key Escrow and Recovery

Standaard vindt er geen Escrow van Private Sleutels plaats.

5 Management, operationele en fysieke beveiligingsmaatregelen

Het bedrijfsonderdeel van KPN dat de certificatiedienstverlening verzorgt is gecertificeerd tegen ISO9001: 2000, ISO27001:2005 en ETSI EN 319 411-1 en ETSI EN 319 411-2. 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-productie (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, 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

- Back-up van elektriciteit met behulp van een eigen elektriciteitsvoorziening;
- 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 omgeving

Indien sprake is van een Private Services Server certificaat, 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 6.2.11).

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 back-up

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 KPN-functies.

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

Autorisatie van het KPN 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 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 in tijdige en op 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.

Indien een incident of andere gebeurtenis op enigerlei wijze de betrouwbaarheid van de certificatiedienstverlening en/of het imago van de PKI voor de overheid kunnen bedreigen of beïnvloeden zal dit onmiddellijk gemeld worden aan de PKIoverheid Policy Authority.

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 op die manier 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 (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 Trusted Employee Policy 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 back-ups;
- datum en tijd van alle hardware wijzigingen;
- datum en tijd van auditlog dumps;
- afsluiting en (her)start van systemen.

Logging vindt plaats op minimaal:

- Routers, firewalls en netwerk systeem componenten;
- Database activiteiten en events;
- Transacties;
- Operating systemen;
- Access control systemen;
- Mail servers.

KPN houdt de volgende gebeurtenissen handmatig of automatisch bij

- Levenscyclus gebeurtenissen ten aanzien van de CA sleutel, waaronder:
  - genereren van sleutels, back-up, 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.
- bedreigingen, 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;
  - firewall en router activiteiten;
  - betreden van- en vertrekken uit de ruimte van de CA.

De log bestanden bevatten minimaal de volgende gegevens:

- bron adressen (IP adressen indien voorhanden);
- doel adressen (sen indien voorhanden);
- tijd en datum;
- gebruikers ID's (indien voorhanden);
- naam van de gebeurtenis;
- beschrijving van de gebeurtenis.

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 logbestanden worden minimaal 18 maanden opgeslagen en daarna worden ze verwijderd.
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 back-up van audit logs worden op dagelijkse basis, op geautomatiseerde wijze, gecreëerd, volledige back-ups 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 f Certificaatbeheerder is getoond;
- de bevindingen en het besluit over de aanvraag;
- de identiteit 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 precieze 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 levensduur 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 Private Services Server 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, 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, 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 (Almere) 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 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 kan ontstaan vanwege de beëindiging van de dienstverlening;
- realiseren van voorzieningen met betrekking tot de overdracht van de verplichtingen aan andere Certificatiedienstverleners, in zoverre 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'.

Voor de Private Services Server certificaten geldt dat deze verplicht worden gegenereerd door en onder verantwoording van de Abonnee in een Veilige Omgeving.

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.

6.1.2 Overdracht van de Publieke Sleutel van de Abonnee

De Abonnee stuurt de Publieke Sleutel naar KPN om deze te laten voorzien van een Private Services Server certificaat. 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 Private Services Server certificaat, gebruikt om de van een Servercertificaat voorziene Publieke Sleutel per e-mail terug te sturen naar het e-mailadres vermeld in de Certificaataanvraag van de Abonnee. Sleutellengten
De sleutellengte van een Certificaat is minstens 2048 bits. De sleutellengte van een SHA-2 CA-Certificaat is 4096 bits.

6.1.3 Generatie van Publieke Sleutel-parameters

Geen opmerkingen.

6.1.4 Gebruik van het sleutelpaar

Zie voor het gebruik van key usage extensies paragraaf 7.1.2. Overzicht Certificaatprofielen.

6.1.5 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 Private Services Server 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

6.2.4 Standaard vindt er geen Escrow van Private Sleutels plaats. Back-up van Private Sleutels

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

Van de Private Sleutels behorende bij Certificaten wordt geen back-up 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.

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

In het geval van Private Services Server certificaten wordt gebruik gemaakt van de door PKIoverheid geboden mogelijkheid om de sleutels van een Private Services Server certificaat 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 Private Services Server certificaat 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

De Private Services-Server certificaten hebben een vaste geldigheidsduur van 3 jaar.

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 Logische toegangsbeveiliging van KPN-systemen

6.4.1 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 multifactor authenticatie.

De integriteit van KPN-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.

6.4.2 Beheer en classificatie van middelen

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

6.5 Beheersmaatregelen technische levenscyclus

6.5.1 Beheersmaatregelen ten behoeve van systeemontwikkeling

KPN ontwikkelt daarnaast, gedeeltelijk, haar eigen Certificate Management System (hierna: 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.

6.5.2 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 wordt gebruikt, naast de in 6.5.1. genoemde maatregelen, is het gebruik van hashes.

6.6 Netwerkbeveiliging

KPN neemt passende 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.
Deze maatregelen zijn preventief, dedectief, repressief en correctief van aard. Ze omvatten ook het regelmatig (minimaal maandelijks) uitvoeren van een security scan en (minimaal jaarlijks) een penetratietest.

6.7 Time-stamping

KPN verzorgt geen time-stamping services.

7 Certificaat-, CRL- en OCSP-profielen

7.1 Certificaatprofielen

7.1.1 Overzicht Certificaatprofielen

De PKIoverheid Certificaten zijn opgebouwd volgens de PKIX X.509 v3 standaard, waarbij de mogelijkheid bestaat dat extensies worden gebruikt.
Certificaatprofielen zijn opgemaakt volgens Deel 3h van het Programma van Eisen van de PKIoverheid, conform het domein van organisatie.

7.1.1.1 Private Services Server certificaten

Basis attributen

Veld	Waarde
Version	2 (X.509v3)
SerialNumber	Uniek 128 bits lang Certificaatnummer
Issuer	CN = KPN PKIoverheid Private Services CA – G1 O = KPN B.V. C = NL
Validity	De geldigheidsperiode van het Private Services Server certificaat is standaard 3 jaar.
Subject	CN = <FQDN> SERIALNUMBER = <KvK nummer> O = <organisatienaam> OU = L = <plaats> S = <provincie> C = <landcode> 1.3.6.1.4.1.311.60.2.1.3 = NL2 2.5.4.15 = <businessCategory>

Standaard extensies

Veld	Essentieel	Waarde
AuthorityKeyIdentifier	Nee	160-bit SHA-1 Hashwaarde van de KPN Private Services CA
SubjectKeyIdentifier	Nee	160-bit SHA-1 Hashwaarde van het Private certificaat
KeyUsage	Ja	n/a
BasicConstraints	Ja	Het CA bit is ingesteld op ‘False’ en pathLenConstraint op ‘none’
CertificatePolicies	Nee	2.16.528.1.1003.1.2.8.6 (Private Services CP) Op dit certificaat is het Private Services CPS PKIoverheid van KPN van

		toepassing. The KPN Private Services PKIoverheid CPS applies to this certificate. https://certificaat.kpn.com/elektronische-opslagplaats/
SubjectAltName	Nee	dNSName CN = <FQDN> In dit veld MOGEN meerdere FQDN's worden gebruikt. Deze FQDN's MOETEN uit dezelfde domeinnaam range komen.
CrlDistributionPoints	Nee	Bevat de URI waarde van de betreffende CRL, die behoort bij het type Certificaat, kan worden opgehaald.
ExtendedKeyUsage	Nee	 serverAuth OID id-kp 1 Set (1.3.6.1.5.5.7.3.1) clientAuth OID id-kp 2 Set (1.3.6.1.5.5.7.3.2)
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 CRL profiel Private Services Server certificaten

Attributen

Veld	Waarde
Version	V2
Issuer	CN = KPN PKIoverheid Private Services CA – G1 O = KPN B.V. C = NL
effective date	Datum van uitgifte
next update	Dit is datum van uitgifte plus 24 uur, effectief wordt de update van de CRL om de 15 minuten geïnitieerd en na generatiegepubliceerd.
signatureAlgorithm	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 B.V. (één van haar rechtsvoorgangers) door KPMG Certification b.v. gecertificeerd tegen het "TTP.NL Scheme for management system certification of Trust Service Providers issuing Qualified Certificates for Electronic Signatures, Public Key Certificates, Website Certificates and / or Time-stamp tokens" tegen ETSI TS 101 456 en voldeed daarmee aan de eisen zoals gesteld aan Certificatiedienstverleners in de toenmalige Wet Elektronische handtekening. Het ETSI TS 101 456 Certificaat is op dezelfde datum in de jaren 2005, 2008, 2011 en 2014 verlengd door de certificerende instantie BSI Management Systems.
KPN is sinds 2014 tevens gecertificeerd tegen ETSI TS 102 042.
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.

eIDAS
Op 1 juli 2016 is de Europese Verordening (VERORDENING (EU) Nr. 910/2014 VAN HET EUROPEES PARLEMENT EN DE RAAD van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG) van kracht geworden.
Deze verordening vervangt de Nederlandse Wet Elektronische Handtekening.
Omdat in deze verordening de eisen t.a.v. frequentie van de audit en de accreditatie zijn opgenomen is voornoemd TTP.NL Scheme per die datum vervallen.

Ook zijn de eerdere ETSI certificeringen in februari 2016 ETSI TS 101 456 en ETSI TS 102 042 vervangen door resp. de ETSI certificeringen ETSI EN 319 411-2 en ETSI EN 319 411-1.
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 EN 319 411-1 en het ETSI EN 319 411-2-certificaat staan 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.

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 Certificaatbeheerders uitbesteed naar AMP.

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 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 Abonnees;
- interne procedures voor behandeling en afhandeling van Abonnee-, Certificaataanvragen en intrekkingsverzoeken;
- gegevens over systemen en infrastructuren;
- 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 voor zover 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 Abonnee maakt zelf het sleutelpaar aan waarvoor het een Private Services Server certificaat 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 Certificaatbeheerder en de Abonnee geven toestemming voor publicatie van certificaatgegevens door instemming met de Bijzonder Voorwaarden. Het voltooien van een aanvraagprocedure door de Certificaatbeheerder 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 privaatrechtelijke bewijsvoering

Het Certificaat en de bij de Certificaataanvraag verstrekte gegevens zullen blijven opgeslagen gedurende een nader aan de Abonnee 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 worden verstrekt met voorafgaande schriftelijke toestemming van de Abonnee.

9.4.8 Verstrekking op verzoek van de eigenaar

KPN verstrekt de Abonnee en/of Certificaatbeheerder desgevraagd de hem betreffende persoonsgegevens. KPN verstrekt de Abonnee desgevraagd persoonsgegevens van een Certificaatbeheerder die namens de 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.

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 blijft 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, 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

Op 1 juli 2016 is de Europese Verordening (VERORDENING (EU) Nr. 910/2014 VAN HET EUROPEES PARLEMENT EN DE RAAD van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG) van kracht geworden.
In deze verordening wordt onder (35) de navolgende tekst gepubliceerd:
“Alle verleners van vertrouwensdiensten moeten zich houden aan de vereisten van deze verordening, in het bijzonder wat betreft veiligheid en betrouwbaarheid, zodat de zorgvuldigheid, transparantie en verantwoording van hun activiteiten worden gewaarborgd. Gelet op de soort diensten die verleners van vertrouwensdiensten verlenen, dient echter met betrekking tot deze vereisten onderscheid te worden gemaakt tussen gekwalificeerde en niet- gekwalificeerde verleners van vertrouwensdiensten.”

NB op basis van dit CPS kunnen alleen private servercertificaten wortden uitgegeven.

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 Definities

Aanvrager: Een natuurlijke of rechtspersoon die een aanvraag tot uitgifte van een Private Services Servercertificaat indient bij KPN.

Abonnee: rechtspersoon die een overeenkomst aangaat met KPN om uitgifte van Private Services Server certificaten aan door de Abonnee aangewezen Certificaatbeheerders 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 moet 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.

Bevoegd vertegenwoordiger
Een natuurlijk persoon die bevoegd is een organisatie te vertegenwoordigen. 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 commanditaire 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.

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 Private Services Server certificaat 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.

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.

Certificate Transparency. Certificate Transparency (CT) is een initiatief van Google met de intentie om te voorkomen dat een CSP certificaten voor internet domeinen zou kunnen uitgeven zonder medeweten van de eigenaar van dit domein.

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 Private Services Server 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. 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.

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 Opslagplaats: locatie waar relevante informatie ten aanzien van de dienstverlening van KPN is te vinden.
Zie: http://certificaat.kpn.com/elektronische-opslagplaats/.

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

.

Fully Qualified Domain Name (FQDN)
Een Fully Qualified Domain Name (FQDN) volgens de definitie van PKIoverheid, is een in het Internet Domain Name System (DNS) geregistreerde volledige naam waarmee een server op het Internet uniek is te identificeren en te adresseren. Met die definitie omvat een FQDN alle DNS nodes, tot en met de naam van het desbetreffende Top Level Domein (TLD) en is een FQDN in het Internet DNS geregistreerd onder een DNS Resource Record (RR) van het type “IN A” en/of “IN AAAA” en/of “IN CNAME”.

Voorbeelden van FQDN’s zijn:
- www.logius.nl
- webmail.logius.nl
- local.logius.nl
- server1.local.logius.nl
- logius.nl (mits geregistreerd onder een DNS RR van het type “IN A” en/of “IN AAAA” en/of “IN CNAME”)

Voorbeelden van non-FQDN’s (deze zijn alleen in uitzonderlijke gevallen toegestaan binnen PKIoverheid) zijn:
- server1.webmail
- server1.local
- server1
- publieke IP adressen (zowel IPv4 als IPv6)

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.

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.

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.

Organisatiegebonden certificaten
Bij organisatiegebonden Private Services Server certificaten 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[1]

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 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.

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.

Privaat IP adres
Een Internet Protocol adres (IP adres) is een identificatienummer toegewezen aan elk apparaat (bijvoorbeeld computer, printer) dat deelneemt aan een computernetwerk dat het Internet Protocol (TCP/IP) gebruikt voor de communicatie.
Private IP adressen zijn niet routeerbaar op het internet en zijn gereserveerd voor particuliere netwerken. De binnen IPv4 voor privégebruik vrijgehouden c.q. gereserveerde IP adressenreeks is (zie RFC 1918):

- 10.0.0.0 – 10.255.255.255;

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

- 172.16.0.0 – 172.31.255.255;
- 192.168.0.0 – 192.168.255.255;

Daarnaast is de reeks van 169.254.0.0 -169.254.255.255 gereserveerd voor Automatic Private IP Addressing (APIPA). Deze IP adressen mogen niet worden gebruikt op het internet.

De binnen IPv6 voor privégebruik vrijgehouden c.q. gereserveerde IP adressen reeks is (zie RFC 4193):
- fc00::/7

Daarnaast is de reeks van fe80::/10 gereserveerd voor Automatic Private IP Addressing (APIPA). Deze IP adressen mogen niet worden gebruikt op het internet.

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.

Publiek IP adres
Publieke IP adressen zijn wereldwijd uniek en kunnen routeerbaar, zichtbaar en benaderbaar zijn vanaf het internet.

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.

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 3h).

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.

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.

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. 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 2 Afkortingen

Afkorting	Betekenis
ACM	Autoriteit Consument & Markt
CA	Certificatie Autoriteit (Certification Authority)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificaten Revocatie Lijst
CSP	Certification Service Provider ofwel Certificatiedienstverlener
ETSI	European Telecommunication Standardisation Institute
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PvE	(PKIoverheid) Programma van Eisen
RA	Registratie Autoriteit (Registration Authority)
Wji	Wet justitiële informatie
Wbp	Wet bescherming persoonsgegevens
Wid	Wet op de identificatieplicht