Certification Practice Statement

Opmerking: Dit is een Nederlandse vertaling van het officiële Engelstalige Certification Practice Statement van Cleverbase. Dit is beschikbaar op de website van Cleverbase. De Engelstalige versie is in alle gevallen leidend.

Inhoudsopgave

Document management

Wijzigingshistorie

Versie	Datum	Door	Wijzigingen
0.1	15-03-2017	Vincent de Haan	Initiële uitgave
1.0	21-04-2017	Vincent de Haan	Finale versie
1.1	20-07-2017	Vincent de Haan	Kleine wijzigingen
1.2	28-08-2017	Vincent de Haan	Wijziging adressen CPS, CRL, OCSP; kleine wijzigingen in par. 5.1.2, authorityInfoAccess toegevoegd aan certificaatprofiel, kleine wijzigingen in par. 9.2
1.3	2-09-2017	Vincent de Haan	Kleine wijzigingen aan de certificaatprofielen
1.4	09-11-2017	René Kleizen	Correctie op CRL en OCSP URL en PublicKeyInfo algoritme
1.5	13-3-2018	Vincent de Haan	Adreswijziging, taalkundige wijzigingen, aanscherping van de certificaatprofielen
1.6	12-4-2018	Vincent de Haan	Wijziging in het veld authorityInfoAccess in het eindgebruikerprofiel
1.7	14-06-2018	Raúl Maduro	Onjuiste link gewijzigd naar https://pki.cleverbase.com/pki-disclosure-statement.pdf Ondersteuning van Nederlandse identiteitskaarten toegevoegd

1 Introductie

1.1 Achtergrond

De PKI voor de overheid is een *public key infrastructure* (PKI) die is opgezet op initiatief van de Nederlandse overheid en die gebruikt kan worden voor elektronische handtekeningen, elektronische authenticatie en vertrouwelijke elektronische communicatie en die is afgestemd op Nederlandse en Europese wetgeving op dit gebied. De certificaten die binnen deze PKI worden uitgegeven, hebben een hoog betrouwbaarheidsniveau. Binnen deze PKI zijn verschillende trust service providers (TSP's) actief. Deze TSP's worden binnen de PKI vertrouwd om certificaten uit te geven. De rootcertificaten binnen deze PKI worden ondertekend door de Staat der Nederlanden.

Cleverbase is een TSP binnen de PKI voor de overheid. Zij is erop gericht om burgers en bedrijven te voorzien van certificaten die zij nodig hebben om betrouwbaar en vertrouwelijk informatie uit te wisselen met de overheid en tussen bedrijven onderling. Hierbij geeft zij certificaten uit nadat de certificaathouder zich in beginsel op afstand heeft geregistreerd. Deze registratie vindt plaats met behulp van een mobiele app waarmee een videogesprek plaatsvindt. Tijdens dit videogesprek worden de identiteit en het identiteitsdocument van de aanvrager gecontroleerd.

Het sleutelmateriaal dat bij het certificaat behoort, bevindt zich in een trustworthy system for server signing (TW4S): de private sleutels van de eindgebruikercertificaten bevinden zich in een hardware secure module in het datacenter van Cleverbase die zodanig is geconfigureerd dat de sleutels onder uitsluitende controle staan van de certificaathouders. Zij oefenen deze controle uit door een aan hun mobiele telefoon gekoppelde app en een zelf gekozen pincode. Het TW4S wordt beheerd door Ubiqu B.V.

1.2 Documenteigenschappen

Dit document is het Certification Practice Statement van Cleverbase. Het is gebaseerd op de eisen die gesteld zijn in het Programma van Eisen voor de PKI voor de overheid[1], ETSI EN 319 411-1, ETSI EN 319 411-2[2] en de eidas-verordening[3]. Voor de indeling wordt aangesloten bij RFC 3647.

Onder dit CPS worden certificaten uitgegeven voor de doelgroep 'persoon burger' onder de certificate policy (CP) die wordt gegeven in deel 3c van het programma van eisen PKIoverheid. De gebruiksdoelen die worden ondersteund, zijn: authenticiteit, onweerlegbaarheid en vertrouwelijkheid. Voor elke doelgroep-gebruiksdoelcombinatie is in het betreffende CP een apart OID gedefinieerd. Een overzicht hiervan wordt hieronder gegeven:

	authenticiteit	onweerlegbaarheid	vertrouwelijkheid*
persoon burger (deel 3c PvE)	2.16.528.1.1003.1.2.3.1	2.16.528.1.1003.1.2.3.2	2.16.528.1.1003.1.2.3.3

* De vertrouwelijkheidscertificaten worden op dit moment niet aan klanten van Cleverbase uitgegeven.

[1] Te raadplegen via https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-tsp/programma-van-eisen/

[2] Beide te raadplegen via http://www.etsi.org/standards

[3] http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32014R0910

1.3 Deelnemers

De PKI voor de overheid heeft, voor zover hier relevant, de volgende deelnemers:

Policy authority. De policy authority heeft als taak het beheren van het gehele stelsel van afspraken en het regelen van het noodzakelijk toezicht. Deze taak wordt namens de Staat der Nederlanden vervuld door Logius.

Cleverbase. Cleverbase ID B.V., geregistreerd bij de Kamer van Koophandel onder nummer 67419925.

Cleverbase CA. De certification authority van Cleverbase is verantwoordelijk voor het uitgeven van certificaten.

Cleverbase RA. De registration authority van Cleverbase is verantwoordelijk voor het vaststellen van de identiteit van aspirant-certificaathouders ten behoeve van door Cleverbase uitgegeven certificaten. De medewerkers van de registration authority worden registration officers genoemd.

Certificaathouder. De certificaathouder is de entiteit die vermeld is in het subjectveld van het certificaat en is de houder van de private sleutel. In het geval van een persoonsgebonden certificaat is de certificaathouder een natuurlijke persoon. In het geval van een certificaat in het domein Burger, is de certificaathouder tevens abonnee.

Abonnee. In het geval van certificaten in het domein Burger is de certificaathouder zelf de abonnee. In het geval van certificaten in het domein Organisatie is de organisatie ten behoeve waarvan het certificaat wordt uitgegeven, abonnee.

Vertrouwende partij. Een vertrouwende partij is eenieder die handelt in vertrouwen op een door Cleverbase uitgegeven certificaat.

Ubiqu. Ubiqu Access B.V. is leverancier van Ubiqutokens die aan certificaathouders van persoonsgebonden certificaten worden uitgegeven. Deze tokens bestaan uit twee delen: een set private sleutels die wordt opgeslagen op een door de TSP beheerde server en een app op de mobiele telefoon van de certificaathouder. Met deze app kan de certificaathouder uitsluitende controle uitoefenen over de private sleutels. Ubiqu beheert deze server, maar Cleverbase heeft over het beheer hiervan de eindverantwoordelijkheid. De certificaathouder heeft exclusieve controle over zijn token, die hij[4] kan uitoefenen met behulp van zijn mobiele telefoon en een pincode.

1.4 Certificaatgebruik

Het certificaatgebruik verschilt per type certificaat. Eerst worden enkele algemene opmerkingen gemaakt, die daarna per certificaattype worden uitgewerkt:

- De certificaten moeten worden gebruikt conform de toepasselijke algemene voorwaarden.
- Er geldt geen beperking voor de waarde van de transactie waarbij het certificaat gebruikt wordt.
- De certificaten kunnen zowel in interacties met de Staat der Nederlanden als in interacties met andere natuurlijke of rechtspersonen gebruikt worden.

Certificaten van het type persoon burger kunnen worden gebruikt door individuele natuurlijke personen in hun hoedanigheid van particulier, dus niet in de context van een bedrijf.

Per type worden verschillende certificaten uitgegeven voor het authentiseren, vertrouwelijk communiceren en elektronisch ondertekenen. Het certificaat mag alleen gebruikt worden voor het doel

[4] Telkens waar in de mannelijke vorm verwezen wordt, wordt ook de vrouwelijke vorm bedoeld.

waarvoor het is uitgegeven. In onderstaande tabel worden deze doelen per certificaat aangegeven. Deze gebruiksdoelen komen overeen met het veld keyUsage in het certificaat.

	Authenticiteit	vertrouwelijkheid	ondertekening
persoon burger (deel 3c PvE)	digitalSignature	keyEncipherment dataEncipherment keyAgreement	nonRepudiation

1.5 Beheer van dit CPS

Dit CPS wordt tweemaal per jaar beoordeeld door Cleverbase. Eventuele onjuistheden of onvolledigheden worden dan bijgewerkt. Tevens vindt beoordeling en bijwerking van dit CPS plaats wanneer de Policy Authority een nieuwe versie van het Programma van Eisen oplevert. De TSP publiceert voorgenomen wijzigingen van dit CPS tijdig op zijn website. Het CPS wordt uiteindelijk vastgesteld door het management van de TSP.

Voor vragen of opmerkingen kan contact opgenomen worden met:

info@cleverbase.com

Of:

Cleverbase ID B.V.
Maanweg 174
2516AB
's-Gravenhage

2 Verantwoordelijkheid voor publicatie en opslag

2.1 Elektronische opslagplaats

Cleverbase heeft een elektronische opslagplaats. Deze is bereikbaar via www.cleverbase.com. De *certificate revocation list* en de OCSP-server zijn te raadplegen via:

CRL: http://pki.cleverbase.com/cleverbase3c.crl

OCSP: http://pki.cleverbase.com/ocsp/3c

De elektronische opslagplaats is in beginsel altijd bereikbaar. In het geval van (gepland) onderhoud of een calamiteit, kan deze bereikbaarheid voor ten hoogste vier uur onderbroken worden.

De elektronische opslagplaats is beveiligd tegen ongeautoriseerde aanpassingen. Slechts de TSP heeft schrijfrechten op de elektronische opslagplaats.

2.2 Publicatie van TSP-informatie

Op de elektronische opslagplaats is de volgende informatie toegankelijk:

- dit Certification Practice Statement,
- de algemene voorwaarden,
- de certificaten (eindgebruikercertificaten zijn slechts toegankelijk voor de certificaathouders),
- de certificaatstatusservice.

Van het CPS en de algemene voorwaarden blijven ook eerdere versies beschikbaar alsmede een aanduiding van de wijzigingen tussen de verschillende versies.

3 Identificatie en authenticatie

Deze paragraaf beschrijft de wijze van identificatie en authenticatie bij de initiële registratie en verlenging. Er worden twee registratieprocessen ondersteund, één waarbij een fysieke ontmoeting vereist is, en één waarbij identificatie op afstand plaatsvindt. Deze processen worden afzonderlijk beschreven.

3.1 Naamgeving

De Certificaathouder wordt in het veld subject van het certificaat geïdentificeerd met een *distinguished name* (DN) als bedoeld in X.501. Voor de verschillende soorten certificaten zijn verschillende onderdelen van de DN verplicht:

	persoon burger
serialNumber	Binnen de CA uniek persoonsnummer
commonName	naam van de certificaathouder volgens het volgende formaat: [alle voornamen voluit] [meisjes-/jongensnaam]
countryName	land van vestiging van de certificaathouder, conform de nationaliteit van het getoonde WID-document
givenName	alle voornamen van de certificaathouder
surName	de geslachtsnaam (meisjes-/jongensnaam) van de certificaathouder

Uit het bovenstaande vloeien ten minste de volgende eigenschappen voort:

- Pseudoniemen of anoniemen certificaten zijn niet toegestaan.
- Elke DN is uniek.
- Elke DN heeft een betekenisvolle relatie met de gerepresenteerde entiteit.

Indien een meningsverschil bestaat over de naamgeving, beslist de registration authority.

Voor meer informatie wordt tevens verwezen naar de certificaatprofielen, opgenomen in hoofdstuk 7 van dit document.

3.2 Initiële identiteitsvalidatie

Bij Cleverbase vindt de registratie van natuurlijke personen in beginsel op afstand plaats met behulp van een daartoe ontwikkelde mobiele app. Indien registratie op afstand niet mogelijk blijkt, kan registratie plaatsvinden door middel van een fysieke ontmoeting.

3.2.1 Initiële identiteitsvalidatie op afstand

De initiële identiteitsvalidatie op afstand vindt plaats door middel van een app voor de mobiele telefoon die de TSP in de gelegenheid stelt de identiteit op afstand vast te stellen en de token op de mobiele telefoon te installeren. Tijdens het registratieproces vinden ten minste de volgende handelingen plaats:

(1) Het e-mailadres van de gebruiker wordt geregistreerd, zodat dit als gebruikersnaam binnen Cleverbase kan dienen.

(2) De Authenticate app (die deel uitmaakt van de Ubiqutoken) wordt op de telefoon geïnstalleerd. De aspirant-certificaathouder kiest een pincode en er wordt een koppeling gemaakt tussen pincode, telefoon en de (toekomstige) identiteit.
(3) Er wordt een selfie gemaakt van de aspirant-certificaathouder. Deze wordt naar de server verstuurd.
(4) Er wordt een foto gemaakt van het Nederlandse paspoort of Nederlandse identiteitskaart van de aspirant-certificaathouder. Deze wordt, samen met de voor de registratie benodigde persoonsgegevens, naar de server verstuurd. (Indien de aspirant-certificaathouder niet over een Nederlands paspoort of Nederlandse identiteitskaart beschikt, kan hij geen certificaat aanvragen bij Cleverbase.)
(5) De app start een videoverbinding met een registration officer. Voorafgaand of tijdens het videogesprek voert deze de volgende controles uit:
    (a) De registration officer controleert of de videoverbinding van voldoende hoge kwaliteit is en geeft eventueel instructies ten aanzien van omgevingslicht en -geluid.
    (b) De registration officer controleert of de opgegeven gegevens overeenkomen met de foto van het identiteitsbewijs.
    (c) De registration officer controleert of het identiteitsbewijs echt en geldig is. Bij deze controle wordt onder meer gecontroleerd of het document als vermist of gestolen geregistreerd is.
    (d) De registration officer controleert de echtheidskenmerken van het identiteitsbewijs.
    (e) De registration officer controleert de identiteit van de aspirant-certificaathouder.
    (f) De registration officer controleert of de persoon reeds eerder een certificaat bij Cleverbase heeft aangevraagd. (In dit geval worden bestaande certificaten ingetrokken.)
    (g) De medewerker verzoekt de aanvrager om een unieke code voor te lezen en een wilsuiting uit te spreken ten behoeve van de certificaataanvraag.
(6) Als alle controles een positief resultaat hebben opgeleverd, keurt de medewerker de certificaataanvraag goed.
(7) Een tweede registration officer controleert de certificaataanvraag en keurt deze goed indien ook hij van oordeel is dat aan de eisen voldaan is.
(8) Per e-mail krijgt de certificaathouder een intrekkingscode die hij kan gebruiken als hij het certificaat later in wil trekken.

De TSP treft maatregelen om de kwaliteit van het hierboven beschreven proces voortdurend te verbeteren. Zij treft in elk geval de volgende maatregelen:

- Periodiek worden oude dossiers gecontroleerd door de interne auditor van Cleverbase en door externe auditors. Indien blijkt dat een bepaalde registration officer ten onrechte certificaataanvragen heeft goedgekeurd, worden de door hem behandelde dossiers opnieuw bekeken.
- Aanvragers met ongebruikelijke identiteitsdocumenten, beschadigde (maar nog wel geldige) identiteitsdocumenten, voortdurende problemen bij het opzetten van een deugdelijke videoverbinding of andere eigenaardigheden waardoor het hierboven beschreven proces niet een integere identiteitsvaststelling kan garanderen, worden uitgenodigd om ten kantore van de TSP door middel van een fysieke ontmoeting hun identiteit vast te laten stellen.

3.2.2 Initiële identiteitsvalidatie door middel van fysieke aanwezigheid

Indien registratie op afstand niet mogelijk is, maar de gebruiker wel beschikt over een telefoon waarop de registratieapp geïnstalleerd kan worden en over een Nederlands paspoort of Nederlandse identiteitskaart , kan hij door middel van fysieke aanwezigheid worden geregistreerd bij Cleverbase. In dit geval komt de aanvrager naar het kantoor van Cleverbase alwaar een medewerker eerst de identiteit en het identiteitsdocument van de aanvrager controleert. Als hij van oordeel is dat de identiteit kan worden

vastgesteld en certificaatuitgifte mogelijk is, wordt onder begeleiding van deze medewerker het registratieproces als beschreven in paragraaf 3.2.1 alsnog uitgevoerd. De fysieke identiteitsvalidatie treedt echter in de plaats van de identiteitsvaststelling op afstand. Indien de gebruiker niet beschikt over een geschikte telefoon of over een Nederlands paspoort of Nederlandse identiteitskaart, is registratie niet mogelijk.

3.3 Identificatie en authenticatie bij vernieuwing van het certificaat

Bij vernieuwing van het certificaat wordt dezelfde procedure doorlopen als bij de eerste aanvraag van een certificaat. In dit geval worden tijdens het registratieproces eventuele oude certificaten die nog geldig zijn, ingetrokken.

3.4 Identificatie en authenticatie voor intrekkingsverzoeken

Ten behoeve van een intrekkingsverzoek kan de certificaathouder zich op de volgende manieren identificeren:

- De certificaathouder gebruikt de aan hem verstrekte blokkeercode en vult deze in op het publieke gedeelte van de website van Cleverbase.
- De certificaathouder neemt telefonisch contact op met Cleverbase en beantwoordt enkele vragen over zijn persoonsgegevens, op basis waarvan de medewerker zijn identiteit vaststelt.
- De certificaathouder stuurt een brief of e-mail aan Cleverbase en voegt hierin een kopie van zijn identiteitsbewijs bij.

4 Operationele eisen certificaatlevenscyclus

4.1 De certificaataanvraag

Hierna wordt per certificaattype beschreven op welke wijze de aanvraag verloopt.

4.1.1 Aanvraag van een certificaat van het type persoon burger

Het certificaat van het type persoon burger wordt aangevraagd door de aspirant-certificaathouder. Op dit moment wordt een overeenkomst gesloten tussen Cleverbase en de aspirant-certificaathouder. De aanvrager dient alvorens de aanvraag te kunnen voltooien, akkoord te gaan met de algemene voorwaarden die conform paragraaf 2.2 zijn gepubliceerd.

Tijdens het aanvraagproces wordt de identiteit van de aspirant-certificaathouder vastgesteld conform paragraaf 3.

De certificaathouder kan het certificaat opvragen via de webportal van de TSP nadat hij heeft ingelogd.

4.2 De verwerking van de certificaataanvraag

Hiervoor wordt verwezen naar paragraaf 4.1.

4.3 De certificaatuitgifte

Hiervoor wordt verwezen naar paragraaf 4.1.

4.4 Acceptatie van het certificaat

De certificaten van het type persoon burger worden stilzwijgend geaccepteerd.

4.5 Sleutelpaar- en certificaatgebruik

Het certificaat wordt gebruikt conform dit CPS, de algemene voorwaarden en de in het certificaat opgenomen wijzen van gebruik (zie paragraaf 1.4). Hiertoe worden de abonnee en de certificaathouder verplicht in de met hen gesloten overeenkomst.

De vertrouwende partij wordt, alvorens op een certificaat te vertrouwen, geacht het volgende te controleren:

(1) de geldigheid van het certificaat en de volledige keten van certificaten tot aan het rootcertificaat,
(2) gebruik van het certificaat conform de in het certificaat en de algemene voorwaarden opgenomen gebruiksdoelen,
(3) de geldigheid van het certificaat en de daarbij behorende keten van certificaten op het moment dat erop wordt vertrouwd door middel van het raadplegen van certificaatstatusinformatie.

4.6 Certificaatvernieuwing

Vernieuwing van het certificaat zonder verandering van het sleutelpaar wordt niet ondersteund. Een vernieuwing wordt behandeld als een nieuwe aanvraag.

4.7 Vernieuwing van het sleutelpaar voor het certificaat

Indien een certificaathouder een nieuw certificaat met een nieuw sleutelpaar aanvraagt, worden dezelfde procedures doorlopen als wanneer hij voor het eerst een certificaat aan zou vragen. Indien de voorwaarden tussentijds gewijzigd zijn, wordt hij hierop gewezen tijdens de aanvraag.

4.8 Aanpassing van certificaten

Er wordt geen mogelijkheid geboden om gegevens in het certificaat aan te passen. Indien gegevens in het certificaat niet meer juist zijn, moet het certificaat worden ingetrokken. Hiertoe wordt de certificaathouder in de algemene voorwaarden verplicht. Indien gewenst kan de certificaathouder een nieuw certificaat aanvragen met de aangepaste gegevens.

4.9 Het intrekken en opschorten van certificaten

Onder bepaalde omstandigheden kan een certificaat worden ingetrokken. In dat geval plaatst de TSP het certificaat op een lijst van ingetrokken certificaten (Certificate Revocation List) en maakt hij middels het OCSP (Online Certificate Status Protocol) bekend dat het certificaat is ingetrokken. In deze paragraaf wordt beschreven onder welke omstandigheden, door wie en op welke wijze een certificaat kan worden ingetrokken.

Het is niet mogelijk een certificaat tijdelijk in te trekken of te deactiveren.

4.9.1 De omstandigheden waaronder een certificaat kan worden ingetrokken

Onder de volgende omstandigheden kan een certificaat worden ingetrokken:

(a) De abonnee verzoekt tot intrekking.

(b) Er is een vermoeden dat vertrouwelijkheid van de private sleutel die overeenkomt met de publieke sleutel in het certificaat, is aangetast. Hiervan is ten minste sprake indien de mobiele telefoon waarmee de Ubiqutoken gekoppeld is, is verloren of gestolen, of indien de vertrouwelijkheid van de PIN-code is aangetast.
(c) De certificaathouder voldoet niet aan zijn verplichtingen op grond van dit CPS of de met hem gesloten overeenkomst.
(d) De informatie in het certificaat is niet (meer) correct en actueel of de informatie in het certificaat is misleidend.
(e) Er zijn aanwijzingen dat het certificaat misbruikt wordt.
(f) Het certificaat blijkt achteraf niet volgens de juiste procedures te zijn uitgegeven.
(g) De TSP staakt zijn werkzaamheden en de CRL- en OSCP-dienstverlening worden niet door een andere TSP overgenomen.
(h) De PA van PKIoverheid stelt vast dat het certificaat niet aan de eisen voldoet.
(i) Het intrekken van het certificaat kan bijdragen aan het voorkomen of bestrijden van een calamiteit.
(j) Er doet zich een andere omstandigheid voor die naar het oordeel van de TSP het intrekken van het certificaat rechtvaardigt ten behoeve van het vertrouwen in de public key infrastructure.
(k) De abonnee, die een natuurlijke persoon is, is overleden.

4.9.2 De partijen die een certificaat kunnen doen intrekken

De intrekking van een certificaat kan plaatsvinden op initiatief van:

(a) de TSP zelf,
(b) de certificaathouder,
(c) de abonnee.

Aangezien de TSP zelf het initiatief kan nemen tot het intrekken van een certificaat, kan eenieder die daartoe aanleiding ziet, de TSP vrijblijvend op de hoogte brengen van omstandigheden die tot intrekking zouden kunnen leiden. Hierna kan de TSP, indien daartoe aanleiding bestaat, overgaan tot intrekking.

4.10 De wijze van intrekken van certificaten

De certificaathouder kan middels de webportal van de TSP zijn eigen certificaten op elk moment intrekken door gebruik te maken van de intrekkingscode die tijdens de aanvraag per e-mail is verstrekt.

Elk van de partijen genoemd in paragraaf 4.9.2 kan tussen 09.00 uur en 17.00 uur telefonisch een intrekkingsverzoek doen door contact op te nemen met de klantenservice van de TSP. Buiten kantoortijden kan een e-mail worden gestuurd naar de klantenservice van de TSP. De contactgegevens daarvan zijn te vinden op de website https://cleverbase.com.

Een intrekkingsverzoek kan, indien niet sprake is van een spoedeisende situatie, tevens per post worden ingediend op het volgende adres:

Cleverbase ID B.V.
Maanweg 174

2516AB
‘s-Gravenhage

Intrekkingsverzoeken die per e-mail of post worden ingediend, dienen te zijn voorzien van een kopie van een geldig legitimatiebewijs.

Indien de TSP een certificaat op eigen initiatief intrekt, wordt de reden hiervan beschreven.

Binnen vier uur na ontvangst van het verzoek vindt intrekking plaats. De intrekking vindt plaats door het certificaat op de certificate revocation list te plaatsen en de OCSP-respons te updaten. Nadat vast is komen te staan dat de intrekking dient plaats te vinden, wordt de certificaatstatus binnen zestig minuten geüpdatet.

Indien de intrekkingsdienstverlening om welke reden dan ook verstoord is, draagt de TSP er zorg voor dat deze verstoring binnen vier uur is verholpen.

Indien de TSP informatie ontvangt die geen intrekkingsverzoek is, maar wel aanwijzingen bevat dat er een probleem is met een certificaat, stelt de TSP binnen vierentwintig uur of zo spoedig mogelijk tijdens kantooruren een onderzoek in dat mogelijk leidt tot intrekking.

Indien de certificaathouder het certificaat zelf intrekt via de webportal of telefonisch, krijgt hij onmiddellijk feedback zodra de intrekking geslaagd is. Indien de intrekking per post wordt verzocht, of indien een ander dan de certificaathouder het initiatief neemt tot intrekking, wordt een e-mail naar de certificaathouder verstuurd.

4.11 Certificaatstatusservice

De TSP biedt een certificaatstatusservice waarmee de geldigheid van het certificaat gecontroleerd kan worden. De adressen waarop deze service geraadpleegd kan worden, zijn opgenomen in het certificaat. Tevens worden zij hier genoemd:

CRL: http://pki.cleverbase.com/cleverbase3c.crl

OCSP: http://pki.cleverbase.com/ocsp/3c

De TSP maakt zowel gebruik van een *certificate revocation list* (CRL) als van het OCSP-protocol.

De CRL wordt ten minste eens per zeven dagen bijgewerkt. Een certificaat blijft op de CRL staan tot de oorspronkelijke geldigheidsduur van het certificaat verlopen is. Onder normale omstandigheden is de responstijd 10 seconden of minder.

Het OCSP-protocol wordt ondersteund met behulp van de *GET method*. Onder normale omstandigheden is de responstijd 10 seconden of minder. De OCSP-respons is altijd minstens zo up-to-date als de CRL doordat deze realtime wordt bijgewerkt. De OCSP-respons is uitsluitend positief indien op basis van de administratie van de TSP bevestigd kan worden dat het certificaat door de TSP is uitgegeven en nog steeds geldig is. De OCSP-service verstrekt informatie over het certificaat tot ten minste zes maanden nadat het certificaat is verlopen.

4.12 Beëindiging van de dienstverlening aan een abonnee

Na afloop van de geldigheidsduur van het certificaat, nodigt de TSP de abonnee uit het certificaat te verlengen. Indien het certificaat niet (tijdig) verlengd wordt, wordt de overeenkomst tussen de TSP en de abonnee van rechtswege beëindigd. De geldigheid van het certificaat komt automatisch te ontvallen. De TSP bewaart de gegevens met betrekking tot het certificaat nog zeven jaar.

Indien het certificaat wordt ingetrokken op grond van paragraaf 4.9, en de abonnee geen nieuw certificaat aanvraagt, wordt de overeenkomst tussen de TSP en de abonnee van rechtswege beëindigd. De geldigheid van het certificaat komt te ontvallen doordat het certificaat, conform paragraaf 4.9, op de *revocation list* geplaatst wordt. De TSP bewaart de gegevens met betrekking tot het certificaat nog zeven jaar.

4.13 Key escrow

De TSP ondersteunt geen key escrow.

5 Management-, operationele en fysieke beheersmaatregelen

5.1 Fysieke beveiligingsmaatregelen

5.1.1 Locatie Den Haag

De TSP is gevestigd in een gedeeld kantoorgebouw in Den Haag. Dit kantoor wordt afgesloten met een afsluitbare deur waarvan de sleutels door Cleverbase beheerd worden.

5.1.2 Locatie(s) Delft en Rotterdam

De datacenters van de TSP zijn in Rotterdam en Delft gevestigd. De datacenters worden door dezelfde externe partij beheerd en zijn op dezelfde wijze beveiligd.

De datacenters zijn voorzien van 24/7 bewaking. Alle ruimtes in het datacenter worden met camera's geobserveerd. Bezoekers moeten zich identificeren en worden begeleid naar hun bestemming. Van de bezoeken wordt een logboek bijgehouden. De kast waarin de aan de TSP toebehorende apparatuur zich bevindt, wordt uitsluitend ten behoeve van de TSP gebruikt en is afsluitbaar.

In het datacenter zijn maatregelen genomen om de beveiliging ook in noodsituaties te garanderen. Er is een noodaggregaat voor onderbreking van de elektriciteitsvoorziening, die ten minste eens per kwartaal getest wordt. Ook is er een klimaatbeheersingssysteem dat zorg voor een stabiele luchttoevoer, temperatuur en luchtvochtigheidsgraad. De ruimtes zijn voorzien van vochtdetectiesensoren. Ook is er een geavanceerd blussysteem aanwezig.

Alle opslag wordt ten minste in tweevoud uitgevoerd, verspreid over twee verschillende datacenters.

Opslagmedia die niet langer gebruikt worden, worden vernietigd.

5.2 Procedurele beheersmaatregelen

De medewerkers van de TSP zijn verdeeld over verschillende vertrouwde rollen met bijbehorende verantwoordelijkheden. De autorisaties die de medewerkers hebben, sluiten aan bij de rol die zij vervullen. De rollen die worden onderscheiden, zijn:

- Security officers: zien toe op de implementatie en naleving van vastgestelde beveiligingsrichtlijnen.
- System auditors: vervullen een toezichthoudende rol en geven 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.
- Systeembeheerders: beheren de TSP-systemen, waarbij het installeren, configureren en onderhouden van de systemen is inbegrepen.
- Systeemoperators: zijn verantwoordelijk voor het dagelijks beheer van de TSP-systemen.
- Registration officers: zijn verantwoordelijk voor het uitvoeren van het registratieproces en voor het verwerken van handmatige intrekkingsverzoeken. Binnen de Registration Officers is er per certificaat sprake van functiescheiding tussen de Registration Officer die de certificaataanvraag behandelt en de Registration Officer die de certificaataanvraag goedkeurt.

5.3 Personele beveiligingsmaatregelen

Voordat medewerkers bij de TSP in dienst treden, worden zij gescreend. Deze screening bestaat ten minste uit het aanvragen van een Verklaring omtrent het gedrag. Ook wordt van elke medewerker het c.v. en een wettelijk identiteitsbewijs gecontroleerd. De intensiteit van de screening wordt afgestemd op de mate van vertrouwelijkheid die gepaard gaat met de rol die de medewerker vervult.

Medewerkers beschikken over voldoende kennis en ervaring om hun taken bij de TSP te vervullen. In het bijzonder draagt de TSP er zorg voor dat zij getraind zijn in de voor de TSP specifieke procedures.

Elke medewerker en ingehuurde derde tekent als onderdeel van zijn arbeidsovereenkomst respectievelijk overeenkomst van opdracht een.

Niet-toegestane handelingen van medewerkers kunnen leiden tot het opleggen van disciplinaire maatregelen door het management van de TSP.

Ook van externen die werkzaamheden verrichten voor de TSP wordt de betrouwbaarheid onderzocht.

5.4 Auditloggingprocedures

De TSP houdt logs bij van diverse gebeurtenissen ten behoeve van de periodiek uitgevoerde audit. De logs worden zodanig bewaard dat zij gedurende tien jaar toegankelijk blijven. Gedurende deze periode wordt de integriteit van de logs gewaarborgd zodat het verwijderen of veranderen van records niet onopgemerkt blijft. De logs worden op verschillende locaties opgeslagen.

De logs kunnen door degenen die daar belang bij hebben (ten minste de auditor), bij de TSP worden opgevraagd. Het management verstrekt de logs tenzij belangen van derden zich hiertegen verzetten of een onevenredig grote technische inspanning hiervoor vereist is.

De logs worden voorzien van een tijdstempel aan de hand van een klok die ten minste dagelijks wordt gesynchroniseerd.

De gebeurtenissen die ten minste gelogd worden, zijn de volgende:

- CA-sleutellevenscyclusgebeurtenissen:
  - Generatie, backup, opslag, herstel, archivering en vernietiging van de CA-sleutel
- Certificaatlevenscyclusgebeurtenissen:
  - Het voorbereiden van de Ubiqutoken
  - Registratie van de certificaathouder, abonnee, certificaatbeheerder en certificaat coördinator
  - Generatie van het certificaat
  - Intrekking van het certificaat
  - Acceptatie en weigering van het certificaat
  - Generatie van de CRL en de OCSP-entries
- Gebeurtenissen met betrekking tot systemen:
  - Installatie, update of verwijdering van software
  - Plaatsing of verwijdering van opslagmedia
  - Toegang tot de fysiek beveiligde ruimte waarin de systemen zijn opgesteld
  - Installatie, update of verwijdering van de HSM
- Gebeurtenissen met betrekking tot:
  - Routers, firewalls en netwerksysteemcomponenten
  - Databaseactiviteiten en –events
  - Transacties
  - Operating systems
  - Access control systemen
  - Mail servers
  - Succesvolle en niet-succesvolle aanvallen op de PKI-systemen
  - Activiteiten van medewerkers op de PKI-systemen
  - Systeemuitval, hardware-uitval en andere abnormaliteiten

- Firewall- en routeractiviteiten
- Betreden van- en vertrekken uit de ruimte van de CA
- Lezen, schrijven en verwijderen van gegevens
- Profielwijzigingen

Indien van toepassing worden in de auditlog de volgende gegevens opgenomen:

- Bron-IP-adres
- Doel-IP-adres
- Datum en tijd
- Gebruikers-ID
- Naam en beschrijving van de gebeurtenis

5.5 Archivering

Alle gegevens die van belang kunnen zijn voor de conformiteitsbeoordeling, worden gearchiveerd. Hieronder worden ten minste verstaan: de gegevens die zijn verzameld tijdens de identiteitsvaststelling, de levenscyclus van certificaten, het gebruik van private sleutels. De te archiveren gegevens kunnen voorkomen in auditlogs, databases of op fysieke documenten. Deze worden elk op de geëigende manier gearchiveerd. Sleutelmateriaal wordt niet gearchiveerd.

Archieven worden gedurende 10 jaar bewaard.

Archieven worden beschermd tegen ongeautoriseerde toegang. In beginsel hebben alleen het management, de interne en de externe auditor toegang tot de archieven. Zij kunnen anderen evenwel toegang verlenen tot (een deel van) de archieven, mits dat noodzakelijk is voor de uitoefening van de taak van deze anderen.

Archieven worden beschermd tegen wijziging en verwijdering. Hiertoe worden zowel organisatorische als technische maatregelen getroffen. Ook worden archieven beschermd tegen verslechtering van opslagmedia. De archieven worden opgeslagen op harddisks die ten minste N+1 worden uitgevoerd en die gemonitord worden.

Van het archief is een volledige off site backup.

5.6 Wijziging van de CA-sleutel

De CA-sleutel heeft een geldigheidsduur die wordt vastgesteld door de PA van PKIoverheid. Als de geldigheidsduur binnen minder dan drie jaar verloopt, wordt een nieuwe CA-sleutel geïnstalleerd. De oude sleutel wordt vanaf dat moment niet meer gebruikt om certificaten mee te ondertekenen, maar slechts om CRLs en OCSP-responsen mee te ondertekenen. Als alle certificaten die met de oude sleutel ondertekend zijn, verlopen zijn, wordt de oude sleutel vernietigd.

5.7 Calamiteiten

De TSP heeft processen ingericht voor het omgaan met calamiteiten. Er is sprake van een calamiteit indien de integriteit van certificaten is aangetast door een oorzaak binnen de invloedsfeer van de TSP. Hieronder wordt ten minste, maar niet uitsluitend verstaan:

- Ongeoorloofde toegang tot de CA-sleutel
- Beide datacenters zijn onbereikbaar

- De leverancier van de Ubiqutoken is onbereikbaar

5.8 CA-beëindiging

Indien de TSP besluit zijn activiteiten te beëindigen, treedt het beëindigingsplan in werking. Dit plan zorgt ervoor dat de beëindiging op een gecontroleerde manier verloopt. Dit beëindigingplan zorgt er ten minste voor dat alle betrokken partijen worden geïnformeerd, de certificaatstatusservice in stand blijft en dat intrekken van certificaten mogelijk blijft zolang er nog niet-ingetrokken certificaten zijn. Ook zullen de gegevens die de TSP verzameld heeft ten behoeve van de registratie op een zodanige manier gearchiveerd worden dat zij vertrouwelijk blijven, maar wel raadpleegbaar indien noodzakelijk.

Bij beëindiging zal de TSP proberen de dienstverlening over te dragen aan een andere TSP, zodat voor de eindgebruikers zo min mogelijk overlast ontstaat.

Het beëindigingsplan wordt jaarlijks geactualiseerd.

6 Technische beveiligingsmaatregelen

6.1 Generatie en installatie van het sleutelpaar

6.1.1 Het CA-sleutelpaar

Het sleutelpaar van de CA wordt gegenereerd binnen een cryptografische module (HSM) van de CA. Het publieke deel van de CA-sleutel wordt fysiek overgebracht naar de root CA in de vorm van een certificate signing request (PKCS#10), die het certificate signing request ondertekent en daarna het certificaat genereert. De HSM is zodanig geconfigureerd dat het CA-sleutelpaar uitsluitend gebruikt kan worden door iemand die controle kan aantonen over het persoonsgebonden sleutelpaar van een registration officer.

6.1.2 Het sleutelpaar van een persoonsgebonden certificaat

Het sleutelpaar van persoonsgebonden certificaten wordt gegenereerd binnen een cryptografische module (HSM) in het datacenter van de TSP. De certificaathouder kan op afstand controle uitoefenen over het sleutelpaar door gebruik te maken van een app op zijn telefoon. Tijdens de certificaataanvraag wordt de app aan de telefoon gekoppeld aan de hand van een identificerend nummer van de telefoon; tevens moet de certificaathouder een pincode bepalen.

Het publieke deel van de sleutel van een persoonsgebonden certificaat wordt aan de CA aangeboden in de vorm van een certificate signing request. De HSM ondertekent dit en genereert op deze wijze het certificaat. Deze procedure speelt zich af binnen de beveiligde omgeving in het datacenter van de TSP.

Het gebruik van de sleutel is conform het certificaatprofiel als beschreven in hoofdstuk 7.

6.2 Bescherming van de private sleutel

Alle private sleutels worden beschermd doordat ze de cryptografische hardware nooit verlaten. De eindgebruikersleutels bevinden zich in een HSM die zo is geconfigureerd dat de sleutel alleen gebruikt wordt, nadat de gebruiker zijn pincode heeft ingevoerd in de door Ubiqu geleverde Authenticate app.

6.3 Activatiegegevens

De activatiegegevens spelen slechts in de interne processen van de TSP een rol en hoeven hier derhalve niet beschreven te worden.

6.4 Betrouwbare systemen

De TSP past een groot aantal beveiligingsmaatregelen toe (two-factor authentication op systemen, cryptografisch beveiligde verbindingen, cryptografisch beveiligde auditlogs, etc.). Deze beveiligingsmaatregelen tezamen zorgen ervoor dat de systemen die de TSP gebruikt, aangemerkt kunnen worden als ‘trustworthy systems’ als bedoeld in ETSI EN 419 261. Er is een daartoe strekkende IT-auditverklaring afgegeven.

7 Certificaat-, CRL- en OCSP-profielen

7.1 Certificaatprofielen

veld		critical	persoon burger (3c)
Version			2
SerialNumber			[uniek nummer binnen de CA met ten minste 8 bytes niet te voorspellen willekeurige data]
Signature			Sha-256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer*	commonName (2.5.4.3)		Cleverbase ID PKIoverheid Burger CA - G3
	organizationIdentifier (2.5.4.97)		NTRNL-67419925
	organizationName (2.5.4.10)		Cleverbase ID B.V.
	countryName (2.5.4.6)		NL
Validity	notBefore		[datum uitgifte][5]
	notAfter		[datum uitgifte + 1095 dagen][5,6]
Subject*	serialNumber		Zie paragraaf 3.1
	commonName		
	countryName		
	givenName		
	surName		
subjectPublicKeyInfo	algorithm		rsaEncryption (1.2.840.113549.1.1.1)
	subjectPublicKey		[publieke sleutel van de certificaathouder]
authorityKeyIdentifier (2.5.29.35)	keyIdentifier	Nee	[sha1 hash van de publieke sleutel van de CA]
subjectKeyIdentifier (2.5.29.14)	keyIdentifier	Nee	[sha1 hash van de publieke sleutel in het certificaat]

[5] De hier genoemde tijdstippen kunnen enkele minuten afwijken, zoals bedoeld in RFC 4270, sectie 5.1.

[6] Het certificaat kan nooit langer geldig zijn dan het bovenliggende rootcertificaat. Het is echter het beleid van Cleverbase om telkens wanneer het rootcertificaat minder dan drie jaar geldig is, dit te vernieuwen, zodat eindgebruikercertificaten altijd een geldigheid van drie jaar kunnen hebben.

keyUsage (2.5.29.15)		Ja	*Authenticiteitscertificaat:* digitalSignature (1000 0000 0) *Vertrouwelijkheidscertificaat:* keyEncipherment dataEncipherment (0011 0000 0) *Onweerlegbaarheidscertificaat:* nonRepudiation (0100 0000 0)
certificatePolicies (2.5.29.32)	policyIdentifier	Nee	*Authenticiteitscertificaat:* 2.16.528.1.1003.1.2.3.1 *Vertrouwelijkheidscertificaat:* 2.16.528.1.1003.1.2.3.3 *Onweerlegbaarheidscertificaat:* 2.16.528.1.1003.1.2.3.2
	cPSuri (1.3.6.1.5.5.7.2.1)		https://pki.cleverbase.com/cps.pdf
	userNotice (1.3.6.1.5.5.7.2.2)		Reliance on this certificate by any party assumes acceptance of the relevant Cleverbase Certification Practice Statement and other documents in the Cleverbase repository.
subjectAltName (2.5.29.17)	otherName	Nee	MS UPN: [Subject.serialNumber]@2.16.528.1.1003.1.3.3.4.1
CRLDistributionPoints (2.5.29.31)	FullName	Nee	http://pki.cleverbase.com/cleverbase3c.crl
ExtKeyUsage (2.5.29.37)		Nee	*Authenticiteitscertificaat:* clientAuthentication (1.3.6.1.5.5.7.3.2) documentSigning (1.3.6.1.4.1.311.10.3.12) emailProtection (1.3.6.1.5.5.7.3.4) *Vertrouwelijkheidscertificaat:* emailProtection (1.3.6.1.5.5.7.3.4)

		encryptingFileSystem (1.3.6.1.4.1.311.10.3.4) *Onweerlegbaarheidscertificaat:* documentSigning (1.3.6.1.4.1.311.10.3.12) emailProtection (1.3.6.1.5.5.7.3.4)
authorityInfoAccess (1.3.6.1.5.5.7.1)	Nee	AccessMethod: id-ad-ocsp (1.3.6.1.5.5.7.48.1) AccessLocation: http://pki.cleverbase.com/ocsp/3c AccessMethod: id-ad-calssuers (1.3.6.1.5.5.7.48.2) AccessLocation: http://pki.cleverbase.com/CleverbaseBurgerG3.cer
QcStatement (1.3.6.1.5.5.7.1.3)	Nee	*Alleen voor het onweerlegbaarheidscertificaat:* id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qct-esign (0.4.0.1862.1.6.1) id-etsi-qcs-QcSSCD (0.4.0.1862.1.4) id-etsi-qcs-QcPDS (0.4.0.1862.1.5) PDS URL = https://pki.cleverbase.com/pki-disclosure-statement.pdf PDS Lang = en

7.2 CRL-profielen

Veld		Critical	Inhoud
Version			1 (versie 2)
Signature			sha-256WithRSAEncryption
Issuer*	commonName (2.5.4.3)		Cleverbase ID PKIoverheid Burger CA - G3
	organizationIdentifier (2.5.4.97)		NTRNL-67419925
	organizationName (2.5.4.10)		Cleverbase ID B.V.
	countryName (2.5.4.6)		NL
ThisUpdate			[tijdstip van uitgifte van de CRL]

NextUpdate		[tijdstip van uitgifte van de CRL + 7 dagen]
revokedCertificates		[ingetrokken certificaten]
CRLNumber	Nee	[opvolgend nummer]

7.3 OCSP-profielen

veld		critical	persoon burger (3c)
Version			2
SerialNumber			[uniek nummer binnen de CA met ten minste 8 bytes unieke data]
Signature			Sha-256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer*	commonName (2.5.4.3)		Cleverbase ID PKIoverheid Burger CA - G3
	organizationIdentifier (2.5.4.97)		NTRNL-67419925
	organizationName (2.5.4.10)		Cleverbase ID B.V.
	countryName (2.5.4.6)		NL
Validity	notBefore		[datum uitgifte]
	notAfter		[datum uitgifte + 1095 dagen]
Subject*	commonName (2.5.4.3)		OCSP Signing Cleverbase ID Burger CA - G3
	organizationIdentifier (2.5.4.97)		NTRNL-67419925
	organizationName (2.5.4.10)		Cleverbase ID B.V.
	countryName (2.5.4.6)		NL
subjectPublicKeyInfo	algorithm	Nee	rsaEncryption (1.2.840.113549.1.1.1)
	subjectPublicKey		Bevat de publieke sleutel
authorityKeyIdentifier (2.5.29.35)	keyIdentifier	Nee	[sha1 hash van de publieke sleutel van de CA]
SubjectKeyIdentifier (2.5.29.14)	keyIdentifier	Nee	[sha1 hash van de publieke sleutel in het certificaat]
KeyUsage (2.5.29.15)		Ja	digitalSignature (1000 0000 0)
CertificatePolicies (2.5.29.32)	policyIdentifier	Nee	2.16.528.1.1003.1.2.3.1

	cPSuri (1.3.6.1.5.5.7.2.1)		https://pki.cleverbase.com/cps.pdf
	userNotice (1.3.6.1.5.5.7.2.2)		Reliance on this certificate by any party assumes acceptance of the relevant Cleverbase Certification Practice Statement and other documents in the Cleverbase repository.
subjectAltName (2.5.29.17)	otherName	Nee	Microsoft UPN: 42@2.16.528.1.1003.1.3.3.4.1
CRLDistributionPoints (2.5.29.31)	FullName	Nee	http://pki.cleverbase.com/cleverbase3c.crl
ExtKeyUsage (2.5.29.37)		Nee	id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9)
OCSPNoCheck (1.3.6.1.5.5.7.48.1.5)		Nee	
authorityInfoAccess (1.3.6.1.5.5.7.1)		Nee	AccessMethod: id-ad-ocsp (1.3.6.1.5.5.7.48.1) AccessLocation: http://pki.cleverbase.com/ocsp/3c

* De distinguished names in dit CPS worden, overeenkomstig RFC 4514, weergegeven in de omgekeerde volgorde ten opzichte van hoe zij in de onderliggende ASN.1-structuur voorkomen.

8 Conformiteitsbeoordeling

Cleverbase is een vertrouwensdienstverlener als bedoeld in de eidas-verordering (EU 910/2014). Zij staat om die reden onder toezicht van het Agentschap Telecom.

Tevens is zij gecertificeerd tegen de normen ETSI EN 319 411-1 en ETSI EN 319 411-2. Deze certificering is verricht door BSI Group The Netherlands B.V., dat hiervoor gecertificeerd is door UKAS. Bij deze certificering is tevens een verklaring afgegeven dat Cleverbase certificaten uitgeeft conform deel 3c van het Programma van Eisen PKIoverheid en de eidas-verordening. De auditor die de conformiteitsbeoordeling verricht, is volledig onafhankelijk van Cleverbase.

De scope van de conformiteitsbeoordeling bedraagt de volgende services:

- Registration service
- Certificate generation service
- Revocation management service
- Revocation status service
- Dissemination service
- Subject device provision service

De conformiteitscertificaten hebben een geldigheid van twee jaar en jaarlijks vindt een tussentijdse audit plaats. Bovendien worden ook regelmatig interne audits uitgevoerd.

Indien onverhoopt afwijkingen geconstateerd worden, wordt een plan opgesteld om deze afwijkingen op korte termijn te herstellen.

De conformiteitsbeoordelingscertificaten zijn te raadplegen op de website van Cleverbase. De onderliggende auditrapporten zijn vertrouwelijk, maar worden wel beschikbaar gesteld aan het Agentschap Telecom.

9 Algemene en juridische bepalingen

9.1 Tarieven

Certificaten kunnen gratis of tegen betaling worden verstrekt. Over eenmalige of periodieke betalingen sluit de TSP een nadere overeenkomst met de abonnee.

Voor het verstrekken van certificaatstatusinformatie of andere informatie met betrekking tot de certificaten wordt geen vergoeding gevraagd. Slechts indien een bijzondere inspanning vereist is om een informatieverzoek te beantwoorden, kunnen hiervoor redelijke kosten in rekening worden gebracht. In dit geval wordt de verzoeker van deze informatie hierover op de hoogte gesteld voordat een betalingsverplichting wordt aangegaan.

9.2 Financiële verantwoordelijkheid

De TSP is niet aansprakelijk voor door hem veroorzaakte schade, tenzij en voor zover in de gevallen bedoeld in art. 13 van de eidas-verordening. Deze beperking van de aansprakelijkheid is tevens vastgelegd in de algemene voorwaarden van de TSP. Indien het certificaat niet op de wijze, als beschreven in het certificaat zelf of in dit CPS, gebruikt wordt, is de TSP niet aansprakelijk.

Ten behoeve van deze aansprakelijkheid heeft de TSP een aansprakelijkheidsverzekering afgesloten met een dekking tot ten minste 1.000.000,- euro.

9.3 Vertrouwelijkheid van bedrijfsinformatie

De TSP beschouwt alle gegevens die verstrekt worden in het kader van de certificatiedienstverlening als vertrouwelijk, behalve de gegevens in certificaten van het type server organisatie.

Eenieder die over vertrouwelijke informatie beschikt, is ervoor verantwoordelijk deze vertrouwelijkheid te waarborgen.

9.4 Bescherming van persoonsgegevens

De TSP heeft een information security management system (ISMS). Hiermee wordt de vertrouwelijkheid van door de TSP verwerkte persoonsgegevens gewaarborgd.

9.5 Intellectuele eigendomsrechten

Op alle documenten die door de TSP naar buiten gebracht worden, rust het auteursrecht van de TSP. Ten overvloede wordt hier vermeld dat dit niet geldt voor documenten die door de certificaathouder met een door de TSP uitgegeven certificaat worden ondertekend. De TSP vrijwaart de klant van aanspraken door derden ten aanzien van eventuele schending van intellectuele-eigendomsrechten door de TSP.

9.6 Verklaringen en garanties

De TSP garandeert hierbij dat hij:

(a) de in dit TPS beschreven procedures in acht neemt,
(b) alle redelijke handelingen heeft verricht om te waarborgen dat de informatie die in de uitgegeven certificaten is opgenomen, correct was op het moment van uitgifte,
(c) certificaten zal intrekken indien bij hem het vermoeden bestaat dat de gegevens in het certificaat niet (meer) accuraat zijn of dat de bij het certificaat behorende private sleutel is gecompromitteerd.

9.7 Beperking van garanties

Er zijn geen andere beperkingen van de garanties dan die in paragraaf 9.6 genoemd zijn.

9.8 Beperkingen van aansprakelijkheid

Er zijn geen andere beperkingen van aansprakelijkheid dan die in paragraaf 9.2 genoemd zijn.

9.9 Geschillenbeslechting

Indien een geschil ontstaat tussen de TSP en een klant van de TSP of een derde, beslist het management van de TSP na de betrokkenen te hebben gehoord en alle betrokken belangen te hebben afgewogen. Een dergelijke beslissing wordt op schrift gesteld en binnen redelijke termijn gegeven. Deze procedure beperkt niet de mogelijkheid om geschillen voor te leggen aan de civiele rechter te Den Haag.

9.10 Toepasselijk recht

Op alle handelingen van de TSP is Nederlands recht van toepassing.