Inhoud

1.1.2 Status

QuoVadis heeft de grootst mogelijke aandacht en zorg besteed aan de gegevens en informatie, die zijn opgenomen in deze CPS. Desalniettemin is het mogelijk dat onjuistheden en onvolkomenheden voorkomen. QuoVadis aanvaardt geen enkele aansprakelijkheid voor schade als gevolg van deze onjuistheden of onvolkomenheden, noch voor schade die wordt veroorzaakt door het gebruik of de verspreiding van deze CPS, indien deze CPS wordt gebruikt buiten het in paragraaf 1.4 van deze CPS beschreven certificaatgebruik.

1.2 Verwijzingen naar de CPS

Elke CP wordt uniek geïdentificeerd door een OID, conform het onderstaande schema.

Domein Organisatie (G2) / Organisatie Services (G3):

OID	CP
2.16.528.1.1003.1.2.5.6	voor het servercertificaat binnen het domein Organisatie, dat de publieke sleutel bevat ten behoeve van authenticiteit & vertrouwelijkheid. Deze OID is als volgt opgebouwd: {joint-iso-itu-t (2). country (16). nederland (528). Nederlandse organisatie (1). nederlandse-overheid (1003). pki voor de overheid (1). cp (2). domein Organisatie (5). server (6)De volgende OID is geregistreerd door PKIoverheid voor opname in alle QuoVadis PKI Overheid Organisatie certificaten:

QuoVadis.CSP.PKIOverheid.ca.g2	policy OID	2.16.528.1.1003.1.3.5.2.1
QuoVadis.CSP.PKIOverheid.ca.g3	policy OID	2.16.528.1.1003.1.3.5.2.1

Voor verdere details zie de tabel in sectie 7.1

1.3 Gebruikersgemeenschap

De gebruikersgemeenschap bestaat uit in Nederland gevestigde abonnees, die organisatorische entiteiten binnen overheid en bedrijfsleven zijn (zie CPS 3.2.2-pkio14) en uit certificaathouders, die bij deze abonnees behoren. Daarnaast zijn er vertrouwende partijen, die handelen in vertrouwen op certificaten van de betreffende certificaathouders.

1.3.1 Partijen binnen de gebruikersgemeenschap

1.3.1.1 Centrale Infrastructuur PKIoverheid

De centrale infrastructuur van de PKI voor de overheid wordt namens de Staat der Nederlanden beheerd door Logius en bestaat per root CA uit de volgende componenten:

Staat der Nederlanden Root CA G2

Staat der Nederlanden Domein Certification Authority – Organisaties G2

Staat der Nederlanden Root CA G3

Staat der Nederlanden Domein Certification Authority – Organisatie Services G3

1.3.1.2 QuoVadis TSP PKI Overheid Organisatie Certification Authority (TSP-PKI Overheid Organisatie CA)

De QuoVadis CSP-PKI Overheid CA's worden 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 R3(e)6(n)6suAo(p)-3(g)6(e)-3(n)-3(o 1 56.04 37 0 1 a5t5072(utET TJETQq0.00000e)5(n)6

contracterende partij is. Binnen de Certificate Policy Extended Validation wordt de volgende invulling aan de term certificaathouder gegeven: ”een apparaat of een systeem (een niet-natuurlijke persoon), bediend door of namens een organisatorische entiteit.”

In deze CPS gebruiken we de naam "service" voor dergelijke certificaathouders. Voor het uitvoeren van de handelingen ten aanzien van de levensloop van het certificaat van de certificaathouder is tussenkomst door een andere partij dan de certificaathouder vereist. De abonnee is hiervoor verantwoordelijk en dient een certificaatbeheerder aan te wijzen om deze handelingen te verrichten.

1.3.3.3 Certificaatbeheerder

Een certificaatbeheerder is een natuurlijke persoon die namens de abonnee handelingen uitvoert ten aanzien van het certificaat van de certificaathouder. De abonnee geeft de certificaatbeheerder opdracht de betreffende handelingen uit te voeren en legt dit vast in een bewijs van certificaatbeheer.

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.

1.3.3.4 Vertrouwende Partijen

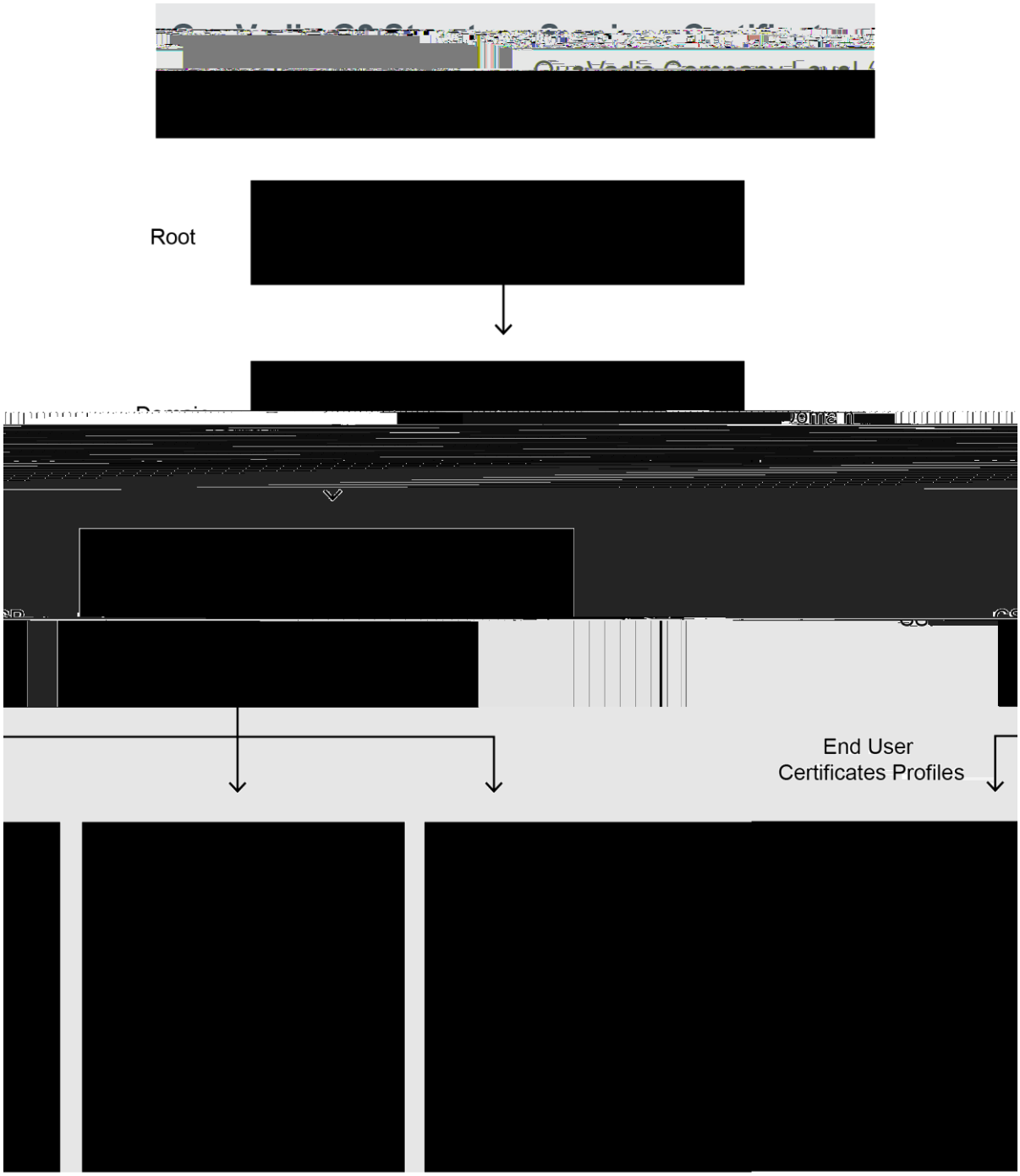
Een vertrouwende partij is iedere natuurlijke of rechtspersoon die ontvanger is van een certificaat en die handelt in vertrouwen op dat certificaat. Anders dan bij persoonsgebonden certificaten ontlenen vertrouwende partijen vooral zekerheid aan de verbondenheid van een service (apparaat of functie) met de organisatorische entiteit waartoe de service behoort. De CP Extended Validation legt derhalve de nadruk op het bieden van zekerheid over de verbondenheid van een door een apparaat, systeem of functie verzonden bericht of geleverde webdienst met de betreffende organisatie. Het vaststellen van de identiteit van de certificaathouder (apparaat of functie) is in dit licht gezien minder van belang dan het vaststellen van diens verbondenheid met de organisatorische entiteit.E te verrichten.

1.4 Certificaatgebruik

Het gebruik van certificaten uitgegeven onder deze CPS heeft betrekking op communicatie van certificaathouders die handelen namens de abonnee.

[OID 2.16.528.1.1003.1.2.5.6] Servercertificatenan b a.1.2.04 442sv-3(t)-3(kv)9(a)-3(n7i(e)-3(rtr)4(o)-3(u

De CA-structuur en de typen certificaten die QuoVadis uitgeeft zijn inzichtelijk gemaakt in onderstaande figuur 1.



Figuur1: Overzicht van de certificaat policies onder G2

Figuur2: Overzicht van de certificaat policies onder G3

2.2.4 Conformatie

QuoVadis conformeert zich aan de huidige versie van de CA/Browser Forum Guidelines for Issuance and Management of Exteded Validation Certificates zoals gepubliceerd op http://www.cabforum.org. Mocht er een inconsistentie aanwezig zijn tussen het PKIoverheid

of de abonnee een bestaande en legale organisatie is;

of de organisatienaam, die in het certificaat wordt opgenomen, juist en volledig is en overeenkomt met de door de abonnee aangemelde organisatienaam;

of het door de abonnee opgegeven adres van de organisatie juist en volledig is en dat het ook het adres is waar zij haar werkzaamheden uitvoert;

of het door de abonnee opgegeven algemene telefoonnummer van de organisatie, juist en volledig is;

of, als blijkt dat de organisatie van de abonnee korter dan drie jaar bestaat, de abonnee beschikt over een actieve betaalrekening;

mogen niet ouder zijn dan 13 maanden anders moeten de gegevens opnieuw worden opgevraagd en geverifieerd. In die gevallen waarbij de informatiebronnen de laatste 13 maanden niet zijn bij gewerkt c.q. aangepast moet worden uitgegaan van de meest recente versie.

3.2.1 Methode om bezit van private sleutel aan te tonen.

QuoVadis waarborgt dat de abonnee het certificate signing request (CSR) op een veilige manier aanlevert.

Het op een veilige manier aanleveren moet als volgt plaatsvinden:

het invoeren van het CSR op de daartoe speciaal ontwikkelde applicatie TrustLink Enterprise (TLE) van QuoVadis waarbij gebruik wordt gemaakt van een SSL verbinding, die gebruikt maakt van een PKIoverheid SSL certificaat of gelijkwaardig of;

het invoeren van het CSR op de HTTPS website van de QuoVadis die gebruikt maakt van een PKIoverheid SSL certificaat of gelijkwaardig of;

het via e-mail verzenden van het CSR voorzien van een gekwalificeerde elektronische handtekening van de certificaatbeheerder die gebruik maakt van een PKIoverheid gekwalificeerd certificaat of gelijkwaardig of;

het invoeren of verzenden van een CSR op een wijze minimaal gelijkwaardig aan bovenstaande manieren.

3.2.2 Authenticatie van de organisatorische eenheid

3.2.2.1

Voor privaatrechtelijke organisaties met en zonder rechtspersoonlijkheid een recent gewaarmerkt uittreksel (maximaal 1 maand oud) uit het Handelsregister van de Kamer van Koophandel.

Als het adres in de bewijsstukken overeenkomt met het adres van de aanvraag zal QuoVadis dit als voldoende bewijs beschouwen dat dit ook het adres is waar de organisatie haar werkzaamheden uitvoert.

Als het adres in de bewijsstukken niet overeenkomt dan zal QuoVadis de opgegeven locatie van de abonnee bezoeken en haar bevindingen vastleggen in een rapportage. In de rapportage moeten minimaal de volgende zaken zijn opgenomen:

Of het adres van de locatie van de abonnee exact overeenkomt met het adres van de aanvraag;

Het type huisvesting van de abonnee en of dit de locatie is waar de organisatie naar alle waarschijnlijk haar werkzaamheden uitvoert;

Of er permanente bewijzeringsborden aanwezig zijn die de locatie van de abonnee identificeren;

Een of meerdere foto’s van (i) de buitenkant van de huisvesting van de abonnee (waarop, indien aanwezig, de bewijzeringsborden en het adresbord van de straat staan) en (ii) de receptiebalie of kantoorwerkruimte van de abonnee.

de identiteit dient te worden gecontroleerd aan de hand van fysieke verschijning van de persoon zelf.

Deze controle moet na elke 13 maanden opnieuw plaats vinden tenzij in de overeenkomst met de abonnee uitdrukkelijk hiervan wordt afgeweken door b.v. op te nemen dat de certificaatbeheerder zijn of haar rol behoudt tot het moment dat dit door de abonnee wordt herzien of tot het moment dat de overeenkomst verloopt of wordt beëindigd. In het aanstelings formulier voor de certificaatbeheerder is bovenstaande afwijking door QuoVadis standaard opgenomen.

3.2.3.3 Verbijzondering verificatie identiteit certificaatbeheerder

Ter verbijzondering van het in 3.2.3-2 gestelde, geldt dat de identiteit van de certificaatbeheerder slechts kan worden vastgesteld met de bij artikel 1 van de Wet op de identificatieplicht aangewezen geldige documenten. QuoVadis zal de geldigheid en echtheid hiervan te controleren.

3.2.3.4 Verificatie certificaatbeheerder

De certificaatbeheerder is een persoon van wie de identiteit dient vastgesteld te worden in samenhang met een organisatorische entiteit.

Er dient bewijs aan QuoVadis te worden overlegd van:

- volledige naam, met inbegrip van achternaam, eerste voornaam, initialen of overige voorna(a)m(en) (indien van toepassing) en tussenvoegsels (indien van toepassing);
- geboortedatum en -plaats, een nationaal passend registratienummer, of andere eigenschappen van de certificaatbeheerder die kunnen worden gebruikt om, voor zover mogelijk, de persoon van andere personen met dezelfde naam te kunnen onderscheiden;
- bewijs dat de certificaatbeheerder gerechtigd is voor een certificaathouder een certificaat te ontvangen namens de rechtspersoon of andere organisatorische entiteit.

Dit bewijs mag niet ouder zijn dan 13 maanden anders moeten de gegevens opnieuw worden opgevraagd en geverifieerd tenzij in de overeenkomst met de abonnee uitdrukkelijk wordt vastgelegd dat de certificaatbeheerder zijn of haar autorisatie behoudt tot het moment dat dit door de abonnee wordt herzien of tot het moment dat de overeenkomst verloopt of wordt beëindigd. In het aanstelings formulier voor de certificaatbeheerder is bovenstaande afwijking door QuoVadis standaard opgenomen.

3.2.5 Authorisatie van de certificaathouder (Service)

3.2.5.1 Controle authorisatie certificaathouder (Service)

QuoVadis zal controleren dat :

Voor elke FQDN die is vermeld in een certificaat, bevestigt QuoVadis dat, vanaf de datum waarop het certificaat is uitgegeven, de aanvrager ofwel de domeinnaamregistrant is of controle over de FQDN heeft door:

1. Rechtstreeks te

7. Bevestiging van de controle van de aanvrager over het IP-adres door de procedure gedocumenteerd voor een "tls-alpn-01”-challenge uit te voeren zoals omschreven in draft 04 van "ACME IP Identifier Validation Extension", beschikbaar op https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4, uitgevoerd in overeenstemming met BR Sectie 3.2.2.5.7.

4 Operationele eisen

4.1 Certificaataanvraag

4.1.1 Voorwaarden overeenkomst

QuoVadis zal, voorafgaand aan de uitgifte van een EV SSL certificaat, een overeenkomst af sluiten met de abonnee en een, door de certificaatbeheerder ondertekende, certificaataanvraag te ontvangen.

De overeenkomst voldoet tenminste aan de volgende voorwaarden:

de overeenkomst moet ondertekend worden door de Bevoegde Vertegenwoordiger of

I. voor digitale certificaten waarvoor een certificaat transparantie pre-certificaat is aangemaakt en ingelogd ten minste twee publieke logboeken en voor welke CAA is gecontroleerd
II. Als de CA of een geaffilieerde van de CA de DNS-operator (zoals gedefinieerd in RFC 7719) van het domein DNS is.

QuoVadis behandelt een record lookup failure als toestemming om uit te geven als:

I. het falen valt buiten de infrastructuur van de CA;
II. de opzoeking minstens één keer is herhaald; en
III. de zone van het domein heeft geen DNSSEC-

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

Hetgeen bepaald is in dit CPS

QuoVadis bepaald dat het certificaat niet is uitgegeven in overeenstemming met de CP of het bijbehorende CPS van QuoVadis of de overeenkomst die QuoVadis met de abonnee heeft gesloten;

QuoVadis bepaald dat informatie in het certificaat niet juist of misleidend is;

QuoVadis haar werkzaamheden staakt en de CRL en OCSP dienstverlening niet wordt overgenomen door een andere TSP;

de abonnee een “code signing” certificaat gebruikt om “hostile code” (waaronder spyware, malware, trojans etc.) digitaal te ondertekenen.

De PA van PKIoverheid vaststelt dat de technische inhoud van het certificaat een onverantwoord risico met zich meebrengt voor abonnees, vertrouwende partijen en derden (b.v. browserpartijen).).

Daarnaast kunnen certificaten worden ingetrokken als maatregel om een calamiteit te voorkomen, c.q. te bestrijden. Als calamiteit wordt zeker de aantasting of vermeende aantasting van de private sleutel van QuoVadis waarmee certificaten worden ondertekend, beschouwd.

De globale reden van intrekking wordt door QuoVadis vastgelegd.

4.9.2.1 Wie mag een verzoek tot intrekking doen

De volgende partijen mogen een verzoek tot intrekking van een eindgebruikercertificaat doen:

De Certificaatbeheerder

De Abonnee

QuoVadis als TSP

ieder andere, naar het oordeel van QuoVadis, belanghebbende partij/persoon.

4.9.3.1 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 4.9.1.1 zich voordoet.

De abonnee of de Certificaatbeheerder kan zich persoonlijk wenden tot de Registration Authority of kan een intrekkingverzoek telefonisch indienen via de QuoVadis supportlijn. De abonnee en de Certificaatbeheerder kunnen hi(ia)-3(d)-W* nBc93.37 Tm0.9t84>BDC q77 Tm0.282 0.337

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 PKIoverheid CA omgeving een certificaat laten intrekken.

4.9.3.2 Beschikbaarheid intrekking management service

De maximale tijdsduur, waarbinnen de beschikbaarheid van de revocation management services hersteld moet zijn, is gesteld op vier uur.

4.9.3.3 Vastlegging reden van intrekking

QuoVadis zal de beweegreden voor de intrekking van een certificaat vastleggen, indien de intrekking geïnitieerd is door QuoVadis.

4.9.3.4 Certificaat status informatie

QuoVadis maakt gebruik van een OCSP en een CRL om de certificaatstatus informatie beschikbaar te stellen.

4.9.3.5 Beschikbaarheid intrekking management service

De intrekking management services is 24 uur per dag, 7 dagen per week beschikbaar d.m.v. de webapplicatie TrustLink Enterprise. (https://tl.quovadisglobal.com)

4.9.3.6 Geldigheid CRL

De geldigheid van een CRL is maximaal 72 uur en wordt elke 12 uur gegenereerd.

4.9.3.6 Issuing subordinatie CA

Als er sprake is van een issuing subordinate CA onder de QuoVadis CA dan:

maakt QuoVadis gebruik van een OCSP en een CRL om de certificaatstatus informatie, met betrekking tot de issuing subordinate CA, beschikbaar te stellen;

legt QuoVadis de beweegreden voor de intrekking van het issuing subordinate CA certificaat vast;

is de geldigheid van de CRL, met betrekking tot de certificaatstatus informatie van het issuing subordinate CA, is maximaal 7 dagen

4.9.5.1 Tijdsduur voor verwerking intrekkingsverzoek

De maximale tijdsduur tussen de ontvangst van een intrekkingsverzoek of intrekkingsrapportage en de wijziging van de revocation status information, die voor alle vertrouwende partijen beschikbaar is, is gesteld op vier uur.

Deze tijdsduur is van toepassing op alle typen certificaat statusinformatie (CRL en OCSP)

4.9.5.2 Tijdsduur voor verwerking intrekkingsverzoek in het geval van een issuing subordinate CA

5

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 Afvalverwerking

Papieren documenten en magnetische media welke vertrouwelijke QuoVadis of commercieel gevoelige inf(tie)Qq0.0000n t(e)-rS1-3(in)6s.0000n t(e)-rS1-3(in)6s.0000n t(e)-rS1-3(in)6s.0000n t(e)o5

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.

5.2.4.3. Identificatie en authentificatie voor elke rol

Elk individu dat een van de vertrouwelijke rollen vervult, ge

5.3.2 Procedures achtergrondcontrole

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

- Werkervaring en professionele referenties

Database activiteiten en events;

Transacties;

Operating systemen;

Access control systemen;

Mail servers.

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.

CA key life cycle management;

Certificate life cycle management;

Succesvolle en niet succesvolle aanvallen PKI systeem;

Activiteiten van medewerkers op het PKI systeem;

Lezen, schrijven en verwijderen van gegevens;

Profiel wijzigingen (Access Management);

Systeem uitval, hardware uitval en andere abnormaliteiten;

Firewall en router activiteiten;

Betreden van- en vertrekken uit de ruimte van de CA

De log bestanden registreren minimaal het volgende:

Bron adressen (IP adressen indien voorhanden);

Doel adressen (IP adressen indien voorhanden);

Tijd en datum;

Gebruikers ID's (indien voorhanden);

Naam van de gebeurtenis;

Beschrijving van de gebeurtenis

Alle loggings zullen van een timestamp worden voorzien en de integriteit van de logbestanden is gewaarborgd. Op basis van een risicoanalyse bepaalt QuoVadis zelf welke gegevens zij opslaat.

5.4.2 Frequentie van verificatie audit logs

De audit logs worden minstens maandelijks geverifieerd en geconsolideerd.

5.4.3 Bewaartermijn van audit logs

Logbestanden voor gebeurtenissen met betrekking tot: CA key life cycle management en; Certificate life cycle management; 7 jaar bewaard en daarna verwijderd.

Logbestanden voor gebeurtenissen met betrekking tot: Bedreigingen en risico's; worden 18 maanden bewaard en daarna verwijderd.

De logbestanden worden zodanig opgeslagen, dat de integriteit en toegankelijkheid van de data gewaarborgd is.

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 PKIoverheid CA's voeren 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 PKIoverheid CA's en de Registration Authority-omgeving.

5.4.6 Audit Logging

Het beveiligde logproces van de QuoVadis PKIoverheid CA'sverloopt 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 PKIoverheid CA'somgeving, 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.

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

5.7.4.1 Continuïteit van de bedrijfsvoering na calamiteit

QuoVadis heeft een business continuity plan (BCP) opgesteld voor minimaal de kerndiensten ‘dissemination service’, ‘revocation management service’ en ‘revocation status service’ met als doel, in het geval zich een security breach of calamiteit voordoet, het informeren en redelijkerwijs beschermen en continueren van QuoVadis haar dienstverlening ten behoeve van abonnees, vertrouwende partijen en derden (waaronder browserpartijen). QuioVadis zal het BCP jaarlijks testen, beoordelen en actualiseren. Het BCP moet in ieder geval de volgende zaken beschrijven:

Eisen aan inwerkingtreding;

Noodprocedure / uitwijkprocedure;

Eisen aan herstarten TSP dienstverlening;

Onderhoudsschema en testplan dat voorziet in het jaarlijks testen, beoordelen en actualiseren van het BCP;

Bepalingen over het onder de aandacht brengen van het belang van business continuity;

Taken, verantwoordelijkheden en bevoegdheden van betrokken actoren;

Beoogde hersteltijd c.q. Recovery Time Objective (RTO);

Vastleggen van de frequentie van back-ups van kritische bedrijfsinformatie en software;

Vastleggen van de afstand van de uitwijkfaciliteit tot de hoofdvestiging van de TSP; en

Vastleggen van procedures voor het beveiligen van de faciliteit gedurende de periode na een security breach of calamiteit en voor de inrichting van een beveiligde omgeving bij de hoofdvestiging of de uitwijkfaciliteit.

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

multi-person control) zorgt ervoor dat niet één enkel persoon de totale controle kan voeren over een kritiek component binnen de infrastructuur.

6.2.3.1 Escrow van de private sleutel

QuoVadis geeft haar sleutels niet in escrow uit.

6.2.4 Private sleutel back-up

De Private Sleutel wordt in versleutelde staat gebackupt, on-site onderhouden en daarnaast in

up

6.5 Computerbeveiliging

6.5.1.1 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,

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 het functioneren van de applicatie.

6.7.1.1 Netwerkbeveiliging

QuoVadis draagt er zorg voor dat alle PKIoverheid ICT systemen met betrekking tot de registration service, certificate generation service, subject device provision service, dissemination service, revocation management service en revocation sttenton ation serv

7 Certificaatprofiel

7.1

Een server certificaat MAG meerdere FQDN’s bevatten van verschillende domeinen op voorwaarde dat deze domeinen geregistreerd zijn op naam van dezelfde abonnee of een machtiging van dezelfde abonnee afkomstig is.

QuoVadis combineert geen FQDN’s in één certificaat die én afkomstig zijn uit verschillende domeinen én geregistreerd staan op naam van verschillende eigenaren.

In het Subject.Commonname veld, SubjectAltName.iPAdress of het SubjectAltName.DNname veld zijn niet opgenomen:

- wildcard FQDN’s

- lokale domeinnamen,

- private IP adressen

-

Hierbij geldt bovendien dat “Any Other Method” uit 3.2.2.5 niet gebruikt mag worden (voor zowel 3.2.2.4.8 als voor IP-adressen direct).

De geverifieerde gegevens kunnen worden hergebruikt bij een volgende aanvraag, mits deze niet ouder zijn dan 825 dagen. Indien de gegevens ouder zijn dan 825 dagen dient bovengenoemde controle opnieuw plaats te vinden.

QuoVadis houdt bovendien per certificaat bij welke validatiemethode(s) is/zijn gebruikt voor de opgenomen FQDN’s. Deze verificatie wordt door QuoVadis in geen geval uitbesteed aan externe (onder)leveranciers.

7.2 Certificaatprofiel – Service certificaten

Het onderstaande certificaatprofiel, Service Server (SSL), levert een overzicht van het certificaatprofiel zoals uitgegeven in overeenstemming met het PKIoverheid Programma van Eisen, deel 3E uit G2.

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
Org identifier	NTRNL-30237456	
Country (C)	Country	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
Locality (L)	Locality	Required absent
State (S)	State	Required if Locality is absent
Country (C)	Country	Fixed
Subject Public Key Information	RSA (2048 bit) / System Generated	Fixed

8 Conformiteitbeoordeling

8.1 Certificatie en registratie bij Agentschap Telecom

QuoVadis is een TSP (trust Service Provider) in de zin van de regulatie EU 910/2014 en als zodanig geregistreerd op de trust list beheert door Agentschap telecom.

Het managementsysteem van QuoVadis inzake het uitgeven van gekwalificeerde certificaten aan het publiek is gecertificeerd op basis van ETSI EN 319 411-2 / ETSI EN 319 411-1.

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 certificatie-audit 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 agentschap telecom: https://www.agentschaptelecom.nl/onderwerpen/zakelijk-gebruik/eidas-elektronische-vertrouwensdiensten/trust-service-providers Een lijst met certificatiedienstverleners die certificaten uitgeven binnen de PKI voor de overheid vindt u hier: https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-tsp/toegetreden-tsps/

Overige accreditaties van QuoVadis is raadpleegbaar op de volgende locatie: https://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 worden geen kosten in rekening 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.

9.4.3.3 CPS

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 TSP

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

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”.

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

Als de private sleutel, die correspondeert met 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.

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 3(rti)13(f)-10.282 0 7iUsi56i9s omstandigheid of ref in

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. Bijgewerkte 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

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.