Certification Practice Statement PKIoverheid Domein Private Services (server) (g1)

Versie: 1.0
Datum: 23 mei 2017
PvE 3h: 4.4

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

Inhoud

risq5(k)q5(k)2hkenrzi-

9.

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

De QuoVadis CSP-PKI Overheid private services 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 in overeenstemming met dit CPS.
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 een 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 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:
_ v ‰‰ Œ š }(v •Ç natuurlijke persoon), bediend }} Œ }(v u v• v }ŒP v]• š}Œ]• Z vš]š]šX _
In deze CP gebruiken we de naam "service" voor dergelijke certificaathouders. Voor het uitvoeren van de handelingen ten aanzien van de levensloop van het certificaat van de certificaathouder is tussenkomst van een andere partij dan de certificaathouder vereist. De abonnee is hiervoor verantwoordelijk en dient een certificaatbeheerder aan te wijzen om deze handelingen te verrichten.

1.3.3.3 Certificaatbeheerder

Een certificaatbeheerder is een natuurlijke persoon die namens de abonnee handelingen uitvoert ten aanzien van het certificaat van de certificaathouder. De abonnee geeft de certificaatbeheerder opdracht de betreffende handelingen uit te voeren en legt dit vast in een bewijs van certificaatbeheer.
Voor het uitvoeren van de operationele handelingen ten behoeve van het systeemcertificaat (o.a. de aanvraag, installatie en beheer, intrekking) is de tussenkomst door een natuurlijke persoon vereist. De abonnee kan dit zelf uitvoeren of wijst hiertoe een functionaris aan, de certificaatbeheerder. In dat geval verleent de abonnee aan de certificaatbeheerder de expliciete toestemming om deze operationele handelingen uit te voeren.

1.3.3.4 Vertrouwende Partijen

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

1.4 Certificaatgebruik

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

[OID 2.16.528.1.1003.1.2.6] Servercertificaten die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het beveiligen van een verbinding tussen een bepaalde client en een server die behoort bij de organisatorische entiteit die als abonnee wordt genoemd in het betreffende certificaat.

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 het 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.

2.

Als bewijs van juistheid en het bestaan van de 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

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

3.2.5 Authorisatie van de certificaathouder (Service)

3.2.5.1 Controle authorisatie certificaathouder (Service)

QuoVadis zal controleren dat :

- het bewijs, dat de certificaathouder geautoriseerd is namens de abonnee om een certificaat aan te vragen en te ontvangen, authentiek is;
- of de certificaatbeheerder toestemming heeft verkregen van de abonnee om aan hem aangaande handelingen uit te voeren (ingeval de certificaatbeheerder het registratieproces uitvoert).

Opmerking

Als de domeinnaam voorkomt op phishtank of eventueel een andere blacklist die is geraadpleegd door QuoVadis tijdens het verificatieproces extra zorgvuldig om te gaan met de aanvraag van het betreffende services server certificaat.
Indien een 100 % phishstatus terug komt op de FQDN die aangevraagd wordt, zal het certificaat niet uitgegevn worden.
De gegevens die de CSP 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 zal QuoVadis, naast het uitvoeren van de bovenstaande controles:

- een verklaring van de geregistreerde domeinnaam eigenaar opvragen (b.v.-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.

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 procedure voor een initiële aanvraag

3.3.1.1 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

3.3.1.2 Controle bij aanvraag vernieuwing certificaat

Het vernieuwen van Service 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 sleutel s na intrekking certificaat

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

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 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 daarvoor gemachtigde 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

f een 16 Tc185.09413.7415 T* n c[oup(0 0 1 70.944 629.86 Tm2 [(pr185.09413.741 0 0 1 208.25 554>> BDC BT /F4 8.096(y)5(si)9(e)-8(k)7(e)5( )-266(t)-7(o)5BDC 5

5.2 Procedurele Beveiliging

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

5.2.1 Procedudurele 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 QuoVadis vallen.
Op basis van de risicoanalyse zal

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 belangenverstrengeling optreden en om de mogelijkheid tot abusievelijke of bewuste compromittering van enig component van de CA infrastructuur te

5.3.5. Sancties op ongeautoriseerde handelingen

Ongeautoriseerde handelingen van personeel kan resulteren in het opleggen van disciplinaire maatregelen door het Management v 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

- 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; Certificate life cycle management; 7 jaar bewaard en daarna verwijderd.

>}P •š v v À}}Œ P µŒš v]•• v u š šŒ l]vP š}šW Œ]P]vP v v Œ]•]
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 PKIov 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. Gearchiveerde 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 als doel de loggings te beveiligen.

5.4.5 Controlelogboek back-up procedures

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

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

5.4.6 Audit Logging

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

5.4.7 Berichtgeving inzake logging

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

5.4.8 Beoordeling van de kwetsbaarheid

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

5.5 Archivering van documenten

5.5.1. Aard van gearchiveerde gegevens

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

- Audit logs;
- Certificaataanvragen en alle daaraan gerelateerde handelingen en formulieren;

- X dat er onmiddellijke berichtgeving wordt verstrekt aan abonnees, Certificaathouders, vertrouwende partijen en andere relevant partijen binnen de PKI voor de overheid.
- X dat het intrekkingproces van alle certificaten die zijn uitgegeven door QuoVadis, ten tijde van beëindiging operationeel blijft
- X Relevante overheidsinstanties, waaronder de PA PKIoverheid, in het kader van toepasselijke wetgeving, op de hoogte te stellen.

Indien mogelijk wordt de intrekking van certificaten gepland in samenhang met de geplande uitgifte van nieuwe certificaten en de OCSP die de activiteiten uwe visis Tctiviteiten uwe 9D(a)4(c)5(e)-8(r)6(e)-6(i)6(ds)6(i)6 -9(uwe)eten uwbm 105.389.MCIDc1 037 1 70.944 670.62 Tm [( )]

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 dat het genereren van een elektronische handtekening.
Het sleutelmateriaal voor Systeemcertificaten wordt gegenereerd door de Certificaatbeheerder.

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 de CSP sub CA dienen te voldoen aan de eisen, die daaraan zijn gesteld in de lijst van aanbevolen cryptografische algoritmes en sleutellengtes als gedefinieerd in ETSI TS 119 312
.

6.1.1.2 Genereren van sleutelparen van de certifdeen

-

9. Algemene en juridische bepalingen

9.1 Tarieven

QuoVadis zal op verzoek alle toepasselijke tarieven beschikbaar stellen. Tarieven voor uitgifte van Certificaten variëren sterk per toepassingsgebied, aantallen en Certificaattypes.

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 van 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.

9.4.6. 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 anderszins 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 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

Quof86 86um deVadis ve-(r) -39(i(d)5(aawo)3(r)4( )-42(e)5(57)6(us)past)-9etrgi57e parie576( )-191(i)657 e57ng5(we)4(z) 5(57)re

x

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 tijdens de deelname binnen de PKI voor de overheid. Enige dergelijke beëindiging of terugtrekking zal niet tot 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, bri