Certification Practice Statement PKIoverheid Domeinen Organisatie (G2), Organisatie Persoon (G3)

Versie: **1.6**
Datum: **1 juni 2018**
PvE 3a: **4.6**

QuoVadis Trustlink B.V.
Nevelgaarde 56
3436 ZZ Nieuwegein
Tel: +31 302324320
Fax: +31 302324329

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

Inhoudsopgave

1. INTRODUCTIE OP CERTIFICATE POLICY 8

1.1 Achtergrond 8

1.1.1 Opzet van de Certificate Policy 8

1.1.2 Status 8

1.2 Verwijzingen naar de CPS 8

1.3 Gebruikersgemeenschap 8
1.3.1 Partijen binnen de gebruikersgemeenschap 9
1.3.2. Registration Authorities 9
1.3.3. Eindgebruikers 9

1.4 Certificaatgebruik 9

1.5 CPS-beheer 11

2. PUBLICATIE EN VERANTWOORDELIJKHEID VOOR ELEKTRONISCHE OPSLAGPLAATS 12

2.1 Elektronische opslagplaats 12

2.2 Publicatie van CSP-informatie 12
2.2.1 Toepasbaarheid CPS 12
2.2.2 De unieke nummers (OID's) 12
2.2.3 Informatie 12

2.4 Toegang tot gepubliceerde informatie 12
2.4.1 Toegang tot gepubliceerde informatie 12

2.5 Klachten afhandeling 12

3. IDENTIFICATIE EN AUTHENTIFICATIE 13

3.1 Naamgeving 13
3.1.1-1 Soorten naamformaten 13
3.1.3-1 Pseudoniemen 13
3.1.4. Geschillen 13

3.2 Initiële identiteitsvalidatie 13
3.2.2.1 verificatie Organisatie 13
3.2.2.2 authenticatie Organisatorische eenheid 13
3.2.3.1 Authenticatie van persoonlijke identiteit 13
3.2.5.1 Autorisatie van de certificaathouder 13
3.2.5.2 Verantwoordelijkheid Abonnee 13

3.3 Identificatie en Authenticatie bij vernieuwing van een Certificaat 14

3.3.1 Aanvraag tot vernieuwing 14
3.3.2 Hergebruik sleutels na intrekking certificaat 14

4 OPERATIONELE EISEN CERTIFICAATLEVENSCYCLUS 15

4.4. Acceptatie van Certificaten 15
4.4.1.2 Acceptatie certificaat 15

4.5 Sleutelpaar en Certificaatgebruik 15
4.5.2.1 Gebruik van publieke sleutel en certificaat door vertrouwende partij 15
4.5.2.2 Melden problemen 15

4.9 Intrekking en opschorting van Certificaten 15
4.9.1.1 Omstandigheden die leiden tot intrekking 15
4.9.2.1 Wie mag een verzoek tot intrekking doen 16
4.9.3.1 Procedure voor een verzoek tot intrekking 16
4.9.3.2 Beschikbaarheid intrekking management service 16
4.9.3.3 Vastlegging reden van intrekking 16
4.9.3.4 Certificaat status informatie 16
4.9.3.5 Beschikbaarheid intrekking management service 16
4.9.3.6 Geldigheid CRL 16
4.9.3.6 Issuing subordinatie CA 16
4.9.5.1 Tijdsduur voor verwerking intrekkingsverzoek 17
4.9.6.1 Controlevoorwaarden bij raadplegen certificaat statusinformatie 17
4.9.6.2 Beschikbaarheid controlevoorwaarden 17
4.9.7 Frequentie uitgifte Certificate Revocation List (CRL) 17
4.9.9.1 Online intrekkings-/statuscontrole 17
4.9.9.2 Online intrekkings-/statuscontrole 17
4.9.9.3 Ondertekening Online intrekkings-/statuscontrole 17
4.9.9.4 OCSP responses 17
4.9.9.5 Informatie OCSP service 17
4.9.9.6 Bijwerken OCSP service 17
4.9.9.5 Ondersteunde methoden OCSP responses 17
4.9.13 Opschorting van certificaten 17

4.10.2 Certificate Status Service 17

5 FYSIEKE, PROCEDURELE EN PERSONELE BEVEILIGING 18

5.1 Fysieke beveiliging 18
5.1.1 Vestigingslocatie operationele CA-dienstverlening 18
5.1.2 Fysieke toegang 18
5.1.3 Stroomvoorziening en Airconditioning 18
5.1.4 Wateroverlast 18
5.1.5 Bescherming en preventie tegen brand 18
5.1.6 Media opslag 18
5.1.7 Afval verwerking 18
5.1.8 Externe back-up 18

5.2 Procedurele Beveiliging 18
5.2.4.1 Vertrouwelijke rollen 19
5.2.4.2 Aantal personen vereist per operationele handeling 19
5.2.3. Identificatie en authentificatie voor elke rol 19

5.2.4. Rollen die scheiding van plichten vereisen 19
5.2.4.2 Rollen die functiescheiding behoeven 19
5.2.5.1 Beheer en beveiliging 19
5.2.5.2 Optioneel beheer en beveiliging 20

5.3 Personele Beveiliging 20
5.3.1. Kwalificaties, ervaring en screening 20
5.3.2. Procedures achtergrondcontrole 20
5.3.3. Trainingsvereisten 20
5.3.4. Trainingsfrequentie 20
5.3.5. Sancties op ongeautoriseerde handelingen 20
5.3.6. Documentatie verstrekt aan personeel 20
5.3.7. Geheimhouding 20

5.4 Procedures ten aanzien van logging 20
5.4.1 Vastleggen van gebeurtenissen 20
5.4.2 Frequentie van verificatie audit logs 21
5.4.3 Bewaartermijn van audit logs 21
5.4.4 Beveiliging van audit logs 21
5.4.5 Controlelogboek back-up procedures 22
5.4.6 Audit Logging 22
5.4.7 Berichtgeving inzake logging 22
5.4.8 Beoordeling van de kwetsbaarheid 22

5.5 Archivering van documenten 22
5.5.1. Aard van gearchiveerde gegevens 22
5.5.2. Bewaarperiode voor het archief 22
5.5.3 Bescherming van het archief 22
5.5.4 Back-up procedures m.b.t. het archief 22
5.5.5 Eisen voor de timestamping van gegevens 22
5.5.6 Archiveringssysteem 22
5.5.7 Procedures om de archiefinformatie te verkrijgen en te verifiëren 22

5.6 Wijziging van de publieke sleutel 23

5.7 Aantasting en Continuïteit 23

5.8 Beëindiging van de dienstverlening van de CA en/of RA 24

6 TECHNISCHE BEVEILIGINGSMAATREGELEN 25

6.1 Generatie en installatie van het sleutelpaar 25
6.1.1 Sleutelpaar generatie 25
6.1.1.1 Genereren van sleutelparen voor de CSP sub CA 25
6.1.2 Overdracht van private sleutel en SSCD aan certificaathouder 25
6.1.5 Sleutellengte 25
6.1.7 Doeleinden voor sleutel gebruik (Vanaf X.509 V3 sleutel gebruiksvelden) 25

6.2 Private sleutel bescherming 25
6.2.1 Standaarden en controles van de cryptografische module (HSM) 25
6.2.2 Private key (N out of M) “Multi-person” controle 25
6.2.3 Escrow van de private sleutel 25
6.2.4 Private sleutel back-up 26
6.2.5 Archivering van de private sleutel 26

6.2.6 Toegang tot private sleutels in cryptografische module 26
6.2.7 Private sleutelopslag op een cryptografische module 26
6.2.8 Activeringsmethoden voor een private sleutel 26
6.2.9 Methoden voor deactivatie van de private sleutel 26
6.2.10 Methode voor de vernietiging van de private sleutel 26
6.2.11 Cryptografische classificatie van de module en SSCD's 26
6.2.11.1 Eisen voor veilige middelen voor het aanmaken van elektronische hand-tekeningen 26
6.2.11.2 Alternatieve eisen voor veilige middelen. 26
6.2.11.3 Overeenstemming eisen voor veilige middelen. 27

6.3 Overige aspecten van sleutelpaar management 27
6.3.1 Archivering van het publieke sleutelpaar 27
6.3.2 Gebruiksduur van sleutels en certificaten 27
6.3.2 Gebruiksduur van sleutels en eindgebruikercertificaten 27

6.4 Activeringsgegevens 27
6.4.1.1 Genereren en installeren van activeringsgegevens 27
6.4.1.2 Deblokkering van activeringsgegevens 27

6.5 Computerbeveiliging 27
6.5.1 Technische maatregelen inzake computerbeveiliging 27
6.5.2 Classificatie van de computerbeveiliging 28

6.6 Beheersmaatregelen technische levenscyclus 28
6.6.1 Beheersmaatregelen ten behoeve van systeemontwikkeling 28
6.6.2 Beheersmaatregelen ten behoeve van beveiligingsontwikkeling 28
6.6.3 Beveiligingsmaatregelen van de levenscyclus 28

6.7 Beveiligingsmaatregelen van het netwerk 28
6.7.1.1 Netwerk beveiliging 28
6.7.1.2 Intern testen Netwerk beveiliging 29
6.7.1.3 Extern testen Netwerk beveiliging 29

7. CERTIFICAATPROFIEL 30

7.1.1 Certificaatprofiel – Authenticiteitcertificaten 30

7.1.2 Certificaatprofiel – Handtekeningcertificaten 31

7.1.3 Certificaatprofiel – Vertrouwelijkheidcertificaten 33

7.2 Certificaatprofiel – CRL 35

7.3 Certificaatprofiel – OCSP 35

8. CONFORMITEITBEOORDELING 36

8.1. Certificatie en registratie bij Agentschap Telecom 36

8.2. De verhouding van de auditor met de beoordeelde entiteit 36

8.3. Scope van de audit 36

8.4. Acties ondernomen vanwege deficiëntie 36

8.6. Publicatie accreditaties en registraties 36

9. ALGEMENE EN JURIDISCHE BEPALINGEN 37

9.1 Tarieven 37
9.1.1. Tarieven voor Certificaatuitgifte of -vernieuwing 37
9.1.2. Tarieven voor Certificaattoegang 37
9.1.3. Tarieven voor toegang tot intrekkings- of statusinformatie 37
9.1.4. Tarieven voor andere diensten 37
9.1.5. Beleid inzake terugbetaling 37

9.2. Financiële verantwoordelijkheid en aansprakelijkheid 37
9.2.1. Verzekeringsdekking 37
9.2.1.1 Verzekeringsdekking 37
9.2.1.2 Verzekeringsdekking 37

9.3. Vertrouwelijkheid van bedrijfsgevoelige gegevens 37
9.3.1. Toepassingsgebied vertrouwelijke informatie 37
9.3.2. Gegevens die als niet-vertrouwelijk worden beschouwd 37
9.3.3. Verantwoordelijkheid vertrouwelijke informatie te beschermen 38

9.4. Vertrouwelijkheid van persoonlijke informatie 38
9.4.1. Vertrouwelijke informatie 38
9.4.2. Vertrouwelijk behandelde informatie 38
9.4.3. Niet-vertrouwelijke informatie 38
9.4.4. Verantwoordelijkheid om vertrouwelijke informatie te beschermen 38
9.4.5. Melding van- en instemming met het gebruik van persoonsgegevens 38
9.4.6. Overhandiging van gegevens op last van een rechterlijke instantie 38

9.5 Intellectuele eigendomsrechten 38

9.6. Aansprakelijkheid en garanties 39
9.6.1. Aansprakelijkheid van de CSP 39
9.6.2.Aansprakelijkheid van Abonnees en Certificaathouders 39
9.6.3.Aansprakelijkheid Vertrouwende Partijen 39

9.7. Uitsluiting van garanties 40

9.8. Beperking van aansprakelijkheid 40
9.8.1. Beperkingen van aansprakelijkheid van QuoVadis 40
9.8.2. Uitgesloten aansprakelijkheid 40
9.8.3. Beperking van aansprakelijkheid QuoVadis 41
9.8.4. Eisen met betrekking tot de aansprakelijkheid van QuoVadis 41

9.9. Schadeloosstelling 41

9.10. Geldigheidstermijn CPS 41
9.10.1. Termijn 41
9.10.2. Beëindiging 41
9.10.3. Effect van beëindiging en overleving 41

9.11. individuele kennisgeving en communicatie met betrokken partijen 42

9.12. Wijziging **42**
9.12.1. Wijzigingsprocedure 42
9.12.2. Notificatie van wijzigingen 42

9.13. Geschillenbeslechting **42**

9.14. Van toepassing zijnde wetgeving **42**

9.15. Naleving relevante wetgeving **42**

9.16. Overige bepalingen **42**

BIJLAGE A – DEFINITIES EN AFKORTINGEN **43**

1. Introductie op Certificate Policy

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 PKI voor de overheid (http://www.logius.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.

1.1.1 Opzet van de Certificate Policy

Voor u ligt het PKIoverheid Organisatie (G2) en Organisatie Persoon (G3) Certification Practice Statement (CPS) van QuoVadis. Dit document beschrijft de procedures en maatregelen die QuoVadis in acht neemt bij het uitgeven van certificaten uit de domeinen Organisatie (G2) en Persoon (G3) van de PKI voor de overheid. Zoals in deel 1 van het PvE is aangegeven bestaan de eisen die onderdeel uitmaken van de CP uit eisen:

- die voortkomen uit het Nederlandse wettelijke kader in relatie tot de elektronische handtekening;
- die voortkomen uit de vigerende versie van de standaard ETSI EN 319 411-2, QCP public + SSCD (ETSI CP OID 0.4.0.1456.1.1);
- die voortkomen uit de vigerende versie van de stadaard ETSI TS 319 411-1 waarbij de policy NCP+ van toepassing is voor authenticiteits- en versleutelingscertificaten.
- die specifiek door en voor de PKIoverheid zijn opgesteld.

QuoVadis ondersteund certificaten uit het domein Organisatie/Bedrijven (G1) niet.

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
2.16.528.1.1003.1.2.5.1	voor het authenticiteitcertificaat, dat de publieke sleutel bevat ten behoeve van identificatie en authenticatie

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 (G2) en Organisatie Persoon (G3) (5).authenticatie (1)

2.16.528.1.1003.1.2.5.2	voor het handtekeningcertificaat, dat de publieke sleutel bevat ten behoeve van de gekwalificeerde elektronische handtekening

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 (G2) en Organisatie Persoon (G3) (5).gekwalificeerde elektronische handtekening (2)

2.16.528.1.1003.1.2.5.3	voor het vertrouwelijkheidcertificaat, dat de publieke sleutel bevat ten behoeve van 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 (G2) en Organisatie Persoon (G3) (5).Vertrouwelijkheid (3)

De volgende OID is geregistreerd door PKIoverheid voor opname in alle QuoVadis Organisatie (G2) en Persoon (G3) certificaten:

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

1.3 Gebruikersgemeenschap

Binnen de domeinen Organisatie en Organisatie Persoon bestaat de gebruikersgemeenschap uit abonnees, die organisatorische entiteiten binnen overheid en bedrijfsleven zijn (zie PKIo 3.2.2-1) en uit certificaathouders, die bij deze abonnees behoren. Tevens zijn er beroepsbeoefenaars die zowel abonnee als certificaathouder zijn. 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 CSP PKI Overheid Organisatie Certification Authority (CSP-PKI Overheid Organisatie CA)*

De QuoVadis CSP-PKI Overheid Organisatie CA G2 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.
QuoVadis ondersteund de uitgifte van certificaten onder de G3 Root op dit moment nog niet.

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 Nieuwegein verzorgt de identificatie en registratie van de abonnee 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*

Een certificaathouder is een 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 ofwel onderdeel van een organisatorische entiteit waarvoor een abonnee de contracterende partij is (organisatiegebonden certificaathouder), ofwel de beoefenaar van een erkend beroep en in die hoedanigheid zelf een abonnee en daarmee de contracterende partij (beroepsgebonden certificaathouder).

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.

1.4 Certificaatgebruik

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

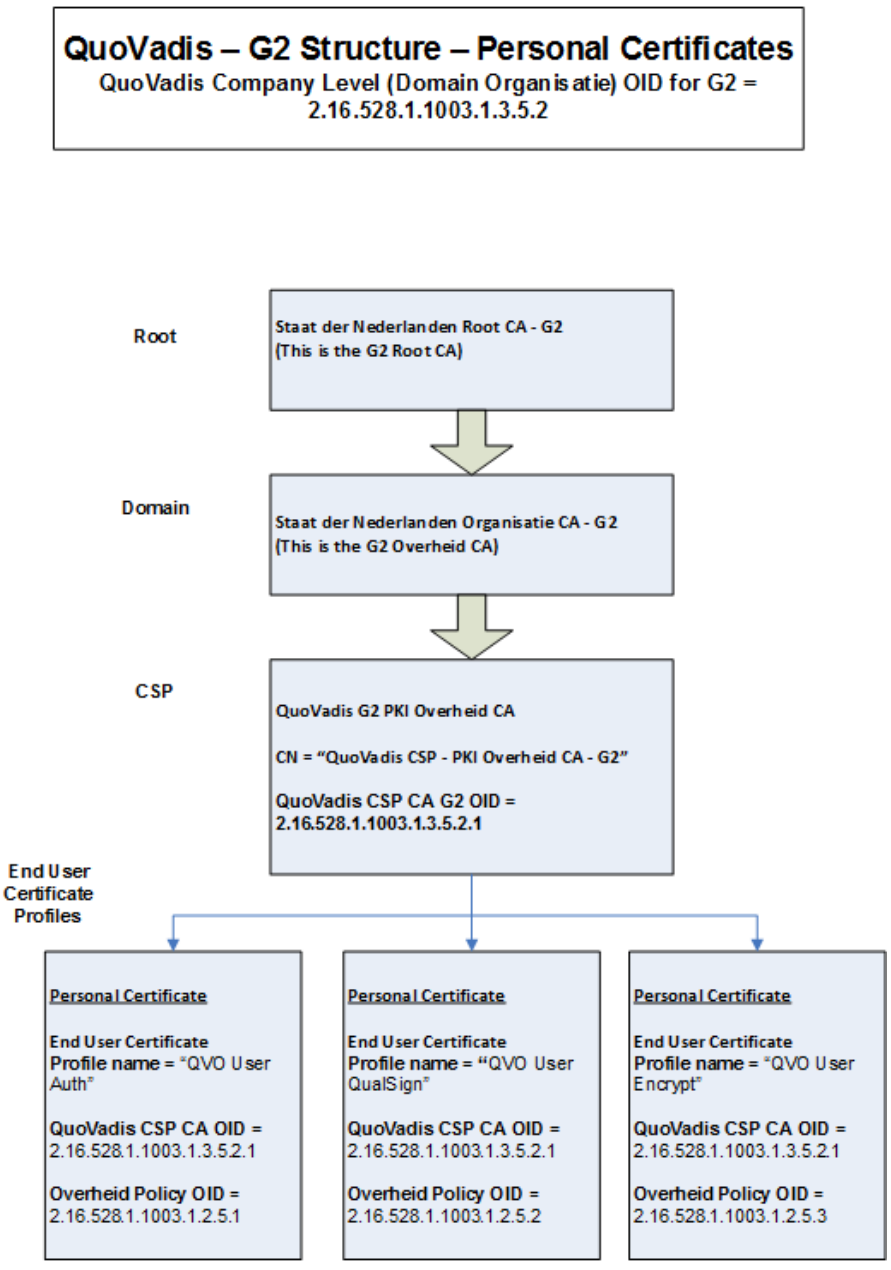
[OID 2.16.528.1.1003.1.2.5.1] Authenticiteitcertificaten, die onder deze CPS worden uitgegeven, kunnen worden gebruikt voor het betrouwbaar identificeren en authenticeren van personen, organisaties en middelen langs elektronische weg. Dit betreft zowel de identificatie van personen onderling als tussen personen en geautomatiseerde middelen.

[OID 2.16.528.1.1003.1.2.5.1] Authenticiteitcertificaten die onder deze CPS worden uitgegeven, kunnen niet worden gebruikt voor het identificeren van personen in gevallen waarbij de wet vereist dat de identiteit van personen alleen met een in de Wet op de identificatieplicht aangewezen document mag worden vastgesteld.

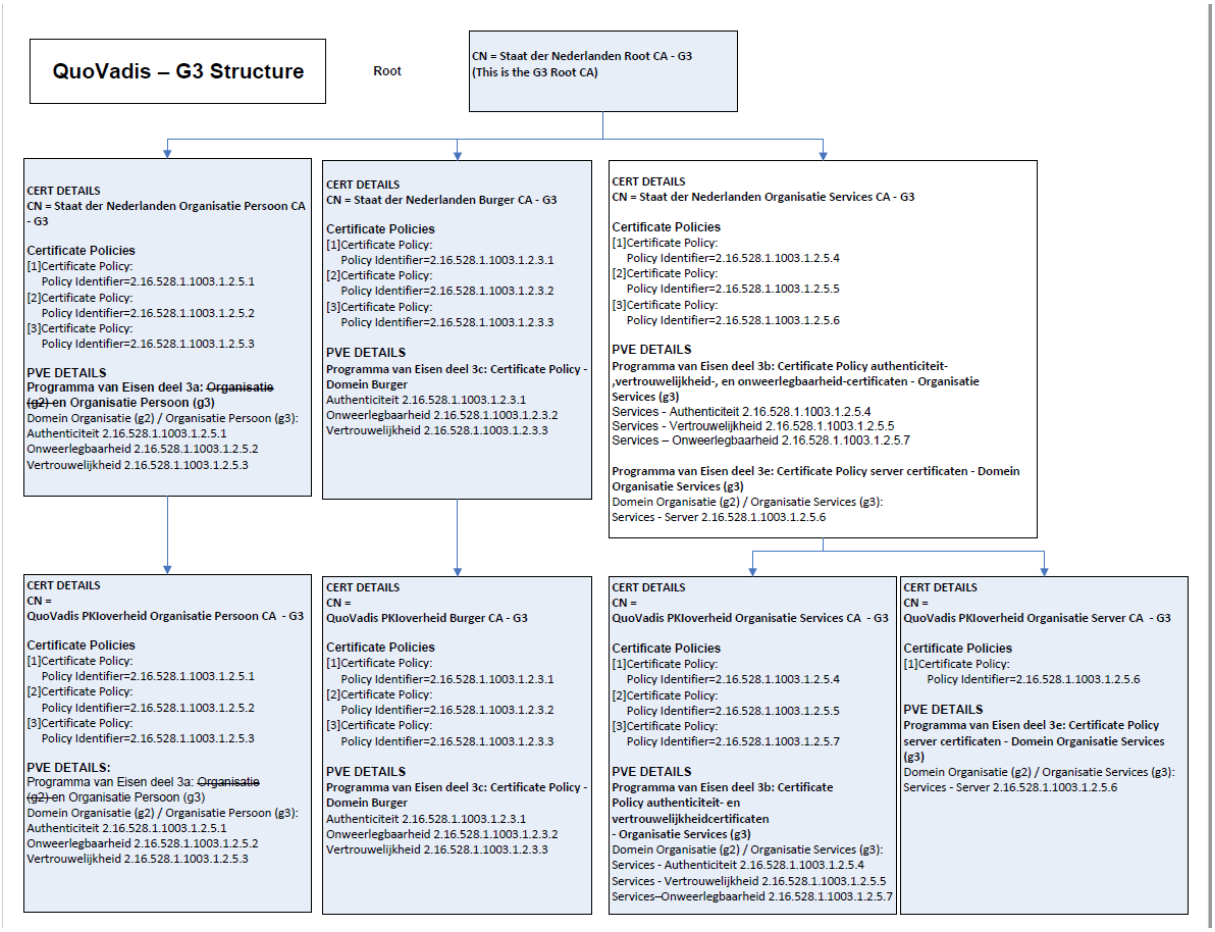
[OID 2.16.528.1.1003.1.2.5.2] Handtekeningcertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt om elektronische handtekeningen te verifiëren, die "dezelfde rechtsgevolgen hebben als een handgeschreven handtekening", zoals wordt aangegeven in artikel 15a, eerste en tweede lid, in Titel 1 van Boek 3 van het Burgerlijk Wetboek onder afdeling 1A en zijn gekwalificeerde certificaten zoals bedoeld in artikel 1.1, lid ss van de Telecomwet.

[OID 2.16.528.1.1003.1.2.5.3] Vertrouwelijkheidcertificaten, die onder deze CP worden uitgegeven, kunnen 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.

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



Figuur1: Overzicht van de certificaat policies.



Figuur2: Overzicht van de certificaat policies onder G3

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 dit QuoVadis CPS wordt elektronisch beschikbaar gesteld in PDF-formaat via:

- http://www.quovadisglobal.com/repository.aspx of
- http://www.quovadisglobal.nl/Beheer/Documenten.aspx

Daar vindt u ook de overeenkomsten en de toepasselijke voorwaarden voor onze dienstverlening.

Informatie over dit CPS kan worden verkregen via onderstaande contactgegevens:

QuoVadis Trustlink B.V.
T.a.v. Policy Management
Nevelgaarde 56 Noord
3436 ZZ Nieuwegein
Tel: +31 30 232 4320
Fax: +31 30 232 4329

Website: http://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 24*7*365 bereikbaar is via:

- http://www.quovadisglobal.com/repository.aspx of
- http://www.quovadisglobal.nl/Beheer/Documenten.aspx

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 hoofdstuk 7 van dit CPS.

2.2.1 Toepasbaarheid CPS

Deze CPS heeft alleen betrekking op de uitgifte van PKIoverheid Organisatie (G2) en Organisatie Persoon (G3) certificaten en is enkel in het Nederlands opgesteld. De indeling van dit CPS is zoveel mogelijk conform de RFC3647 standaard opgezet

2.2.2 De unieke nummers (OID's)

De unieke nummers (OID's) die refereren naar de toepasselijke CP voor PKIoverheid persoonsgebonden certificaten in het domein organisatie (PvE PKIoverheid deel 3a) zijn:

- [OID 2.16.528.1.1003.1.2.5.1] Authenticiteitcertificaten
- [OID 2.16.528.1.1003.1.2.5.2] Handtekeningcertificaten
- [OID 2.16.528.1.1003.1.2.5.3] Vertrouwelijkheidcertificaten

2.2.3 Informatie

Alle informatie is in het Nederlands en Engels beschikbaar. De Nederlandse versie van alle documentatie is leidend.

2.4 Toegang tot gepubliceerde informatie

2.4.1 Toegang tot gepubliceerde informatie

De elektronische opslagplaats is 24 uur per dag, 7 dagen per week voor een ieder beschikbaar, met uitzondering van systeemdefecten of onderhoudswerkzaamheden. In geval van onvoorziene onbeschikbaarheid, wordt de beschikbaarheid van de elektronische opslagplaats (dissemination service) hersteld binnen 24 uur.

De toegangscontrole tot de elektronische opslagplaats is zodanig ingericht dat alleen leesrechten zijn toegekend voor derden die deze informatie raadplegen.
Uitsluitend QuoVadis heeft schrijfrechten op de elektronische opslagplaats.

2.5 Klachten afhandeling

Indien er klachten of opmerkingen zijn kan contact opgenomen via de QuoVadis supportlijn +31 (0)30 232 4320 tijdens kantooruren of via info.nl@quovadisglobal.com en zullen zij, mede bepaald door de aard van de klacht, na overleg met de directie van QuoVadis Trustlink B.V. door de betreffende afdeling behandeld en opgelost worden.

3. Identificatie en Authentificatie

3.1 Naamgeving

3.1.1-1 Soorten naamformaten

QuoVadis voldoet aan de eisen die aan naamformaten zijn gesteld in het Programma van Eisen, deel 3 – bijlage A Certificaat-, CRL- en OCSP-profielen.

3.1.3-1 Pseudoniemen

Het gebruik van anonieme certificaten of pseudoniemen is niet toegestaan.

3.1.4. 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

3.2.2.1 verificatie Organisatie

QuoVadis zal – bij organisatiegebonden certificaten – verifiëren dat de abonnee een bestaande organisatie is

3.2.2.2 authenticatie Organisatorische eenheid

QuoVadis zal – bij organisatiegebonden certificaten – verifiëren dat de door de abonnee aangemelde organisatienaam die in het certificaat wordt opgenomen juist en volledig is.

3.2.3.1 Authenticatie van persoonlijke identiteit

Bij uitgifte van certificaten aan natuurlijke personen zal QuoVadis verifiëren dat de door de certificaathouder aangemelde volledige naam die in het certificaat wordt opgenomen juist en volledig is, met inbegrip van achternaam, eerste voornaam, initialen of overige voorna(a)m(en) (indien van toepassing) en tussenvoegsels (indien van toepassing).

3.2.5.1 Autorisatie van de certificaathouder

Bij organisatiegebonden certificaathouders zal QuoVadis controleren dat:

- het bewijs, dat de certificaathouder geautoriseerd is namens de abonnee om een certificaat te ontvangen, authentiek is;
- de in dit bewijs genoemde naam en identiteitskenmerken overeenkomen met de onder 3.2.3-pkio21 vastgestelde identiteit van de certificaathouder.

Bij beroepsgebonden certificaathouders zal QuoVadis controleren dat:

- het bewijs, dat de certificaathouder geautoriseerd is het erkende beroep uit te oefenen, authentiek is;
- de in dit bewijs genoemde naam en identiteitskenmerken overeenkomen met de onder 3.2.3-pkio21 vastgestelde identiteit van de certificaathouder.

Als authentiek bewijs voor het uitoefenen van een erkend beroep wordt alleen beschouwd:
a. ofwel een geldig bewijs van inschrijving in een door de betreffende beroepsgroep erkend (beroeps)register waarbij een wettelijk geregeld tuchtrecht van toepassing is;
b. ofwel een benoeming door een Minister;
c. ofwel een geldig bewijs (b.v. een vergunning) dat aan de wettelijke eisen voor het uitoefenen van het beroep wordt voldaan.

Onder geldig bewijs wordt verstaan een bewijs dat niet is verlopen of (tijdelijk of voorlopig is) ingetrokken.
In PvE deel 4 staat een limitatieve lijst met onder a en b bedoelde beroepen.

3.2.5.2 Verantwoordelijkheid Abonnee

Abonnee is een rechtspersoon (organisatiegebonden certificaten):
In de overeenkomst die QuoVadis sluit met de abonnee is opgenomen dat de abonnee de verantwoordelijkheid heeft om, als er relevante wijzigingen plaats hebben in de relatie tussen abonnee en certificaathouder, deze onmiddellijk aan QuoVadis kenbaar te maken door middel van een intrekkingsverzoek. Relevante wijzigingen kunnen in dit verband bijvoorbeeld beëindiging van het dienstverband en schorsing zijn.

Abonnee is een natuurlijk persoon (beroepsgebonden certificaten):
In de overeenkomst die QuoVadis sluit met de abonnee is opgenomen dat de abonnee de verantwoordelijkheid heeft om, als er relevante wijzigingen plaats hebben gevonden, deze onmiddellijk aan QuoVadis kenbaar te maken door middel van een intrekkingsverzoek. Een relevante wijziging in dit verband is in ieder geval het niet langer beschikken over een geldig bewijs zoals aangegeven bij 3.2.5-1.

3.3 Identificatie en Authenticatie bij vernieuwing van een Certificaat

3.3.1 Aanvraag tot vernieuwing

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

3.3.1.1 Hergebruik sleutels bij vernieuwing certificaat

QuoVadis vernieuwd geen Organisatie of Beroeps certificaten zonder vernieuwing van de sleutels.

3.3.1.2 Controle bij aanvraag vernieuwing certificaat

Het vernieuwen van Organisatie of Beroeps certificaten gaat altijd vooraf door een controle of aan alle eisen die onder [3.1] en [3.2] zijn gesteld, is voldaan.

3.3.2 Hergebruik sleutels na intrekking certificaat

QuoVadis zal na intrekking van het certificaat de desbetreffende sleutels niet opnieuw certificeren.

4 Operationele eisen certificaatlevenscyclus

4.4. Acceptatie van Certificaten

4.4.1.2 Acceptatie certificaat

Na uitgifte van een certificaat, dient de certificaathouder expliciet de overhandiging van het sleutelmateriaal behorend bij het certificaat aan QuoVadis te bevestigen.
Acceptatie van certificaten heeft geacht te hebben plaatsgevonden na afronding van de Certificaatuitgifte middels TrustLink Enterprise.

Met de acceptatie van het certificaat en het gebruik daarvan gaat 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.

4.5 Sleutelpaar en Certificaatgebruik

4.5.2.1 Gebruik van publieke sleutel en certificaat door vertrouwende partij

In de gebruikersvoorwaarden die aan de vertrouwende partijen ter beschikking wordt gesteld is opgenomen dat de vertrouwende partij wordt geacht de geldigheid te controleren van de volledige keten van certificaten tot aan de bron (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.

Daarnaast is opgenomen dat de abonnee zelf zorg draagt voor een tijdige vervanging in het geval van een naderende afloop geldigheid, en noodvervanging in geval van compromittatie en/of andere soorten van calamiteiten met betrekking tot het certificaat of van bovenliggende certificaten. Van de abonnee wordt verwacht dat hij zelf adequate maatregelen neemt om de continuïteit van het gebruik van certificaten te borgen.

De geldigheid van een certificaat dient niet verward te worden met de bevoegdheid van de certificaathouder een bepaalde transactie namens een organisatie te doen. De PKI voor de overheid regelt geen autorisatie; daarvan moet een vertrouwende partij zichzelf op andere wijze overtuigen

4.5.2.2 Melden problemen

In geval van problemen met het certificaat kan contact opgenomen via de QuoVadis supportlijn +31 (0)30 232 4320 tijdens kantooruren, na kantoor uren in geval van calamiteit via +1 651 229 3456 of via support@quovadisglobal.com en zullen zij, mede bepaald door de aard van het probleem, passende actie ondernemen. Indien er melding wordt gemaakt via e-mail wordt per e-mail direct een ontvangst bevestiging verstuurd en kan het probleem 24x7 behandeld worden.

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.

4.9.1.1 Omstandigheden die leiden tot intrekking

Certificaten zullen worden ingetrokken wanneer:

- de abonnee aangeeft dat het oorspronkelijke verzoek voor een certificaat niet was toegestaan en de abonnee verleent met terugwerkende kracht ook geen toestemming;
- QuoVadis beschikt over voldoende bewijs dat de privésleutel van de abonnee (die overeenkomt met de publieke sleutel in het certificaat) is aangetast of er is het vermoeden van compromittatie, of er is sprake van inherente beveiligingszwakheid, of dat het certificaat op een andere wijze is misbruikt. Een sleutel wordt als aangetast beschouwd in geval van ongeautoriseerde toegang of vermoede ongeautoriseerde toegang tot de private sleutel, verloren of vermoedelijk verloren private sleutel of SSCD, gestolen of vermoedelijk gestolen sleutel of SSCD of vernietigde sleutel of SSCD.
- een abonnee niet aan zijn verplichtingen voldoet zoals verwoord in de CP of het bijbehorende CPS van QuoVadis of de overeenkomst die QuoVadis met de abonnee heeft afgesloten;

QuoVadis op de hoogte wordt gesteld of anderszins zich bewust wordt dat het gebruik van de domeinnaam in het certificaat niet langer wettelijk toegestaan is (b.v. door een uitspraak van een rechter);

- QuoVadis op de hoogte wordt gesteld of anderszins zich bewust wordt van een wezenlijke verandering in de informatie, die in het certificaat staat. Voorbeeld daarvan is: verandering van de naam van de certificaathouder (service);
- 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 CSP;
- 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 certificaathouder
- de abonnee
- QuoVadis als CSP
- 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, kan een intrekkingverzoek telefonisch indienen via de QuoVadis supportlijn of kan dit indienen via de QuoVadis website. De abonnee en de Certificaatbeheerder kunnen hierbij worden gevraagd zich te authenticeren, op een wijze zoals gespecificeerd in par. 3.4.

De online intrekkingsfaciliteit via de QuoVadis website https://tl.quovadisglobal.com is 24 uur per dag en 7 dagen per week beschikbaar. De QuoVadis supportlijn +31 (0)30 232 4320 is eveneens buiten kantooruren bereikbaar via +1 651 229 3456. De Registration Authority ten kantore van QuoVadis +31 (0)30 232 4320 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-PKI Overheid Organisatie 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 OCSP en 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 vertraging 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)

4.9.6.1 Controlevoorwaarden bij raadplegen certificaat statusinformatie

Een eindgebruiker die de certificaat statusinformatie raadpleegt, dient de authenticiteit van deze informatie te verifiëren door de elektronische handtekening waarmee de informatie is getekend en het bijbehorende certificatiepad te controleren**.**

4.9.6.2 Beschikbaarheid controlevoorwaarden

De in [4.9.6.1] genoemde verplichting is door QuoVadis opgenomen in de gebruikers-voorwaarden die ter beschikking worden gesteld aan de vertrouwende partijen.

4.9.7 Frequentie uitgifte Certificate Revocation List (CRL)

QuoVadis zal de CRL ten behoeve van eindgebruiker certificaten tenminste een keer in de 7 kalenderdagen bijwerken en opnieuw uitgeven en de datum van het veld " Volgende update" zal niet meer dan 10 kalenderdagen zijn na de datum van het veld "Ingangsdatum".

4.9.9.1 Online intrekkings-/statuscontrole

QuoVadis ondersteunt het Online Certificate Status Protocol (OCSP)

4.9.9.2 Online intrekkings-/statuscontrole

Ondersteuning van het Online Certificate Status Protocol (OCSP), gebeurt in overeen-stemming met IETF RFC 6960.

4.9.9.3 Ondertekening Online intrekkings-/statuscontrole

Ter verbijzondering van het in IETF RFC 6960 gestelde worden de OCSP responses van QuoVadis digitaal ondertekend door ofwel:

- de private (CA) sleutel waarmee ook het certificaat is ondertekend waar-van de status wordt gevraagd, of;
- een door QuoVadis aangewezen responder die beschikt over een OCSP-Signing certificaat dat voor dit doel is uitgegeven door de QuoVadis, of;
- een responder die beschikt over een OCSP-Signing certificaat dat valt binnen de hiërarchie van de PKI voor de overheid.

4.9.9.4 OCSP responses

Ter verbijzondering van het in IETF RFC 6960 gestelde wordt het gebruik van vooraf berekende OCSP responses (precomputed responses) door QuoVadis niet gebruikt.

4.9.9.5 Informatie OCSP service

De informatie die wordt verstrekt middels OCSP is ten minste even actueel en betrouwbaar als de informatie die wordt gepubliceerd door middel van een CRL, gedurende de geldigheid van het afgegeven certificaat en bovendien tot ten minste zes maanden na het tijdstip waarop de geldigheid van het certificaat is verlopen of, indien dat tijdstip eerder valt, na het tijdstip waarop de geldigheid is beëindigd door intrekking.

4.9.9.6 Bijwerken OCSP service

QuoVadis werkt de OCSP service tenminste een keer in de 4 kalenderdagen bij. De maximale vervaltermijn van de OCSP responses is 10 kalenderdagen.

4.9.9.5 Ondersteunde methoden OCSP responses

QuoVadis ondersteund de GET methode bij het aanbieden van OCSP responses volgens RFC 5019.

Http gebaseerde OCSP verzoeken kunnen zowel de GET als de POST methode gebruiken voor het indienen van een verzoek. Om http caching mogelijk te maken ondersteund QuoVadis tevens de GET methode.

4.9.13 Opschorting van certificaten

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

4.10.2 Certificate Status Service
De maximale tijdsduur, waarbinnen QuoVadis de beschikbaarheid van de revocation status information hersteld, is gesteld op vier uur.

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 locatie 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.

5.2.1 Risico analyse

QuoVadis zal de risicoanalyse minimaal jaarlijks, of als de PA daartoe opdracht geeft, of het NCSC daartoe advies geeft, opnieuw uitvoeren. De risicoanalyse moet alle PKIoverheid processen raken die onder de verantwoordelijkheid van de CSP vallen.

Op basis van de risicoanalyse zal QuoVadis een informatiebeveiligingsplan ontwikkelen, implementeren, onderhouden, handhaven en evalueren. Dit plan beschrijft een samenhangend geheel van passende administratieve, organisatorische, technische en fysieke maatregelen en procedures waarmee QuoVadis de beschikbaarheid, exclusiviteit en integriteit van alle PKIoverheid processen, aanvragen en de gegevens die daarvoor worden gebruikt, waarborgt.

5.2.2 audit externe organisaties

Het is bedrijfsbeleid dat QuoVadis geen PKI operaties delegeert naar andere organisaties.

5.2.4.1 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 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.

5.2.4.2 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-Organisatie CA.
QuoVadis handhaaft de functiescheiding tussen medewerkers die de uitgifte van een certificaat controleren en medewerkers die de uitgifte van een certificaat goedkeuren.

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 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.

5.2.4.2 Rollen die functiescheiding behoeven

QuoVadis handhaaft functiescheiding tussen medewerkers die de uitgifte van een certificaat controleren en medewerkers die de uitgifte van een certificaat goedkeuren.

5.2.5.1 Beheer en beveiliging

QuoVadis zal de risicoanalyse minimaal jaarlijks, of als de PA daartoe opdracht geeft, of het NCSC daartoe advies geeft, opnieuw uitvoeren. De risicoanalyse moet alle PKIoverheid processen raken die onder de verantwoordelijkheid van de CSP vallen.
Op basis van de risicoanalyse zal QuoVadis een informatiebeveiligingsplan ontwikkelen, implementeren, onderhouden, handhaven en evalueren. Dit plan beschrijft een samenhangend geheel van passende administratieve, organisatorische, technische en fysieke maatregelen en procedures waarmee QuoVadis de beschikbaarheid, exclusiviteit en integriteit van alle PKIoverheid processen, aanvragen en de gegevens die daarvoor worden gebruikt, waarborgt.

5.2.5.2 Optioneel beheer en beveiliging

Naast een audit uitgevoerd door een geaccrediteerd auditor MAG QuoVadis een audit uitvoeren bij zijn externe leveranciers van PKIoverheid kerndiensten om zich ervan te verwittigen dat deze leveranciers de relevante eisen van het PVE van PKIoverheid conform de wensen van de CSP en rekening houdend met zijn bedrijfsdoelstellingen, -processen en -infrastructuur hebben geïmplementeerd en geoperationaliseerd.
QuoVadis is vrij in de keuze om zelf een eigen audit uit te (laten) voeren dan wel gebruik te gaan maken van reeds bestaande audit resultaten zoals die van de formele certificeringsaudits, de diverse interne en externe audits, Third party mededelingen (TPM's) en (buitenlandse) compliancy rapportages.
Ook is QuoVadis gerechtigd om inzage te verkrijgen in het onderliggende bewijsmateriaal zoals audit dossiers en overige, al dan niet systeem-, documentatie.
Uiteraard beperkt zich het bovenstaande tot de bij de leveranciers gehoste CSP-processen, -systemen en –infrastructuur voor PKIo kerndiensten.

Het is bedrijfsbeleid dat QuoVadis geen PKI operaties delegeert naar externe leveranciers.

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 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.

Logging vindt plaats op minimaal:

- Routers, firewalls en netwerk systeem componenten;
- 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 CSP-Organistatie 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- Organistatie CA en de Registration Authority-omgeving.

5.4.6 Audit Logging

Het beveiligde logproces van de QuoVadis CSP- Organistatie 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- Organistatie 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 timestamping van gegevens

QuoVadis ondersteunt timestamping 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- Organistatie 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- Organisatie 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.

5.7.1.1 Procedures voor afhandeling incidenten en aantasting

QuoVadis zal de PA, het NCSC, de auditor en de certificerende instantie na onmiddellijk op de hoogte te stellen van een security breach en/of calamiteit, na analyse en vaststelling en dient de PA, het NCSC , de auditor en de certificerende instantie van het verdere verloop op de hoogte te houden.

Onder security breach wordt in de PKIoverheid context verstaan:
Een inbreuk op de CSP kerndiensten: registration service, certificate generation service, subject device provisioning service, dissemination service, revocation management service en revocation status service.

Dit is in ieder geval maar niet limitatief:

- het ongeoorloofd uitschakelen of onbruikbaar maken van een kerndienst;
- ongeautoriseerde toegang tot een kerndienst t.b.v. het afluisteren, onderscheppen en of veranderen van berichtenverkeer;
- ongeautoriseerde toegang tot een kerndienst t.b.v. het ongeoorloofd verwijderen, wijzigen of aanpassen van computergegevens.

5.7.1.2 Procedures voor afhandeling incidenten en aantasting

QuoVadis informeert de PA onmiddellijk over de 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. Hieronder vallen in ieder geval ook, maar niet uitsluitend, security breaches en/of calamiteiten met betrekking tot andere, door QuoVadis uitgevoerde, PKI diensten, niet zijnde PKIoverheid. Daarnaast heeft QuoVadis zich geabboneerd op de beveiligingsadviezen van de NCSC.

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 de CSP dienstverlening ten behoeve van abonnees, vertrouwende partijen en derden (waaronder browserpartijen). QuoVadis zal het BCP jaarlijks testen, beoordelen en actualiseren. Het BCP beschrijft in ieder geval de volgende zaken :

- Eisen aan inwerkingtreding;
- Noodprocedure / uitwijkprocedure;
- Eisen aan herstarten CSP 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 CSP; 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 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-Organisatie 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.

6.1.1.1 Genereren van sleutelparen voor de CSP sub CA

Het algoritme en de lengte van de cryptografische sleutels die worden gebruikt voor het genereren van de sleutels voor QuoVadis PKI Overheid sub CA voldoen aan de eisen, die daaraan zijn gesteld in de lijst van aanbevolen cryptografische algoritmes en sleutellengtes, zoals gedefinieerd in ETSI TS 119 312.

6.1.1.2 Genereren van sleutelparen van de certificaathouders

Het genereren van de sleutels van certificaathouders (c.q. gegevens voor het aanmaken van elektronische handtekeningen) dient te geschieden in een middel dat voldoet aan de eisen genoemd in {12} CWA 14169 "Secure signature-creation devices "EAL 4+"" of gelijkwaardige beveiligingscriteria.

6.1.1.3 Algoritme van sleutelparen van de certificaathouders

Het algoritme en de lengte van de cryptografische sleutels dat QuoVadis gebruikt voor het genereren van de sleutels van certificaathouders voldoet aan de eisen, die daaraan zijn gesteld in de lijst van cryptografische algoritmes en sleutellengtes, zoals gedefinieerd in ETSI TS 119 312

6.1.2 Overdracht van private sleutel en SSCD aan certificaathouder

Certificaathouders zijn zelf verantwoordelijk voor de generatie van de prive-sleutels die in hun Certificaat aanvragen, tenzij uitdrukkelijk met QuoVadis overeengekomen. QuoVadis biedt geen escrow, herstel-of back-up faciliteiten.

6.1.5 Sleutellengte

De QuoVadis CSP-Organisatie CA maakt gebruik van een 4.096 bit sleutellengte op basis van sha256WithRSAEncryption.
De lengte van de cryptografische sleutels van de certificaathouders voldoen aan de eisen, die daaraan zijn gesteld in de lijst van cryptografische algoritmes en sleutellengtes, zoals gedefinieerd in ETSI TS 119 312-1.
Voor de overige informatie over de uitgegeven certificaten verwijzen wij naar de certificaatprofielen, die zijn opgenomen in hoofdstuk 7 van dit CPS.

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

De sleutelgebruiksextensie (key usage) in X.509 v3 certificaten (RFC5280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile) definieert het doel van het gebruik van de sleutel vervat in het certificaat. QuoVadis heeft het gebruik van sleutels in het certificaat aan gegeven, conform de eisen die daaraan zijn gesteld in bijlage A 'Certificaat- en CRL- en OCSP-profielen' van dit CPCPS – zie Hoofdstuk 7 inzake Certificaatprofielen.
De QuoVadis CSP-Organisatie CA private sleutel wordt uitsluitend 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-Organisatie 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-Organisatie CA sleutels niet in escrow uit bij een onafhankelijke derde.

6.2.3.1-4 Escrow van private sleutels van certificaathouders

QuoVadis maakt geen backup van de private sleutels derhalve is tevens het vertrouwelijkheidcertificaat niet in Escrow.

6.2.4 Private sleutel back-up

De Private Sleutel van de QuoVadis CSP-Organisatie CA wordt in versleutelde staat gebackupt, on-site onderhouden en daarnaast in een beveiligde off-site locatie bewaard.
Private sleutels van Certificaathouders worden door QuoVadis niet gebackupt.

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 het handtekeningcertificaat en het authenticiteitcertificaat te archiveren.

6.2.6 Toegang tot private sleutels in cryptografische module

De sleutels van de QuoVadis CSP-Organisatie 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-Organisatie 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-Organisatie 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 van de QuoVadis CSP-Organisatie CA worden vernietigd wanneer zij niet meer nodig zijn, of wanneer de Certificaten waarmee zij corresponderen zijn verlopen of ingetrokken.
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 metaal schredder). Dergelijke vernietiging wordt altijd gedocumenteerd.

6.2.11 Cryptografische classificatie van de module en SSCD’s

De cryptografische modules die door de QuoVadis CSP- Organisatie 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+ en aan de eisen, gesteld bij of krachtens het Besluit elektronische handtekeningen artikel 5, onderdelen a,b,c en d.

6.2.11.1 Eisen voor veilige middelen voor het aanmaken van elektronische hand-tekeningen

De door QuoVadis uitgegeven of aanbevolen veilige middelen voor het aanmaken van elektronische handtekeningen (SSCD's) voldoen aan de eisen gesteld in document {7} CWA 14169 "Secure signature-creation devices "EAL 4+"" en aan de eisen, gesteld bij of krachtens het Besluit elektronische handtekeningen artikel 5, onderdelen a,b,c en d.

6.2.11.2 Alternatieve eisen voor veilige middelen.

In plaats van conformiteit aan CWA 14169 aan te tonen mag QuoVadis SSCD's uitgeven of aanbevelen die volgens een ander protection profile zijn gecertificeerd tegen de Common Criteria (ISO/IEC 15408) op niveau EAL4+ of die een vergelijkbaar betrouwbaarheidsniveau

hebben. Dit dient dan te worden vastgesteld door een testlaboratorium dat geaccrediteerd is voor het uitvoerenvan Common Criteria evaluaties.

6.2.11.3 Overeenstemming eisen voor veilige middelen.

De overeenstemming van SSCD's met de eisen zoals genoemd in PKIo-eis nr104 als vermeld onder 6.2.11 moet zijn vastgesteld door een volgens de Telecommunicatiewet (TW) artikel 18.17, derde lid, aangewezen instantie voor de keuring van veilige middelen voor het aanmaken van elektronische handtekeningen. Zie hiervoor ook de Regeling elektronische handtekeningen, art. 4 en 5.

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 7 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- Organisatie CA (G2) eindigt op 23-03-2020.
- De geldigheidsduur van de PKIoverheid Organisatie certificaten is maximaal 36 maanden kan naar keuze worden aangegeven op het certificaataanvraagformulier.

6.3.2 Gebruiksduur van sleutels en eindgebruikercertificaten

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

6.4 Activeringsgegevens

6.4.1.1 Genereren en installeren van activeringsgegevens

Activeringsgegevens worden door de Certificaathouder altijd geheim gehouden. Activeringsgegevens zijn strikt persoonlijk, mogen niet worden gedeeld en besaat uit minimaal 8 karakters, waarvan tenminste 1 cijfer, 1 hoofdletter en een leesteken. Een voorbeeld van een adequate procedurele maatregel is bijvoorbeeld het opslaan van de activeringsgegevens in een enveloppe in een afgesloten kluis.

6.4.1.2 Deblokkering van activeringsgegevens

QuoVadis ondersteund geen deblokkering van het SSCD.

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 op SSCD 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 het functioneren van de applicatie.

6.7.1.1 Netwerk beveiliging

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 status service:

- zijn voorzien van de laatste updates en;
- de webapplicatie alle invoer van gebruikers controleert en filtert en;
- de webapplicatie de dynamische uitvoer codeert en;
- de webapplicatie een veilige sessie met de gebruiker onderhoudt en;
- de webapplicatie op een veilige manier gebruik maakt van een database.

QuoVadis gebruikt hiervoor de "Checklist beveiliging webapplicaties" van het NCSC als guidance.

6.7.1.2 Intern testen Netwerk beveiliging

QuoVadis voert minimaal maandelijks, met behulp van een audit tool, een security scan uit op haar PKIoverheid infrastructuur. QuoVadis documenteert het resultaat van elke security scan en de maatregelen die hierop zijn genomen.

6.7.1.3 Extern testen Netwerk beveiliging

QuoVadis laat minimaal een keer per jaar een pentest uitvoeren op de PKIoverheid internet facing omgeving door een onafhankelijke, ervaren, externe leverancier. QuoVadis documenteert de bevindingen van de pentest, en de maatregelen die hierop worden genomen.

7. Certificaatprofiel

7.1.1 Certificaatprofiel – Authenticiteitcertificaten

De onderstaande certificaatprofiel levert een overzicht van het certificaatprofiel zoals uitgegeven in overeenstemming met het PKIoverheid Programma van Eisen, deel 3a.

PKI Overheid User Authentication - QVO User Auth EKUs				
Basic Contents	**OID**	**Value**	**Fixed/ optional**	**Notes**
Version		2 (V3)	Fixed	
SerialNumber		Automatically generated	Required	
SignatureAlgorithm	1.2.840.113549.1.1.5	Sha256RSA	Fixed	
Issuer•CountryName	2.5.4.6	NL	Fixed	
Issuer•OrganisationName	2.5.4.10	QuoVadis Trustlink BV	Fixed	
Issuer•OrganisationIdentifier	?	NTRNL-30237459	Fixed	
Issuer•OrganizationUnitName	2.5.4.11	Issuing Certification Authority	Fixed	
Issuer•CommonName	2.5.4.3	QuoVadis PKIoverheid Organisatie Persoon CA - G3	Fixed	
Validity•NotBefore		Max 3 years	Required	
Validity•NotAfter		Max 3 years	Required -Max 3	
Subject•CommonName	2.5.4.3	CommonName	Required	Namingconvention changed
Subject•givenname	?	Given Name	Required	Required in G3 optional in G2
Subject•surname	?	Surname	Required	Required in G3 optional in G2
Subject•SerialNumber	2.5.4.5	Subject•SerialNumber	Required	
Subject•OrganisationName	2.5.4.10	Subject•OrganisationName	Required	
SubjectCountryName	2.5.4.6	Country	Required/ Fixed	
SubjectPublicKeyInfo	1.2.840.113549.1.1.1	RSA (2048 Bits)	Required	
Standard Extensions			Fixed	
AuthorityKeyIdentifier	2.5.29.35		Required	
KeyIdentifier		Key ID	Required	
SubjectKeyIdentifier	2.5.29.14		Required	
KeyIdentifier		Key ID	Required	
KeyUsage (CRITICAL)	2.5.29.15		Fixed	
KeyUsage		Digital Signature (80)	Fixed	
CertificatePolicies	2.5.29.32		Fixed	
CertPolicyID		2.16.528.1.1003.1.2.5.1	Fixed	
URL	1.3.6.1.5.5.7.2.1	http://www.quovadisglobal.com/repository	Fixed	
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	
subjectAltName			Optional	
Rfc822Name		Rfc822 email address	Optional	
User Principle Name (MS UPN)	1.3.6.1.4.1.311.20.2.3	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1.	Required	
User Principle Name (MS UPN)	1.3.6.1.4.1.311.20.2.3	user@domain (used for Single Sign on)	Optional	
extKeyUsage			Required	
Id-kp-clientAuth	1.3.6.1.5.5.7.3.2	Client Authentication	Required	

ID_KP_DOCUMENT_SIGNING	1.3.6.1.4.1.311.10.3.12	document Signing	Required	
id_kp_emailProtection	1.3.6.1.5.5.7.3.4	E-Mail Protection	required	
				No longer allowed in G3
CRLDistributionPoints			Fixed	
DistributionPoint•FullName		http://crl.quovadisglobal.com/pkiopersong3.crl	Fixed	
Private Extensions			Fixed	
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1		Fixed	
Id-ad-ocsp	1.3.6.1.5.5.7.48.1	http://uw.ocsp.quovadisglobal.com	Fixed	
Id-ad-caIssuers	1.3.6.1.5.5.7.48.2	http://trust.quovadisglobal.com/pkiopersong3.crt	Fixed	

7.1.2 Certificaatprofiel – Handtekeningcertificaten

De onderstaande certificaatprofiel levert een overzicht van het certificaatprofiel zoals uitgegeven in overeenstemming met het PKIoverheid Programma van Eisen, deel 3a.

PKI Overheid User Authentication - QVO User QualSign				
Basic Contents	**OID**	**Value**	**Fixed/ optional**	**Notes**
Version		2 (V3)	Fixed	
SerialNumber		Automatically generated	Required	
SignatureAlgorithm	1.2.840.113549.1.1.5	Sha256RSA	Fixed	
Issuer•CountryName	2.5.4.6	NL	Fixed	
Issuer•OrganisationName	2.5.4.10	QuoVadis Trustlink BV	Fixed	
Issuer•OrganisationIdentifier	?	NTRNL-30237459	Fixed	
Issuer•OrganizationUnitName	2.5.4.11	Issuing Certification Authority	Fixed	
Issuer•CommonName	2.5.4.3	QuoVadis PKIoverheid Organisatie Persoon CA - G3	Fixed	
Validity•NotBefore		Max 3 years	Required	
Validity•NotAfter		Max 3 years	Required - Max 3	
Subject•CommonName	2.5.4.3	CommonName	Required	
Subject•givenname	?	Given Name	Required	Required in G3 optional in G2
Subject•surname	?	Surname	Required	Required in G3 optional in G2
Subject•SerialNumber	2.5.4.5	Subject•SerialNumber	Required	
Subject•OrganisationName	2.5.4.10	Subject•OrganisationName	Required	
SubjectCountryName	2.5.4.6	Country	Required	
SubjectPublicKeyInfo	1.2.840.113549.1.1.1	RSA (2048 Bits)	Required	
Standard Extensions			Fixed	
AuthorityKeyIdentifier	2.5.29.35		Required	
KeyIdentifier		Key ID	Required	
SubjectKeyIdentifier	2.5.29.14		Required	
KeyIdentifier		Key ID	Required	
KeyUsage (CRITICAL)	2.5.29.15		Fixed	
KeyUsage		Non-Repudiation (40)	Fixed	
CertificatePolicies	2.5.29.32		Fixed	
CertPolicyID		2.16.528.1.1003.1.2.5.2	Fixed	
URL	1.3.6.1.5.5.7.2.1	http://www.quovadisglobal.com/repository	Fixed	
User Notice		Reliance on this certificate by any party assumes acceptance of the relevant	Fixed	

		QuoVadis Certification Practice Statement and other documents in the QuoVadis repository (http://www.quovadisglobal.com).		
subjectAltName			Optional	
Rfc822Name		Rfc822 email address	Optional	
User Principle Name (MS UPN)	1.3.6.1.4.1.311.20.2.3	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1	Required	
extKeyUsage			Required/ optional	
ID_KP_DOCUMENT_SIGNING	1.3.6.1.4.1.311.10.3.12	document Signing	Required	
id_kp_emailProtection	1.3.6.1.5.5.7.3.4	E-Mail Protection	required	
CRLDistributionPoints			Fixed	
DistributionPoint•FullName		http://crl.quovadisglobal.com/pkiopersong3.crl	Fixed	
Private Extensions			Fixed	
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1		Fixed	
Id-ad-ocsp	1.3.6.1.5.5.7.48.1	http://uw.ocsp.quovadisglobal.com	Fixed	
Id-ad-caIssuers	1.3.6.1.5.5.7.48.2	http://trust.quovadisglobal.com/pkiopersong3.crt	Fixed	
qcStatements	1.3.6.1.5.5.7.1.3		Fixed	
id-etsi-qcs-QcCompliance	id-etsi-qcs-1	0.4.0.1862.1.1	Fixed	
d-etsi-qcs-QcSSCD	id-etsi-qcs 4	0.4.0.1862.1.4	Fixed	
id-etsi-qct-esign	id-etsi-qcs-QcType-1	0.4.0.1862.1.6.1	Fixed	
id-etsi-qcs-QcPDS	Id-etsi-qcs 5	0.4.0.1862.1.5	Fixed	Include referral to PDS

7.1.3 Certificaatprofiel – Vertrouwelijkheidcertificaten

De onderstaande certificaatprofiel levert een overzicht van het certificaatprofiel zoals uitgegeven in overeenstemming met het PKIoverheid Programma van Eisen, deel 3a.

PKI Overheid User Encryption - QVO User encr EKUs				
Basic Contents	**OID**	**Value**	**Fixed/ optional**	**Notes**
Version		2 (V3)	Fixed	
SerialNumber		Automatically generated	Required	
SignatureAlgorithm	1.2.840.113549.1.1.5	Sha256RSA	Fixed	
Issuer•CountryName	2.5.4.6	NL	Fixed	
Issuer•OrganisationName	2.5.4.10	QuoVadis Trustlink BV	Fixed	
Issuer•OrganisationIdentifier	?	NTRNL-30237459	Fixed	
Issuer•OrganizationUnitName	2.5.4.11	Issuing Certification Authority	Fixed	
Issuer•CommonName	2.5.4.3	QuoVadis PKIoverheid Organisatie Persoon CA - G3	Fixed	
Validity•NotBefore		Max 3 years	Required	
Validity•NotAfter		Max 3 years	Required -Max 3	
Subject•CommonName	2.5.4.3	CommonName	Required	
Subject•givenname	?	Given Name	Required	Required in G3 optional in G2
Subject•surname	?	Surname	Required	Required in G3 optional in G2
Subject•SerialNumber	2.5.4.5	Subject•SerialNumber	Required	
Subject•OrganisationName	2.5.4.10	Subject•OrganisationName	Required	
SubjectCountryName	2.5.4.6	Country	Required/ Fixed	
SubjectPublicKeyInfo	1.2.840.113549.1.1.1	RSA (2048 Bits)	Required	
Standard Extensions			Fixed	
AuthorityKeyIdentifier	2.5.29.35		Required	
KeyIdentifier		Key ID	Required	
SubjectKeyIdentifier	2.5.29.14		Required	
KeyIdentifier		Key ID	Required	
KeyUsage (CRITICAL)	2.5.29.15		Fixed	
Key usage		Key encipherment	fixed	
Key usage		Data encipherment	Fixed	
CertificatePolicies	2.5.29.32		Fixed	
CertPolicyID		2.16.528.1.1003.1.2.5.3	Fixed	
URL	1.3.6.1.5.5.7.2.1	http://www.quovadisglobal.com/repository	Fixed	
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	
subjectAltName			Optional	
Rfc822Name		Rfc822 email address	Optional	
User Principle Name (MS UPN)	1.3.6.1.4.1.311.20.2.3	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1	Required	
User Principle Name (MS UPN)	1.3.6.1.4.1.311.20.2.3	user@domain (used for Single Sign on)	Optional	
extKeyUsage			Required/ Optional	
Id_efs_crypto	1.3.6.1.4.1.311.10.3.4	Encrypting File System	Required	
id_kp_emailProtection	1.3.6.1.5.5.7.3.4	E-Mail Protection	Required	

CRLDistributionPoints			Fixed	
DistributionPoint•FullName		http://crl.quovadisglobal.com/pkiopersong3.crl	Fixed	
Private Extensions			Fixed	
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1		Fixed	
Id-ad-ocsp	1.3.6.1.5.5.7.48.1	http://uw.ocsp.quovadisglobal.com	Fixed	
Id-ad-caIssuers	1.3.6.1.5.5.7.48.2	http://trust.quovadisglobal.com/pkiopersong3.crt	Fixed	

7.2 Certificaatprofiel – CRL

De onderstaande CRL-certificaatprofiel levert een overzicht van het certificaatprofiel zoals uitgegeven in overeenstemming met het PKIoverheid Programma van Eisen, deel 3a.

Basic Contents	OID	Value	Fixed/Required/ Optional
Version		V2	Fixed
SignatureAlgorithm	1.2.840.113549.1.1.11	sha256RSA	Fixed
Issuer•CountryName	2.5.4.6	NL	Fixed
Issuer•OrganisationName	2.5.4.10	QuoVadis Trustlink BV	Fixed
Issuer•OrgIdentifier		NTRNL-30237459	Fixed
Issuer•CommonName	2.5.4.3	QuoVadis PKIoverheid Organisatie Persoon CA - G3	Fixed
Effective date		Date	Required
Next update		Date	Required
revokedCertificates		List of revoked Certificates	Required
CRL Extensions			Fixed
AuthorityKeyIdentifier	2.5.29.35		Fixed
KeyIdentifier		Key ID	Fixed
CRL Number	2.5.29.20		Required
CRL Number		CRL Number	Required

7.3 Certificaatprofiel – OCSP

De onderstaande OCSP-certificaatprofiel levert een overzicht van het certificaatprofiel zoals uitgegeven in overeenstemming met het PKIoverheid Programma van Eisen, deel 3a.

Basic Contents	OID	Value	Fixed/Required/ Optional
Version		2 (V3)	Fixed
SerialNumber	2.5.4.5	Automatically generated	Required
SignatureAlgorithm	1.2.840.113549.1.1.5	sha256RSA	Fixed
Issuer•CountryName	2.5.4.6	NL	Fixed
Issuer•OrganisationName	2.5.4.10	QuoVadis Trustlink BV	Fixed
Issuer•OrganisationName		NTRNL-30237459	
Issuer•CommonName	2.5.4.3	QuoVadis PKIoverheid Organisatie Persoon CA – G3	Fixed
Validity•NotBefore		10 years	Required
Validity•NotAfter		10 years	Required
Subject•CommonName	2.5.4.3	QuoVadis OCSP Authority Signature	Required
Subject•OrganisationName	2.5.4.10	QuoVadis Limited	Required
Subject•OrganisationUnitName	2.5.4.11	OCSP Responder	Optional
SubjectCountryName	2.5.4.6	BM	Required
SubjectPublicKeyInfo	1.2.840.113549.1.1.1	RSA (2048 bits)	Required
Standard Extensions			Fixed
AuthorityKeyIdentifier	2.5.29.35		Fixed
KeyIdentifier		Key ID	Fixed
SubjectKeyIdentifier	2.5.29.14		Required
KeyIdentifier		Key ID	Required
KeyUsage (CRITICAL)	2.5.29.15		Fixed
KeyUsage		Digital Signature	Fixed
CertificatePolicies	2.5.29.32		Fixed
CertPolicyID		[2] Certificate Policy: Policy Identifier = 1.3.6.1.4.1.8024.1.300	Fixed
extKeyUsage (CRITICAL)			Fixed
id-kp-OCSPSigning	1.3.6.1.5.5.7.3.9	OCSP Signing	Fixed
ocspNoCheck	1.3.6.1.5.5.7.48.1.5		Fixed
ocspNoCheck	1.3.6.1.5.5.7.48.1.5	ocspNoCheck is present	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. QuoVadis verkreeg in 2008 het conformiteitscertificaat hiervoor met nummer ETS-010, afgegeven door de geaccrediteerde certificatie-instelling BSI Management Systems B.V. (BSI) te Amsterdam. Daarbij is tevens aangegeven dat QuoVadis ook voldoet aan de aanvullende eisen zoals neergelegd in de regulatie eu 910-2014. Het conformiteitscertificaat heft een geldigheid van drie jaren en is tussentijds onderhevig aan tussentijdse controle-audits (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, 3b. Delen 3C(2014), , 3F(2014), 3G,Hen I (2016) zijn hier vervolgens aan toegevoegd. Deel 3Eis gevolgd uit de splitsing van deel B in 2014.

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 certificatie-audit 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 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

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;

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.

9.2.1.1 Verzekeringsdekking

QuoVadis heeft een bedrijfsaansprakelijkheidsverzekering (inclusief dekking voor productaansprakelijkheid) ten bedrage van $10.000.000,00 per jaar.
De verzekering dekt minimaal het volgende af:
1. vorderingen tot schadevergoeding die voortvloeien uit een handeling, fout of omissie of eenonopzettelijke schending van het contract, of verwaarlozing in de uitgifte of handhaving van EV-certificaten door QuoVadis en;
2. vorderingen tot schadevergoeding die voortvloeien uit schending van het eigendomsrecht van een derde partij (met uitzondering van het auteursrecht, en schending van het handelsmerk) of vorderingen die voortvloeien uit schending van de privacy of belastering van een derde partij door QuoVadis.

9.2.1.2 Verzekeringsdekking

De bedrijfsaansprakelijkheidsverzekering (inclusief dekking voor productaansprakelijkheid) is afgesloten bij een verzekeringsmaatschappij die minimaal over een “A-“ rating beschikt bij een bekend ratingbureau.

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-Organisatie CA:

- De compromittering van de private sleutel van de QuoVadis CSP-Organisatie CA, in welk geval er een openbaarmaking mag worden gepubliceerd dat de private sleutel is gecompromitteerd;
- De opheffing van de QuoVadis CSP-Organisatie 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 als zodanig 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 ondertekend 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 EV-SSL certificaat”;
  (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, entiteit 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 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 praktijken 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 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. 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 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 "niveau 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

Voor definities en afkortingen aangaande deze CPS verwijzen wij naar het, door Logius beheerde, PvE deel 4.

Dit deel kan gevonden worden op: https://www.logius.nl/producten/toegang/pkioverheid/aansluiten/programma-van-eisen/