Certification Practice Statement PKIoverheid Domeinen Private Services G1

Versie: 1.3
Datum: 12 juli 2019
PvE 3G: 4.7

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

Domein Private services (g1):
Services ï Athenticiteit 2.16.528.1.1003.1.2.8.4
Services ï Vertrouwelijkheid 2.16.528.1.1003.1.2.8.5

4 Operationele eisen 26
4.1 Certificaataanvraag..... 26
4.1.1

5.5.1 Aard van gearchiveerde gegevens 45
5.5.3 Bescherming van het archief 46
5.5.4 Back-up procedures m.b.t. het archief 46
5.5.5 Eisen

9.1.5 Beleid inzake terugbetaling 69
9.2 Financiële verantwoordelijkheid en aansprakelijkheid 70
9.2.1 Verzekeringsdekking 70
9.3 Vertrouwelijkheid van bedrijfsgevoelige gegevens 70
9.3.1 Toepassingsgebied vertrouwelijke informatie 70
9.3.2 Gegevens die als niet-vertrouwelijk worden beschouwd 71
9.3.3 Verantwoordelijkheid vertrouwelijke informatie te beschermen 71
9.4 Vertrouwelijkheid van persoonlijke informatie 71
9.4.1 Vertrouwelijke informatie 71
9.4.2 Vertrouwelijk behandelde informatie 71
9.4.3 Niet-vertrouwelijke informatie 72
9.4.4 Verantwoordelijkheid om vertrouwelijke informatie te beschermen 72
9.4.5 Melding van- en instemming met het gebruik van persoonsgegevens 72
9.4.6 Overhandiging van gegevens op last 0.369 R1 /MCID 13 >BDC q0.00000912 0 612 792 reW* nBT/F1 9.9

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 (TSP) worden gesteld voor het uitgeven en beheren van deze certificaten worden gesteld, zijn beschreven in het Prograoorden

toepassing zijn. Voor Netsec geldt dat eisen 1h, 3a, 3e, 4c.i en 4f niet normatief zijn (ETSI CP OID 0.4.0.2042.1.7);

- die specifiek door en voor de PKIoverheid zijn opgesteld.

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 Verwijzinge2aflijkheidre5(eS0.00000912 0 612 792 reW* n

Voor verdere details zie de tabel in sectie 7.1

1.3 Gebruikersgemeenschap

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

1.3.1 Partijen binnen de gebruikersgemeenschap

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 private root CA ï G1
- Staat der Nederlanden Private Services CA ï G1

QuoVadis TSP PKI Overheid private services Certification Authority (TSP-PKI Overheid private services CA)

De QuoVadis PKI Overheid private services CA G1 wordt beheerd in het beveiligde datacenter van QuoVadis in Bermuda en deze geeft de certificaten uit ten behoeve van certificaathouders binnen de PKI voor de overheid en in overeenstemming met dit CPS.

Een overzicht van certificaten die worden uitgegeven is opgenomen in 1.4.

1.3.2 Registration Authorities

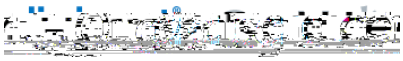
QuoVadis Registration Authority (QuoVadis RA)

De QuoVadis Registration Authority in Nieuwegein verzorgt de identificatie en registratie van de abonnee en de certificaatbeheerder en verzorgt de intrekkingen van uitgegeven certificaten. Om een PKI Overheid certificaat te verkrijgen moet de registrant een aantal aanvraagformulieren invullen. Deze zijn omschreven in paragraaf 3.2 van de QuoVadis Certificaatprocedures. De aanvraag kan tevens on-line gedaan worden via https://www.quovadisglobal.nl waar een aanvraag module draait die in ons Data Centre in Zwitserland wordt gehost

1.3.3 Eindgebruikers

Abonnee

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



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 onderdeel van een organisatorische entiteit waarvoor een abonnee de contracterende partij is. Binnen de Certificate Policy Extended Validation wordt de volgende invulling aan de term certificaathouder gegeven: ‘een apparaat of een systeem (een niet-

1.5 CPS-beheer

2 Publicatie en verantwoordelijkheid voor

Services - Vertrouwelijkheid OID 2.16.528.1.1003.1.2.8.5

2.2.3 Informatie

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

2.2.4 Conformatie

QuoVadis conformeert zich aan de huidige versie van de CA/Browser Forum Guidelines for Issuance and Management of Exteded Validation Certificates zoals gepubliceerd op http://www.cabforum.org. Mocht er een inconsistentie aanwezig zijn tussen het PKIoverheid Programma van Eisen deel 3G en de betreffende Requirements, waardoor niet tenminste tegemoet wordt gekomen aan de hierin beschreven minimale eisen, dit ter beoordeling door de PA, dan prevaleert het gestelde in de Requirements.

2.2.5 Structuur CPS

Dit CPS van QuoVadis is gestructureerd volgens RFC 2527, RFC 3647 of het

3 Identificatie en Authentificatie

3.1 Naamgeving

3.1.1 Soorten naamformaten

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

3.1.2 Noodzaak gebruik betekenisvolle namen

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

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

3.1.3 Pseudoniemen

Het gebruik van anonieme certificaten of pseudoniemen is niet toegestaan.

3.1.4 Regels voor interpreteren verschillende naamsvormen

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

3.1.5 Uniciteit van namen.

De DistinguishedName van de Service in een certificaat dat onder dit CPS is uitgegeven, is te allen tijde uniek voor deze Service en wordt niet uitgegeven aan een andere Service.

Het is de taak van de QuoVadis RA te verifiëren dat de DistinguishedName van de certificaathouder nog niet is opgenomen in de elektronische opslagplaats voor certificaten (de QuoVadis X.500 directory).

QuoVadis mag, indien nodig, additionele nummers of letters aan de CommonName van het certificaat-subject toevoegen om zodoende onderscheid te maken tussen twee bestaande certificaten die anders dezelfde subjectnaam zouden hebben.

Elk Certificaat krijgt verder een uniek serienummer toegewezen, dat een eenduidige en unieke identificatie van de Service mogelijk maakt.

3.1.6 Erkenning, authenticatie en de rol van handelsmerken

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

3.1.7 Geschillen

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

3.2 Initiële identiteitsvalidatie

3.2.0.1 Initiële identiteitsvalidatie

De gegevens die QuoVadis gebruikt om te verifiëren:

- of de abonnee een bestaande en legale organisatie is;
- of de organisatienaam, die in het certificaat wordt opgenomen, juist en volledig is en overeenkomt met de door de abonnee aangemelde organisatienaam;
- of het door de abonnee opgegeven adres van de organisatie juist en volledig is en dat het ook het adres is waar zij haar werkzaamheden uitvoert;
- of het door de abonnee opgegeven algemene telefoonnummer van de

3.2.1 Methode om bezit van private sleutel aan te tonen.

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

Het op een veilige manier aanleveren moet als volgt plaatsvinden:

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

- Het type huisvesting van de abonnee en of dit de locatie is waar de organisatie naar alle waarschijnlijk haar werkzaamheden uitvoert;
- Of er permanente bewijzeringsborden aanwezig zijn die de locatie van de abonnee identificeren;
- Een of meerdere foto's van (i) de buitenkant van de huisvesting van de abonnee (waarop, indien aanwezig, de bewijzeringsborden en het adresbord van de straat staan) en (ii) de receptiebalie of kantoorwerkruimte van de abonnee.

Als alternatief zal QuoVadis ook een verklaring van een externe accountant of notaris accepteren waarin het opgegeven adres wordt bevestigd en ook dat dit het adres is waar de organisatie haar werkzaamheden uitvoert.

Verificatie telefoonnummer organisatie

QuoVadis verifiërt dat het door de abonnee opgegeven algemene telefoonnummer van de organisatie, juist en volledig is. Als bewijs van juistheid en het bestaan van het opgegeven algemene telefoonnummer van de organisatie zal QuoVadis:

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

Verificatie leeftijd organisatie

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

Als bewijs van juistheid en het bestaan van de opgegeven bet

Als bewijs v-3(h)-5(e)-3(t)] TJETQq0.00000912 0 612 792 reW* nBT/F1 12 Tf1 0 0 1 108.02 328.13 Tm0.282 0.33

beëindigd. In het aanstelings formulier voor de certificaatbeheerder is bovenstaande afwijking door QuoVadis standaard opgenomen.

Verbijzondering verificatie identiteit certificaatbeheerder

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

Verificatie certificaatbeheerder

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

Er dient bewijs aan QuoVadis te worden overlegd van:

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

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

3.2.5 Authorisatie van de certificaathouder (Service)

3.2.5.1 Controle auth rg04n 0.369 rg0.282 0.337 0.369 RG[te)4(n)-3(z)10(ij)4t765 rg0.0.3(rde

- of de certificaatbeheerder toestemming heeft verkregen van de abonnee om aan hem opgedragen handelingen uit te voeren (ingeval de certificaatbeheerder het registratieproces uitvoert).

Opmerking

De "certificaatbeheerder" die handelingen overneemt van de certificaathouder behoeft

moet gebruik maken van een command line-programma, indien gebruik wordt gemaakt van een WHOIS service die gegevens aanbiedt via HTTP én;

- in de WHOIS service, de naam, het woonadres en de administratieve contactpersoon van de organisatie verifiëren en deze gegevens vergelijken met de geverifieerde abonnee gegevens en vastleggen dat er geen inconsistentie is tussen beide gegevens én;
- verifiëren dat de domeinnaam niet voorkomt op een spam- en/of phishing blacklist. Gebruik hiervoor tenminste http://www.phishtank.com.

Als de domeinnaam voorkomt op phishtank of eventueel een andere blacklist die is geraadpleegd, zal QuoVadis tijdens het verificatieproces extra zorgvuldig om te gaan met de aanvraag van het betreffende services certificaat.

De gegevens die de TSP gebruikt om te verifiëren dat de abonnee de geregistreerde eigenaar is van de in de aanvraag vermelde domeinnaam (FQDN) mogen niet ouder zijn dan 13 maanden anders moeten de gegevens opnieuw worden opgevraagd en geverifieerd.

Als de abonnee aangeeft dat het exclusief geautoriseerd is door de geregistreerde domeinnaam eigenaar om, namens de geregistreerde domeinnaam eigenaar, de domeinnaam te gebruiken dan zal QuoVadis, naast het uitvoeren van de bovenstaande controles:

- een verklaring van de geregistreerde domeinnaam eigenaar opvragen (b.v. via e-mail of telefoon) waarin de geregistreerde domeinnaam eigenaar moet bevestigen dat de abonnee het exclusieve gebruiksrecht heeft inzake de domeinnaam (FQDN) én;
- een schriftelijke en ondertekende verklaring van een notaris of externe accountant opvragen en verifiëren waarin moet staan voor welke domeinnaam (FQDN) de abonnee, namens de geregistreerde domeinnaam eigenaar, het exclusieve gebruiksrecht heeft gekregen én;
- verifiëren dat de domeinnaam (FQDN) geen generiek TopLevelDomein (gTLD) of land code TopLevelDomein (ccTLD) betreft. Voor deze domeinnamen mag alleen de abonnee als geregistreerde domeinnaam eigenaar een aanvraag doen.
- Een verklaring van de geregistreerde domeinnaam eigenaar of notaris of externe accountant mag niet ouder zijn dan 13 maanden. De validatie van het FQDN is conform paragraaf 3.2.2.4. uit de baseline requirements.
- Voor elke FQDN die is vermeld in een certificaat, bevestigt QuoVadis dat, vanaf

‡ 1. Rechtstreeks te communiceren met de domeinnaamregistrant per e-mail, fax of post met de domeinnaamregistrator. Uitgevoerd in overeenstemming met BR sectie 3.2.2.4.2 met een

respons te ontvangen met behulp van de Random Value, uitgevoerd in overeenstemming met BR Paragraaf 3.2. 2.4.14;

‡ 10. Bevestiging van de controle van de aanvrager over de FQDN door het telefoonnummer van het Domain Contact te bellen en een bevestigend antwoord te krijgen om de geautoriseerde Domeinnaam te valideren. Elk telefoongesprek kan de controle over meerdere geautoriseerde domeinnamen bevestigen op voorwaarde dat hetzelfde domeincontacttelefoonnummer wordt vermeld voor elke geverifieerde domeinnaam die wordt geverifieerd en ze bieden een bevestigend antwoord voor elke geautoriseerde domeinnaam, uitgevoerd in overeenstemming met BR Paragraaf 3.2.2.4.15; en

‡ 11. Bevestiging van de controle van de aanvrager over de FQDN door het telefoonnummer van de DNS TXT Record Phone Contact te bellen en een bevestigingsantwoord te verkrijgen om de geautoriseerde Domeinnaam te valideren. Elk telefoongesprek kan de controle over meerdere geautoriseerde domeinnamen bevestigen op voorwaarde dat hetzelfde telefoonnummer van de telefoonnummer van de DNS TXT Record Phone wordt vermeld voor elke geautoriseerde domeinnaam die wordt vermeld geverifieerd en ze bieden een bevestigende reactie voor elke geautoriseerde domeinnaam, uitgevoerd in overeenstemming met BR Sectie 3.2.2.4.16.

‡ Hoogrisicodomeinen

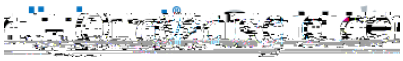
‡ QuoVadis onderhoudt een lijst van High Risk Domains en heeft technische controles geïmplementeerd om de uitgifte van certificaten aan bepaalde domeinen te voorkomen. QuoVadis volgt gedocumenteerde procedures die extra verificatie-activiteit voor hoog-risico certificaataanvragen identificeren en vereisen, voorafgaand aan de goedkeuring van het certificaat.

3.2.5.4 Authenticatie voor een IP-adres

‡ Voor elk IP-adres vermeld in een certificaat, bevestigt QuoVadis dat de aanvrager vanaf het moment dat het certificaat werd uitgegeven het IP-adres beheerde door:

‡ 1. Praktische controle over het IP-adres te laten tonen door de aanvrager door de aanwezigheid van een Request Roken of Random Value in de inhoud van een bestand of webpagina te bevestigen in de vorm van een metatag in "/.well-known/pki- validatieòop het IP-adres, uitgevoerd in overeenstemming met BR Sectie 3.2.2.5.1;

‡ 2. Bevestiging van de controle van de aanvrager over het IP-adres door een Random Value te verzenden via e-mail, fax, sms of post en vervolgens een



Hergebruik sleutels bij vernieuwing certificaat

QuoVadis vernieuwd geen Service certificaten zonder vernieuwing van de sleutels.

Dit betekent tevens dat voor het nieuwe certificaat altijd een nieuw sleutelpaar moet worden gegenereerd door de abonnee

dat het services server certificaat alleen op een server wordt gezet die ten minste bereikbaar is met een van de FQDNôs in dit services server certificaat;

‡ de abonnee moet verklaren dat het Services certificaat alleen wordt gebruikt in overeenstemming met de regelgeving die op haar bedrijfsvoering van toepassing is en alleen in relatie met de werkzaamheden van de abonnee en in overeenstemming met de bepalingen van de voorliggende overeenkomst;

o11‡(sv)10(o)-3(e)-3(ri)5(n)-3(g)6(v)8(a)-13(n)-3(t)-3(o)6(e)-3(p)-3(a)-3(ssing)4( )] TJETQq0.0000091

4.4 Acceptatie van Certificaten

4.4.1.1 Verificatie bevoegd vertegenwoordiger

QuoVadis zal de handtekening van de Bevoegde Vertegenwoordiger op de abonnee

niet geheel accuraat blijkt te zijn, dan dient de Certificaatbe-heerder deze tijdens het uitgifte process aan te passen of als achteraf blijkt dat de gegevens in het certificaat onjuist zijn per omgaande een verzoek tot intrekking te doen. De acceptatie van het Certificaat bevestigt de abonnee of Certificaatbeheerder middels de afronding van de uitgifte procedure in TrustLink Enterprise.

4.5 Sleutelpaar en Certificaatgebruik

4.5.2.1 Verplichtingen van de Certificaatbeheerder

In de gebruikersvoorwaarden die, door de certificaatbeheerder, 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 (het

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.

Indien vereist door de BR (alle TLS / SSL-certificaten) of andere branchevereisten, zal de QuoVadis OCSP-responder op een aanvraag voor de status van een certificaat dat nog niet is uitgegeven, niet reageren met een "good" status

4.9.9.8 Ondersteunde OCSP responses

Als de OCSP responder van QuoVadis een statusverzoek ontvangt van een certificaat dat niet is uitgegeven, dan zal de responder niet antwoorden metstatus ñgoodò De QuoVadis registreerd dergelijke verzoeken aan de responder als onderdeel van de beveiligingsprocedures en zal indien noodzakelijk hierop acteren.

4.9.13 Schorsing van certificaten

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

4.10.1 Operationele eigenschappen

QuoVadis zal met betrekking tot zijn OCSP en CRL dienstverlening passende server capaciteit aanhouden waarmee een response tijd wordt gegarandeerd van 10 seconden of minder onder normale omstandigheden.

4.10.2 Certificate Status Service

De maximale tijdsduur, waarbinnen QuoVadis de beschikbaarheid van de revocation

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.

De RA werkzaamheden worden verricht vanuit QuoVadis Trustlink B.V. gevestigd te Nieuwegein. Quovadis Trustlink B.V. maakt voor identiteitsvaststelling, in bepaalde gevallen, tevens gebruik van de diensten geleverd door de AMP Groep gevestigd in Houten.

5.1.2

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 Afvalverwerking

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:

- De security officer ziet toe op de implementatie en naleving van de vastgestelde beveiligingsrichtlijnen.

Systeem auditor

- De systeem auditor vervult een toezichthoudende rol en geeft een onafhankelijk oordeel over de wijze waarop de bedrijfsprocessen zijn ingericht en over de wijze waarop aan de eisen ten aanzien van de betrouwbaarheid is voldaan.

Systeembeheerder

- De systeembeheerder beheert de TSP-systemen, waarbij het installeren, configureren en onderhouden van de systemen is inbegrepen.

CSP-operators

- De TSP-operators zijn verantwoordelijk voor het dagelijks bedienen van de CSP-systemen voor onder meer registratie, het genereren van certificaten, het leveren van een SSCD/QSCD aan de certificaathouder en revocation management.

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 PKIoverheid CAûs.

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

CA-sleutelpaargeneratie en initialisatie vereist per geval de actieve participatie van ten

- 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 rampenscenarioûs 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;

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

QuoVadis 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.

5.4.6 De back-up procedures gelden voor de PKIoverheid omgeving, inclusief de QuoVadisPKI Overheid CAûs en de Registration Authority-

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 PKIoverheid CAôs systeem werken. 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 CRLôs

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 ñDisaster Recovery Programmaò vastgelegd in het QuoVadis Calamiteitenplan. Het doel van dit plan is om kernactiviteiten van het bedrijf zo snel

‡

dienst (intrekkingsfaciliteit) en het bewaren van de gearchiveerde documenten inzake registratie.

sleutelparen van de certificaathouders

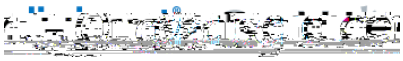
- In de overeenkomst die wordt gesloten tussen TSP en abonnee, is een verklaring opgenomen dat de abonnee de private sleutel genereert, opslaat en gebruikt op een gekwalificeerd middel voor elektronische handtekeningen zoals een HSM dat voldoet aan de eisen genoemd in CWA 14169 Secure signature-creation devices of EN 419 211 voor Qualified signature-creation devices "EAL 4+" of gelijkwaardige beveiligingscriteria zoals FIPS 140-2 level 3.
- Hiervan dient de abonnee bij de aanvraag bewijs te overhandigen door middel van het overleggen van de certificering van het veilig middel en indien nodig een screenshot van de instelling van het veilige middel op FIPS140-2 level 3.
- Een bepaling wordt opgenomen in de overeenkomst tussen de TSP en de abonnee waarin staat dat de abonnee verklaart dat de private sleutel (en de daarbij behorende toegangsinformatie b.v. een PINcode), behorend bij de publieke sleutel in het betreffende gekwalificeerde middel is gegenereerd en in de toekomst geheim wordt gehouden en beschermd.
- Hierbij dient de abonnee bewijs te overhandigen van het PKI ceremoniescript dat wordt gehanteerd bij de implementatie van het gekwalificeerde middel voor elektronische handtekeningen en het genereren van het sleutelpaar.
- de TSP aanwezig is bij de PKI ceremonie voor in gebruik name van het gekwalificeerde middel voor elektronische handtekeningen en het genereren van het sleutelpaar. Hiermee kan de TSP zich ook vergewissen van de effectiviteit van getroffen beveiligingsmaatregelen.
- de Abonnee bij registratie ten minste een schriftelijke verklaring overlegt, aantoonbaar te voldoen aan de eisen en/of de voorwaarden die het gekwalificeerde middel voor elektronische handtekeningen stelt aan het gebruik ervan dan wel de certificering van het middel stelt aan de omgeving waarbinnen het geheel wordt beheerd en het beheer zelf.
- De abonnee een schriftelijke verklaring overlegt dat de certificaathouder, systeembeheerders van het gekwalificeerd middel voor elektronische handtekeningen expliciet heeft gemandateerd voor het beheer en dat altijd sprake is van dual control voor toegang tot dit middel.

6.1.2.1 Levering van de private sleutel aan de 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 SSL-sleutel generatie, escrow, herstel-of back-up faciliteiten.

6.1.5.1 Sleutellengte

De lengte van de cryptografische sleutels van de certificaathouders voldoet aan de eisen, die daaraan zijn gesteld in de lijst van cryptografische algoritmes en sleutellengtes, zoals gedefinieerd in ETSI TS 119 312-1.



6.2.5 Archivering van de private sleutel

QuoVadis archiveert in geen geval private sleutels van Certificaathouders.

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

6.2.11.1 Veilige middelen

D

6.3 Overige aspecten van sleutelpaar management

6.3.2.1 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 QuoVadis PKIoverheid Private Services CA - G1 eindigt op 11/Nov/2028.
- De geldigheidsduur van de PKIoverheid Service certificaten uitgegeven onder verantwoordelijkheid van deze CP is maximaal 36 maanden kan naar keuze worden aangegeven op het certificaataanvraagformulier.

6.3.2.3 Geldigheidsduur van sleutels en certificaten

Op het moment van uitgifte van het eindgebruikercertificaat is de resterende geldigheidsduur van de QuoVadis PKI Overheid CA's altijd langer dan de gespecificeerde geldigheidsduur van het certificaat voor de Certificaathouder.

6.4 Activeringsgegevens

Activatiedata bescherming

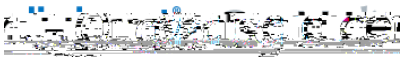
Activeringsgegevens worden door de Certificaathouder/Certificaatbeheerder altijd geheim gehouden. Activeringsgegevens zijn strikt persoonlijk en mogen niet worden gedeeld. Met inachtneming van adequate procedurele maatregelen mogen de activeringsgegevens voor Extended Validation systeemcertificaten worden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

Activeringsgegevens

QuoVadis verbindt activeringsgegevens aan het gebruik van een SUD, ter bescherming van de private sleutels van de certificaathouders.

Deblokkeren activeringsgegevens

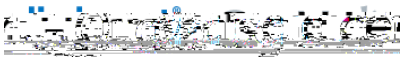
QuoVadis ondersteund geen deblokade van geblokeerde activerings gegevens.



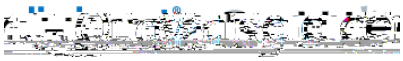
6.5 Computerbeveiliging

Technische maatregelen inzake computerbeveiliging

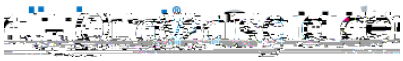
QuoVadis hanteert en onderhoudt een informatiebeveiligingsbeleid waarin wordt gedocumenteerd wat het QuoVadis beleid, de normen en de richtlijnen met betrekking



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			



Private Extensions		Fixed
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	Fixed



Private Extensions	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;
-

9

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 AVG. 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

voorschrijven 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.

Registration1in3(v)10(a)-3(n)-3(r92 r000912 0 612 792 reW*nBT/F1 15.96 Tf1 0 0 1 203 224.57 Tm

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

Certificaatinhoud

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

Certificaatintrekkingslijst

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

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 enschrandelingen beschreven in deze CPS

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 ñeen gekwalificeerd certificaat als bedoeld in artikel 1.1. onderdeel ss Telecommunicatiewetò gelezen wordt: ñeen authenticiteitscertificaatò
  b) voor ñondertekenaarò gelezen wordt: ñcertificaathouderò;
  c) voor ñelektronische handtekeningenò gelezen wordt: ñauthenticiteitskenmerkenò.

- 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 ñeen gekwalificeerd certificaat als bedoeld in artikel 1.1. onderdeel ss Telecommunicatiewetò gelezen wordt: ñeen EV-SSL certificaatò;
  b) voor ñondertekenaarò gelezen wordt: ñcertificaathouderò;
  c) voor ñaanmaken van elektronische handtekeningenò gelezen wordt: ñaanmaken van vercijferde dataò;
  d) voor ñverifi±ren van elektronische handtekeningenò gelezen wordt: ñontcijferen verifi±rمحي l

h) voor ñverifi±ren van elektronische handtekeningenò gelezen wordt: ñontcijferen van authenticiteitskenmerken en vercijferde dataò

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 ï verlies, speciaal verlies of schade, en binnen deze paragraaf betekent ñverliesò 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

- 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 praktijen gebruikt om te beschermen tegen schendingen van beveiliging als gevolg van dergelijke hardware, software of algoritmen;
- Stroomuitval, stroomonderbreking, of andere onderbrekingen van elektriciteit, op voorwaarde dat QuoVadis commercieel redelijke methoden gebruikt om te beschermen 02 427.15 Tm0.9rm0.612 0.612 0.616 rg0.612 0.612 0.616 RG[<0087>]TJETQq0cp

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 ngen zo

9.11 individuele kennisgeving en communicatie met betrokken partijen

Electronische post, brievenbuspost, fax en webpaginaûs 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 ñniveau van vertrouwenòniet die gedeelten van de specificatie met betrekking tot de aansprakelijkheid van partijen. Referentie aan het ñniveau van vertrouwenòslaan 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.

9.17 uitgegeven certificaat typen uit deze CPS

Van de onder deze cps benoemde cerificaatprofielen worden enkel uitgegeven het authenticiteit en vertrouwelijkheid certificaat. Het zegelcertificaat wordt tot nader order niet uitgegeven.