Certification Practice Statement PKI Overheid Extended Validation

Versie: 1.7
Datum: 12 juli 2019
PvE 3f: 4.7

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

EV Policy OID 2.16.528.1.1003.1.2.7

Levering van 10(pri)-8(v)6(ate)-7(s)-4(l)5(e)-9(ute)4(l)-65 aan de certifi8 0.40W* nBT1 EM

1 Introductie op Certificate Policy

die specifiek door en voor de PKIoverheid Extended Validation zijn opgesteld.

De nummering van de hoofdstukken in dit CPS volgen de nummering van PvE3f PKIoverheid. De nummering heeft daardoor bewust geen sequentiële volgorde.

1.1.2 Status

QuoVadis heeft de grootst mogelijke aandacht en zorg besteed aan de gegevens en

1.3.1 Partijen binnen de gebruikersgemeenschap

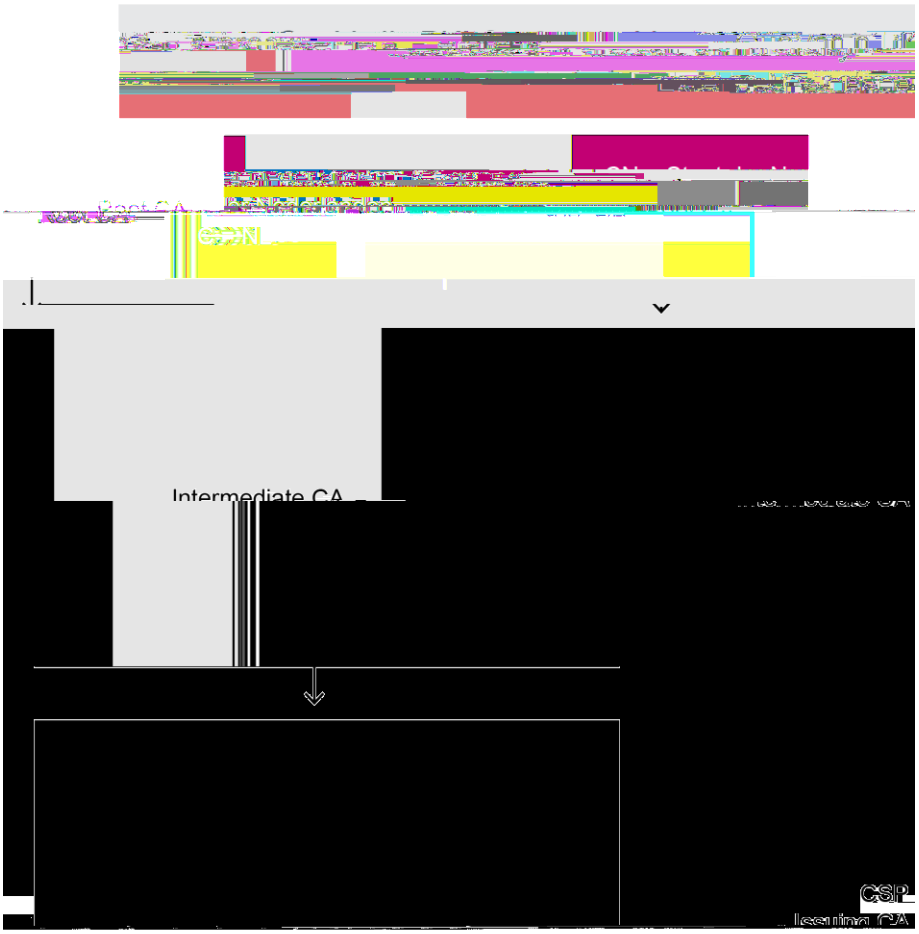
1.3.1.1 Centrale Infrastructuur PKIoverheid

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

Extended Validation Certificaten (EV-SSL): QuoVadis geeft het volgende certificaat uit (voor systemen).

Een Extended Validation Certificaat, dat onder deze CPS wordt uitgegeven kan worden gebruikt voor het beveiligen van een verbinding tussen een bepaalde client en een server die behoort bij de organisatorische entiteit (abonnee) die wordt genoemd in het betreffende certificaat.

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



Figuur1: Overzicht van de certificaat policies.

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.

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 TSP-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 te hebben op de uitgifte van PKIoverheid EV SSL

zij een wettelijk afdwingbare overeenkomst afsluit met een abonnee die gebaseerd is op de eisen zoals beschreven in dit CP én;

zij een revocatie informatie aanbiedt die 24x7 online beschikbaar is met informatie over de status van een EV SSL certificaat én;

zij alle eisen zoals beschreven in dit voorliggende CP bij de uitgifte van EV SSL certificaten zal opvolgen en uitvoeren en zal overgaan tot revocatie/intrekking van een EV SSL certificaat indien noodzakelijk.

2.2.6 Doel PKIoverheid EV-SSL certificaat

EV SSL-certificaten zijn bedoeld voor gebruik bij het vaststellen van web-based data communicatie kanalen via TLS / SSL-protocollen.

De primaire doelen van een EV SSL-certificaat zijn:

Identificeren van de juridische entiteit die een website beheert;

Zorgen voor een redelijke mate van zekerheid aan een gebruiker van een Internet-browser dat de website die door de gebruiker wordt bezocht onder controle is door de geïdentificeerde rechtspersoon die in het EV-certificaat met naam, adres, vestigingsplaats, Jurisdictie en het registratienummer vermeld staat; en

Bevordering van de uitwisseling van encryptiesleutels om de gecodeerde communicatie van informatie via het internet tussen de gebruiker van een internet browser en een website staat.

Het secundaire doel van een EV certificaat is te helpen bij het vaststellen van de legitimiteit van een bedrijf die beweert een Website te beheren of uitvoerbare code te verspreiden, en als instrument kan worden gebruikt om te helpen bij het aanpakken van problemen met betrekking tot phishing, malware, en andere vormen van online identiteitsfraude. Door het verstrekken van meer betrouwbare, derde partij geverifieerde, identiteit en adres informatie met betrekking tot het bedrijf, kunnen EV Certificaten helpen om:

Het moeilijker te maken om phishing en andere online identiteitsfraude aanslagen met Certificaten te realiseren;

Bedrijven te assisteren die het doelwit van phishing-aanvallen of online identiteitsfraude kunnen worden door hen te voorzien van een instrument om zich beter te identificeren voor de gebruikers, en

Rechtshandhaving organisaties assisteren bij hun onderzoek bij phishing en andere online identiteitsfraude, inclusief waar nodig, contact op te nemen, te onderzoeken, of het nemen van juridische stappen tegen het in het certificaat vermelde service.

Voor organisaties binnen de overheid een recent gewaarmerkt uittreksel (maximaal 1 maand oud) uit het Handelsregister van de Kamer van Koophandel of, indien inschrijving in het Handelsregister nog niet heeft plaatsgevonden, een kopie van de betreffende pagina uit de meest recente versie van de Staatsalmanak waar het adres van de betreffende overheidsorganisatie staat vermeldt;

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

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

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

(waarop, indien aanwezig, de bewijzeringsborden en het adresbord van de straat staan) en 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.

3.2.2.4 Verificatie telefoonnummer organisatie

QuoVadis verifiëert 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

3.2.2.5 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 doordat zij over een actieve betaalrekening beschikt.

Als bewijs van juistheid en het bestaan van de opgegeven betaalrekening moet de TSP tenminste één van de volgende bewijsstukken opvragen en verifiëren:

Een verklaring van een financiële instelling die in Nederland een vergunning heeft van DNB en valt onder het Nederlandse depositogarantiestelsel waaruit blijkt dat de abonnee over een actieve betaalrekening beschikt;

Een verklaring van een externe accountant dat de abonnee over een actieve betaalrekening beschikt bij een financiële instelling die in Nederland een vergunning heeft van DNB en valt onder het Nederlandse depositogarantiestelsel.

3.2.2.6 Niet-geverifieerde gegevens

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

3.2.3 Authenticatie van persoonlijke identiteit

3.2.3.1 Verificatie bevoegde vertegenwoordiger abonnee

QuoVadis verifiërt wie de Bevoegde Vertegenwoordiger (of Vertegenwoordiging) van de abonnee is.

Als bewijs van de juistheid en het bestaan van de door de abonnee opgegeven Bevoegde Vertegenwoordiger (of Vertegenwoordiging) zal QuoVadis tenminste de volgende bewijsstukken opvragen en verifiëren:

Voor organisatorische entiteiten binnen de overheid een recent gewaarmerkt uittreksel (maximaal 1 maand oud) uit het Handelsregister van de Kamer van Koophandel of, indien inschrijving in het Handelsregister nog niet heeft plaatsgevonden, een kopie van de betreffende pagina uit de meest recente versie van de Staatsalmanak (http://staatsalmanak.sdu.nl) waarin de Bevoegde Vertegenwoordiger (of Vertegenwoordiging) staat vermeldt;

Voor organisatorische entiteiten binnen het bedrijfsleven een recent gewaarmerkt uittreksel (maximaal 1 maand oud) uit het Handelsregister van de Kamer van Koophandel waarin de Bevoegde Vertegenwoordiger (of Vertegenwoordiging) staat vermeldt.

QuoVadis zal tevens nagaan of de Bevoegde Vertegenwoordiger op de meest recente EU lijst van verboden terroristische personen en organisaties voorkomt:

https://www.consilium.europa.eu/nl/policies/fight-against-terrorism/terrorist-list/

QuoVadis zal geen EV SSL certificaat uitgeven aan een organisatie of haar Bevoegde Vertegenwoordiger die op deze lijst staat.

3.2.3.2 Verificatie identiteit certificaatbeheerder

QuoVadis zal overeenkomstig Nederlandse wet- en regelgeving de identiteit en, indien van toepassing, specifieke eigenschappen te controleren van de certificaatbeheerder. Bewijs van de identiteit dient te worden gecontroleerd aan de hand van fysieke verschijning van de persoon zelf.

bewijs dat de certificaatbeheerder gerechtigd is voor een certificaathouder een certificaat te ontvangen namens de rechtspersoon of andere organisatorische entiteit. Dit bewijs mag niet ouder zijn dan 13 maanden anders moeten de gegevens opnieuw worden opgevraagd en geverifieerd tenzij in de overeenkomst met de abonnee uitdrukkelijk wordt vastgelegd dat de certificaatbeheerder zijn of haar autorisatie behoudt tot het moment dat dit door de abonnee wordt herzien of tot het moment dat de overeenkomst verloopt of wordt beëindigd.

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

3.2.5 Authorisatie van de certificaathouder (Service)

3.2.5.1 Controle authorisatie certificaathouder (Service)

QuoVadis zal controleren dat :

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 opgedragen handelingen uit te voeren (ingeval de certificaatbeheerder het registratieproces uitvoert).

Opmerking

De "certificaatbeheerder" die handelingen overneemt van de certificaathouder behoeft niet noodzakelijkerwijs dezelfde persoon te zijn als de systeembeheerder of personeels-functionaris. Tevens is het toegestaan dat de kennis van de activeringsgegevens van het sleutelmateriaal (bijvoorbeeld PIN) door verschillende personen wordt gedeeld als de inrichting van het beheer dat vereist. Echter, aangeraden wordt het aantal personen dat kennis heeft van de PIN zo beperkt mogelijk te houden. Ook is het verstandig maatregelen te treffen die de toegang tot de PIN beperken. Een voorbeeld hiervan is

Indien een 100 % phish status terug komt op de FQDN die aangevraagd wordt, zal het certificaat niet uitgegeven worden.

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 de datum waarop het certificaat is uitgegeven, de aanvrager ofwel de domeinnaamregistrant is of controle over de FQDN heeft door:

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 random value (geldig tot maximaal 30 dagen na aanmaak)

2. Rechtstreeks te communiceren met de domeinnaamregistrant door hun telefoonnummer te bellen en een antwoord te krijgen ter bevestiging van het verzoek van de aanvrager om de FQDN te valideren. Het gebruikte telefoonnummer moet het

9. Bevestiging van de controle door de aanvrager over de FQDN door een Random Value per e-mail te verzenden naar de DNS TXT Record e-mailcontact voor de autorisatiedomeinnaam voor de FQDN en vervolgens een bevestigende 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.

4 Operationele eisen en certificaatlevenscyclus

4.1 Certificaataanvraag

4.1.1 Voorwaarden overeenkomst

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

De overeenkomst voldoet tenminste aan de volgende voorwaarden:

de overeenkomst moet ondertekend worden door de Bevoegde Vertegenwoordiger of Vertegenwoordiging van de abonnee;

de abonnee moet verklaren dat de gegevens die worden verstrekt in het kader van een EV SSL certificaat aanvraagproces volledig en juist zijn;

de abonnee moet verklaren dat passende maatregelen zullen worden genomen om de private sleutel (en de daarbij behorende toegangsinformatie b.v. een PINcode), behorend bij de publieke sleutel in het betreffende EV SSL certificaat, onder zijn controle en geheim te houden en te beschermen;

de abonnee moet verklaren dat het niet het EV SSL certificaat zal installeren en gebruiken alvorens het op juistheid en volledigheid gecontroleerd te hebben;

Indien de domeinnaam (FQDN) zoals vermeld in een services server certificaat identificeerbaar en adresseerbaar is via het internet, moet de abonnee verklaren dat het services server certificaat alleen op een server wordt gezet die ten minste

de abonnee moet verklaren dat het EV SSL 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;

de abonnee moet verklaren dat het per direct geen gebruik meer zal maken van het EV SSL certificaat als duidelijk is dat de gegevens in het EV SSL certificaat onjuist of onvolledig zijn of als er aanwijzingen zijn dat de private sleutel, behorend bij de publieke sleutel van het betreffende EV SSL certificaat, gecompromitteerd is geraakt;

de abonnee moet verklaren dat het per direct geen gebruik meer zal maken van de private sleutel, behorend bij de publieke sleutel van het betreffende EV SSL

certificaat, als de geldigheid van het EV SSL certificaat is verlopen of als het EV SSL certificaat is ingetrokken;

De abonnee moet verklaren te reageren op instructies van de TSP binnen de door de TSP gestelde termijn in geval van aantasting van de private sleutel of certificaatmisbruik;

De abonnee moet aanvaarden dat de TSP gerechtigd is om het EV SSL certificaat in te trekken indien de abonnee de gebruikersovereenkomst heeft geschonden of de TSP heeft ontdekt dat het EV SSL certificaat wordt gebruikt voor criminele activiteiten zoals phishing, fraude of het verspreiden van malware.

4.1.2 Voorwaarden aanvraag

Voorafgaand aan de uitgifte van een EV SSL certificaat moet QuoVadis een volledig ingevuld en door de certificaatbeheerder, namens de abonnee, ondertekende aanvraag hebben ontvangen.

De aanvraag be

Bij het verwerken van CAA-records verwerkt QuoVadis de issue, issuewild- en iodef-eigendomskenmerken zoals gespecificeerd in RFC 6844, zoals gewijzigd door Errata 5065 (Appendix A). QuoVadis kan wellicht niet handelen op de inhoud van de iodef-eigendomscode. QuoVadis zal geen digitaal certificaat uitgeven als een onbekende eigenschap wordt gevonden met de kritieke vlag.

QuoVadis zal wellicht CAA-records niet controleren voor de volgende uitzonderingen:

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

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

i. het falen valt buiten de infrastructuur van de CA;
ii. de opzoeking minstens één keer is herhaald; en
iii. de zone van het domein heeft geen DNSSEC-validatieketen in de ICANN-root.

QuoVadis documenteert potentiële uitgaven die door een CAA-record zijn voorkomen en verzend van dergelijke uitgeversverzoeken naar het contact dat in de CAA iodef-record (en) is vermeld, indien aanwezig. QuoVadis ondersteunt mailto: en https: URL-schema's in het i0.282 0.337 0.369 rg0.282 0.337 0.369 RG[(r2nien)4(a)-P0 6jsen https: U

QuoVadis kan een brief zenden naar de abonnee ter attentie van de Bevoegde Vertegenwoordiger. De Bevoegde Vertegenwoordiger moet dan telefonisch of via e-mail bevestigen dat het inderdaad zijn of haar handtekening betreft op de overeenkomst.

4.4.1.2 Acceptatie certificaat

Na uitgifte van een certificaat, dient de certificaathouder of certificaatbeheerder 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

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 ontvangstbevestiging verstuurd en kan het probleem 24x7 behandeld worden.

4.5.2.3 Certificate Transparancy

QuoVadis voldoet aan de vereisten van Certificate Transparancy als vereist in 4.5.2-pkio145

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

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 als TSP

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

4.9.2.1 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.

4.9.3.6 Geldigheid CRL

De geldigheid van een CRL is maximaal 72 uur en wordt minimaal elke 12 uur gegenereerd. Indien er een intrekking heeft plaats gevonden wordt de CRL binnen 5 minuten gegenereerd.

4.9.3.7 Issuing subordinatie CA

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

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

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

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

4.9.5.1 Tijdsduur voor verwerking intrekkingsverzoek

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

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

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

In het geval van een issuing subordinate CA geldt dat de maximale tijdsduur, tussen het beslismoment om een issuing subordinate CA in te trekken (vastgelegd in een rapportage) en de wijziging van de revocation status information, die voor alle vertrouwende partijen beschikbaar is, is gesteld op 72 uur.

4.9.5.3 Dienstverlening OCSP en CRL

QuoVadis heeft met betrekking tot zijn OCSP en CRL dienstverlening passende server

verstuurd naar de OCSP dienst (OCSP responder) van QuoVadis. In de OCSP response staat de opgevraagde status van het betreffende certificaat.

De status kan de volgende waarden aannemen: goed, ingetrokken of ingetrokken met reden CertificateHold.

Als een OCSP response om enige reden uitblijft, kan daaruit geen conclusie worden getrokken met betrekking tot de status van het certificaat. De URL van de OCSP responder waarmee de intrekkingstatus van een Certificaat gevalideerd kan worden, staat in het certificaat.

Een OCSP respons is altijd door de OCSP responder verzonden en ondertekend. Een Vertrouwende Partij dient de handtekening onder de OCSP respons te verifiëren met het systeemcertificaat dat meegestuurd wordt in de OCSP respons. Dit systeemcertificaat is uitgegeven door dezelfde Certification Authority (CA) als de CA die het Certificaat heeft uitgegeven waarvan de status wordt opgevraagd.

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

4.9.9.4 Bijwerken OCSP service

QuoVadis werkt de OCSP service tenminste een keer in de 3 kalenderdagen bij. De maximale vervaltermijn van de OCSP responses is 7 kalenderdagen.

4.9.9.5 Ondersteunde methoden OCSP responses

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;

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 PKIoverheid EV 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

5.2.4.3 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

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 TSP 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 TSP-processen, -systemen en infrastructuur voor PKIo kerndiensten.

5.3 Personele Beveiliging

5.3.1 Kwalificaties, ervaring en screening

QuoVadis vereist dat personeel over de vereiste kwalificaties en relevante ervaring beschikt beschikt en een geheimhoudingsverklaring ondertekend.

De personen die de Vertrouwelijke Rollen vervullen moeten een toepasselijke beveiligingscreening procedure hebben ondergaan. De Vertrouwende Rollen in Nederland beschikken over een Verklaring omtrent het Gedrag van het ministerie van Justitie.

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

5.3.2 Identiteitscontrole en screening werknemer

QuoVadis stelt de identiteit en betrouwbaarheid van de

Bij het vaststellen van de betrouwbaarheid van de medewerker voert QuoVadis tenminste de volgende acties uit:

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

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.

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 Bewaartermijn van audit logs

QuoVadis zal Logbestanden voor gebeurtenissen met betrekking tot:

- CA key life cycle management en;
- Certificate life cycle management;

7 jaar bewaren en daarna verwijderen.

Logbestanden voor gebeurtenissen met betrekking tot:

5.4.5

5.5.1.1 Opslag informatie

QuoVadis slaat alle informatie op die is gebruikt voor het verifiëren van de identiteit van de abonnee en certificaatbeheerder, met inbegrip van referentienummers van de documentatie die is gebruikt voor verificatie, evenals beperkingen ten aanzien van de geldigheid.

5.5.5

- Eisen aan inwerkingtreding;
- Noodprocedure / uitwijkprocedure;
- Eisen aan herstarten TSP dienstverlening;
- Onderhoudsschema en testplan dat voorziet in het jaarlijks testen, beoordelen en actualiseren van het BCP;
- Bepalingen over het onder de aandacht brengen van het belang van business continuity;
- Taken, verantwoordelijkheden en bevoegdheden van betrokken actoren;
- Beoogde hersteltijd c.q. Recovery Time Objective (RTO);
- Vastleggen van de frequentie van back-ups van kritische bedrijfsinformatie en software;
- Vastleggen van de afstand van de uitwijkfaciliteit tot de hoofdvestiging van de TSP; en
- Vastleggen van procedures voor het beveiligen van de faciliteit gedurende de periode na een security breach of calamiteit en voor de inrichting van een beveiligde omgeving bij de hoofdvestiging of de uitwijkfaciliteit.

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

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

QuoVadis specificeert de procedures die worden gevolgd bij het beëindigen van het leveren 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.

6 Technische beveiligingsmaatregelen

6.1 Generatie en installatie van het sleutelpaar

6.1.1 Sleutelpaar generatie

De sleutel van de QuoVadis PKI Overheid CA zijn 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/QSCD), een veilig middel voor het genereren van een elektronische handtekening.

QuoVadis bewaakt de QSCD-certificeringsstatus tot het einde van de geldigheidsperiode van het certificaat en neemt passende maatregelen in geval van wijziging in deze status door bijvoorbeeld het verlopen van de certificeringsgeldigheidsperiode of voortijdige intrekking van deze certificering. Als eerste stap zal de QuoVadis Policy Management Authority (PMA) worden geïnformeerd over deze statusverandering en deze zal op basis van de dan aangetroffen situatie uitvoering geven aan evt. verdere maatregelen.

6.1.1.1 Genereren van sleutelparen voor de TSP sub CA

Het algoritme en de lengte van de cryptografische sleutels die worden gebruikt voor het genereren van de sleutels voor de TSP sub CA dienen te 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 genereren van de sleutel van de certificaathouder waarbij QuoVadis ook de private sleutel genereert (PKCS#12) is niet toegestaan onder dit CPS.

6.1.1.4 Sleutelparen van de certificaathouders

QuoVadis geeft geen code signing certificaten uit onder deze CPS.

6.1.2 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-

6.2 Private sleutel bescherming

6.2.1 Standaarden en controles van de cryptografische module (HSM)

De private sleutels van QuoVadis PKIoverheid EV 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 -

t 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 -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 TSP-EV CA sleutels niet in escrow uit.

6.2.4 Private sleutel back-up

Op het moment van uitgifte van het eindgebruikercertificaat is de resterende geldigheidsduur van de QuoVadis PKIoverheid EV CA 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.

6.4.1.1 Activeringsgegevens

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

Gebruik van x.509 certificaten voor alle administrators

6.5.1.2 Specifieke technische maatregelen inzake computerbeveiliging

QuoVadis maakt geen gebruik van externe Registration Authorities.

6.5.1.3 Specifieke technische maatregelen inzake ongeautoriseerde toegang

QuoVadis voorkomt ongeautoriseerde toegang tot de kerndiensten registration service, certificate generation service, subject device provision service, dissemination service, revocation management service en revocation status service. Hiertoe worden deze kerndiensten fysiek of logisch gescheiden van niet-PKI n

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

7 Certificaatprofiel

7.1 Aanvulling op ETSI TS 119 312 bij uitgifte ECC

In aanvulling op ETSI TS 119 312 zal QuoVadis kiezen uit 1 van de volgende opties voor het Signature veld in een certificaat:

sha256WithRSAEncryption: 1.2.840.113549.1.1.11

(OBJECT IDENTIFIER ::= { iso(1)

member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 })

OF

ecdsa-with-SHA256: 1.2.840.10045.4.3.2

{OBJECT IDENTIFIER ::= { iso(1) member-body(2)

us(840)ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }})

OF

sha384WithRSAEncryption : 1.2.840.113549.1.1.12

{OBJECT IDENTIFIER ::= { iso(1)

member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 }

OF

ecdsa-with-SHA384:1.2.840.10045.4.3.3

{OBJECT IDENTIFIER ::= { iso(1) member-body(2)

us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }

7.1.1 Subject.CommonnName

Het Subject.CommonName (indien opgenomen) bevat een FQDN (Fully Qualified Domain Name) Een FQDN MOET ook terugkomen in het SubjectAltName.DNsName veld

De geverifieerde gegevens mogen worden hergebruikt bij een volgende aanvraag, mits deze niet ouder zijn dan 825 dagen. Indien de gegevens ouder zijn dan 825 dagen dient

1.2.840.
113549.
1.9.1

Certificate Transparency

CertPolicyID		[1] Certificate Policy: Policy Identifier = 2.16.528.1.1003.1.2.7	Fixed
extKeyUsage			Fixed
id-kp-OCSPSigning	1.3.6.1.5.5.7.3.9	OCSP Signing	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.

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, RegistratieaTm0.5 0.765 rg0.00392 0.455.024 397.99 Tm0.282 0.337 0.369 rg0.282 0.337

informatie, met als enige uitzondering de intrekking van het certificaat van de QuoVadis PKIoverheid EV CA:

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

De opheffing van de QuoVadis PKIoverheid EV 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.

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 TSP 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)

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.

10 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/