Certification Practice Statement PKIoverheid

Versie: **1.0**
Datum: **30 juni 2009**

QuoVadis Trustlink B.V.
Maliesingel 22
3531 BG Utrecht
Tel: +31 302324320
Fax: +31 302324329

Inhoudsopgave

1. Introductie

1.1 Achtergrond

De PKI voor de overheid is een initiatief van de Nederlandse overheid en vormt een raamwerk met eisen en afspraken die het gebruik van een elektronische Handtekening, elektronische authenticatie en vertrouwelijke elektronische communicatie mogelijk maakt, gebaseerd op certificaten met een hoog betrouwbaarheidsniveau. De eisen die aan de Certification Service Provider (CSP) worden gesteld voor het uitgeven en beheren van deze certificaten worden gesteld, zijn beschreven in het Programma van Eisen PKIoverheid (http://www.pkioverheid.nl).

QuoVadis, in Nederland, handelend onder de naam QuoVadis Trustlink B.V., is een leidende internationale aanbieder van certificaten. QuoVadis is opgericht in 1999 en houdt tevens kantoor in Zwitserland, het Verenigd Koninkrijk en Bermuda. QuoVadis in Nederland is als CSP gecertificeerd en tevens toegetreden tot de PKI voor de overheid.

De infrastructuur van de PKI voor de overheid waaraan QuoVadis deelneemt, bestaat uit een hiërarchie met meerdere niveaus. Op elk niveau worden diensten geleverd conform strikte normen om de betrouwbaarheid van de gehele PKI voor de overheid zeker te stellen.

De Policy Authority PKIoverheid (PA) is verantwoordelijk voor het beheer van de centrale infrastructuur. De PKI voor de overheid is zo opgezet dat overheidsorganisaties en marktpartijen als certificatiedienstverlener (Certification Service Provider – CSP) 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 het handhaven van de afspraken en daarmee op de betrouwbaarheid van de gehele PKI voor de overheid.

1.2 Documentnaam en identificatie

Voor u ligt het PKIoverheid Certification Practice Statement (CPS) van QuoVadis. Dit document beschrijft de procedures en maatregelen die QuoVadis in acht neemt bij het uitgeven van certificaten in het domein Organisatie van de PKI voor de overheid. Deze maatregelen zijn in overeenstemming met de eisen uit ETSI TS 101456, de aanvullende eisen uit het Besluit Elektronische Handtekeningen en het Programma van Eisen PKIoverheid delen 3a en 3b.

1.3 Deelnemende partijen

1.3.1 Certification Authorities

1.3.1.1 Centrale Infrastructuur PKIoverheid

De centrale infrastructuur van de PKI voor de overheid wordt namens de Staat der Nederlanden beheerd door GBO.overheid en bestaat uit de volgende componenten:

- Staat der Nederlanden Root Certification Authority
- Staat der Nederlanden Domein Certification Authority - Organisaties

1.3.1.2 QuoVadis CSP Certification Authority (CSP-CA)

De Quo Vadis CSP-CA wordt beheerd in het beveiligde datacenter van QuoVadis in Bermuda en deze geeft de certificaten uit ten behoeve van certificaathouders binnen de PKI voor de overheid en in overeenstemming met dit CPS. Een overzicht van certificaten die worden uitgegeven is opgenomen in 1.4.

1.3.2. Registration Authorities

1.3.2.1 QuoVadis Registration Authority (QuoVadis RA)

De QuoVadis Registration Authority in Utrecht verzorgt de identificatie en registratie van de certificaathouder en de certificaatbeheerder en verzorgt de intrekkingen van uitgegeven certificaten.

1.3.3. Eindgebruikers

1.3.3.1 Abonnee

Een abonnee is natuurlijke of rechtspersoon die met een CSP een overeenkomst sluit namens een of meer certificaathouders voor het laten certificeren van de publieke sleutels. Een abonnee kan tevens certificaathouder zijn.

1.3.3.2 Certificaathouder

Bij de persoonlijke certificaten is de entiteit, gekenmerkt in een certificaat als de houder van de private sleutel die is verbonden met de publieke sleutel die in het certificaat is gegeven. De certificaathouder is onderdeel van een organisatorische entiteit waarvoor een abonnee de contracterende partij is. De abonnee accordeert bij de aanvraag dat de certificaathouder een certificaat mag ontvangen met daarin de organisatiegegevens van de abonnee.

Bij de systeemcertificaten (Services) is de certificaathouder een apparaat of een systeem (een niet-natuurlijke persoon), bediend door de abonnee of door een daartoe aangewezen certificaatbeheerder.

1.3.3.2 Certificaatbeheerder

Voor het uitvoeren van de operationele handelingen ten behoeve van het systeemcertificaat (o.a. de aanvraag, installatie en beheer, intrekking) is de tussenkomst door een natuurlijke persoon vereist. De abonnee kan dit zelf uitvoeren of wijst hiertoe een functionaris aan, de certificaatbeheerder. In dat geval verleent de abonnee aan de certificaatbeheerder de expliciete toestemming om de operationele handelingen uit te voeren.

1.3.4. Vertrouwende Partijen

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

1.4 Certificaatgebruik

QuoVadis geeft binnen de PKI voor de overheid de onderstaande typen certificaten uit. De Certificaten mogen uitsluitend voor het daarvoor bestemde doel worden gebruikt, in overeenstemming met dit CPS, de gebruikersvoorwaarden en het Key Usage veld in het certificaat.

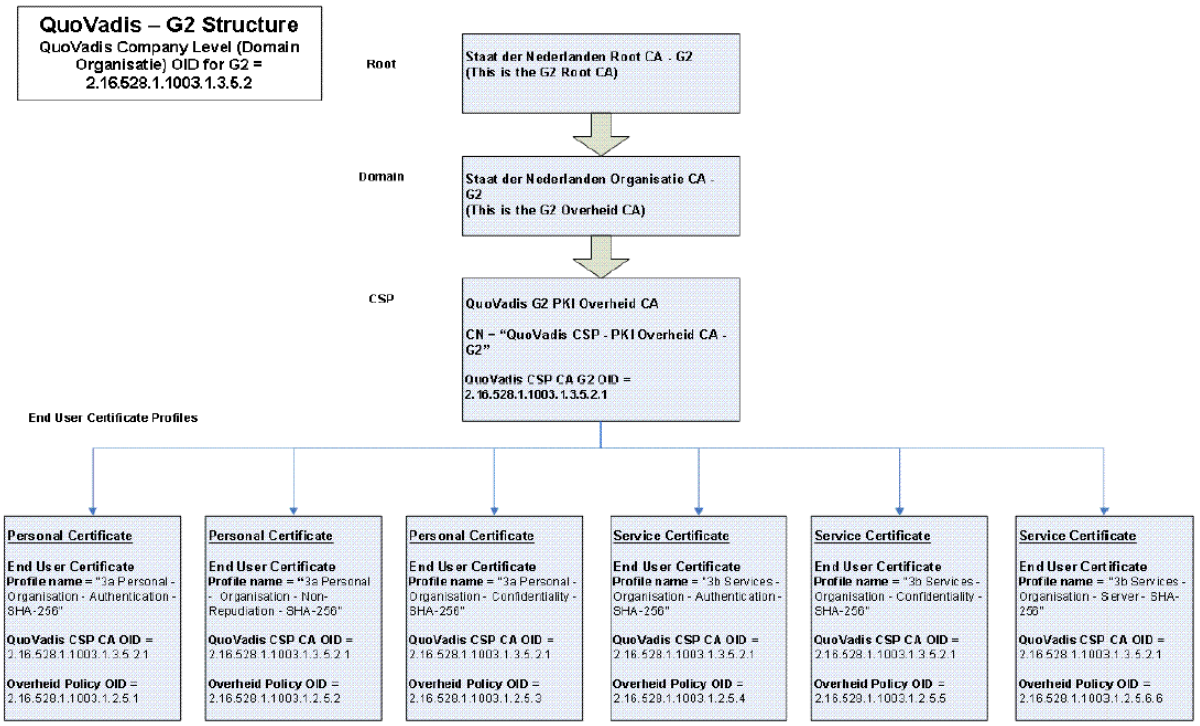
Certificaten voor Personen: QuoVadis geeft de volgende certificaten uit aan personen. Een persoon ontvangt de volgende certificaten, opgeslagen op een veilig middel (SSCD):

- Een *Handtekeningcertificaat* dat onder deze CPS wordt uitgegeven kan worden gebruikt om een elektronische handtekening te verifiëren, die "dezelfde rechtsgevolgen heeft als een handgeschreven handtekening", zoals wordt aangegeven in artikel 15a, eerste en tweede lid, in Titel 1 van Boek 3 van het Burgerlijk Wetboek onder afdeling 1A en is een gekwalificeerd certificaat zoals bedoeld in artikel 1.1, lid ss van de Telecomwet;
- Een *Authenticiteitcertificaat* dat onder deze CPS wordt uitgegeven kan worden gebruikt voor het langs elektronische weg betrouwbaar identificeren en authenticeren van een persoon als behorende bij een organisatorische entiteit;
- Een *Vertrouwelijkheidcertificaat* dat onder deze CPS wordt uitgegeven, kan worden gebruikt voor het beschermen van de vertrouwelijkheid van gegevens, die worden uitgewisseld en/of opgeslagen in elektronische vorm. Dit betreft zowel de uitwisseling tussen personen onderling als tussen personen en geautomatiseerde middelen.

Systeemcertificaten (Services): QuoVadis geeft daarnaast de volgende niet-persoonlijke certificaten uit (voor systemen).

- Een *Server certificaat*, dat onder deze CPS worden uitgegeven kan worden gebruikt voor het beveiligen van een verbinding tussen een bepaalde client en een server die behoort bij de organisatorische entiteit (abonnee) die wordt genoemd in het betreffende certificaat.
- Een *Service certificaat (authenticatie)*, dat onder deze CPS worden uitgegeven kan worden gebruikt voor het langs elektronische weg betrouwbaar identificeren en authenticeren van de service als behorende bij de organisatorische entiteit, die verantwoordelijk is voor de betreffende service, alsmede het versleutelen van data.
- Een *Service certificaat (vertrouwelijkheid)*, dat onder deze CPS worden uitgegeven kan worden gebruikt worden gebruikt voor het beschermen van de vertrouwelijkheid van gegevens, die worden uitgewisseld en/of opgeslagen in elektronische vorm.

De CA-structuur en de typen certificaten die QuoVadis uitgeeft zijn inzichtelijk gemaakt in onderstaande figuur.



Figuur1

1.5 CPS-beheer

De Policy Management Organisatie van QuoVadis beheert dit CPS en ziet er op toe dat de toepasselijke eisen adequaat zijn verankerd in de QuoVadis documentatie en procedures, op alle betrokken bedrijfslocaties.

De toepasselijke versie van het QuoVadis CPS wordt elektronisch beschikbaar gesteld in PDF-formaat op: www.quovadisglobal.com/repository. Daar vindt u ook de overeenkomsten en de toepasselijke voorwaarden voor onze dienstverlening.

Een nieuwe versie van het CPS - met wijzigingsvoorstellen - wordt voorafgaand aan de ingangsdatum gepubliceerd. Informatie over modificatie binnen dit CPS kunnen worden gevonden in sectie 9.12.

Informatie over dit CPS en voorgenomen wijzigingen daarop kan worden verkregen via onderstaande contactgegevens:

QuoVadis Trustlink B.V.
T.a.v. Policy Management
Maliesingel 22
3531 BG Utrecht
Tel: +31 302324320
Fax: +31 302324329

Website: www.quovadisglobal.nl
E-mail: info.nl@quovadisglobal.com

2. Publicatie en verantwoordelijkheid voor elektronische opslagplaats

2.1 Elektronische opslagplaats

QuoVadis heeft een elektronische opslagplaats die bereikbaar is via: www.quovadisglobal.com/repository

2.2 Publicatie van CSP-informatie

De opslagplaats maakt de volgende zaken toegankelijk:

- CPS
- Overeenkomst en toepasselijke gebruiksvoorwaarden
- Certificaten van certificaathouders (mits daar door de certificaathouder toestemming voor is verleend)
- Certificate Revocation List (CRL)

De locatie van de Elektronische opslagplaats en Online Certificate Status Protocol (OCSP) responders worden tevens weergegeven in het toepasselijke veld van de betreffende Certificaatprofielen welke zijn opgenomen in de bijlage bij dit CPS.

De unieke nummers (OID's) die refereren naar de toepasselijke Certificate Policies voor persoonlijke certificaten in het Domein Organisatie (PvE PKIoverheid deel 3a) zijn:

Authenticiteit	2.16.528.1.1003.1.2.5.1
Onweerlegbaarheid	2.16.528.1.1003.1.2.5.2
Vertrouwelijkheid	2.16.528.1.1003.1.2.5.3

De unieke nummers (OID's) die refereren naar de toepasselijke Certificate Policies voor systeemcertificaten (PvE PKIoverheid deel 3b) zijn:

Services – Authenticiteit	2.16.528.1.1003.1.2.5.4
Services – Vertrouwelijkheid	2.16.528.1.1003.1.2.5.5
Services – Server	2.16.528.1.1003.1.2.5.6

2.3 Moment of frequentie van publicatie

De informatie in de elektronische opslagplaats wordt zo snel als mogelijk is gepubliceerd en/of geactualiseerd.

2.4 Toegang tot gepubliceerde informatie

De toegangscontrole tot de elektronische opslagplaats is zodanig ingericht dat alleen leesrechten zijn toegekend voor derden die deze informatie raadplegen.
Het raadplegen van certificaten kan alleen door individuele certificaatinformatie als zoekterm in te voeren. Uitsluitend QuoVadis heeft schrijfrechten op de elektronische opslagplaats.

De elektronische opslagplaats is 24 uur per dag, 7 dagen per week voor een ieder beschikbaar, met uitzondering van systeemdefecten of onderhoudswerkzaamheden. Ingeval

van onvoorziene onbeschikbaarheid, wordt de beschikbaarheid van de elektronische opslagplaats (dissemination service) hersteld binnen 24 uur.

3. Identificatie en Authentificatie (I&A)

3.1 Naamgeving

3.1.1 Soorten naamformaten

De naam in het subject veld van het certificaat moet de Certificaathouder duidelijk identificeren en weergegeven zijn in een leesbare en begrijpelijke vorm, in overeenstemming met de X.500 standaard voor Distinguished Names (DN).

Elke certificaathouder moet een unieke en direct identificeerbare X.501 DN hebben. Deze DN kan bestaan uit de volgende attributen:

- Land (C)
- Organisatie (O)
- Organisatorische eenheid (OU)
- Common name (CN)
- SerialNumber

3.1.2 Noodzaak gebruik betekenisvolle namen

De naamgeving in de uitgegeven certificaten is betekenisvol, ondubbelzinnig en uniek en stelt elke vertrouwende partij in de gelegenheid de identiteit van de certificaathouder vast te stellen.

De inhoud van het Certificaat moet een betekenisvolle associatie hebben met de naam van de betreffende persoon, organisatie of het apparaat. In het geval van personen moet de naam bestaan uit de eerste voornaam, overige voorletters en achternaam. Voor organisaties moet de naam op een betekenisvolle manier de naam van de geregistreerde juridische entiteit (van de abonnee) weergeven en in geval van een apparaat tevens de geregistreerde domeinnaam van de organisatie (abonnee) weergeven die verantwoordelijk is voor dat apparaat.

3.1.3. Pseudoniemen

Het gebruik van anonieme certificaten of pseudoniemen is niet toegestaan.

3.1.4. Regels voor interpreteren verschillende naamsvormen

De regels voor interpretatie van naamsvormen worden teruggevonden in de International Telecommunication (ITU) en Internet Engineering Task Force (IETF) standaarden, zoals de ITU-T X.500 serie van standaarden en toepasbare IETF RFCs.

3.1.5 Uniciteit van namen.

De DistinguishedName van de Certificaathouder in een certificaat dat onder dit CPS is uitgegeven, is te allen tijde uniek voor deze Certificaathouder en wordt niet uitgegeven aan een andere Certificaathouder. Het is de taak van de QuoVadis RA te verifiëren dat de DistinguishedName van de certificaathouder nog niet is opgenomen in de elektronische opslagplaats voor certificaten (de QuoVadis X.500 directory).

QuoVadis mag, indien nodig, additionele nummers of letters aan de CommonName van het certificaat-subject toevoegen om zodoende onderscheid te maken tussen twee bestaande certificaten die anders dezelfde subjectnaam zouden hebben.
Elk Certificaat krijgt verder een uniek serienummer toegewezen, dat een eenduidige en unieke identificatie van Certificaathouders mogelijk maakt.

3.1.6 Erkenning, authenticatie en de rol van handelsmerken

Voor zover de naam van een organisatie voorkomt in een algemeen erkend openbaar register, een oprichtingsakte, een instellingsbesluit of in een ander wettelijk erkend document ter identificatie van organisaties, zal in het Certificaat deze naam van de organisatie worden opgenomen. QuoVadis voert geen onderzoek uit (zoals een handelsnaamonderzoek) naar het juridisch rechtmatig gebruik van een organisatienaam.

3.1.7. Geschillen

Ingeval van geschillen over de op te nemen naamgeving in een certificaat, beslist QuoVadis op basis van een belangenafweging welke naam opgenomen wordt.

3.2 Initiële identiteitsvalidatie

3.2.1. Methode om bezit van private sleutel aan te tonen.

QuoVadis zal vaststellen dat elke Aanvrager van een certificaat in het bezit is van een private sleutel die overeenkomt met de publieke sleutel die opgenomen is in de aanvraag voor een certificaat. QuoVadis zal dit doen door middel van het gebruik van een beveiligd protocol, zoals de IETF PKIX Certificate Management Protocol, inclusief PKCS#10.

3.2.2. Authenticatie van de organisatorische eenheid

De Certificaathouders die als subject zijn genoemd in de Certificaten voor Personen en in de Systeemcertificaten behoren altijd bij de organisatorische entiteit van de abonnee.

Tijdens de registratieprocedure worden formulieren gehanteerd die als registratie dienen van de door de abonnee aangeleverde gegevens.
Ten behoeve van de authenticatie van de organisatorische eenheid wordt in elk geval vastgelegd:

- De volledige naam van de organisatorische entiteit;
- De relevante registratieinformatie van de organisatorische entiteit en het daarbij behorende bewijs;

Op basis van de formulieren en de daarbij aangeleverde bewijsmiddelen verifieert Registration Authority:

- dat de abonnee als organisatorische entiteit een bestaande organisatie is;
- dat de de door de abonnee aangemelde organisatienaam die in het certificaat wordt opgenomen juist en volledig is.

3.2.3. Authenticatie van persoonlijke identiteit.

De Certificaathouders die als subject zijn genoemd in de Certificaten voor Personen en in de Systeemcertificaten behoren altijd bij de organisatorische entiteit van de abonnee.

Tijdens de registratieprocedure worden formulieren gehanteerd die als registratie dienen van de door de abonnee aangeleverde gegevens.
Ten behoeve van de authenticatie van de persoonlijke identiteit van de abonnee, certificaathouder (of indien van toepassing - de certificaatbeheerder) worden in elk geval vastgelegd:

- De volledige naam, met inbegrip van achternaam, eerste voornaam, overige voorna(a)m(en) of de initialen van de overige voorna(a)m(en);
- Geboortedatum en -plaats,
- Nationaal passend registratienummer, of andere eigenschappen van de certificaathouder die kunnen worden gebruikt om, voor zover mogelijk, de persoon van andere personen met dezelfde naam te kunnen onderscheiden;
- Bij de certificaatbeheerder:
  - het bewijs (formulier) waarin is vastgelegd dat de certificaatbeheerder gerechtigd is voor een certificaathouder een certificaat te ontvangen namens de rechtspersoon of andere organisatorische entiteit;

Bij systeemcertificaten worden in elk geval vastgelegd:

- De in het certificaat op te nemen naam van de certificaathouder (systeem);
- Bij SSL-certificaat: de domeinnaam

Op basis van de formulieren en de daarbij aangeleverde bewijsmiddelen verifieert Registration Authority:

- de persoonlijke identiteit van de abonnee, de certificaathouder (en indien van toepassing – de certificaatbeheerder) op basis van persoonlijke verschijning en aan de hand van een in art. 1 van de Wet op de Identificatieplicht genoemd identiteitsdocument;
- De geldigheid en echtheid van het hier boven genoemde identiteitsdocument, op basis van de daarvoor gepubliceerde echtheidskenmerken;
- In het geval dat er een e-mailadres is opgenomen in het Certificaat zal QuoVadis het e-mailadres verifiëren middels het zenden van een verificatie-mail naar dit mailadres met een reply-verzoek aan de eindgebruiker om ontvangst, en daarmee de geldigheid van het e-mailadres, te bevestigen.

Bij systeemcertificaten worden in elk geval geverifieerd:

- De in het certificaat op te nemen naam van de certificaathouder (systeem);
- Bij SSL-certificaat: domeinnaam en eigenaarschap daarvan op basis van controle bij de Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority.

In de overeenkomst met de abonnee is de verklaring opgenomen dat de abonnee verantwoordelijk is om, indien er relevante wijzigingen hebben plaatsgevonden in de relatie

tussen abonnee en Certificaatbeheerder, deze onmiddellijk aan QuoVadis kenbaar te maken door middel van een intrekkingverzoek (bijvoorbeeld beëindiging dienstverband).

3.2.4. Niet-geverifieerde gegevens

Tijdens de registratieprocedure worden formulieren gehanteerd die als registratie dienen van de door de abonnee aangeleverde gegevens. Hierin zijn gegevens opgenomen die dienen voor de correspondentiedoeleinden en/of die optioneel in het certificaat kunnen worden opgenomen. Hierbij kan worden gedacht aan de adresgegevens van de organisatorische entiteit of de naam van de afdeling (OU).

3.2.5. Autorisaties van de Certificaathouder en Certificaatbeheerder

Tijdens de registratieprocedure worden formulieren gehanteerd die als registratie dienen van de door de abonnee aangeleverde gegevens.
Ter autorisatie van de Certificaathouder en Certificaatbeheerder wordt in elk geval vastgelegd:

- dat de certificaathouder (en – indien van toepassing – de Certificaatbeheerder) bij de organisatorische entiteit van de abonnee hoort;
- dat de certificaathouder geautoriseerd is namens de abonnee om een certificaat te ontvangen.
- Bij de certificaatbeheerder:
  - de toestemming van de abonnee om aan hem opgedragen handelingen uit te voeren;
  - dat de certificaatbeheerder gerechtigd is voor een certificaathouder een certificaat te ontvangen namens de rechtspersoon of andere organisatorische entiteit.

Op basis van de formulieren en de daarbij aangeleverde bewijsmiddelen verifieert Registration Authority:

- dat het bewijs dat de certificaathouder geautoriseerd is namens de abonnee om een certificaat te ontvangen, authentiek is en dat de in dit bewijs genoemde naam en identiteitskenmerken overeenkomen met de vastgestelde identiteit van de certificaathouder;
- Bij de certificaatbeheerder:
  - of de certificaatbeheerder toestemming heeft verkregen van de abonnee om aan hem opgedragen handelingen uit te voeren.

3.3 Identificatie en Authenticatie bij vernieuwing van een Certificaat

QuoVadis hanteert geen specifieke procedures bij vernieuwing van een certificaat. De aanvraag tot vernieuwing van een certificaat gebeurt conform de procedures voor een initiële aanvraag. Dit betekent tevens dat voor het nieuwe certificaat altijd een nieuw sleutelpaar wordt gegenereerd.

3.4 Identificatie en Authenticatie bij intrekking van een Certificaat

Een aanvraag tot intrekking van een certificaat kan alleen worden ingediend door een daartoe bevoegd persoon (zie Par. 4.9).

De abonnee, de certificaathouder en de Certificaatbeheerder die een verzoek tot intrekking wil indienen identificeert en authenticeert zich door:

- Het fysiek verschijnen bij de Registration Authority en daarbij ter identificatie te overleggen een in artikel 1 van de Wet op de Identificatieplicht genoemd, geldig identiteitsdocument. De Registration Officer verricht de verificatie.
- De intrekking te verrichten via de website van QuoVadis en daarbij ter identificatie een bestaand gedeeld geheim of intrekkingswachtwoord in te voeren. Het betreffende QuoVadis backofficesysteem verricht de verificatie;
- Telefonische communicatie en daarbij ter identificatie een bestaand gedeeld geheim of intrekkingswachtwoord te vermelden. De Registration Officer verricht de verificatie.

4 Operationele eisen

4.1. Certificaataanvraag

Aanvraag tot levering van PKIoverheid certificaten wordt pas ingediend door de abonnee nadat de overeenkomst tussen QuoVadis en Abonnee is afgesloten.
De aanvraag voor Certificaten voor Personen wordt ingediend door de abonnee met gebruikmaking van het daartoe bestemde formulier.
De aanvraag voor een systeemcertificaat wordt ingediend door de Certificaatbeheerder met gebruikmaking van het daartoe bestemde formulier. Dit kan uitsluitend nadat de Certificaatbeheerder door abonnee geautoriseerd is deze handelingen uit te voeren.

4.2. Verwerken Certificaataanvraag

De abonnee dient het ingevulde aanvraagformulier in bij QuoVadis, met daarbij als bijlage(n) de formulieren voor de aanvraag van Certificaten voor Personen.
De Certificaatbeheerder dient het ingevulde aanvraagformulier Systeemcertificaat in bij QuoVadis, met daarbij het formulier Autorisatie Certificaatbeheerder voorzover dit nog niet bij QuoVadis in bezit is.

Voor Certificaten voor Personen vindt vervolgens bij de Registration Authority de procedure plaats ter identificatie en authenticatie van de Certificaathouder(s) conform 3.2 van dit CPS. Hierbij worden de door abonnee ingestuurde formulieren gehanteerd.
Voor Systeemcertificaten vindt bij de Registration Authority de procedure plaats ter identificatie en authenticatie van de Certificaatbeheerder conform 3.2 van dit CPS. Hierbij wordt het door Certificaatbeheerder opgeleverde aanvraagformulier en het door abonnee ingestuurde formulier Autorisatie Certificaatbeheerder gehanteerd.

4.3 Certificaatuitgifte

Voor Certificaten voor Personen en voor Systeemcertificaten voor authenticatie en vertrouwelijkheid wordt na het succesvol afronden van de identificatie en authenticatieprocedure van de Certificaathouder/Certificaatbeheerder, in aanwezigheid van de Registration Officer een SSCD geprepareerd. Het sleutelmateriaal wordt gegenereerd en vervolgens worden door de Registration Officer de certificaataanvragen voor de PKIoverheid certificaten ingediend bij de QuoVadis CSP-CA.
Na generatie van de certificaten worden deze – samen met de complete PKIoverheid certificaathierarchie - op het SSCD geplaatst en aan de Certificaathouder/Certificaatbeheerder afgeleverd. Aanvullende informatie over de Technische beveiligingsmaatregelen is opgenomen in hoofdstuk 6 van dit CPS.

Voor systeemcertificaten voor SSL wordt door de Certificaatbeheerder een Certificate Signing Request (CSR) gegenereerd en opgeleverd aan de Registration Authority. Deze CSR wordt door de Registration Officer geverifieerd aan de hand van het aanvraagformulier Systeemcertificaat en vervolgens wordt het systeemcertificaat voor SSL gegenereerd. Het systeemcertificaat voor SSL kan door de Certificaatbeheerder worden gedownload en worden opgeslagen op een drager. Aanvullende informatie over de Technische beveiligingsmaatregelen is opgenomen in hoofdstuk 6 van dit CPS.

4.4. Acceptatie van Certificaten

Acceptatie van certificaten heeft geacht te hebben plaatsgevonden na afronding van de Certificaatuitgifte en de overdracht van het SSCD aan de certificaathouder. De certificaathouder of de certificaatbeheerder tekent voor ontvangst van het SSCD.

Voorafgaand aan de acceptatie van het certificaat heeft de certificaathouder reeds aangegeven of de certificaten voor publicatie in de elektronische opslagplaats zijn vrijgegeven. De certificaathouder geeft daarvoor zijn expliciete toestemming.

Met de acceptatie van het certificaat en het gebruik daarvan gaat de Certificaathouder/de Certificaatbeheerder akkoord met:

- Hetgeen bepaald is in dit CPS
- De Algemene Voorwaarden
- De plicht om (toegang tot) de private sleutel die correspondeert met de publieke sleutel opgenomen in het Certificaat adequaat te beveiligen, het SSCD op een zorgvuldige wijze te gebruiken en om redelijke voorzorgsmaatregelen te treffen om verlies, diefstal, modificatie of ongeautoriseerd gebruik van de private sleutel te voorkomen.

De Certificaathouder/Certificaatbeheerder is voorafgaand aan acceptatie van het certificaat gehouden de in het Certificaat opgenomen gegevens te controleren op juistheid. Indien het Certificaat niet geheel accuraat blijkt te zijn, dan dient de Certificaathouder/Certificaatbeheerder per omgaande een verzoek tot intrekking te doen. Bij acceptatie van het Certificaat bevestigt de abonnee of Certificaathouder ontvangst van het Certificaat middels een handtekening op de ontvangstbevestiging.

4.5 Sleutelpaar en Certificaatgebruik

4.5.1 Verplichtingen van de Certificaathouder

Binnen PKIoverheid mag een Certificaathouder de private sleutel en corresponderende publieke sleutel in het Certificaat alleen gebruiken voor het daartoe bestemde gebruik. De Certificaathouder accepteert de Certificaathouderovereenkomst met het accepteren van het Certificaat en stemt, door acceptatie van het Certificaat, onvoorwaardelijk in het Certificaat te gebruiken op een manier die overeenkomt met de Key-Usage field extensions die zijn opgenomen in het Certificaatprofiel.

4.5.2 Verplichtingen van Vertrouwende partijen

De vertrouwende partij is verplicht de geldigheid te controleren van de volledige keten van Certificaten tot aan het stamcertificaat waarop wordt vertrouwd.
Verder dient de vertrouwende partij zeker te stellen:

- Dat het certificaat conform het daarvoor bedoelde gebruik wordt gebruikt;
- Dat het Certificaat overeenkomstig enige Key-Usage field extensions wordt gebruikt;
- Dat het Certificaat geldig is op het moment dat er op wordt vertrouwd door het raadplegen van de certificaat status informatie in de CRL of via het OCSP-protocol.

4.6 Certificaatvernieuwing

Certificaatvernieuwing zonder verandering van de publieke sleutel die in het Certificaat is opgenomen wordt onder dit CPS niet door QuoVadis ondersteund. Een nieuw Certificaat is altijd gebaseerd op een nieuw sleutelpaar.

4.7 Certificaat Re-key

Voorafgaand aan het verstrijken van de geldigheidsduur van certificaten, wordt de Certificaathouder hiervan in kennis gesteld en dienen nieuwe Certificaten te worden uitgegeven conform de procedure voor een in initiële uitgifte.

4.8 Aanpassing

Noodzakelijke aanpassingen in de inhoud van een Certificaat, leidt tot de uitgifte van een nieuw certificaat conform de procedure voor een in initiële uitgifte.

4.9 Intrekking en opschorting van Certificaten

De intrekking van een certificaat zorgt ervoor dat dit ongeldig wordt verklaard en dat deze status wordt opgenomen in de certificaat status informatie. Een eenmaal ingetrokken Certificaat kan daarna niet meer de status ‘geldig’ krijgen.

4.9.1 Omstandigheden die leiden tot intrekking

Certificaten zullen worden ingetrokken indien de informatie in het Certificaat verandert of veroudert of wanneer de private sleutel die met het certificaat correspondeert, is gecompromitteerd of vermoedelijk gecompromitteerd is. Het certificaat wordt ingetrokken in de volgende gevallen:

- Wanneer de private sleutel behorende bij het certificaat is aangetast. Een sleutel wordt als aangetast beschouwd in geval van ongeautoriseerde toegang of vermoede ongeautoriseerde toegang tot private sleutel, verloren of vermoedelijk verloren private sleutel of SSCD, gestolen of vermoedelijk gestolen sleutel of SSCD of vernietigde sleutel of SSCD;
- Er is incorrecte informatie opgenomen in het Certificaat; Het Certificaat is niet uitgegeven overeenkomstig de bepalingen uit dit CPS of de Certificaathouder heeft inaccurate, onware of misleidende informatie verstrekt;
- Verandering van de naam van de certificaathouder;
- De Certificaathouder is niet meer geautoriseerd is om te handelen uit naam van de organisatorische entiteit van de abonnee, bijvoorbeeld ingeval van beëindiging of schorsing van het dienstverband of beroepsuitoefening;
- Er is een verandering opgetreden in de relatie tussen de abonnee en de Certificaathouder;
- Overlijden van de certificaathouder,
- Schending van contractuele verplichtingen, inclusief de verplichtingen die voortvloeien uit dit CPS;
- Beëindiging van de organisatorische entiteit;
- Wanneer de private sleutel behorende bij het certificaa is gebruikt om spyware, Trojans, virussen, rootkits, browser hijackers te ondertekenen, publiceren of verspreiden of

andere inhoud, voor phising, of gedrag dat schadelijk, kwaadwillig, vijandig is of om kwaadwillige inhoud op het systeem van een gebruiker zonder diens toestemming te downloaden;
- Compromittering van de QuoVadis CSP-CA;

De reden van intrekking wordt door QuoVadis vastgelegd.

4.9.2 Wie mag een verzoek tot intrekking doen

De volgende partijen mogen een verzoek tot intrekking doen:
- De Certificaathouder
- De Abonnee
- QuoVadis als CSP

4.9.3 Procedure voor een verzoek tot intrekking

QuoVadis zal een certificaat intrekken na ontvangst van een geldig verzoek daartoe. Een intrekkingverzoek moet onmiddellijk aan QuoVadis worden doorgegeven nadat een omstandigheid zoals hierboven genoemd in onder 4.9.1 zich voordoet.

De abonnee of de Certificaathouder kan zich persoonlijk wenden tot de Registration Authority, kan een intrekkingverzoek telefonisch indienen via de QuoVadis supportlijn of kan dit indienen via de QuoVadis website. De abonnee en de Certificaathouder kunnen hierbij worden gevraagd zich te authenticeren, op een wijze zoals gespecificeerd in par. 3.4.

De online intrekkingsfaciliteit via de QuoVadis website is 24 uur per dag en 7 dagen per week beschikbaar. De QuoVadis supportlijn is eveneens buiten kantooruren beschikbaar. De Registration Authority ten kantore van QuoVadis is uitsluitend tijdens kantooruren beschikbaar.
In het geval van systeemdefecten, service-activiteiten, of andere factoren die buiten het bereik van QuoVadis liggen, zal QuoVadis al het mogelijke doen om te zorgen dat de onbeschikbaarheid van de intrekkingsfaciliteit niet langer dan vier (4) uur zal duren. Ingeval van onbeschikbaarheid heeft de Registration Authority de mogelijkheid via een noodprocedure direct op de QuoVadis CSP-CA omgeving een certificaat laten intrekken.

4.9.4 Urgentie indienen intrekkingsverzoek

Een intrekkingsverzoek dient onmiddellijk na het intreden van de omstandigheden genoemd in 4.9.1 worden ingediend.

4.9.5 Tijdsduur waarbinnen QuoVadis het intrekkingverzoek moet hebben verwerkt

Binnen vier uur na ontvangst van een Intrekkingsverzoek door QuoVadis wordt het certificaat ingetrokken en wordt het Certificaat met de status “ingetrokken” in de certificaat statusinformatie opgenomen. Ingetrokken certificaten blijven in elk geval in de certificaat status informatie opgenomen zolang de geldigheid van het certificaat niet is verstreken.

4.9.6 Controle Certificaat status door vertrouwende partijen

Vertrouwende partijen dienen de status van het Certificaat te controleren voordat zij er op vertrouwen. De Certificaat status informatie wordt aangeboden middels het publiceren van de Certificate Revocation List (CRL) en via het Online Certificate Status Protocol (OCSP).

4.9.7 Frequentie uitgifte Certificate Revocation List (CRL)

De standaard interval voor het uitgeven van een nieuwe CRL is gesteld op 12 uur.
Na intrekking van een Certificaat wordt onmiddellijk een nieuwe CRL uitgegeven. De CRL wordt gepubliceerd in de elektronische opslagplaats en is en 24 uur per dag, 7 dagen per week beschikbaar. In het geval van systeemdefecten, service-activiteiten, of andere factoren die buiten het bereik van QuoVadis liggen, zal QuoVadis al het mogelijke doen om te zorgen dat de onbeschikbaarheid van de revocation status services niet langer dan vier (4) uur zal duren.

4.9.8 Maximale vertraging uitgifte Certificate Revocation List

De CRL wordt onmiddellijk na generatie uitgegeven en gepubliceerd.

4.9.9 Online intrekkings-/statuscontrole beschikbaarheid

QuoVadis biedt naast de raadplegiong van CRL de mogelijkheid de certificaat status te controleren via het Online Certificate Status Protocol (OCSP).

4.9.10 Vereiste On-line intrekkingscontrole

De geldigheid van een PKIoverheid certificaat moet door een vertrouwende partij online gecontroleerd worden, gebruik makend van de CRL of van het Online Certificate Status Protocol. OCSP is ingericht conform RFC 2560.
OSCP-responses worden digitaal ondertekend door de private sleutel van de QuoVadis CSP-CA , ofwel door een door de QuoVadis gehanteerde OCSP-responder die beschikt over een OCSP-Signing Certificaat dat voor dit doel is uitgegeven door de QuoVadis CSP-CA.
QuoVadis maakt bij OCSP geen gebruik van zogenaamde precomputed responses.
Voor de informatie op het OCSP gelden dezelfde standaarden voor actualiteit en betrouwbaarheid als voor de CRL, zoals in dit CPS beschreven

Certificaat status informatie is bovendien ten minste 6 maanden beschikbaar na het tijdstip waarop de geldigheid van het Certificaat is verlopen of, indien dat tijdstip eerder valt, na het tijdstip waarop de geldigheid door intrekking is beëindigd.

4.9.11 Schorsing van certificaten

QuoVadis ondersteunt bij haar dienstverlening binnen de PKI voor de overheid geen opschorting of schorsing van certificaten.

4.10 Certificate Status Service

De status van certificaten, uitgegeven Binnen PKIoverheid, is gepubliceerd in een Certificate Revocation List of wordt beschikbaar gesteld door middel van het Online Certificate Status Protocol.

4.11 Beëindiging van dienstverlening aan abonnee

De beëindiging van de dienstverlening aan de abonnee gebeurt overeenkomstig hetgeen daarover bepaald is in de overeenkomst tussen QuoVadis en abonnee. Dit kan leiden tot intrekking van de certificaten van certificaathouders die binnen de organisatorische entiteit van de abonnee zijn uitgegeven.

4.12 Key Escrow en key recovery

QuoVadis geeft haar CSP-CA sleutels niet in escrow uit bij een onafhankelijke derde. Key recovery diensten voor het terug halen van private decryptiesleutels van eindgebruikers worden door QuoVadis onder dit CPS niet aangeboden.

5 Fysieke, procedurele en personele beveiliging

5.1 Fysieke beveiliging

QuoVadis beheert en implementeert op passende wijze de fysieke beveiligingsmaatregelen om toegang tot de hardware en software, gebruikt voor de CA-operaties, te beperken.

5.1.1 Vestigingslocatie operationele CA-dienstverlening

QuoVadis voert haar operationele CA-diensten uit vanaf een beveiligd datacenter, gevestigd in een gebouwencomplex te Bermuda. Dit datacentrum houdt zich aan de strikte regels en hoge beveiligingsstandaarden opgesteld door een onafhankelijk gecertificeerde partij. Toepasselijke normen en standaarden voor de beveiligingsvoorzieningen omvatten onder andere maatregelen tegen:

- brand (volgens DIN 4102 F90 standaard) met een automatisch FM200 blussysteem;
- rook en vochtigheid (volgens DIN 18095 standaard);
- overval en vandalisme (ET2 volgens DIN 18103 standaard);
- elektromagnetische invloeden en straling (zoals een elektromagnetische puls).

QuoVadis beschikt over een gecertificeerde BS-EN 1047 toepassing en een ISO9000/1/2 aansprakelijkheidsverzekering.

5.1.2 Fysieke toegang

QuoVadis staat fysieke toegang tot haar beveiligde operationele omgeving enkel toe aan daartoe bevoegde personen. De fysieke verplaatsingen van personen binnen de beveiligde omgeving worden opgeslagen in een log-file en worden periodiek geëvalueerd. Fysieke toegang tot de beveiligde omgeving wordt gecontroleerd door een combinatie van toegangspassen en biometrische identificatie.

5.1.3 Stroomvoorziening en Airconditioning

De beveiligde omgeving is aangesloten op de reguliere standaard energievoorziening. Alle kritieke componenten zijn verder aangesloten op een UPS-unit, teneinde tijdens de eventuele uitval van elektra ongecontroleerde onbeschikbaarheid van kritieke systemen te voorkomen.

5.1.4 Wateroverlast

Binnen de beveiligde omgeving zijn maatregelen getroffen tegen wateroverlast. De omgeving is gevestigd op een hoger gelegen etage met verhoogde vloeren. Ook zijn de muren afgedicht en houdt het de lokatie zich aan de veiligheidseisen neergelegd in DIN 18095.

5.1.5 Bescherming en preventie tegen brand

De beveiligde omgeving biedt bescherming tegen brand volgens de richtlijnen van DIN 4102 F9, door middel van een automatisch FM200 blussysteem.

5.1.6 Media opslag

Alle magnetische media die informatie betreffende de PKIoverheid-dienstverlening van QuoVadis, waaronder back-up files, worden opgeslagen in opslagvoorzieningen, kasten en brandvaste kluizen met bestendigheid tegen brand en elektromagnetische onderbreking (EMI). Deze bevinden zich in de beveiligde omgeving of op een beveiligde externe opslaglocatie.

5.1.7 Afval verwerking

Papieren documenten en magnetische media welke vertrouwelijke QuoVadis of commercieel gevoelige informatie bevatten, worden beveiligd vernietigd door middel van:

- In het geval van magnetische media:
  - Toebrengen van onherstelbare fysieke schade of gehele vernietiging van de betreffende informatiedrager;
  - Gebruik van een daarvoor geschikt apparaat voor het wissen of overschrijven van de informatie; en
- In het geval van gedrukte informatie, wordt het document versnipperd of vernietigd op een daarvoor geschikte wijze.

5.1.8 Externe back-up

Een externe locatie wordt gebruikt voor de opslag van back-up software en data. De externe locatie:

- is 24 uur per dag en 7 dagen per week beschikbaar voor geautoriseerd personeel, met als doel het terughalen van software en data;
- beschikt over adequate fysieke beveiligingsmaatregelen (software en data zijn bijvoorbeeld opgeslagen in vuurvaste kluizen de en opslag bevindt zich achter deuren met toegangscontrole, in omgevingen die alleen toegankelijk zijn voor daartoe geautoriseerd personeel).

5.2 Procedurele Beveiliging

QuoVadis waarborgt dat de procedures met betrekking tot fysieke en technische beveiliging worden nageleefd conform dit CPS en andere relevante interne operationele documenten. Het is bedrijfsbeleid dat QuoVadis geen PKI operaties delegeert naar andere organisaties.

5.2.1. Vertrouwelijke rollen

Om zeker te stellen dat een enkel persoon de beveiliging niet kan omzeilen, zijn de verantwoordelijkheden verdeeld over meerdere rollen en personen. Dit is onder andere bewerkstelligd door het creëren van separate rollen en accounts op de verschillende componenten van het CA-systeem, en elke rol heeft daarbij beperkte autorisaties. Toezicht kan alleen worden uitgevoerd door een persoon die niet direct betrokken is bij de uitgifte van certificaten (bijvoorbeeld een Security Officer die systeem records of audit logs bekijkt

om zeker te stellen dat andere personen handelen binnen hun verantwoordelijkheden en binnen het toepasselijke beveiligingsbeleid).

De toepasselijke rollen zijn:

- **Certification Authority Officers** die verantwoordelijk zijn voor CA hardware en software en de generatie en ondertekening van uitgifte CA sleutels.
- **Registration Authority Officers** die verantwoordelijk zijn voor het verrichten van functies van de Registration Authority en de interface met QuoVadis.
- **QuoVadis Chief Security Officer** die verantwoordelijk is voor het verifiëren van de integriteit van de QuoVadis CSP-CA en de configuratie en operations daarvan.
- **Auditor** die verantwoordelijk is voor het houden van toezicht en het geven van een onafhankelijk oordeel over de wijze waarop de bedrijfsprocessen zijn ingericht en over de wijze waarop aan de eisen ten aanzien van de betrouwbaarheid wordt voldaan.
- **Systeembeheerder** die verantwoordelijk is voor het beheer van de QuoVadis-systemen, inclusief het installeren, configureren en onderhouden van de systemen.

5.2.2. Aantal personen vereist per operationele handeling

Er zijn minstens twee personen toegewezen per vertrouwelijke rol om altijd adequate ondersteuning te waarborgen, met uitzondering van de Auditor rol. Sommige rollen zijn toegewezen aan verschillende personen om ervoor te zorgen dat er geen belangenverstrengelingen optreden en om de mogelijkheid tot abusievelijke of bewuste compromittering van enig component van de CA infrastructuur te voorkomen, met name de private sleutel van de QuoVadis CSP-CA.

CA-sleutelpaargeneratie en initialisatie vereist per geval de actieve participatie van ten minste twee Vertrouwelijke Rollen. Dergelijk gevoelige handelingen vereisen tevens de actieve participatie en toezicht van hoger management.

5.2.3. Identificatie en authentificatie voor elke rol

Elk individu dat een van de vertrouwelijke rollen vervult, gebruikt een door QuoVadis uitgegeven certificaat, opgeslagen op een SSCD, teneinde zichzelf voor operationele handelingen te identificeren aan de diverse systemen die gebruikt worden voor het uitgeven en beheren van PKIoverheid certificaten.

5.2.4. Rollen die scheiding van plichten vereisen

Verrichtingen die betrekking hebben op de Root Certificaat en uitgifte CA-rollen zijn gescheiden tussen M van N medewerkers, waarbij M gelijk is aan of groter dan 2 (een M-van-N persoonscontrole betekent dat er een minimum aanwezig is van “M” personen uit een totaal van “N” personen die geautoriseerd zijn de taak uit te voeren). De verwezenlijking en het behoud van de system audit logs zijn gescheiden van de personen die dergelijke systemen bedienen.

5.3 Personele Beveiliging

5.3.1. Kwalificaties, ervaring en screening

QuoVadis vereist dat personeel over de vereiste kwalificaties en relevante ervaring beschikt. De personen die de Vertrouwelijke Rollen vervullen moeten een toepasselijke beveiligingscreening procedure hebben ondergaan. De Vertrouwende Rollen in Nederland beschikken over een Verklaring omtrent het Gedrag van het ministerie van Justitie.

QuoVadis is niet aansprakelijk zijn voor gedrag van werknemers dat buiten de uitoefening van de functie ligt en waarover QuoVadis derhalve geen controle heeft, inclusief, maar niet beperkt tot (bedrijfs)spionage, sabotage, misdadig gedrag.

5.3.2. Procedures achtergrondcontrole

Procedures voor achtergrondcontrole bevatten, maar zijn niet beperkt tot, controle en bevestiging van:

- Werkervaring en professionele referenties
- Onderwijskwalificaties
- Verklaring omtrent het gedrag

5.3.3. Trainingsvereisten

QuoVadis biedt zijn personeel on-the-job en professionele training aan om geschikte en vereiste niveaus van competentie te onderhouden om de verantwoordelijkheden van de baan uit te voeren.

5.3.4. Trainingsfrequentie

QuoVadis biedt het personeel een programma van periodieke trainingen.

5.3.5. Sancties op ongeautoriseerde handelingen

Ongeautoriseerde handelingen van personeel kan resulteren in het opleggen van disciplinaire maatregelen door het Management van QuoVadis. De noodzaak tot het opleggen van maatregelen en de inhoud ervan wordt van geval tot geval vastgesteld door QuoVadis Management.

5.3.6. Documentatie verstrekt aan personeel

QuoVadis voorziet het personeel van alle benodigde handleidingen, procedurebeschrijvingen en trainingsmaterialen die nodig zijn om de functie en rol te kunnen vervullen.

5.3.7. Geheimhouding

QuoVadis zal al het mogelijke doen om te zorgen dat het personeel vertrouwelijke informatie vertrouwelijk behandelt. Het ondertekenen van een geheimhoudingsverklaring maakt deel uit van de aanstelling bij QuoVadis.

5.4 Procedures ten aanzien van logging

5.4.1 Vastleggen van gebeurtenissen

Alle gebeurtenissen betrokken bij de generatie van de CA sleutelparen worden vastgelegd en gelogd. Dit omvat onder andere alle gebruikte configuratiegegevens van dit proces.

De soorten data die door QuoVadis worden geregistreerd omvatten, maar zijn niet beperkt tot;

- Alle gegevens betrokken bij het registratieproces van elk individueel Certificaat zullen voor toekomstige verwijzing, indien nodig, worden geregistreerd.
- Alle gegevens en procedures betrokken bij de uitgifte en de verspreiding van Certificaten zullen worden geregistreerd.
- Alle gegevens relevant voor de publicatie van de Certificaten en certificaat status informatie zullen worden geregistreerd.
- Alle intrekkingsdetails van een Certificaat worden opgeslagen, waaronder ook de reden van intrekking.
- Het beheer van de beveiligde technische levenscyclus van het certificaat en de hardware wordt geregistreerd.
- Loggingbestanden, die al het netwerkverkeer van en naar Betrouwbare Systemen registreren, worden opgeslagen en gecontroleerd.
- Alle configuratiegegevens van de back-up locatie worden geregistreerd. Alle procedures betrokken bij het back-upproces worden geregistreerd.
- Van alle opgeslagen data, zoals hierboven genoemd, wordt een back-up gemaakt. Daarom zullen er twee exemplaren van al het verslag/controlemateriaal zijn, die op afzonderlijke locaties, tegen rampenscenario's beschermd, worden opgeslagen.
- Alle activiteiten ten aanzien van de installatie van nieuwe of bijgewerkte software.
- Alle activiteiten ten aanzien van hardware updates.
- Alle activiteiten ten aanzien van shutdowns en restarts.
- Tijd en datum van log dumps.
- Tijd en datum van de dump van transactiearchieven.
- Veranderingen van het beveiligingsprofiel.

Alle loggings zullen van een time-stamp worden voorzien en de integriteit van de logbestanden is gewaarborgd.

5.4.2 Frequentie van verificatie audit logs

De audit logs worden minstens maandelijks geverifieerd en geconsolideerd.

5.4.3 Bewaartermijn van audit logs

De audit logs worden bewaard voor een periode van niet minder dan elf (11) jaar. Verder worden de audit logs opgeslagen voor een periode van minstens elf (11) jaar, gerekend vanaf het moment dat QuoVadis haar verrichtingen als CSP beëindigt.

5.4.4 Beveiliging van audit logs

De relevante verzamelde loggings worden regelmatig geanalyseerd op pogingen om de integriteit van enig onderdeel van de PKIoverheid dienstverlening in gevaar te brengen.

Uitsluitend CA officers en auditoren mogen de volledige audit logs inzien. QuoVadis besluit of de specifieke audit logs in bepaalde situaties ook door anderen moeten worden bekeken en stelt die loggings vervolgens ter beschikking. Geconsolideerde logs zijn beschermd tegen modificatie of vernietiging.

Alle audit logs zijn beveiligd middels een versleuteling in de vorm van een sleutel en certificaat, welke speciaal is gegenereerd met als doel de loggings te beveiligen.

5.4.5 Controlelogboek back-up procedures

De QuoVadis CSP-CA voert dagelijks een on-site back-up uit van de audit logs. Het back-up proces omvat wekelijkse fysieke verwijdering van de kopie van de audit logs van de QuoVadis-locatie en opslag naar een beveiligde externe locatie.

De back-up procedures gelden voor de PKIoverheid omgeving, inclusief de QuoVadis CSP-CA en de Registration Authority-omgeving.

5.4.6 Audit Logging

Het beveiligde logproces van de QuoVadis CSP-CA verloopt geheel onafhankelijk van de software van QuoVadis. De beveiligde logprocessen worden geactiveerd bij het opstarten van het systeem en beëindigd bij de shut-down ervan.

5.4.7 Berichtgeving inzake logging

Wanneer een gebeurtenis wordt gelogd, hoeft daarvan geen kennisgeving plaats te vinden aan de persoon, de organisatorische entiteit, het apparaat of de applicatie die deze gebeurtenis heeft uitgevoerd of veroorzaakt.

5.4.8 Beoordeling van de kwetsbaarheid

Zowel de beoordelingen van de baseline als constante dreigingen en risicovolle kwetsbaarheden worden uitgevoerd op alle onderdelen van de QuoVadis CSP-CA omgeving, met inbegrip van het materiaal, de fysieke plaats, de documenten, de gegevens, de software, het personeel, de administratieve processen en de mededelingen.

5.5 Archivering van documenten

5.5.1. Aard van gearchiveerde gegevens

QuoVadis archiveert documentatie conform haar beleid inzake document toegangscontrole en maakt deze pas toegankelijk na een geautoriseerde aanvraag.
Voor elk certificaat bevat het archief de informatie gerelateerd aan activiteiten omtrent de creatie, de uitgifte, het gebruik, de intrekking, de geldigheidsduur en de vernieuwing. Dit dossier met documentatie bevat al het relevante bewijsmateriaal, waaronder:

- Audit logs;

- Certificaataanvragen en alle daaraan gerelateerde handelingen en formulieren;
- Inhoud van uitgegeven Certificaten;
- Bewijs van Certificaatacceptatie en ondertekende overeenkomsten
- Intrekkingsverzoeken en alle gerelateerde handelingen en vastleggingen;
- Gepubliceerde intrekkingslijsten van certificaten;
- Auditbevindingen zoals besproken binnen dit CPS.

5.5.2. Bewaarperiode voor het archief

De archieven van QuoVadis worden bewaard en beschermd tegen modificatie of vernietiging voor een periode van 11 (elf) jaar.

5.5.3 Bescherming van het archief

De archieven worden adequaat beschermd tegen modificatie of vernietiging. De toegang tot het archief is beperkt. Uitsluitend CA Officers, de QuoVadis Chief Security Officer en Auditoren mogen het gehele archief inzien. De inhoud van de archieven zal niet in zijn geheel worden vrijgegeven, behalve wanneer dit vereist is op grond van wetgeving of op last van een rechterlijk bevel of van een andere juridisch bevoegde instantie.

5.5.4 Back-up procedures m.b.t. het archief

QuoVadis handhaaft en implementeert back-up procedures zodanig dat, in het geval van het verlies of de vernietiging van de primaire archieven, per direct een volledige reeks reserve-exemplaren beschikbaar is.

5.5.5 Eisen voor de time-stamping van gegevens

QuoVadis ondersteunt time-stamping voor al haar gegevens. Alle gelogde gebeurtenissen die binnen de dienstverlening van QuoVadis worden vastgelegd omvatten de datum en het tijdstip van het moment waarop de gebeurtenis plaatsvond. Deze datum en tijd zijn gebaseerd op de systeemtijd waarop het QuoVadis CSP-CA systeem werkt. QuoVadis gebruikt procedures om te waarborgen dat alle systemen die binnen de PKIoverheid omgeving operationeel zijn, vertrouwen op een betrouwbare tijdbron.

5.5.6 Archiveringssysteem

Het archiveringssysteem van QuoVadis wordt uitsluitend gebruikt als een intern systeem binnen QuoVadis.

5.5.7 Procedures om de archiefinformatie te verkrijgen en te verifiëren

Uitsluitend CA Officers, de QuoVadis Chief Security Officer en Auditoren mogen het gehele archief inzien. De inhoud van de archieven zal niet in zijn geheel worden vrijgegeven, behalve wanneer dit vereist is op grond van wetgeving of op last van een rechterlijk bevel of van een andere juridisch bevoegde instantie. QuoVadis kan beslissen loggings van individuele transacties vrij te geven, wanneer de abonnee of diens vertegenwoordigers hierom vragen. Een redelijke tegemoetkoming in de administratieve kosten per verzoek wordt hiervoor in rekening gebracht.

5.6 Wijziging van de publieke sleutel

De wijziging van de publieke sleutel van de CA gebeurt aan de hand van een daarvoor opgestelde procedure. Tegen het eind van de levensduur van de CA private sleutel, stopt QuoVadis het gebruik van deze private sleutel voor het ondertekenen van publieke sleutels en gebruikt de expirerende private sleutel uitsluitend nog om CRLs en OSCP-responder Certificaten, verbonden met die private sleutel, te ondertekenen.
Er wordt een nieuw CA signing sleutelpaar uitgegeven en vervolgens worden alle vanaf dat moment uitgegeven Certificaten en CRL's ondertekend met de nieuwe private sleutel. Dit betekent dat zowel oude als nieuwe CA sleutelparen gelijktijdig actief kunnen zijn.

5.7 Aantasting en Continuïteit

QuoVadis heeft een "Disaster Recovery Programma", vastgelegd in het QuoVadis Calamiteitenplan. Het doel van dit plan is om kernactiviteiten van het bedrijf zo snel mogelijk te herstellen wanneer systemen of handelingen zijn aangetast door brand, stakingen etc.

QuoVadis heeft verder een Bedrijfscontinuïteitsplan, dat de directe voortzetting van de specifieke diensten met betrekking tot de intrekking van certificaten mogelijk maakt ingeval zich een onverwachte noodsituatie heeft voorgedaan. Het QuoVadis Bedrijfscontinuïteitsplan als een intern vertrouwelijk document dat niet geschikt is voor externe distributie.
Het QuoVadis bedrijfscontinuïteitsplan beschrijft onder andere:

- Te volgen Procedures bij incidenten en compromittering.
- Te volgen Procedures voor gegevensverwerking, software, en/of corrupte data.
- Te volgen Procedures voor de compromittering van de CA private sleutel
- Te volgen Procedures voor de intrekking van de publieke sleutel van de CA.
- Mogelijkheden en procedures voor bedrijfscontinuïteit na een Ramp.

QuoVadis heeft verder een plan inzake sleutelcompromittering ("Key Compromise Plan") waarin gedetailleerd wordt beschreven welke activiteiten plaats dienen te vinden ingeval van compromittering van de QuoVadis CA private sleutel. Dit plan bevat procedures voor:

- Intrekking van alle certificaten die zijn ondertekend met de desbetreffende QuoVadis CA private sleutel; en
- Het onmiddellijk op de hoogte brengen van de abonnees, en alle certificaathouders wiens certificaten door de betreffende QuoVadis CSP-CA zijn uitgegeven.

Bij een calamiteit wordt verder de Policy Authority PKIoverheid onmiddellijk op de hoogte gesteld en wordt deze gedurende het verloop van de calamiteit op de hoogte gehouden. QuoVadis informeert de Policy Authority PKIoverheid actief over risico's, gevaren of gebeurtenissen die op enigerlei wijze de betrouwbaarheid van de dienstverlening en/of het imago van de PKI voor de Overheid kunnen bedreigen of beïnvloeden.

5.8 Beëindiging van de dienstverlening van de CA en/of RA

Wanneer QuoVadis genoodzaakt is de dienstverlening te beëindigen, dan zullen de negatieve gevolgen van deze beëindiging tot een minimum worden beperkt.

QuoVadis specificeert de procedures die worden gevolgd bij het beëindigen van het leveren van certificaatdiensten. De procedures moeten minimaal tot doel hebben:

- dat iedere vorm van onderbreking, veroorzaakt door de beëindiging van de QuoVadis certificatiedienstverlening, tot een minimum is beperkt.
- dat gearchiveerde documenten van QuoVadis worden behouden.
- dat er onmiddellijke berichtgeving wordt verstrekt aan abonnees, Certificaathouders, vertrouwende partijen en andere relevante partijen binnen de PKI voor de overheid.
- dat het intrekkingproces van alle certificaten die zijn uitgegeven door QuoVadis, ten tijde van beëindiging operationeel blijft.
- Relevante overheidsinstanties, waaronder de PA PKIoverheid, in het kader van toepasselijke wet- en regelgeving, op de hoogte te stellen.

Indien mogelijk wordt de intrekking van certificaten gepland in samenhang met de geplande uitgifte van nieuwe certificaten door een CSP die de activiteiten van QuoVadis binnen de PKI voor de overheid overneemt.

Indien mogelijk dient de CSP die de activiteiten van QuoVadis binnen de PKI voor de overheid overneemt gelijksoortige procedures, richtlijnen en verplichtingen te hanteren als die QuoVadis hanteerde. De CSP die de activiteiten van QuoVadis binnen de PKI voor de overheid overneemt dient verder certificaten uit te geven aan alle Certificaathouders wiens certificaten zijn ingetrokken. Dit kan met zich meebrengen dat de abonnee en de Certificaathouders zich in de opvolgende situatie zich dienen te conformeren aan de procedures en vereisten van de nieuwe CSP. De nieuwe CSP draagt in elk geval zorg voor het gedurende zes maanden beschikbaar stellen van de certificaat status informatie, het operationeel houden van de revocatie management dienst (intrekkingsfaciliteit) en het bewaren van de gearchiveerde documenten inzake registratie.

6 Technische beveiligingsmaatregelen

6.1 Generatie en installatie van het sleutelpaar

6.1.1 Sleutelpaar generatie

De sleutel van de QuoVadis CSP-CA is gegenereerd en opgeslagen binnen een cryptografische module die minimaal voldoet aan de standaarden FIPS 140-2 level 3 en/of Common Criteria EAL4 AUGMENTED (EAL4+). De sleutels voor de autoriserende Registratie Officers worden gegenereerd op een Signature Creation Device (SSCD), een veilig middel voor het genereren van een elektronische handtekening.
Het sleutelmateriaal voor Certificaten voor Personen worden gegenereerd op een SSCD in het bijzijn van de Certificaathouder. De Certificaathouder is verantwoordelijk voor het beveiligen van het SSCD met een Persoonlijk Identificatie Nummer rechtstreeks op het SSCD.
Het sleutelmateriaal voor Systeemcertificaten wordt gegenereerd door de Certificaatbeheerder.

6.1.2 Levering van de private sleutel aan de certificaathouder

De private sleutel die op een SSCD gegenereerd is, blijft te allen tijde in de met een PIN beveiligde omgeving op het SSCD opgeslagen. Dit is het geval voor de Certificaten voor Personen en voor de Systeemcertificaten voor authenticatie en vertrouwelijkheid. De Certificaathouder bevestigt na levering de ontvangst van het SSCD met het sleutelmateriaal aan de RA.
De private sleutel die door de Certificaatbeheerder wordt gegenereerd ten behoeve van een SSL-certificaat wordt door middel van een beschermde gegevensstructuur opgeslagen (zoals bepaald in PKCS#12). Het met een wachtwoord beveiligde bestand mag naar keuze op een beperkt aantal opslagmedia worden opgeslagen, te weten: een smartcard, een HSM of in software. Ingeval de private sleutel in software wordt opgeslagen dan wordt met de abonnee en Certificaatbeheerder expliciet overeen gekomen dat er aanvullende, compenserende maatregelen dienen te worden getroffen in de omgeving waar de private sleutel wordt gebruikt.

6.1.3 Levering van een publieke sleutel aan de CSP

Publieke sleutels voor Certificaten voor Personen en voor Systeemcertificaten die binnen een SSCD worden gegenereerd worden door middel van een PKCS#10 request ter certificatie aangeboden aan de QuoVadis CSP-CA. Publieke sleutels voor Systeemcertificaten (SSL) die niet binnen de SSCD, maar op lokatie worden gegenereerd, moeten worden aangeleverd op een veilige en betrouwbare manier, zoals door middel van een Certificate Signing Request (CSR).

6.1.4 Distributie CA publieke sleutel aan vertrouwde partijen

De publieke sleutels van de QuoVadis CSP-CA binnen de PKI voor de overheid, alsmede de Domein CA en de Root CA van de Staat der Nederlanden worden op de SSCD vastgelegd. De Root CA van de Staat der Nederlanden is als stamcertificaat van de PKI voor de Overheid opgenomen in de populaire browsers en/of in de besturingssystemen.

6.1.5 Sleutellengte

De QuoVadis CSP-CA maakt gebruik van een 4.096 bit sleutellengte op basis van sha256WithRSAEncryption.
De Certificaten voor Personen en de Systeemcertificaten maken gebruik van 2,048 bits sleutels op basis van sha256WithRSAEncryption
Voor de overige informatie over de uitgegeven certificaten verwijzen wij naar de certificaatprofielen, die zijn opgenomen in hoofdstuk 7 van dit CPS.

6.1.6 Publieke sleutel parameter generatie en kwaliteitscontrole

Voor certificaathouders: De kwaliteit van de parameters, welke wordt gebruikt voor de aanmaak van publieke sleutels, wordt bepaald door de gebruikte SSCD en door de gebruikte programmatuur van de Certificaathouder.

Voor de QuoVadis CSP-CA: Alle hardwareplatformen voldoen aan de eisen van FIPS 186-2, welke waarborgen biedt voor de juiste parameters en hun kwaliteit (bijvoorbeeld inzake *random key generation en primaliteit*).

6.1.7 Doeleinden voor sleutel gebruik (Vanaf X.509 V3 sleutel gebruiksvelden)

Sleutels mogen uitsluitend worden gebruikt voor doeleinden zoals beschreven in dit CPS – zie H7 inzake Certificaatprofielen. De QuoVadis CSP-CA private sleutel mag uitsluitend worden gebruikt voor het ondertekenen van publieke sleutels (certificaten) en CRLs/OCSP responses.

6.2 Private sleutel bescherming

6.2.1 Standaarden en controles van de cryptografische module (HSM)

De private sleutels van QuoVadis CSP-CA zijn gegenereerd en opgeslagen in een cryptografische module welke voldoet aan de die ten minste voldoet aan de FIPS 140-2 level 3 en/of EAL 4 beveiligingsstandaarden.
De HSM-modules worden altijd opgeslagen in een beveiligde omgeving en zijn onderhevig aan strikte beveiligingsprocedures gedurende de gehele levenscyclus.

6.2.2 Private key (N out of M) “Multi-person” controle

Toegang tot de HSM’s is beperkt tot personen in Vertrouwende Rollen en geschiedt op basis van hiertoe geprepareerde smartcards met een bijhorende passphrase. Deze smartcards en passphrases zijn toegewezen aan meerdere personen in Vertrouwende Rollen. Dergelijke vereiste aanwezigheid van meerdere personen alvorens toegang te verkrijgen (“N out of M” multi-person control) zorgt ervoor dat niet één enkel persoon de totale controle kan voeren over een kritiek component binnen de infrastructuur.

6.2.3 Escrow van de private sleutel

QuoVadis geeft haar CSP-CA sleutels niet in escrow uit bij een onafhankelijke derde.

6.2.4 Private sleutel back-up

De Private Sleutel wordt in versleutelde staat gebackupt, on-site onderhouden en daarnaast in een beveiligde off-site lokatie bewaard.
Private sleutels van Certificaathouders worden door QuoVadis niet gebackupt. Het is niet toegestaan een backup te maken van de private sleutel voor de elektronische handtekening.

6.2.5 Archivering van de private sleutel

QuoVadis archiveert in geen geval private sleutels van Certificaathouders.
QuoVadis biedt geen diensten aan voor het bewaren en terughalen van private decryptiesleutels (key recovery voor vertrouwelijkheidsleutels). Het is niet toegestaan de private sleutel voor de elektronische handtekening te archiveren.

6.2.6 Toegang tot private sleutels in cryptografische module

De sleutels van de QuoVadis CSP-CA worden opgeslagen in een HSM (zie 6.2.1). Ze worden daarbinnen opgeslagen in versleutelde staat (waarbij gebruik wordt gemaakt van een encryptie sleutel om een “cryptografische verpakking” te maken voor de sleutel). De private sleutels mogen nooit in plaintext vorm bestaan buiten de cryptografische module. Wanneer de private sleutel moet worden getransporteerd tussen twee cryptografische modules, moet deze gedecodeerd worden overgebracht van de ene naar de andere module, onder strikte beveiligingsmaatregelen. Toegang tot het sleutelmateriaal is uitsluitend door aanwezigheid van meerdere personen in Vertrouwende Rollen te verkrijgen, zoals beschreven in 6.2.2.

6.2.7 Private sleutelopslag op een cryptografische module

De private sleutels die op een cryptografische module zijn opgeslagen zijn beveiligd gedurende hun gehele levenscyclus.

6.2.8 Activeringsmethoden voor een private sleutel

De activering van de private sleutels van de QuoVadis CSP-CA is beschreven in 6.2.2. De private sleutels van de Certificaathouders worden geactiveerd door middel van een PIN-code.

6.2.9 Methoden voor deactivatie van de private sleutel

De Private sleutel van de operationele QuoVadis CSP-CA wordt normaliter niet gedeactiveerd, maar blijft in productie in de beveiligde omgeving. Overige cryptografische modules woorden na gebruik gedeactiveerd, bijvoorbeeld, door middel van een handmatige logout procedure of een passieve time-out. Cryptografische Modules die niet in gebruik zijn worden verwijderd en opgeslagen.

6.2.10 Methode voor de vernietiging van de private sleutel

Private sleutels worden vernietigd wanneer zij niet meer nodig zijn, of wanneer de Certificaten waarmee zij corresponderen zijn verlopen of ingetrokken.
Alle Certificaathouders/Certificaatbeheerders hebben de verplichting om hun private sleutels tegen misbruik te beschermen. Private sleutels worden vernietigd op een wijze die verlies, diefstal, wijziging, onbevoegde onthulling of onbevoegd gebruik voorkomt.

Wanneer de geldigheidsduur van een sleutelpaar afloopt, of in andere gevallen waarin vernietiging vereist is, zal het daartoe geautoriseerde personeel van QuoVadis de private sleutel vernietigen (bijvoorbeeld door re-initialisering of zeroization van de Cryptografische Module of door fysieke beschadiging toe te brengen (b.v., met een metaalontvezelmachine of een hamer). Dergelijke vernietiging wordt altijd gedocumenteerd.

6.2.11 Cryptografische classificatie van de module en SSCD's

De cryptografische modules die door de QuoVadis CSP-CA worden gebruikt, zijn gecertificeerd op basis van de standaard FIPS 140-2 level-3 en/of Common Criteria EAL 4.

De veilige middelen die QuoVadis verschaft aan Certificaathouders voor het aanmaken van elektronische handtekeningen (de SSCD, zowel de processor als het operating system), zijn gecertificeerd op basis van de standaard FIPS 140-2 level 3 (wat gelijkwaardig is aan certificatie op basis van Common Criteria EAL4+ (AUGMENTED).

6.3 Overige aspecten van sleutelpaar management

6.3.1 Archivering van het publieke sleutelpaar

De publieke sleutels in certificaten zullen worden geregistreerd en worden gearchiveerd in de elektronische opslagplaats. De sleutels blijven in het archief voor de duur van ten minste 11 jaar gerekend vanaf het verstrijken van de geldigheid ervan. Er wordt geen afzonderlijk archief van publieke sleutels onderhouden.

6.3.2 Gebruiksduur van sleutels en certificaten

Gebruiksperiodes voor de publieke- en private sleutels zijn gelijk aan de gebruiksperiode van het Certificaat welke de publieke sleutel verbindt aan een Certificaathouder.
De maximum geldigheidsperiodes voor certificaten binnen de PKI voor de overheid zijn als volgt:

- De geldigheid van de QuoVadis CSP-CA eindigt op 23-03-2020.
- De geldigheidsduur van de PKIoverheid certificaten voor Personen en Systemen is naar keuze: 1, 2 of 3 jaar. Dit wordt aangegeven op het aanvraagformulier.

Op het moment van uitgifte van het eindgebruikercertificaat is de resterende geldigheidsduur van de QuoVadis CSP-CA altijd langer dan de gespecificeerde geldigheidsduur van het certificaat voor de Certificaathouder.

6.4 Activeringsgegevens

6.4.1 Activatiedata - generatie en installatie

Een unieke persoonlijke identificatiecode (PIN) wordt gegenereerd tijdens het initialiseren van de SSCD teneinde de private sleutel te beschermen.

6.4.2 Activatiedata bescherming

Activeringsgegevens worden bij tijdens de registratieprocedure aangemaakt in het bijzijn van de Certificaathouder of op beveiligde wijze worden gegenereerd en (altijd gescheiden van het SSCD) verzonden.

Activeringsgegevens worden door de Certificaathouder/Certificaatbeheerder altijd geheim gehouden. Activeringsgegevens voor Certificaten voor Personen zijn strikt persoonlijk en mogen niet worden gedeeld. Met inachtneming van adequate procedurele maatregelen mogen de activeringsgegevens voor Systeemcertificaten worden gedeeld. Een voorbeeld van een adequate procedurele maatregel is bijvoorbeeld het opslaan van de activeringsgegevens in een enveloppe in een afgesloten kluis.

6.5 Computerbeveiliging

6.5.1 Technische maatregelen inzake computerbeveiliging

QuoVadis hanteert en onderhoudt een informatiebeveiligingsbeleid waarin wordt gedocumenteerd wat het QuoVadis beleid, de normen en de richtlijnen met betrekking tot informatiebeveiliging zijn. Dit beleid is goedgekeurd door het QuoVadis management en medegedeeld aan alle werknemers.

Technische maatregelen inzake computerbeveiliging omvatten ondermeer, maar zijn niet beperkt tot:

- Toegangscontrole tot de CA diensten en PKI rolverdeling, zie 5.1
- Gedwongen scheidingen van de autorisaties en rollen, zie 5.2
- De identificatie en de authentificatieprocedures van personeel dat in Vertrouwelijke Rollen opereert, zie Sectie 5.3
- Het gebruik van cryptografie voor sessiecommunicatie en database beveiliging, wederzijdse authenticatie en versleuteling door middel van SSL/TLS wordt gebruikt voor alle communicatie
- Archivering van de audit logs, zie 5.4 en 5.6
- Gebruik van x.509 certificaten voor alle administrators

6.5.2 Classificatie van de computerbeveiliging

De classificatie van de QuoVadis computerveiligheid is uitgewerkt in het informatiebeveiligingsbeleid en wordt bereikt door real-time monitoring en analyse, maandelijkse beveiligingscontrole door de QuoVadis Chief Security Officer en jaarlijkse beveiligingscontroles door externe auditoren.

6.6 Beheersmaatregelen technische levenscyclus

6.6.1 Beheersmaatregelen ten behoeve van systeemontwikkeling

QuoVadis maakt gebruik van standaardproducten van erkende leveranciers die voldoen aan de beveiligingsclassificaties die vereist worden door in het Programma van Eisen PKIoverheid (zie 6.1 en 6.2).

QuoVadis volgt de Certificate Issuing and Management Components (CIMC) Family of Protection Profiles, welke de eisen bepaalt voor componenten die uitgeven, intrekken en publieke sleutel certificaten beheren, zoals X.509 publieke sleutel certificaten. CIMC is gebaseerd op de Criteria/ISO IS15408 normen.

Software die door QuoVadis is ontwikkeld en wordt ingezet voor gebruik in de dienstverlening binnen de PKI voor de overheid, wordt ontwikkeld in een gecontroleerde omgeving welke voldoet aan strikte veiligheidseisen. De software die binnen QuoVadis zelf is ontwikkeld en wordt ingezet binnen een van de PKI-kerndiensten, dient te voldoen aan de toepasselijke eisen voor betrouwbare systemen zoals opgenomen in CEN Workshop Agreement (CWA) 14167-1.

6.6.2 Beheersmaatregelen ten behoeve van beveiligingsontwikkeling

QuoVadis volgt de Certificate Issuing and Management Components (CIMC) Family of Protection Profiles, welke de eisen bepaalt voor componenten die uitgeven, intrekken en publieke sleutel certificaten beheren, zoals X.509 publieke sleutel certificaten. CIMC is gebaseerd op de Criteria/ISO IS15408 normen.

6.6.3 Beveiligingsmaatregelen van de levenscyclus

Alle hard- en software die ten behoeve van de QuoVadis dienstverlening binnen de PKI voor de overheid wordt ingezet, moeten op een zodanige wijze worden aangekocht en geleverd dat het risico op ongeautoriseerde handelingen tot een minimum wordt beperkt.

Gedurende de operations gebruikt QuoVadis een configuratie management procedure voor de installatie en het doorlopend onderhoud van de CA-systemen. Wanneer de CA-software voor het eerst wordt geladen, levert deze een methode voor het verifiëren van de software op het systeem, met daarbij de volgende garanties:

- Afkomstig van de softwareontwikkelaar/-leverancier
- Is niet gewijzigd voorafgaand aan de installatie
- Betreft de versie die is bestemd voor gebruik

De QuoVadis Chief Security Officer verifieert periodiek de integriteit van de CA's software en houdt toezicht op de configuratie van de CA systemen.

6.7 Beveiligingsmaatregelen van het netwerk

Alle toegang tot QuoVadis informatie en documentatie via een netwerk is beveiligd door middel van firewalls en routers. Firewalls en routers die worden gebruikt voor apparatuur van QuoVadis beperkt de beschikbare diensten van en de toegang tot het QuoVadis materiaal tot diegenen die dit voor de uitoefening van de functie nodig hebben.

Alle ongebruikte netwerkpoorten en -diensten zijn uitgeschakeld om ervoor te zorgen dat apparatuur van QuoVadis is beveiligd tegen het toebrengen van schade op het netwerk. Alle netwerksoftware die aanwezig is op QuoVadis apparaten, is benodigd voor voor het functioneren van de applicatie.

6.8 Time-Stamping

De QuoVadis Time-Stamping Autoriteit gebruikt PKI technologie en betrouwbare tijdsbronnen teneinde betrouwbare tijdsstempels af te geven.

De handelwijze inzake tijdstempelen is vastgelegd in een Time-Stamping Policy. De structuur en de inhoud van de QuoVadis Time-Stamping Policy zijn opgesteld conform de standaard ETSI TS 102 023.

7. Certificaatprofielen

7.1 Certificaten voor Personen

De onderstaande certificaatprofielen leveren een overzicht van de certificaatprofielen die worden uitgegeven in overeenstemming met het PKIoverheid Programma van Eisen, deel 3a.

7.1.1 Certificaten voor Personen – Authenticatie

Veld	Waarde	Kritiek
Version	Version 3	Fixed
Serial Number	Unique Number System Generated	Fixed
Signature Algorithm	sha256WithRSAEncryption	Fixed
Issuer		
Common Name (CN)	QuoVadis CSP - PKI Overheid CA - G2	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	QuoVadis Trustlink BV	Fixed
Country (C)	NL	Fixed
Valid From	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Valid To	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Subject		
Common Name (CN)	Forename, initials (or full middle name), surname	Holder Variable
Organisational Unit (OU)	Organisational Unit details (Optional)	Holder Variable
Organisation (O)	Organisation Name	Holder Variable
Country (C)	Country	Fixed
Subject Public Key Information	RSA (2048 bit) / System Generated	Fixed
Subject Serial Number	Used to differentiate between names where the subject field would otherwise be identical	Determined by CSP
Extensions		
Authority Key Identifier	Directory Attributes Certificate Issuer	Fixed
Subject Key Identifier	ID of Certificate Holder key	Fixed
Key Usage	Digital Signature	Fixed
Enhanced Key Usage	Smartcard Login (OID 1.3.6.1.4.1.311.20.2.2) (Optional)	Holder Variable
Enhanced Key Usage	Code Signing (OID 1.3.6.1.5.5.7.3.3) (Optional)	Holder Variable
Enhanced Key Usage	email Protection (OID 1.3.6.1.5.5.7.3.4) (Optional)	Holder Variable
Certificate Policies	Policy Identifier= 2.16.528.1.1003.1.2.5.1 http://www.quovadisglobal.com/repository User notice: Reliance on this certificate by any party assumes acceptance of the relevant	Fixed

Veld	Waarde	Kritiek
	QuoVadis Certification Practice Statement and other documents in the QuoVadis repository (http://www.quovadisglobal.com).	
Authority Information Access	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/qvocag2.crt	Fixed
Subject Alternative Name - otherName	2.16.528.1.1003.1.3.5.2.1.<Subject ID> (Where <Subject ID> is the unique ID number of the Certificate Holder)	Holder Variable
Subject Alternative Name - rfc822Name	RFC822 Name=<email address>	Holder Variable
CRL Distribution	http://crl.quovadisglobal.com/qvocag2.crl	Fixed
Thumbprint Algorithm	Sha1	Fixed
Thumbprint	System Generated	Fixed

7.1.2 Certificaten voor Personen – Elektronische handtekening (Non Repudiation)

Veld	Waarde	Kritiek
Version	Version 3	Fixed
Serial Number	Unique Number System Generated	Fixed
Signature Algorithm	sha256WithRSAEncryption	Fixed
Issuer		
Common Name (CN)	QuoVadis CSP - PKI Overheid CA - G2	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	QuoVadis Trustlink BV	Fixed
Country (C)	NL	Fixed
Valid From	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Valid To	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Subject		
Common Name (CN)	Forename, initials (or full middle name), surname	Holder Variable
Organisational Unit (OU)	Organisational Unit details (Optional)	Holder Variable
Organisation (O)	Organisation Name	Holder Variable
Country (C)	Country	Fixed
Subject Public Key Information	RSA (2048 bit) / System Generated	Fixed
Subject Serial Number	Used to differentiate between names where the subject field would otherwise be identical	Determined by CSP
Extensions		
Authority Key Identifier	Directory Attributes Certificate Issuer	Fixed
Subject Key Identifier	ID of Certificate Holder key	Fixed
Key Usage	Non-Repudiation	Fixed

Veld	Waarde	Kritiek
Certificate Policies	Policy Identifier= 2.16.528.1.1003.1.2.5.2 http://www.quovadisglobal.com/repository User notice: Reliance on this certificate by any party assumes acceptance of the relevant QuoVadis Certification Practice Statement and other documents in the QuoVadis repository (http://www.quovadisglobal.com).	Fixed
Authority Information Access	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/qvocag2.crt	Fixed
Subject Alternative Name - otherName	2.16.528.1.1003.1.3.5.2.1.<Subject ID> (Where <Subject ID> is the unique ID number of the Certificate Holder)	Holder Variable
Subject Alternative Name - rfc822Name	RFC822 Name=<email address>	Holder Variable
CRL Distribution	http://crl.quovadisglobal.com/qvocag2.crl	Fixed
Thumbprint Algorithm	Sha1	Fixed
Thumbprint	System Generated	Fixed
QcStatement	0.4.0.1862.1.1	Fixed

7.1.3 Certificaten voor Personen – Vertrouwelijkheid

Veld	Waarde	Kritiek
Version	Version 3	Fixed
Serial Number	Unique Number System Generated	Fixed
Signature Algorithm	sha256WithRSAEncryption	Fixed
Issuer		
Common Name (CN)	QuoVadis CSP - PKI Overheid CA - G2	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	QuoVadis Trustlink BV	Fixed
Country (C)	NL	Fixed
Valid From	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Valid To	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Subject		
Common Name (CN)	Forename, initials (or full middle name), surname	Holder Variable
Organisational Unit (OU)	Organisational Unit details (Optional)	Holder Variable
Organisation (O)	Organisation Name	Holder Variable
Country (C)	Country	Fixed
Subject Public Key Information	RSA (2048 bit) / System Generated	Fixed
Subject Serial Number	Used to differentiate between names where the subject field would otherwise be identical	Determined by CSP
Extensions		
Authority Key Identifier	Directory Attributes Certificate Issuer	Fixed
Subject Key Identifier	ID of Certificate Holder key	Fixed
Key Usage	Key Encipherment, Data Encipherment, Key Agreement	Fixed
Certificate Policies	Policy Identifier= 2.16.528.1.1003.1.2.5.3 http://www.quovadisglobal.com/repository User notice: Reliance on this certificate by any party assumes acceptance of the relevant QuoVadis Certification Practice Statement and other documents in the QuoVadis repository (http://www.quovadisglobal.com).	Fixed
Authority Information Access	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/qvocag2.crt	Fixed
Subject Alternative Name - otherName	2.16.528.1.1003.1.3.5.2.1.<Subject ID> (Where <Subject ID> is the unique ID number of the Certificate Holder)	Holder Variable
Subject Alternative Name - rfc822Name	RFC822 Name=<email address>	Holder Variable

Veld	Waarde	Kritiek
CRL Distribution	http://crl.quovadisglobal.com/qvocag2.crl	Fixed
Thumbprint Algorithm	Sha1	Fixed
Thumbprint	System Generated	Fixed

7.2 Certificaatprofielen – Systeemcertificaten

De onderstaande certificaatprofielen leveren een overzicht van de certificaatprofielen die worden uitgegeven in overeenstemming met het PKIoverheid Programma van Eisen, deel 3b.

7.2.1 Systeemcertificaten - Authenticatie

Veld	Waarde	Kritiek
Version	Version 3	Fixed
Serial Number	Unique Number System Generated	Fixed
Signature Algorithm	sha256WithRSAEncryption	Fixed
Issuer		
Common Name (CN)	QuoVadis CSP - PKI Overheid CA - G2	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	QuoVadis Trustlink BV	Fixed
Country (C)	NL	Fixed
Valid From	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Valid To	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Subject		
Common Name (CN)	Subject Common Name (e.g. Fully Qualified Domain Name)	Holder Variable
Organisational Unit (OU)	Organisational Unit details (Optional)	Holder Variable
Organisation (O)	Organisation Name	Holder Variable
Country (C)	Country	Fixed
Subject Public Key Information	RSA (2048 bit) / System Generated	Fixed
Subject Serial Number	Used to differentiate between names where the subject field would otherwise be identical	Determined by CSP
Extensions		
Authority Key Identifier	Directory Attributes Certificate Issuer	Fixed
Subject Key Identifier	ID of Certificate Holder key	Fixed
Key Usage	Digital Signature	Fixed
Enhanced Key Usage	Smartcard Login (OID 1.3.6.1.4.1.311.20.2.2) (Optional)	Holder Variable
Certificate Policies	Policy Identifier= 2.16.528.1.1003.1.2.5.4 http://www.quovadisglobal.com/repository User notice: Reliance on this certificate by any	Fixed

Veld	Waarde	Kritiek
	party assumes acceptance of the relevant QuoVadis Certification Practice Statement and other documents in the QuoVadis repository (http://www.quovadisglobal.com).	
Authority Information Access	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/qvocag2.crt	Fixed
Subject Alternative Name - otherName	2.16.528.1.1003.1.3.5.2.1.<Service ID> (Where <Service ID> is the relevant ID number of the Service)	Holder Variable
Subject Alternative Name - rfc822Name	RFC822 Name=<email address> (optional)	Holder Variable
CRL Distribution	http://crl.quovadisglobal.com/qvocag2.crl	Fixed
Thumbprint Algorithm	Sha1	Fixed
Thumbprint	System Generated	Fixed

7.2.2 Systeemcertificaten - Vertrouwelijkheid

Veld	Waarde	Kritiek
Version	Version 3	Fixed
Serial Number	Unique Number System Generated	Fixed
Signature Algorithm	sha256WithRSAEncryption	Fixed
Issuer		
Common Name (CN)	QuoVadis CSP - PKI Overheid CA - G2	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	QuoVadis Trustlink BV	Fixed
Country (C)	NL	Fixed
Valid From	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Valid To	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Subject		
Common Name (CN)	Subject Common Name (e.g. Fully Qualified Domain Name)	Holder Variable
Organisational Unit (OU)	Organisational Unit details (Optional)	Holder Variable
Organisation (O)	Organisation Name	Holder Variable
Country (C)	Country	Fixed
Subject Public Key Information	RSA (2048 bit) / System Generated	Fixed
Subject Serial Number	Used to differentiate between names where the subject field would otherwise be identical	Determined by CSP
Extensions		
Authority Key Identifier	Directory Attributes Certificate Issuer	Fixed
Subject Key Identifier	ID of Certificate Holder key	Fixed
Key Usage	Key Encipherment, Data Encipherment, Key Agreement	Fixed
Enhanced Key Usage	Smartcard Login (OID 1.3.6.1.4.1.311.20.2.2)	Holder Variable

Veld	Waarde	Kritiek
	(Optional)	
Certificate Policies	Policy Identifier= 2.16.528.1.1003.1.2.5.5 http://www.quovadisglobal.com/repository User notice: Reliance on this certificate by any party assumes acceptance of the relevant QuoVadis Certification Practice Statement and other documents in the QuoVadis repository (http://www.quovadisglobal.com).	Fixed
Authority Information Access	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/qvocag2.crt	Fixed
Subject Alternative Name - otherName	2.16.528.1.1003.1.3.5.2.1.<Service ID> (Where <Service ID> is the relevant ID number of the Service)	Holder Variable
Subject Alternative Name - rfc822Name	RFC822 Name=<email address> (optional)	Holder Variable
CRL Distribution	http://crl.quovadisglobal.com/qvocag2.crl	Fixed
Thumbprint Algorithm	Sha1	Fixed
Thumbprint	System Generated	Fixed

7.2.3 Systeemcertificaten – Server - SSL

Veld	Waarde	Kritiek
Version	Version 3	Fixed
Serial Number	Unique Number System Generated	Fixed
Signature Algorithm	sha256WithRSAEncryption	Fixed
Issuer		
Common Name (CN)	QuoVadis CSP - PKI Overheid CA - G2	Fixed
Organisational Unit (OU)	Issuing Certification Authority	Fixed
Organisation (O)	QuoVadis Trustlink BV	Fixed
Country (C)	NL	Fixed
Valid From	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Valid To	MM/DD/YYYY HH:MM A.M/P.M	Fixed
Subject		
Common Name (CN)	Subject Common Name (e.g. Fully Qualified Domain Name)	Holder Variable
Organisational Unit (OU)	Organisational Unit details (Optional)	Holder Variable
Organisation (O)	Organisation Name	Holder Variable
Country (C)	Country	Fixed
Subject Public Key Information	RSA (2048 bit) / System Generated	Fixed
Subject Serial Number	Used to differentiate between names where the subject field would otherwise be identical	Determined by CSP

Veld	Waarde	Kritiek
Extensions		
Authority Key Identifier	Directory Attributes Certificate Issuer	Fixed
Subject Key Identifier	ID of Certificate Holder key	Fixed
Key Usage	Digital Signature, Key Encipherment, Key Agreement	Fixed
Enhanced Key Usage	Smartcard Login (OID 1.3.6.1.4.1.311.20.2.2) (Optional)	Holder Variable
Certificate Policies	Policy Identifier= 2.16.528.1.1003.1.2.5.6 http://www.quovadisglobal.com/repository User notice: Reliance on this certificate by any party assumes acceptance of the relevant QuoVadis Certification Practice Statement and other documents in the QuoVadis repository (http://www.quovadisglobal.com).	Fixed
Authority Information Access	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/qvocag2.crt	Fixed
Subject Alternative Name - otherName	2.16.528.1.1003.1.3.5.2.1.<Service ID> (Where <Service ID> is the relevant ID number of the Service)	Holder Variable
Subject Alternative Name - rfc822Name	RFC822 Name=<email address> (optional)	Holder Variable
CRL Distribution	http://crl.quovadisglobal.com/qvocag2.crl	Fixed
Thumbprint Algorithm	Sha1	Fixed
Thumbprint	System Generated	Fixed

8. Conformiteitbeoordeling

8.1. Certificatie en registratie bij OPTA

QuoVadis is een CSP (certificatiedienstverlener) in de zin van de Telecomwet en alszodanig geregistreerd bij de OPTA onder nummer 941826 (zie par. 8.6).
Het managementsysteem van QuoVadis inzake het uitgeven van gekwalificeerde certificaten aan het publiek is gecertificeerd op basis van ETSI TS 101456. QuoVadis verkreeg in 2008 het conformiteitscertificaat hiervoor met nummer ETS-010, afgegeven door de geaccrediteerde certificatieinstelling BSI Management Systems B.V. (BSI) te Amsterdam. Daarbij is tevens aangegeven dat QuoVadis tevens voldoet aan de aanvullende eisen zoals neergelegd in het Besluit Elektronische Handtekeningen. Het conformiteitscertificaat heft een geldigheid van drie jaren en is tussentijds onderhevig aan tussentijdse controleaudits (na 12 en 24 maanden). In 2009 heeft QuoVadis van BSI een auditverklaring ontvangen waarin is aangegeven dat voldaan wordt aan de eisen uit het Programma van Eisen PKIoverheid, delen 3a en 3b.

8.2. De verhouding van de auditor met de beoordeelde entiteit

De auditor en QuoVadis welke wordt ge-audit, mogen geen relatie hebben die de auditors onafhankelijkheid aantast en objectiviteit volgens Generally Accepted Auditing Standards. Tot deze relaties behoren, financieel, wettelijk, sociaal of andere relaties welke tot een conflict kunnen leiden.

8.3. Scope van de audit

De scope van de certificatieaudit betreft de volgende onderwerpen en processen:

- Registration Service;
- Certificate Generation Service;
- Dissemination Service;
- Revocation Management Service;
- Revocation Status Service
- Subject Device Provision Service.

8.4. Acties ondernomen vanwege deficiëntie

Ingeval tijdens een audit non-conformiteiten zijn geconstateerd, wordt door QuoVadis een Corrective Action Plan (CAP) opgesteld waarin corrigerende maatregelen worden voorgesteld om de non-conformiteiten weg te nemen. De certificerende instelling dient goedkeuring te verlenen aan het CAP.
Tussentijds worden door QuoVadis interne audits uitgevoerd waarin de opvolging van de corrigerende acties worden gecontroleerd.
Tenslotte wordt bij een volgende certificatieaudit de implementatie van de corrigerende maaregel door de certificerende instelling gecontroleerd.

8.6. Publicatie accreditaties en registraties

De registratie van QuoVadis als certificatiedienstverlener is gepubliceerd op de website van OPTA:
http://www.opta.nl/nl/registraties/geregistreerde-partijen/zoekresultaat/?query=quo+vadis

Een lijst met certificatiedienstverleners die certificaten uitgeven binnen de PKI voor de overheid vindt u hier:
http://www.pkioverheid.nl/voor-certificaatverleners/toegetreden-certificaatverleners/

Overige accreditaties van QuoVadis is raadpleegbaar op de volgende lokatie:
http://www.quovadisglobal.com/accreditations.aspx.

9. Algemene en juridische bepalingen

9.1 Tarieven

QuoVadis zal op verzoek alle toepasselijke tarieven beschikbaar stellen. Tarieven voor uitgifte van Certificaten variëren sterk, gebaseerd op aantallen en Certificaattypes. Jaarlijkse tarieven voor gekwalificeerde Certificaten uitgegeven aan individuele openbare aanvragers zijn €100.00 (euro).

9.1.1. Tarieven voor Certificaatuitgifte of -vernieuwing

Er zouden kosten in rekening kunnen worden gebracht betreffende de uitgifte of vernieuwing van Certificaten. Details hierover zijn opgenomen in de relevante contractuele documentatie betreffende de uitgifte of vernieuwing van dergelijke Certificaten.

9.1.2. Tarieven voor Certificaattoegang

Er zouden kosten in rekening kunnen worden gebracht betreffende toegang tot de QuoVadis elektronische opslagplaats voor het downloaden van Certificaten. Details hierover zijn opgenomen in de relevante contractuele documentatie.

9.1.3. Tarieven voor toegang tot intrekkings- of statusinformatie

Er zouden kosten in rekening kunnen worden gebracht betreffende toegang tot de QuoVadis elektronische opslagplaats voor Certificaatintrekking- of statusinformatie. Details hierover zijn opgenomen in de relevante contractuele documentatie.

9.1.4. Tarieven voor andere diensten

Er kunnen kosten in rekening worden gebracht betreffende het volgende:

- Intrekking van Certificaten
- Certificaatstatus en – validatie; en

9.1.5. Beleid inzake terugbetaling

QuoVadis kan een beleid inzake terugbetaling in het leven roepen. Details hierover zijn opgenomen in de relevante contractuele documentatie.

9.2. Financiële verantwoordelijkheid en aansprakelijkheid

QuoVadis is verantwoordelijk voor het beheren van haar financiële boekhouding en vastleggingen op commercieel redelijke wijze en zal gebruik maken van de diensten van een internationaal accountantsbureau voor financiële diensten, waaronder periodieke controles.

9.2.1. Verzekeringsdekking

QuoVadis heeft adequate regelingen getroffen, om aansprakelijkheden die verband houden met de onderhavige dienstverlening af te dekken. De dekking bedraagt $10.000.000,00.

9.3. Vertrouwelijkheid van bedrijfsgevoelige gegevens

9.3.1. Toepassingsgebied vertrouwelijke informatie

Enige persoonlijke- of bedrijfsinformatie in het bezit van QuoVadis, gerelateerd aan de aanvraag van de Certificaathouder en de uitgifte van Certificaten, wordt als vertrouwelijk beschouwd en zal niet worden vrijgegeven zonder voorafgaande toestemming van de betreffende Certificaathouder, tenzij anders vereist door wetgeving of om aan de vereisten van dit CPS te voldoen.

9.3.2. Gegevens die als niet-vertrouwelijk worden beschouwd

Informatie in Certificaten of die opgeslagen is in de elektronische opslagplaats worden niet beschouwd als vertrouwelijk, tenzij statuten of speciale overeenkomsten dit voorschrijven.

9.3.3. Verantwoordelijkheid vertrouwelijke informatie te beschermen

QuoVadis, Abonnees, Certificaathouders, vertrouwende partijen en alle anderen zijn verantwoordelijk voor de bescherming van vertrouwelijke bedrijfsinformatie die in hun bezit is.

9.4. Vertrouwelijkheid van persoonlijke informatie

QuoVadis voldoet aan de eisen van de Wet Bescherming Persoonsgegevens. QuoVadis heeft zich geregistreerd bij het College Bescherming Persoonsgegevens als zijnde verantwoordelijk voor het verwerken van persoonsgegevens ten behoeve van de Certificatiedienstverlening.

9.4.1. Vertrouwelijke informatie

QuoVadis, Registratieautoriteiten, Abonnees, Certificaathouders, vertrouwende partijen en alle anderen die gebruik maken of toegang hebben tot persoonsgegevens, zullen zich houden aan relevante wetgeving en regelgeving inzake de bescherming van persoonsgegevens.

9.4.2. Vertrouwelijk behandelde informatie

Alle informatie betreffende Certificaathouders die niet publiekelijk beschikbaar is door middel van de inhoud van uitgegeven Certificaten, CRLs of van de elektronische opslagplaats worden vertrouwelijk behandeld.

9.4.2.1. Registratievastleggingen

Alle registratievastleggingen zullen als vertrouwelijke informatie beschouwd en behandeld worden.

9.4.2.2. Certificaatintrekking

Met uitzondering van de intrekkingsredenen opgenomen in een CRL wordt de gedetailleerde reden voor de intrekking van een Certificaat gezien als vertrouwelijke informatie, met als enige uitzondering de intrekking van het certificaat van de QuoVadis CSP-CA:

- De compromittering van de private sleutel van de QuoVadis CSP-CA, in welk geval er een openbaarmaking mag worden gepubliceerd dat de private sleutel is gecompromitteerd;

- De opheffing van de QuoVadis CSP-CA binnen de PKI voor de overheid, in welk geval er voorafgaande openbaarmaking mag worden gepubliceerd van de opheffing.

9.4.3. Niet-vertrouwelijke informatie

9.4.3.1. Certificaatinhoud

De inhoud van Certificaten, uitgegeven door QuoVadis, is publieke informatie en dient niet als vertrouwelijk te worden beschouwd.

9.4.3.2. Certificaatintrekkingslijst

Certificaten, gepubliceerd in elektronische opslagplaats worden niet beschouwd als vertrouwelijke informatie.

9.4.3.3. CPS

Deze QuoVadis CPS is een publiekelijk document en is geen vertrouwelijke informatie en zal niet alszodanig worden behandeld.

9.4.4. Verantwoordelijkheid om vertrouwelijke informatie te beschermen

Informatie die aan QuoVadis wordt verstrekt door handelingen beschreven in deze CPS wordt als vertrouwelijk aangemerkt. QuoVadis zal om geen enkele reden persoonlijke Certificaathouderinformatie verstrekken aan enige derde partij, tenzij dit wordt vereist door wetgeving of op last van een rechterlijk bevel.

9.4.5. Melding van- en instemming met het gebruik van persoonsgegevens

In het proces van het accepteren van een Certificaat hebben alle Certificaathouders ingestemd met de verwerking, door en namens QuoVadis, en met het gebruik, zoals in het registratieproces beschreven, van hun persoonlijke gegevens, die zijn verstrekt tijdens het registratieproces. Zij hebben tevens de mogelijkheid gekregen om af te zien van het gebruik van hun persoonlijke gegevens voor bepaalde doeleinden. Ook zijn zij al dan niet overeengekomen bepaalde persoonlijke informatie zichtbaar te maken in de elektronische opslagplaats en voor verstrekking aan derden.
Certificaathouders stemmen uitdrukkelijk in met de verplaatsing van persoonlijke gegevens, in de vorm van gegevens die zijn opgenomen in de Certificaatvelden, buiten Nederland en stemmen al dan niet in met de publicatie van het Certificaat in de elektronische opslagplaats die de Certificaatinformatie publiekelijk toegankelijk maakt voor vertrouwende partijen die met de toepasselijke query string zoeken binnen de elektronische opslagplaats. Persoonlijke gegevens, verkregen tijdens het registratieproces die niet zijn opgenomen in het Certificaat, zullen niet worden verplaatst buiten Nederland.

9.4.6. Overhandiging van gegevens op last van een rechterlijke instantie

In principe zullen geen vertrouwelijke gegevens in het bezit van QuoVadis worden vrijgegeven aan opsporingsinstanties of –ambtenaren, tenzij de Nederlandse wet- en regelgeving hiertoe dwingt middels een gerechtelijk bevel.

9.5 Intellectuele eigendomsrechten

Alle intellectuele eigendomsrechten inclusief alle auteursrechten op Certificaten en QuoVadis documenten (elektronisch of in andere vorm) zijn eigendom van QuoVadis en zullen dit blijven. Om verwarring te voorkomen worden documenten die zijn ondergetekend of versleuteld met een QuoVadis Certificaat, niet aangemerkt als QuoVadis documenten in relatie tot deze paragraaf, en is QuoVadis niet verantwoordelijk voor de inhoud van dergelijke documenten of aantekeningen.

Private en publieke sleutels zijn eigendom van de abonnee en Certificaathouder.

QuoVadis garandeert jegens haar abonnees en certificaathouders dat de door haar uitgegeven certificaten en dragers van de private en publieke sleutel, inclusief de daarbij behorende en geleverde apparatuur en documentatie, geen inbreuk maakt op intellectuele eigendomsrechten, waaronder auteursrechten, merkenrechten en gebruikte programmatuur waarvan deze berusten bij haar (toe)leveranciers.

9.6. Aansprakelijkheid en garanties

9.6.1. Aansprakelijkheid van de CSP

QuoVadis verklaart hierbij dat:
(a) zij redelijke stappen heeft ondernomen om de informatie die is opgenomen in een Certificaat te verifiëren op accuraatheid ten tijde van de uitgifte, en (b) Certificaten zullen worden ingetrokken indien QuoVadis vermoedt of erop is gewezen dat de inhoud van een Certificaat niet meer accuraat is, of dat de sleutel, geassocieerd met een Certificaat, op enige wijze is gecompromitteerd.
QuoVadis is alleen aansprakelijk jegens Certificaathouders of vertrouwende partijen voor onmiddellijk verlies voortvloeiend uit het door QuoVadis schenden van bepalingen uit deze CPS of van enige andere aansprakelijkheid uit overeenkomst, onrechtmatige daad of anders, inclusief de aansprakelijkheid voor nalatigheid tot een in 9.8. opgenomen maximum bedrag, voor enige gebeurtenis of reeks verwante gebeurtenissen (in een periode van 12 maanden).
De CSP sluit alle aansprakelijkheid uit voor schade die ontstaat indien het Certificaat niet wordt gebruikt conform het beoogde Certificaatgebruik, zoals beschreven in paragraaf 1.4 van dit CPS.
QuoVadis kan, op aanwijzen van de PA van de PKI voor de overheid, in het handtekeningcertificaat beperkingen ten aanzien van het gebruik ervan opnemen, mits de betreffende beperkingen duidelijk zijn voor derden. QuoVadis is niet aansprakelijk voor schade als gevolg van gebruik van een handtekeningcertificaat in strijd met een dergelijk opgenomen beperking.

QuoVadis accepteert geen enkele vorm van aansprakelijkheid voor geleden schade van vertrouwende partijen, met daarop de volgende uitzonderingen:

- QuoVadis is in beginsel aansprakelijk overeenkomstig artikel 6.19b, eerste tot en met derde lid, van het Burgerlijk Wetboek, met dien verstande dat:
  (a) voor “een gekwalificeerd certificaat als bedoeld in artikel 1.1. onderdeel ss Telecommunicatiewet” gelezen wordt: “een authenticiteitscertificaat”

(b) voor “ondertekenaar” gelezen wordt: “certificaathouder”;
(c) voor “elektronische handtekeningen” gelezen wordt: “authenticiteitskenmerken”.

- QuoVadis is in beginsel aansprakelijk overeenkomstig artikel 6.19b, eerste tot en met derde lid, van het Burgerlijk Wetboek, met dien verstande dat:
  (a) voor “een gekwalificeerd certificaat als bedoeld in artikel 1.1. onderdeel ss Telecommunicatiewet” gelezen wordt: “een vertrouwelijkheidscertificaat”;
  (b) voor “ondertekenaar” gelezen wordt: “certificaathouder”;
  (c) voor “aanmaken van elektronische handtekeningen” gelezen wordt: “aanmaken van vercijferde data”;
  (d) voor “verifiëren van elektronische handtekeningen” gelezen wordt: “ontcijferen van vercijferde data”.
  (e) voor “een gekwalificeerd certificaat als bedoeld in artikel 1.1. onderdeel ss Telecommunicatiewet” gelezen wordt: “een servercertificaat”;
  (f) voor “ondertekenaar” gelezen wordt: “certificaathouder”;
  (g) voor “aanmaken van elektronische handtekeningen” gelezen wordt: “verifiëren van authenticiteitskenmerken een aanmaken van vercijferde data”;
  (h) voor “verifiëren van elektronische handtekeningen” gelezen wordt: “ontcijferen van authenticiteitskenmerken en vercijferde data”.

9.6.2.Aansprakelijkheid van Abonnees en Certificaathouders

Certificaathouders garanderen dat:

- de private sleutel beschermd is en er nooit toegang is geweest voor een ander persoon
- alle representaties, die door de Certificaathouder zijn gemaakt, juist zijn
- alle informatie in het Certificaat juist en accuraat is
- het Certificaat wordt gebruikt conform de bedoelde, geautoriseerde en rechtmatige gebruik overeenkomstig dit CPS
- zij onmiddellijk intrekking verzoeken van het Certificaat in het geval dat: (a) enige informatie, opgenomen in het Certificaat, incorrect of inaccuraat is of wordt, of (b) de private sleutel die correspondeert met de publieke sleutel in het Certificaat (vermoedelijk) is misbruikt of gecompromitteerd.

9.6.3.Aansprakelijkheid Vertrouwende Partijen

Vertrouwende Partijen garanderen dat:

- zij voldoende informatie zullen verzamelen over een Certificaat en zijn houder om een besluit op basis van goede informatie te maken over in hoeverre er op een Certificaat vertrouwd kan worden.
- zij zijn als enige verantwoordelijk voor het maken van de beslissing te vertrouwen op een Certificaat (met uitzondering van het genoemde in 9.6.1)
- zij de juridische consequenties dragen als gevolg van het nalaten van het handelen overeenkomstig de verplichtingen van vertrouwende partijen conform dit CPS.

9.7. Uitsluiting van garanties

Voor zover toegestaan door de toepasbare wetgeving zal deze CPS, de Certificaathouderovereenkomst en enig andere contractuele documentatie, toepasselijk binnen de PKI voor de overheid, garanties van QuoVadis uitsluiten.

9.8. Beperking van aansprakelijkheid

9.8.1. Beperkingen van aansprakelijkheid van QuoVadis

QuoVadis zal in geen geval verantwoordelijk zijn voor het verlies van winst, verlies van verkoop of omzet, verlies of schade aan reputatie, verlies van contracten, verlies van klanten, verlies van het gebruik van enige software of data, verlies of gebruik van enige computer of andere apparatuur (tenzij direct het gevolg door breuk van dit CPS), verspilde tijd van management of ander personeel, verliezen of aansprakelijkheden met betrekking tot of in samenhang met andere contracten, indirecte schade of verlies, gevolgschade of –verlies, speciaal verlies of schade, en binnen deze paragraaf betekent “verlies” zowel een gedeeltelijk verlies van of daling in waarde als volledig of totaal verlies.

De aansprakelijkheid van QuoVadis richting een bepaald persoon betreffende schade die op enige wijze optreedt onder, uit naam van, binnen of gerelateerd aan deze CPS, Certificaathouderovereenkomst, het toepasselijke contract of gerelateerde overeenkomst, hetzij in contract, garantie, onrechtmatige daad of enig andere wettelijke theorie, is, onderworpen aan wat verderop uiteen is gezet, beperkt zijn tot daadwerkelijke schade die door deze persoon is geleden. QuoVadis zal niet aansprakelijk zijn voor indirecte, gevolg-, incidentele, speciale, voorbeeld- of bestraffende schade met betrekking tot enige persoon, zelfs als QuoVadis is gewezen op de mogelijkheid van dergelijke schade, ongeacht hoe dergelijke schade of verantwoordelijkheid is opgetreden, hetzij in onrechtmatige daad, achteloosheid, rechtvaardigheid, contract, statuut, gewoonterecht of anderzijds. Als voorwaarde aan deelname binnen de PKI voor de overheid (inclusief, zonder beperking, het gebruik van of vertrouwen op Certificaten) stemt iedere persoon die binnen de PKI voor de overheid deelneemt onherroepelijk in dat zij geen aanspraak wil maken op, of op andere wijze zoeken naar, voorbeeld-, gevolg-, speciale, incidentele of bestraffende schade en bevestigt onherroepelijk aan QuoVadis de aanvaarding van het voorgaande als een conditie en aansporing om deze persoon toe te staan deel te nemen binnen de PKI voor de overheid.

9.8.2. Uitgesloten aansprakelijkheid

QuoVadis zal op geen enkele wijze aansprakelijk zijn voor enig verlies betreffende of voortkomende uit een (of meerdere) van de volgende omstandigheden of oorzaken:

- Als het Certificaat, gehouden door de eisende partij of op andere wijze onderwerp van enige eis, is gecompromitteerd door ongeautoriseerde onthulling of gebruik van het Certificaat, of enig wachtwoord of activeringsgegevens die de toegang hiertoe controleren;
- Als het Certificaat, gehouden door de eisende partij of op andere wijze onderwerp van enige eis uitgegeven is als gevolg van onjuiste voorstelling, fout of feit, of nalatigheid van enige persoon, enititeit of organisatie;

- Als het Certificaat, gehouden door de eisende partij of op andere wijze onderwerp van enige eis is verlopen of ingetrokken voor de datum van omstandigheden die leiden tot enige claim;
- Als het Certificaat, gehouden door de eisende partij of op andere wijze onderwerp van enige eis is gewijzigd of op enige wijze is veranderd of op een andere manier is gebruikt dan toegestaan door de voorwaarden van deze CPS en/of de relevante Certificaathouderovereenkomst of enige toepasbare wet- of regelgeving;
- Als de private sleutel, die correspondeertmet het Certificaat, gehouden door de eisende partij of op andere wijze onderwerp van enige eis, is gecompromitteerd;
- Als het Certificaat, gehouden door de eisende partij, uitgegeven is op een wijze die in overtreding is met enige toepasbare wet- of regelgeving;
- Computer hardware of software, of mathematische algoritmen, zijn ontwikkeld die de neiging hebben publieke sleutelcryptografie of asymmetrische cryptosystemen onzeker te maken, op voorwaarde dat QuoVadis commercieel redelijke praktijen gebruikt om te beschermen tegen schendingen van beveiliging als gevolg van dergelijke hardware, software of algoritmen;
- Stroomuitval, stroomonderbreking, of andere onderbrekingen van elektriciteit, op voorwaarde dat QuoVadis commercieel redelijke methoden gebruikt om te beschermen tegen dergelijke storingen;
- Uitval van een of meerdere computersystemen, communicatie-infrastructuur, verwerking, of opslagmedia of –mechanismen of enig subcomponent van voorgaande, niet onder exclusieve controle van QuoVadis en/of diens onderaannemers; of
- Een of meer van de volgende gebeurtenissen: een natuurramp of overmacht (inclusief, zonder beperking, overstroming, aardbeving, of andere natuurlijke of weergerelateerde oorzaak); een arbeidsstoring; oorlog, opstand of openlijke militaire vijandigheden; tegenstrijdige wetgeving of overheidsactie, verbod, embargo of boycot; rellen of burgerlijke ongeregeldheden; vuur of explosie; catastrofale epidemie; handelsembargo; beperking of beletsel (met inbegrip van, zonder beperking, exportcontroles); enig gebrek aan beschikbaarheid of integriteit van telecommunicatie; wettelijke dwang, met inbegrip van enige beslissing, gemaakt door een hof van bekwame jurisdictie, waaraan QuoVadis onderworpen is; en enige gebeurtenis of omstandigheid of reeks omstandigheden die buiten de controle van QuoVadis vallen.

9.8.2.1 Beperking Certificaatverlies

Onverminderd een andere bepaling van dit hoofdstuk zal de aansprakelijkheid van QuoVadis voor breuk van zijn verplichtingen overeenkomstig deze CPS, met uitzondering van fraude of opzettelijk wangedrag van QuoVadis, onderworpen zijn aan een monetaire grens die bepaald is aan de hand van het type Certificaat, gehouden door de eisende partij, en die absoluut beperkt is tot de monetaire bedragen die hieronder zijn weergegeven.

Verliesbeperkingen/ Beperkingen vertrouwen	Maximum per Certificaat
Certificaten voor Personen	US $250,000
Systeemcertificaten	US $250,000

In geen geval zal de aansprakelijkheid van QuoVadis de verliesbeperkingen, die in bovenstaande tabel staan, overstijgen. De verliesbeperkingen zijn toepasselijk op de levenscyclus van een bepaald Certificaat met de bedoeling dat de verliesbeperkingen de totale mogelijke cumulatieve aansprakelijkheid van Quovadis reflecteert per Certificaat per jaar (ongeacht het aantal eisen per Certificaat). De voorgaande beperking is van toepassing ongeacht het aantal transacties of actieoorzaken met betrekking tot een bepaald Certificaat in enig jaar van de levenscyclus van dat Certificaat.

9.8.3. Beperking van aansprakelijkheid QuoVadis

QuoVadis heeft een aantal maatregelen geïntroduceerd om haar aansprakelijkheden te verminderen of te beperken in het geval dat beschermingsmiddelen voor het beschermen van bronnen er niet in slagen om:

- misbruik van deze bronnen door geautoriseerd personeel te voorkomen
- toegang tot deze bronnen door ongeautoriseerde individuen te verbieden

Deze maatregelen omvatten, maar zijn niet beperkt tot:

- het identificeren van onvoorziene gebeurtenissen en toepasselijke herstelacties in een bedrijfscontinuiteitsplan en Disaster Recovery Plan;
- het regelmatig uitvoeren van back-ups van systeemdata;
- het uitvoeren van een back-up van de huidige werkende software en bepaalde software configuratie-files;
- het opslaan van alle back-ups in beveiligde locale en gedecentraliseerde opslag;
- het handhaven van beveiligde gedecentraliseerde opslag van overig materiaal, benodigd voor rampenherstel;
- het periodiek testen van lokale en gedecentraliseerde back-ups om zeker te stellen dat de informatie herwinbaar is in het geval van een storing;
- het periodiek beoordelen van het bedrijfscontinuiteitsplan en Disaster Recovery Plan, inclusief de identificatieanalyse, evaluatie en prioritering van risico's; en
- het periodiek controleren van ononderbroken voeding.

9.8.4. Eisen met betrekking tot de aansprakelijkheid van QuoVadis

9.8.4.1. Notificatieperiode

QuoVadis zal geen verplichtingen hebben overeenkomstig enige eis voor breuk van haar verplichtingen tenzij de eisende partij QuoVadis binnen negentig (90) dagen nadat de eisende partij wist of redelijkerwijs had moeten weten van de claim, en in geen geval meer dan drie jaar na afloop van het Certificaat die de eisende partij hield, hiervan op de hoogte stelt.

9.8.4.2. Beperkende handelingen en onthulling van ondersteunende informatie

Als voorwaarde voor uitbetaling van QuoVadis betreffende enige eis onder de voorwaarden van deze CPS zal een eisende partij alle verdere handelingen en dingen doen en uitvoeren, en alle dergelijke overeenkomsten, instrumenten en documenten uitvoeren en aanleveren

die QuoVadis redelijkerwijs verzoekt om een claim van verlies, gemaakt door de eisende partij, te kunnen onderzoeken.

9.9. Schadeloosstelling

De bepalingen en verplichtingen betreffende schadevergoedingen zijn opgenomen in de relevante contractuele documentatie.

9.10. Geldigheidstermijn CPS

9.10.1. Termijn

Deze CPS is geldig vanaf het moment van publicatie in de QuoVadis elektronische opslagplaats. Herzieningen op de CPS zijn geldig vanaf het moment van publicatie in de QuoVadis Elektronische opslagplaats.

9.10.2. Beëindiging

Deze CPS zal geldig blijven tot deze is herzien of verplaatst door een andere versie.

9.10.3. Effect van beëindiging en overleving

De bepalingen binnen dit CPS zullen de beëindiging of terugtrekking van een Certificaathouder of vertrouwende partij binnen de PKI voor de overheid overleven met betrekking tot alle handelingen gebaseerd op het gebruik van of het vertrouwen op een Certificaat of andere deelname binnen de PKI voor de overheid. Enige dergelijke beëindiging of terugtrekking zal niet zo optreden om enig recht op actie of remedie te benadelen of beïnvloeden die gevolg waren aan enig persoon tot en met de datum van terugtrekking of beëindiging.

9.11. individuele kennisgeving en communicatie met betrokken partijen

Electronische post, brievenbuspost, fax en webpagina's zullen beschikbare middelen zijn die QuoVadis gebruikt om enig van de berichten, vereist door deze CPS, aan te bieden, tenzij op specifiek andere wijze aangeboden. Elektronische mail, brievenbuspost en fax zullen alle geldige middelen zijn om enige berichtgeving, vereist overeenkomstig dit CPS, aan QuoVadis te verstrekken tenzij specifiek op andere wijze aangeboden (bijvoorbeeld met betrekking tot intrekkingprocedures).

9.12. Wijziging

9.12.1. Wijzigingsprocedure

Wijzigingen aan dit CPS zullen in de vorm van een gewijzigd CPS of vervangend CPS zijn. Bijgewerkt versies van deze CPS zullen aangewezen of tegenstrijdige bepalingen van de vermelde versie van het CPS vervangen.

Er zijn twee mogelijke soorten van beleidsverandering:

- de uitgifte van een nieuwe CPS; of
- een verandering of aanpassing van een beleid in het bestaande CPS.

De enige veranderingen die mogen worden gemaakt aan dit CPS zonder berichtgeving zijn redactionele of typografische correcties die geen consequenties hebben voor enige participanten binnen de PKI voor de overheid.

9.12.2. Notificatie van wijzigingen

De nieuwe of gewijzigde CPS worden gepubliceerd in de elektronische opslagplaats, op de website http://www.quovadisglobal.nl/Repository.aspx.

Als een beleidsverandering consequenties heeft voor Certificaathouders, zal QuoVadis de wijziging bekend maken aan zijn geregistreerde abonnees en/of Certificaathouders middels notificatie als weergegeven in 9.11.
Enige verandering dat het niveau van vertrouwen*, dat mag worden geplaatst op Certificaten uitgegeven onder deze CPS of onder beleid dat refereert aan dit CPS, verhoogt, vereist een voorafgaande kennisgeving van dertig (30) dagen.
Enige verandering dat het niveau van vertrouwen*, dat mag worden geplaatst op Certificaten uitgegeven onder deze CPS of onder beleid dat refereert aan dit CPS, verlaagt, vereist een voorafgaande kennisgeving van vijfenveertig (45) dagen.

*In dit gedeelte bevat “niveau van vertrouwen” niet die gedeelten van de specificatie met betrekking tot de aansprakelijkheid van partijen. Referentie aan het “nveau van vertrouwen” slaan louter op de technische/administratieve functies en enige verandering waarin is voorzien onder deze clausule zal deze specificatie niet materieel veranderen tenzij er een specifieke bedrijfsreden is dit te doen.
Indien er een voornemen is de CA-structuur te veranderen, dient QuoVadis informatie hieromtrent voor te leggen aan de PA.

9.13. Geschillenbeslechting

Enige controversie of eis tussen twee of meer deelnemers binnen de PKI voor de overheid (met QuoVadis als deelnemer binnen de PKI voor de overheid), voortkomend uit of gerelateerd aan deze CPS zal deze worden voorgelegd aan een bevoegde rechter.

9.14. Van toepassing zijnde wetgeving

Op alle overeenkomsten die door QuoVadis worden afgesloten is het Nederlands recht van toepassing, tenzij anders is bepaald.

9.15. Naleving relevante wetgeving

QuoVadis is een Certificatiedienstverlener ingevolge de Telecommunicatiewet. QuoVadis conformeert zich aan de toepasselijke wet- en die betrekking heeft op haar rol als Certificatiedienstverlener.

9.16. Overige bepalingen

Enige bepaling binnen dit CPS die ongeldig of onuitvoerbaar wordt verklaard, zal buiten werking treden. Dit laat onverlet de toepasselijkheid van de resterende bepalingen in dit CPS.

Bijlage A – Definities en Afkortingen

Definities

Aanvrager: een natuurlijke of rechtspersoon die een aanvraag tot uitgifte van een Certificaat indient bij QuoVadis. De Aanvrager hoeft niet dezelfde partij te zijn als de Abonnee of de Certificaathouder, maar is wel één van beide.

Abonnee: de natuurlijke persoon of rechtspersoon die zich aanmeldt bij QuoVadis om uitgifte van PKIoverheid Certificaten aan door hem aangewezen Certificaathouders te bewerkstelligen.

Accreditatie: Procedure waarbij een autoriteit bezittende organisatie een formele erkenning uitspreekt dat een entiteit bekwaam is specifieke taken uit te voeren

Algemene Voorwaarden: de Algemene Voorwaarden PKIoverheid Certificaten, zoals van toepassing op alle bij de uitgifte en het gebruik van PKIoverheid Certificaten betrokken partijen.

Algoritme: Een verzameling instructies die stap voor stap uitgevoerd dienen te worden om een rekenkundig proces uit te voeren of een specifiek type problemen op te lossen.

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

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

Authentificatie: zie Authenticatie.

Autoriseren: Het verlenen van een bevoegdheid tot het verrichten van handelingen (zoals inzien, aanpassen of bewerken) op informatie of middelen.

Beschikbaarheid Het aanwezig zijn en het toegankelijk zijn van de relevante gegevens. Wat betreft infrastructuur: de mate waarin een systeem bruikbaar is op het moment dat hier een behoefte aan bestaat.

CA-Certificaat: een Certificaat van een Certification Authority.

Calamiteit (E: Disaster) Een ongeplande situatie waarbij verwacht wordt dat de duur van het niet beschikbaar zijn van één of meer diensten de afgesproken drempelwaarden zal overschrijden.

Certificaat: de Publieke Sleutel van een Eindgebruiker, samen met aanvullende informatie. Een Certificaat is vercijferd met de Private Sleutel van de Certification Authority die de Publieke Sleutel heeft uitgegeven, waardoor het Certificaat onvervalsbaar is.

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

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

Certificaat & kaart management: De procedures met betrekking tot het beheer van de certificaten en smartcards.

Certificaatgeldigheidsduur (E: Certificate validity period): Het tijdsinterval gedurende welke de Certification Authority de bruikbaarheid van het certificaat garandeert. De Certification Authority houdt tot ten minste 6 maanden na het verlopen van de geldigheidsduur informatie bij betreffende de status van een certificaat.

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.

Certificate Revocation List: zie Certificaten Revocatie Lijst.

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

Certificatie
Een brede (zowel technisch als niet-technisch) evaluatie van de beveiligingseigenschappen van een informatiesysteem of, zoals in het kader van de PKI voor de overheid, een managementsysteem. Certificatie wordt uitgevoerd als een onderdeel van een proces, waarbij wordt nagegaan in welke mate een managementsysteem overeenkomt met een vastgestelde verzameling van eisen (ETSI TS 101 456). De regels voor de certificering zijn

vastgelegd in een schema: Scheme for Certification of Certification Authorities against ETSI TS 101 456.

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 QuoVadis 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 Certificate Policy.

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

Certification Service Provider - CSP (NL: Certificatiedienstverlener): *Een natuurlijke of rechtspersoon die certificaten afgeeft of andere diensten in verband met elektronische handtekeningen verleent.* [Wet EH] In het kader van de PKI voor de overheid kan de CSP ook diensten verlenen in verband met identiteit en vertrouwelijkheid. Een CSP heeft als functie het verstrekken en beheren van certificaten en sleutelinformatie, met inbegrip van de hiervoor voorziene dragers (bijvoorbeeld smartcards). De CSP heeft tevens de eindverantwoordelijkheid voor het leveren van de certificatiediensten. Daarbij maakt het niet uit of de CSP de feitelijke werkzaamheden zelf uitvoert of deze uitbesteedt aan anderen. Het is bijvoorbeeld niet ondenkbaar dat een CSP de CA-functie en/of de RA-functie uitbesteedt. Zie ook het plaatje bij "*Hiërarchisch model*".

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

Certification Service Provider (CSP): zie Certificatiedienstverlener.

CommonName – CN: Een aanduiding van de certificaathouder, in het geval van een persoonsgebonden certificaat bestaande uit: achternaam, voorna[a]m[en] en eventueel voorletters. Ook de certificaatuitgever kan worden aangeduid met een CommonName, in dat geval zal deze meestal bestaan uit een bedrijfsnaam aangevuld met het van toepassing zijnde domein van de PKI voor de overheid.

Cryptografische module: De verzameling van hardware, software, firmware, of enige combinatie hiervan die cryptografische processen implementeert, inclusief cryptografische algoritmen en die bevat is binnen de cryptografische grenzen van de module.

Digitale Handtekening: zie Geavanceerde Elektronische Handtekening.

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

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

Eindgebruikercertificaat (E: End user certificate): Een certificaat uitgegeven door een Certification Service Provider aan een entiteit, zoals een persoon, een computer of een stukje informatie, die zelf geen certificaten kan uitgeven. Omdat naar de eindgebruiker die een certificaat van een Certification Service Provider ontvangt, vaak wordt verwezen als zijnde de cliënt, wordt dit certificaat ook wel een cliënt-certificaat genoemd. Ook wordt soms de term "*Gebruikercertificaat*" gehanteerd.

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

Elektronische identiteit: De gegevens in elektronische vorm die worden toegevoegd aan of op logische wijze verbonden met andere elektronische gegevens en fungeren als uniek kenmerk van de identiteit van de eigenaar. Soms wordt de term "Digitale identiteit" gebruikt.

Encryptie: Een proces waarmee gegevens met behulp van een wiskundig algoritme en een cryptografische sleutel worden vercijferd, zodat deze onleesbaar worden voor onbevoegden. De betrouwbaarheid van de encryptie hangt af van het algoritme, de implementatie daarvan, de lengte van de cryptografische sleutel en de gebruiksdiscipline. Bij symmetrische encryptie wordt bij het vercijferen en ontcijferen gebruik gemaakt van één en dezelfde, geheime, sleutel. Bij asymmetrische encryptie wordt gebruik gemaakt van een sleutelpaar. De ene sleutel, de private sleutel, is slechts bekend bij de eindgebruiker van deze sleutel en moet strikt geheim worden gehouden. De andere, de publieke sleutel, wordt verspreid

onder communicatiepartners. Wat met de private sleutel is vercijferd, kan alleen met de bijbehorende publieke sleutel worden ontcijferd, en omgekeerd.**Elektronische Opslagplaats**: locatie waar relevante informatie ten aanzien van de dienstverlening van QuoVadis is te vinden. Zie: *https://www.quovadisglobal.nl*

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.

European Electronic Signature Standardization Initiative – EESSI Een workshop op Europees niveau met als taak het vormgeven van de concretisering via standaardisatieafspraken van de Europese Richtlijn 1999/93/EG voor elektronische handtekeningen.

European Telecommunications Standards Institute – ETSI Een organisatie die verantwoordelijk is voor het bepalen van standaarden en normen op telecommunicatiegebied die geldig zijn voor geheel Europa.

Europese Richtlijn In het kader van PKI wordt hiermee bedoeld het document 1999/93/EG van het Europees parlement en de Raad, d.d.13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (Publicatieblad nr.L013 d.d. 19/01/2000, p.12-20).

Evaluation Assurance Level – EAL: Een pakket bestaande uit betrouwbaarheidscomponenten uit ISO/IEC 15408 Deel 3 die een punt vertegenwoordigen op de betrouwbaarheidsschaal zoals die is gedefinieerd in de Common Criteria.

Extended Normalized Certificate Policy – NCP+: Een Certificate Policy voor niet-gekwalificeerde certificaten die hetzelfde kwaliteitsniveau geeft als voor gekwalificeerde certificaten geldt (in de QCP), maar buiten de werking van de Europese Richtlijn. Deze wordt gebruikt in situaties waar het gebruik van een SUD nodig wordt geacht.

Federal Information Processing Standard – FIPS: Een officiële standaard voor de Verenigde Staten en uitgegeven door de NIST. In het kader van PKI zijn vooral FIPS 140 (“Security Requirements for Cryptographic Modules”) en FIPS 186-2 (“Digital Signature Standard”) van belang.

Geavanceerde Elektronische Handtekening: een Elektronische Handtekening die voldoet aan de volgende eisen:
a) Zij is op unieke wijze aan de ondertekenaar verbonden;
b) Zij maakt het mogelijk de ondertekenaar te identificeren;
c) Zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
d) Zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;

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

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

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

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

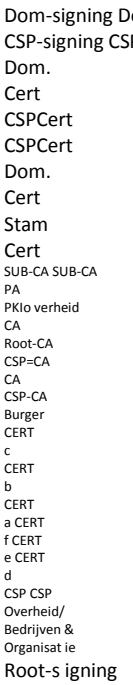
Groepscertificaat: een op een SUD opgeslagen combinatie van twee Niet-Gekwalificeerde Certificaten die tezamen de functies van vertrouwelijkheid en authenticiteit ondersteunen en die voldoen aan de volgende vereisten:
1) Ze zijn uitgegeven aan een dienst of een functie door QuoVadis, en
2) Ze zijn uitgegeven op basis van de binnen de PKI voor de Overheid geldende 'Certificate Policy Services' (PvE deel 3b)

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

Hashfunctie: Een functie die een bericht van willekeurige lengte omzet in een reeks met een vaste lengte en voldoet aan de volgende voorwaarden:
- Het is praktisch onuitvoerbaar om voor een gegeven uitvoer een invoer te vinden die deze uitvoer als resultaat heeft ("one-way");
- Het is praktisch onuitvoerbaar om voor een gegeven invoer een tweede invoer te vinden die dezelfde uitvoer als resultaat heeft ("zwak collision-free");
- Het is praktisch onuitvoerbaar om twee willekeurige berichten te vinden die dezelfde uitvoer als resultaat hebben ("sterk collision-free").

Hashwaarde: Het resultaat (uitvoer) van een hashfunctie. De hashwaarde wordt ook wel "message digest" genoemd.

Hiërarchisch model: De PKI voor de overheid gaat uit van een hiërarchisch model. Dat betekent dat het vertrouwen in een keten doorgegeven wordt. Een eindgebruiker kan daarmee alle Certification Authorities vertrouwen die onder dezelfde stam-CA vallen.



Identificatie
Het vaststellen van de identiteit van een persoon (of zaak).

Identiteit en Authenticiteit Certificaat: Zie "*Authenticiteitcertificaat*".

Identiteitcertificaat
Zie "*Authenticiteitcertificaat*".

Incident: Een gebeurtenis die geen onderdeel uitmaakt van de standaardwerking van een dienst en die een onderbreking van, of een reductie in, de kwaliteit van die dienst veroorzaakt of kan veroorzaken.

Integriteit: De zekerheid dat gegevens volledig zijn en niet zijn gewijzigd, ongeacht of dat opzettelijk, niet opzettelijk door menselijk toedoen of anderszins is gebeurd.

Internet Engineering Task Force – IETF: Een internationale organisatie die zich in wil zetten voor de ontwikkeling van de internet architectuur vanuit technisch-wetenschappelijk oogpunt.

Lightweight Directory Access Protocol – LDAP: Een open protocol dat applicaties in staat stelt om informatie uit directories te verkrijgen, zoals bijvoorbeeld e-mail adressen en sleutels.

Lokale Registratie Autoriteit (LRA): de organisatie-eenheid of functie aan wie de uitvoering van de taak van Registratie Autoriteit is opgedragen en die fysiek de identificatie gegevens van een aanvrager verzamelt, controleert, registreert en doorstuurt ten behoeve van de Certificaat uitgifte.

Middel voor het vervaardigen van handtekeningen: zie Signature Creation Device.

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

Non-repudiation (NL: Onloochenbaarheid, Onweerlegbaarheid): De eigenschap van een bericht om aan te tonen dat bepaalde gebeurtenissen of handelingen hebben plaatsgevonden, zoals het verzenden en ontvangen van elektronische documenten. Binnen de PKI voor de overheid wordt non-repudiation (van de inhoud van een bericht) bewezen door middel van het handtekeningcertificaat.

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

Ondertekenaar (E: Signatory): (Voor de toepassing van de Telecommunicatiewet*) Degene die een middel voor het aanmaken van elektronische handtekeningen als bedoeld in artikel 1.1, onderdeel uu Telecommunicatiewet gebruikt.* [Wet EH]
In het kader van de PKI voor de overheid wordt onder de certificaathouder van het handtekeningcertificaat de ondertekenaar verstaan en wordt de term 'ondertekenaar' zelf niet gehanteerd.

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

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

Overheids-CA: een CA die binnen de hiërarchie van de PKI voor de overheid 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.

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

Overheid/Bedrijven en Organisatie: Binnen de PKI voor de overheid bestaan de domeinen Overheid/Bedrijven en Organisatie uit alle organisaties binnen overheid en bedrijfsleven.

Persoonlijk Certificaat: een op een SSCD opgeslagen combinatie van twee Niet-Gekwalificeerde Certificaten die tezamen de functies van authenticiteit en vertrouwelijkheid ondersteunen, alsmede een Gekwalificeerd Certificaat dat de functie van onweerlegbaarheid ondersteunt, en die voldoen aan de volgende vereisten:
1) Ze zijn uitgegeven aan een natuurlijke persoon door QuoVadis, en
2) Ze zijn uitgegeven op basis van de binnen de PKI voor de Overheid geldende 'Certificate Policy Domein Overheid en Bedrijven" (PvE deel 3a).

PKI voor de overheid: 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 PKI voor de Overheid door QuoVadis uitgegeven Persoonlijk Certificaat, Servercertificaat of Groepscertificaat .

PKI voor de overheid: de Public Key Infrastructure van de Staat der Nederlanden.

Policy Authority PKIoverheid – PA PKIoverheid: De Policy Authority (PA) voor de hiërarchie van de PKI voor de overheid. De PA ondersteunt de minister van Binnenlandse Zaken en Koninkrijksrelaties bij het beheer over de PKI voor de overheid. De dienstverlening van de PA is onder te verdelen in het beheren van de bovenste lagen van de infrastructuur, het toelaten van CSP's tot de infrastructuur en het houden van toezicht op de betrouwbaarheid van de PKI voor de overheid. Zie ook het plaatje bij "*Hiërarchisch model*".

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

Private key: zie Private Sleutel.

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

Public key: zie Publieke Sleutel.

Public key cryptografie Het systeem waarbij een mechanisme van publieke sleutels en private sleutels wordt gebruikt. Dit houdt in dat er twee sleutels worden gebruikt. Eén

sleutel wordt geheim gehouden (de private sleutel) en de andere sleutel mag publiekelijk worden verspreid (de publieke sleutel). Alles wat met de publieke sleutel vercijferd wordt is alleen met de private sleutel te ontcijferen en andersom. Het is een vorm van asymmetrische encryptie.

Public Key Cryptography Standard – PKCS: Een standaard op het gebied van public key cryptografie, ontwikkeld door RSA-laboratories. In het kader van de PKI voor de overheid zijn vooral PKCS#7 (Cryptographic Message Syntax Standard), PKCS#11 (Cryptographic Token Interface Standard), PKCS#12 (Personal Information Exchange Syntax Standard) en PKCS#15 (Cryptographic Token Information Format Standard) van belang.

Public Key Infrastructure – PKI: Een samenstelling van architectuur, techniek, organisatie, procedures en regels, gebaseerd op public key cryptografie. Het doel is het hiermee mogelijk maken van betrouwbare elektronische communicatie en betrouwbare elektronische dienstverlening.

Publieke sleutel (E: Public key): 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. Ook wordt de term “openbare sleutel” (Onder andere in de Europese Richtlijn) gebruikt. In de wet EH wordt echter “publieke sleutel” gebruikt. Beide zijn bedoeld als vertaling van de Engelstalige term “public key”.

Qualified Certificate Policy (QCP): Een Certificate Policy die een uitwerking van de vereisten bevat die zijn omschreven in artikel 18.15, eerste en tweede lid van de Telecommunicatiewet.

Regeling elektronische handtekeningen: De regeling die gelijktijdig met de wet EH van kracht is geworden. De regeling geeft nadere regels met betrekking tot elektronische handtekeningen, zoals technische en organisatorische uitwerking van gestelde eisen. Nr. WJZ/03/02263.

Registratie Autoriteit (RA): een Registratie Autoriteit zorgt voor de verwerking van Certificaataanvragen en alle daarbij behorende taken waarbij de verificatie van de identiteit van de Certificaathouder de belangrijkste is. In dit verband opereert QuoVadis als RA.

Request for Comments – RFC: Een voorstel voor een standaard afkomstig van de IETF. Hoewel een RFC niet de formele status van een standaard heeft, worden in praktijk de RFC’s normaliter gevolgd.

Revocation management service: Een dienst die verzoeken, die te maken hebben met intrekking van certificaten, behandelt en rapporteert, om zo de te nemen maatregelen te bepalen. De resultaten worden verspreid door middel van de Revocation Status Service.

Revocation service: Een dienst van een CSP waarbij deze certificaten intrekt bij beëindiging van de overeenkomst, constatering van fouten in het certificaat of bij compromittatie van de private sleutel die hoort bij de in het certificaat opgenomen publieke sleutel. De ingetrokken certificaten worden opgenomen in de Certificate Revocation List.

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 Certificatie Autoriteit 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.

Rivest-Shamir-Adleman algoritme – RSA-algoritme: Een cryptografische methode die gebruik maakt van een tweeledige sleutel. De private sleutel wordt bewaard door de eigenaar; de publieke sleutel wordt gepubliceerd. Data wordt vercijferd met de publieke sleutel van de ontvanger en kan alleen ontcijferd worden met de private sleutel van de ontvanger. Het RSA-algoritme is rekenintensief, waardoor het vaak wordt gebruikt om een digitale envelop te maken, die een met RSA vercijferde DES sleutel bevat en met DES vercijferde data.

Root-signing Het ondertekenen van het certificaat van de Root-CA – het stamcertificaat – door de Root- CA zelf. Zie ook het plaatje bij "*Hiërarchisch model*".

Secure Hash Algorithm – SHA: Een bepaald algoritme dat een concrete invulling geeft voor een Hashfunctie. Het nog veel gebruikte SHA-1 is ontwikkeld door de Amerikaanse overheid en maakt een Message Digest van 160 bits aan. De Advanced Encryption Standard en SHA-2 zijn opvolgers hiervan.

Secure Signature Creation Device (SSCD): een middel voor het aanmaken van Elektronische Handtekeningen dat voldoet aan de eisen gesteld krachtens artikel 18.17, eerste lid van de Telecommunicatiewet. Dit kan bijvoorbeeld een smartcard of een USB token zijn.

Secure User Device (SUD): Een middel dat de gebruikers private sleutel(s) bevat, deze sleutel(s) tegen compromittatie beschermt en elektronische ondertekening, authenticatie of ontcijfering uitvoert namens de gebruiker.

Servercertificaat: een binnen de Veilige Omgeving van de Abonnee opgeslagen combinatie van twee Niet-Gekwalificeerde Certificaten die tezamen de functies van authenticiteit en vertrouwelijkheid ondersteunen en die voldoen aan de volgende vereisten:

1) Ze zijn door QuoVadis uitgegeven aan een server, en
2) Ze zijn uitgegeven op basis van de binnen de PKI voor de Overheid geldende 'Certificate Policy Services' (PvE deel 3b).

Services Certificaat: een Servercertificaat of een Groepscertificaat .

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

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

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

Secure Sockets Layer – SSL: Een protocol gecreëerd door Netscape voor het beheer van de veiligheid van bericht verzendingen in een netwerk en de toegang tot web servers. Het woord sockets verwijst hierbij naar de methode om data heen en weer tussen een client en een server programma te sturen in een netwerk of tussen programmalagen in dezelfde computer.

Security policy: De verzameling van regels, neergelegd door de beveiligingsautoriteit, die het gebruik van en de maatregelen ten aanzien van beveiligingsdiensten en faciliteiten regelen.

Self-signed certificaat: Een certificaat voor een Certification Authority, getekend door die Certification Authority zelf. Dit kan alleen bij het stamcertificaat van een hiërarchie.

Services certificaat: Een certificaat waarmee een dienst, functie of apparaat, bijvoorbeeld een server, wordt gekoppeld aan een rechtspersoon of andere organisatie. In het geval van een server wordt het certificaat aangeboden aan een browser, die toegang zoekt tot de server. Hierdoor kan deze vertrouwende partij zekerheid krijgen omtrent de identiteit van de eigenaar van de server. Een services certificaat is geen gekwalificeerd certificaat.

Sessiesleutel: Een symmetrische sleutel die één keer wordt gebruikt voor een berichtenuitwisseling of een telefoongesprek (een sessie). Na afloop van de berichtenuitwisseling of het telefoongesprek wordt de sleutel weggegooid.

Signing key (NL: Tekensleutel): De private sleutel die wordt gebruikt om een elektronische handtekening te zetten. Er kan onderscheid worden gemaakt tussen een signing key van een Certification Authority en een signing key van een eindgebruiker. Met de signing key van de eindgebruiker plaatst deze diens elektronische handtekening. Met de signing key van de Certification Authority worden onder andere de uitgegeven certificaten getekend en wordt de Certificate Revocation List getekend.

Sleutelpaar: In een asymmetrisch cryptografische systeem is dit een private sleutel en zijn wiskundig verbonden publieke sleutel. Deze hebben de eigenschap dat met behulp van de publieke sleutel een elektronische handtekening kan worden geverifieerd die met een private sleutel is gemaakt. In het geval van encryptie betekent deze eigenschap dat informatie die met de publieke sleutel is vercijferd met behulp van de private sleutel kan worden ontcijferd (of andersom).

Smartcard: Een plastic kaart ter grootte van een creditcard die in een chip elektronica bevat, inclusief een microprocessor, geheugenruimte en een voedingsbron. De kaarten kunnen worden gebruikt om informatie op te slaan en zijn makkelijk mee te nemen. In de toekomst zal de elektronische Nederlandse Identiteitskaart (eNIK) een smartcard zijn.

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

Subordinate CA – Sub CA: Een Certification Authority welk onderdeel is van een Certificatiedienstverlener of die onder verantwoordelijkheid van de Certificatiedienstverlener handelt. Bij de PKI voor de overheid wordt het certificaat van de Sub CA getekend met de signing key van de CSP Certification Authority. Zie verder "*Certification Authority*" en zie ook het plaatje bij "*Hiërarchisch model*".

Token: Een beveiligd stukje hard- of software waarin de private sleutels van de eindgebruiker opgeslagen worden. Een hardware token kan ook cryptografische berekeningen uitvoeren. Voorbeelden van hardware tokens zijn een smartcard en een USB-token.

USB-token: Een USB-token is een token vergelijkbaar met een smartcard, maar heeft een andere vorm. Het is een medium om certificaten op te slaan. Het verschil is dat voor een USB-token geen extra smartcardreader hoeft te worden geïnstalleerd. Daarentegen is het niet mogelijk om eindgebruikerkenmerken op de USB-token op de nemen, zoals een foto of persoonsgegevens.

Validity data (NL: Geldigheidsgegevens): Aanvullende gegevens, verzameld door de ondertekenaar en/of de controlerende partij, benodigd om de juistheid en geldigheid van een elektronische handtekening te controleren om zo aan de vereisten van de Certificate Policy te voldoen.

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

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

Vertrouwelijkheid: De garantie dat gegevens daadwerkelijk en uitsluitend terechtkomen bij degene voor wie zij zijn bedoeld, zonder dat iemand anders ze kan ontcijferen. Buiten de private sector wordt hiervoor ook wel de term “exclusiviteit” gebruikt.

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.

Afkortingen

Afkorting	Betekenis
CA	Certificatie Autoriteit (Certification Authority)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificaten Revocatie Lijst
CSP	Certification Service Provider ofwel certificatiedienstverlener
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunication Standardisation Institute
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
LDAP	Lightweight Directory Access Protocol
LRA	Lokale Registratie Autoriteit
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OPTA	Onafhankelijke Post- en Telecommunicatie Autoriteit
PIN	Persoonlijk Identificatie Nummer
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PUK	Persoonlijk Unlock Kengetal
RA	Registratie Autoriteit (Registration Authority)
SSCD	Secure Signature Creation Device
SUD	Secure User Device
VPN	Virtual Private Network
WBP	Wet Bescherming Persoonsgegevens
WID	Wet op de Identificatieplicht