Certificate Practice Statement DigiNotar PKIoverheid

DOMEIN OVERHEID en BEDRIJVEN

GEBASEERD OP CPS DIGINOTAR GEKWALIFICEERD

versie 1.2.2 Augustus 2007

DigiNotar wordt als entiteit door PKIoverheid uniek geïdentificeerd door 2.16.528.1.1003. 1.3.2.3

De certificaat policy voor de onder dit CPS uitgegeven certificaten is:

Authenticiteit	2.16.528.1.1003. 1.2.2.1
Onweerlegbaarheid	2.16.528.1.1003. 1.2.2.2
Vertrouwelijkheid	2.16.528.1.1003. 1.2.2.3

Gebaseerd op: ETSI TS 101 456
“Policy requirements for certification authorities issuing qualified certificates”

Inhoudsopgave

1. Introductie

1.1 Achtergrond

1.1.1 Notarissen in de digitale wereld: DigiNotar

Net als in de gewone wereld, is ook in de digitale wereld van internet behoefte aan zekerheid en betrouwbaarheid. In die behoefte voorziet van oudsher de notaris wanneer er afspraken op papier moeten worden vastgelegd of handtekeningen moeten worden gelegaliseerd. Ook kan hij nu zorgdragen voor zekerheid en betrouwbaarheid bij de elektronische uitwisseling van gegevens.

1.1.2 Organisatie van het DigiNotar samenwerkingsverband

De DigiNotar Certificaat Diensten worden verleend door samenwerking tussen DigiNotar en de bij DigiNotar aangesloten TTP notarissen. DigiNotar en de DigiNotar TTP notaris hebben ieder een eigen functie bij het verlenen van de DigiNotar Certificaat Diensten. De DigiNotar TTP notaris is verantwoordelijk voor de werkzaamheden als RA. DigiNotar is verantwoordelijk voor de technische realisatie van de verleende diensten en voor haar werkzaamheden als CA.
Voor de afgifte van gekwalificeerde certificaten in het PKI overheid domein zijn alleen DigiNotar TTP notarissen als RA actief die als zodanig gecertificeerd zijn.

1.1.3 Andere RA's dan de DigiNotar TTP notaris

Ook andere organisaties kunnen in het PKI overheid domein als RA met DigiNotar als CA samenwerken mits deze organisaties als zodanig gecertificeerd zijn.

1.2 Doel van het Certificate Practice Statement

1.2.1 Wat is het CPS DigiNotar voor gekwalificeerde certificaten?

Dit document geeft een handleiding en algemene voorwaarden voor de CSP (Certificate Service Provider) activiteiten van de DigiNotar organisatie voor gekwalificeerde certificaten binnen het Domein Overheid van PKI overheid en is voor deze certificaten het Certificate Practice Statement (CPS) van DigiNotar.

Het document is gebaseerd op de Certificate Policy – Domein Overheid en Bedrijven (PvE deel 3a) van PKI overheid voor gekwalificeerde certificaten dat samen met dit CPS en de met Abonnees gesloten overeenkomsten de voorwaarden behelzen waaronder certificaten worden afgegeven.

Het document vormt een onderdeel van de contractuele afspraken over de verstrekking van gekwalificeerde certificaten binnen het Domein Overheid van PKI overheid en bevat een beschrijving van de rechten en verplichtingen van partijen in verband met het gebruik daarvan.

Het CPS DigiNotar PKI overheid is aan verandering onderhevig en zal daarom periodiek worden aangepast.

1.3 Gebruikersgemeenschap en toepassingsgebied

1.3.1 Gebruikersgemeenschap

Binnen het Domein Overheid en Bedrijven bestaat de gebruikersgemeenschap uit Abonnees, die organisatorische entiteiten binnen de overheid en bedrijfsleven[1] mogen vertegenwoordigen en uit certificaathouders, die bij deze Abonnees behoren. Daarnaast zijn er vertrouwende partijen, die handelen in vertrouwen op certificaten van de betreffende certificaathouders.

De partijen binnen de gebruikersgemeenschap zijn Abonnees, certificaathouders en vertrouwende partijen.

- Een Abonnee is een natuurlijke of rechtspersoon die met een CSP een overeenkomst sluit namens een of meer certificaathouders voor het laten certificeren van de publieke sleutels. Een Abonnee kan tevens certificaathouder zijn.

- Een certificaathouder is een entiteit, gekenmerkt in een certificaat als de houder van de private sleutel die is verbonden met de publieke sleutel die in het certificaat is gegeven. De certificaathouder is onderdeel van een organisatorische entiteit waarvoor een Abonnee de contracterende partij is.

- Een vertrouwende partij is iedere natuurlijke of rechtspersoon die ontvanger is van een certificaat en die handelt in vertrouwen op dat certificaat.

1.3.2 Toepassingsgebied

1. Het gebruik van certificaten uitgegeven onder dit CPS heeft betrekking op communicatie van of met de certificaathouders die handelen namens de Abonnee.

2. Handtekeningcertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt om elektronische handtekeningen te verifiëren, die “voldoen aan vereisten van een handtekening in relatie tot gegevens

[1] De indeling in Domeinen Overheid en Bedrijfsleven zal door de Policy Autoriteit worden gewijzigd. Hierop vooruitlopend is het toepassingsgebied van het Domein Overheid uitgebreid.

in elektronische vorm, op dezelfde wijze als een handgeschreven handtekening voldoet aan die vereisten in relatie tot gegevens op papier" zoals wordt aangegeven in artikel 5.1 van de richtlijn nr. 1999/93/EG.

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

4. Vertrouwelijkheidcertificaten, die onder deze CPS worden uitgegeven, kunnen worden gebruikt voor het beschermen van de vertrouwelijkheid van gegevens, die worden uitgewisseld en/of opgeslagen in elektronische vorm. Dit betreft zowel de uitwisseling tussen personen onderling als tussen personen en geautomatiseerde middelen.

1.3.3 Geen eigendomsoverdracht van het Certificaat

De Abonnee verkrijgt het recht het Certificaat tezamen met het Sleutelpaar te (doen) gebruiken conform het bepaalde in dit CPS. Het Certificaat blijft eigendom van DigiNotar.

1.4 Verhouding tussen CP en CPS

Het document is gebaseerd op de Certificate Policy – Domein Overheid en Bedrijven (PvE deel 3a) van PKI overheid voor gekwalificeerde certificaten dat samen met dit CPS en de met Abonnees gesloten overeenkomsten de voorwaarden behelzen waaronder gekwalificeerde certificaten binnen het Domein Overheid van PKI overheid worden afgegeven.

1.5 Verwijzingen naar dit CPS.

In ieder Certificaat dat onder dit CPS en het daarbij behorende CP wordt uitgegeven is een OID opgenomen dat verwijst naar dit CPS en het CP, conform het volgende schema.

Het OID is als volgt opgebouwd:

De basis is het nummer dat door het Normaliseringsinstituut en PKIoverheid aan DigiNotar is toegekend:

Categorie	**Nummer**
JOINT-ISO-ITU-T	2
Country	16
Netherlands	528
Organisation	1
Overheid	1003

Dit leidt dus tot het volgende publieke OID voor PKIoverheid: 2.16.528.1.1003

Binnen PKIoverheid wordt DigiNotar als entiteit uniek geïdentificeerd door 2.16.528.1.1003. 1.3.2.3

Het CP waaronder de certificaten uit het domein overheid worden uitgegeven wordt geïdentificeerd door:

Authenticiteit 2.16.528.1.1003. 1.2.2.1

Onweerlegbaarheid 2.16.528.1.1003. 1.2.2.2

Vertrouwelijkheid 2.16.528.1.1003. 1.2.2.3

1.6 Onderhoud, opvragen, commentaar

Het CPS DigiNotar PKI overheid - Domein Overheid is opgesteld en wordt onderhouden door:

DigiNotar B.V.
Vondellaan 8
1942 LJ Beverwijk
Telefoon: 0251 - 268888
Fax: 0251 - 268800
E-mail: info@diginotar.nl
WWW: http://www.diginotar.nl

De citeertitel van dit document is 'CPS DigiNotar PKIoverheid – Domein Overheid'.

Het is bedoeld voor belanghebbenden die certificaten uitgegeven onder dit CPS gebruiken of daarop afgaan. Het CPS DigiNotar PKI overheid – Domein Overheid is te verkrijgen via de DigiNotar website, via het bovenstaande e-mailadres en in papieren vorm via het bovenstaande adres. Wanneer het document op papier wordt aangevraagd, zullen verzend- en administratiekosten in rekening worden gebracht.

2. Definities en afkortingen

Voor definities en afkortingen wordt verwezen naar het PvE deel 4 van PKI overheid

3. Algemene Bepalingen

3.1 Verplichtingen: DigiNotar en de RA

Alle, in het kader van het CPS en de overeenkomsten waarvan het CPS deel kan uitmaken, door DigiNotar en de RA verrichte werkzaamheden worden voortvarend met inachtneming van de van toepassing zijnde procedures uitgevoerd.

DigiNotar en de RA verrichten de werkzaamheden – tenzij expliciet anders overeengekomen of anders vermeld - gedurende Werkdagen van 09.00 uur 's morgens tot 17.00 uur ’s middags.

De RA zal zijn praktijk voeren met inachtneming van de richtlijnen van DigiNotar.

De RA zal, in het kader van diens TTP dienstverlening, zijn apparatuur, programmatuur, telecommunicatiefaciliteiten, systeembeheer en procedures inrichten volgens de richtlijnen van DigiNotar. De RA zal de verificatie- en controleprocedure, aan de hand van de door de Abonnee en/of Certificaathouder geleverde informatie, met de grootste zorgvuldigheid conform het CPS uitvoeren.

3.2 Verplichtingen van de Abonnee

3.2.1 Garanties en aansprakelijkheid van de Abonnee

De Abonnee staat ervoor in dat:

a) de gegevens in het Certificaat te allen tijde juist en volledig zijn;

b) het Certificaat wordt gebruikt in overeenstemming met de toepasselijke wettelijke en andere regelgeving (zoals privacywetgeving, het Burgerlijk Wetboek, Telecommunicatiewetgeving en dergelijke);

c) het Certificaat wordt gebruikt overeenkomstig het bepaalde in het CPS en de overeenkomsten waarvan het CPS deel kan uitmaken en die met het CPS verband houden;

d) het in het CPS, en in de contractuele afspraken waarvan het CPS deel kan uitmaken, bepaalde deugdelijk door de Certificaathouder(s) wordt nageleefd.

De Abonnee is verantwoordelijk voor de keuze en (fysieke) beveiliging van zijn programmatuur, apparatuur en telecommunicatiefaciliteiten en de beschikbaarheid van zijn informatie- en communicatiesystemen, waarmee hij het elektronische berichtenverkeer tot stand brengt.

De Abonnee zal adequate maatregelen nemen ter bescherming van zijn systeem tegen virussen en andere programmatuur oneigenlijke elementen.

3.2.2 Vrijwaring door de Abonnee

De Abonnee vrijwaart DigiNotar en de betreffende RA voor alle aanspraken van derden, gebaseerd op de stelling dat de informatie in een door de CSP verstrekt Certificaat niet langer juist of volledig is.

De Abonnee is jegens DigiNotar en/of de RA aansprakelijk voor alle schade die laatstgenoemden mochten lijden als gevolg van aanspraken van derden die verband houden met de door DigiNotar en/of de RA verleende diensten of geleverde producten, als gevolg van door Abonnee en/of Certificaathouder onjuist aangeleverde informatie, tenzij dit te wijten is aan de opzet of grove schuld van DigiNotar en/of de RA.

De Abonnee en de Certificaathouder zijn, vanaf het moment van de afgifte van het Certificaat, verantwoordelijk voor het beheer en gebruik van de Private sleutel, de in het Certificaat vastgelegde informatie en (voor zover van toepassing) de toegekende persoonlijke Pincode, de toegekende Revocation Passphrase, het aan het Sleutelpaar toegekende Wachtwoord, een en ander conform het CPS en de contractuele afspraken waarvan het CPS deel kan uitmaken.

De Abonnee en voor zoveel mogelijk de Certificaathouder zal na het moment van de afgifte van het Certificaat de Private sleutel zorgvuldig beheren en technische, personele en organisatorische maatregelen nemen om de Private sleutel en zijn systeem beveiligen tegen verlies of diefstal en onbevoegd gebruik, op welke wijze dan ook.
De certificaathouder dient zijn SSCD (Smartcard of ander token waarop de private sleutel(s) geplaatst is(zijn)) te beveiligen zoals men ook andere waardevolle persoonlijke eigendommen beveiligt, zoals creditcard of paspoort. De certificaathouder dient de PIN code die wordt gebruikt om toegang te krijgen tot de certificaten, gescheiden van de drager van het sleutelmateriaal (de SSCD) te bewaren.

De Abonnee en de Certificaathouder dienen de RA tijdig schriftelijk (getekende post, getekende fax, ondertekende e-mail) te informeren over elke wijziging die voor het afgegeven Certificaat van belang is, zoals wijzigingen in de naam, (e-mail)adres, woonplaats (NAW gegevens), bevoegdheden en over wijzigingen in de rechtsvorm van de onderneming, één en ander voor zover deze informatie bij de Abonnee casu quo de Certificaathouder zelf bekend is of behoord te zijn.

De Abonnee is in alle gevallen aansprakelijk voor de schade die is ontstaan door het te laat intrekken of laten wijzigen van een Certificaat, na de afgifte van het Certificaat, ongeacht of de noodzaak tot intrekken, wijzigen aan hem kan worden toegerekend, tenzij de te late intrekking of wijziging te wijten is aan de

CSP, waarbij de bepalingen van dit CPS, de CP dan wel de ETSI norm voor zover de bepalingen van dit CPS en/of het CP hiermee in strijd zijn, bepalend zijn òf de te late intrekking aan de CSP te wijten is.

De Abonnee en de Certificaathouder dienen het verlies, de diefstal of het onbevoegde gebruik van de aan hem afgegeven Private sleutel, persoonlijke PINcode, Wachtwoord en tevens onregelmatigheden in zijn systeem of andere relevante omstandigheden onmiddellijk bij constatering daarvan aan de RA te melden.

3.2.3 Verplichtingen van de Abonnee ten aanzien van de Certificaathouders voor wie hij Certificaten heeft aangevraagd

De Abonnee zal ervoor zorg dragen dat de Certificaathouder(s) die gebruik maakt (maken) van een door de Abonnee aangevraagd Certificaat bekend zijn en akkoord gaan met het CPS, het CP en de overigens van toepassing zijnde bepalingen. De Abonnee is naast de Certificaathouder verantwoordelijk voor de juiste naleving van het CPS ten aanzien van de Certificaathouder(s) voor wie hij Certificaten heeft aangevraagd.

De Abonnee dient erop toe te zien en de Certificaathouder te verplichten dat:

a) de Certificaathouder te allen tijde de Private sleutel en de toegang daartoe (bijvoorbeeld de PIN code) zorgvuldig zal gebruiken, strikt geheim zal houden en zal bewaren;

b) de Certificaathouder het Certificaat slechts gebruikt voor het doel waarvoor hij door de Abonnee is geautoriseerd en met inachtneming van de in verband daarmee geldende beperkingen;

c) de Certificaathouder het Certificaat niet gebruikt in strijd met het in dit CPS, het CP of de daarmee samenhangende contractuele regelingen bepaalde;

d) de Certificaathouder gerechtigd is de in het Certificaat vermelde (handels)naam en woord- en beeldmerken te gebruiken;

e) de Certificaathouder juiste en volledige informatie verstrekt aan DigiNotar casu quo de betreffende RA in overeenstemming met de vereisten van dit CPS met name voor wat betreft de registratie;

f) de Certificaathouder het handtekening - sleutelpaar (gecertificeerd met een gekwalificeerd Handtekeningcertificaat) alleen gebruikt voor het zetten van een elektronische handtekening en met inachtneming van de overige beperkingen die aan de Abonnee zijn kenbaar gemaakt.

g) de Certificaathouder zo snel mogelijk als redelijkerwijs verwacht mag worden DigiNotar casu quo de betreffende RA op de hoogte brengt als zich

een onregelmatigheid voordoet, tot aan het einde van de in het Certificaat aangegeven geldigheidsduur.

h) de Certificaathouder, voorzover deze gebruik maakt van een PINcode om toegang te krijgen tot de Certificaten, deze gescheiden van de drager van het sleutelmateriaal (de SSCD) bewaart.

3.2.4 Beperkingen in het gebruik

De Abonnee zal zich houden aan de toepasselijke Nederlandse, Europese, overige (inter)nationale wet- en regelgeving en de bepalingen van het CPS met betrekking tot het doel waarvoor hij het Certificaat wenst te gebruiken, de keuze van de wederpartij met wie hij elektronische berichten uitwisselt en meer in het bijzonder de inhoud van het berichtenverkeer dat hij met gebruikmaking van het Certificaat wenst te verrichten, waaronder voor zover van toepassing tevens vallen de door hem gesloten overeenkomsten met consumenten en de door hem toegepaste Encryptie. Het is de Abonnee en de Certificaathouder(s) verboden om het Certificaat te gebruiken buiten de door het CP, het CPS of in het Certificaat aangegeven doeleinden en gebruikersgroep.

Overschrijdingen van beperkingen in de hoogte van het belang of buiten de gebruikersgroep waarvoor het Certificaat geschikt is, komen geheel voor rekening van Abonnee en/of Certificaathouder.

3.3 Verplichtingen van de vertrouwende partijen

3.3.1 Algemeen

Een vertrouwende partij (de op het Certificaat vertrouwende derde), dient, indien deze in redelijkheid wil kunnen vertrouwen op een Certificaat:

a) de intrekking van het Certificaat door middel van de meest actuele informatie over intrekking, zoals door DigiNotar onder meer via haar Website (www.diginotar.nl) beschikbaar is gesteld, te verifiëren, waarbij een Certificaat eerst geldt als ingetrokken zodra de informatie daaromtrent op de Website is gepubliceerd;

b) de geldigheid zoals deze blijkt uit het Certificaat te verifiëren;

c) de geldigheid van de volledige keten van certificaten tot aan de bron (het stamcertificaat van de Staat der Nederlanden) te verifiëren;

d) kennis te nemen van alle beperkingen betreffende het gebruik van het Certificaat zoals deze kunnen blijken uit het Certificaat dan wel uit de voorwaarden (CP, CPS), die door DigiNotar op haar Website algemeen beschikbaar zijn gesteld;

e) alle overige voorzorgsmaatregelen te nemen die in overeenkomsten of elders zijn voorgeschreven.

3.4 Aansprakelijkheid

3.4.1 Beperking aansprakelijkheid RA en CA, algemeen.

In het kader van de afgifte van Gekwalificeerde certificaten stelt DigiNotar zich aansprakelijk conform de eisen van de richtlijn Elektronische handtekeningen, 1999/93/EG.

Dit houdt in dat DigiNotar in ieder geval aansprakelijk is voor schade die diensten of natuurlijke of rechtspersonen, die in redelijkheid op dit Certificaat vertrouwen, ondervinden, in samenhang met:

- de juistheid, op het tijdstip van afgifte, van alle gegevens in het Gekwalificeerde certificaat en de opneming in het Gekwalificeerde certificaat van alle voor een dergelijk Certificaat voorgeschreven gegevens;

- de garantie dat de in het Gekwalificeerde certificaat geïdentificeerde ondertekenaar, op het tijdstip van de afgifte van het Certificaat, houder was van de gegevens voor het aanmaken van de handtekening, die met de in het Certificaat gegeven of geïdentificeerde gegevens voor het verifiëren van de handtekening overeenstemmen;

- de garantie dat de gegevens voor het aanmaken van de handtekening en die voor het verifiëren van de handtekening – voor zover zij beide door DigiNotar zijn gegenereerd - complementair kunnen worden gebruikt;

een en ander **tenzij** DigiNotar bewijst dat zij niet nalatig heeft gehandeld.

DigiNotar is aansprakelijk voor de schade die bij diensten of natuurlijke of rechtspersonen die in redelijkheid op het Certificaat hebben vertrouwd, is ontstaan doordat de intrekking van het Certificaat niet werd verwerkt binnen de daarvoor toegestane periode, waarbij inbegrepen het bijwerken en publiceren van certificate status information.

tenzij DigiNotar bewijst dat zij niet nalatig heeft gehandeld, waarbij geldt dat degene die zich beroept op niet (tijdige) intrekking aannemelijk dient te maken dat hij een verzoek tot intrekking heeft gedaan en op welk tijdstip.

DigiNotar is niet aansprakelijk voor schade, die voortvloeit uit gebruik van een Gekwalificeerd Certificaat, waarbij de op het Certificaat aangegeven beperkingen worden overschreden.

DigiNotar sluit alle aansprakelijkheid uit voor schade indien het Certificaat niet conform het beschreven toepassingsgebied is/wordt gebruikt.

Voorwaarde voor het ontstaan van enig recht op schadevergoeding is steeds dat de gelaedeerde na het ontstaan daarvan zo spoedig als redelijkerwijs mogelijk is de schade schriftelijk middels aangetekend schrijven bij DigiNotar of de betreffende RA heeft gemeld. Indien de gelaedeerde met andere Abonnees, Certificaathouders of derden afspraken heeft gemaakt die leiden tot afwijkende verantwoordelijkheden casu quo risico's dan standaard uit het gebruik van de Certificaten voortvloeit, zal dit jegens de RA en DigiNotar niet tot grotere verantwoordelijkheden en/of aansprakelijkheden en/of hogere schadevergoedingen kunnen leiden dan wanneer deze afspraken niet zouden zijn gemaakt.

De RA en DigiNotar zijn ieder slechts draagplichtig voor het voor zijn/haar rekening komende deel van de dienstverlening, hetgeen de voor hen eventueel geldende beperkingen, uitsluitingen of uitbreidingen van aansprakelijkheid onverlet laat.

3.4.2 Beperking aansprakelijkheid, specifiek.

Noch DigiNotar, noch de RA staat in voor:

a) de afgifte van een Certificaat op grond van door de Abonnee verkeerd verstrekte informatie, voor zover het inferieur zijn van deze informatie op grond van de op basis van dit CPS vereiste controles in redelijkheid niet ontdekt had kunnen worden;

b) wijzigingen in de identiteit en/of bevoegdheden van de Abonnee en/of de Certificaathouder en/of overige gegevens na de afgifte van een Certificaat;

c) het gebruik van een Certificaat na het tijdstip van afgifte ervan;

d) met name is de aansprakelijkheid uitgesloten ingeval een gebrek in het verzonden bericht of in de verzending of ontvangst daarvan ernstige schade, zoals lichamelijk letsel, dood of milieuschade ten gevolge heeft, daaronder begrepen doch niet daartoe beperkt, in het kader van het gebruik van nucleaire systemen, verkeers(-controle)systemen en medische toepassingen;

e) de inhoud van het met het Certificaat tot stand te brengen elektronische berichtenverkeer;

f) het gebruik van een Certificaat na de intrekking of schorsing daarvan;

g) fouten die veroorzaakt zijn door de transmissie van gegevens door de Abonnee en/of Certificaathouder, de programmatuur, apparatuur, telecommunicatiefaciliteiten gebruikt door de Abonnee en/of Certificaathouder.

h) DigiNotar en de RA zijn niet aansprakelijk voor vertraging en gebreken in de uitvoering van de werkzaamheden die te wijten zijn aan (technische)

storingen zoals transmissiefouten, storingen aan apparatuur en systeemprogrammatuur, defecten in de apparatuur en programmatuur, opzet zoals fraude, illegaal gebruik van programmatuur, sabotage, diefstal van gegevens en bedieningsfouten door derden, fouten van derden met als gevolg netwerkuitval, stroomuitval, brand, blikseminslag, aanzienlijke waterschade, een breuk in een telefoonkabel, oorlogsgeweld of natuurrampen en meer in het algemeen oorzaken die niet de redelijk in acht te nemen zorg van DigiNotar en/of de RA betreffen;

i) voor het overige aanvaarden DigiNotar en de RA geen andere aansprakelijkheid dan welke deze hebben op grond van het CP, het CPS en eventueel de ETSI norm, voor zover het CP of het CPS hiermee in strijd zou zijn. Ten aanzien van het DigiNotar samenwerkingsverband als zodanig is iedere aansprakelijkheid volledig uitgesloten.

3.5 Financiële verantwoordelijkheid en aansprakelijkheid

DigiNotar stelt geen beperkingen aan de waarde van de transacties waarvoor gekwalificeerde certificaten onder dit CPS kunnen worden gebruikt.

Behoudens het overigens in dit CPS gestelde aanvaardt DigiNotar aansprakelijkheid voor zowel directe als indirecte schade per schadeveroorzakende gebeurtenis tot een bedrag van
Een Miljoen Euro (€ 1.000.000,00). Het vorenstaande laat onverlet de mogelijkheden tot verhaal.

3.6 Interpretatie en handhaving

3.6.1 Van toepassing zijnde wetgeving

Alle overeenkomsten tussen de Abonnee, de RA en, voor zover van toepassing, DigiNotar worden beheerst door Nederlands recht.

3.6.2 Bevoegde rechter

De Abonnee kiest woonplaats ten kantore van DigiNotar. Alle geschillen voortvloeiend uit of verband houdend met deze overeenkomsten worden beslecht door de bevoegde rechter waar DigiNotar is gevestigd.

Alle rechtsbetrekkingen met Certificaathouders, vertrouwende partijen en derden welke betrekking hebben op de (uitgifte van) certificaten onder dit CPS worden eveneens beheerst door Nederlands Recht en zullen eveneens worden beslecht door vorenbedoelde bevoegde rechter.

3.6.3 Ongeldigheid

De ongeldigheid van een bepaling in een overeenkomst tussen de Abonnee en de RA dan wel DigiNotar tast de geldigheid en de afdwingbaarheid van de overige bepalingen van die overeenkomst niet aan. Partijen zullen in overleg treden teneinde ten spoedigste overeenstemming te bereiken over een vervangende bepaling die de inhoud en strekking van de ongeldige bepaling zoveel mogelijk benadert.

Eensgelijks geldt in zijn algemeenheid voor de bepalingen van dit CPS en het van toepassing zijnde CP.

3.6.4 Geschillenbeslechting

Geschillen kunnen worden voorgelegd aan de gewone rechter waar de RA dan wel DigiNotar is gevestigd.

In geval van klachten betreffende diensten geleverd in het kader van dit CPS kan de klacht schriftelijk ingediend worden bij DigiNotar, ter attentie van de directie en onder vermelding van ‘Klacht’. Dit zal de DigiNotar klachtenprocedure in werking stellen.

3.7 Tarieven

Tarieven voor de te verrichten diensten kunnen worden opgevraagd bij DigiNotar.

3.8 Publicatie van certificaatinformatie

De informatie omtrent de publieke sleutel van:

“DigiNotar PKIoverheid CA Overheid”

is gepubliceerd op www.diginotar.nl.

3.9 Privacy

De Abonnee geeft toestemming aan de RA alsmede aan DigiNotar om het serienummer, de statusinformatie en de voor openbaarmaking bestemde informatie van het Certificaat op de certificatendatabank van DigiNotar, zoals in de LDAP Directory en de DigiNotar CRL, openbaar te maken.

De RA casu quo DigiNotar draagt zorg voor de nodige voorzieningen van technische en organisatorische aard ter beveiliging van een (persoons)gegeven tegen verlies of aantasting daarvan en tegen onbevoegde kennisneming, wijziging of verstrekking van het (persoons)gegeven.

DigiNotar en de RA zullen bij de beveiliging van de persoonsgegevens de relevante wet- en regelgeving stipt in acht nemen.

3.10 Frequentie van publicatie

DigiNotar draagt er zorg voor dat dit CPS vierentwintig uur per dag, zeven dagen per week via de Website van DigiNotar beschikbaar is behoudens in geval van systeemdefecten, serviceactiviteiten, of andere factoren die buiten het bereik van DigiNotar liggen.

In de laatste gevallen maakt DigiNotar zich er sterk voor om ervoor te zorgen dat de informatie niet langer niet beschikbaar is dan 24 uur.

3.11 Toegang tot gepubliceerde informatie/Elektronische opslagplaats

Alle voor de Certificaathouders en vertrouwende partijen benodigde informatie met betrekking tot de uitgifte van certificaten, waaronder met name begrepen de informatie omtrent de intrekking van certificaten (Revocation Status Information) is beschikbaar op de website van DigiNotar (www.DigiNotar.nl).

3.12 Conformiteit aan relevante regelgeving.

De dienstverlening van DigiNotar en de door haar ingeschakelde entiteiten voldoen aan de eisen van de “Policy requirements for certification authorities issuing qualified certificates” (ETSI 101 456 V1.2.1 (2002-04), de Richtlijn nr. 1999/93/EG en de Nederlandse wetgeving.

DigiNotar zal zich hiertoe jaarlijks laten beoordelen door een certificerende instelling die kan aantonen dat DigiNotar en de door haar ingeschakelde entiteiten voldoen aan de eisen van betrouwbaarheid en bekwaamheid als gesteld in de standaard EN 45011 of EN 45012.

3.13 Vertrouwelijkheid

De informatie, die Certificaathouders aan DigiNotar en/of de RA verstrekken, zal niet zonder de toestemming van de eindgebruiker, een rechterlijk bevel of een andere wettelijke grondslag worden onthuld.

Certificaten zijn alleen opvraagbaar in die gevallen waarin de toestemming van de Certificaathouder is verkregen.

DigiNotar draagt er zorg voor dat de vereisten van de geldende privacywet- en regelgeving worden nageleefd.
De Abonnee en de Certificaathouder zijn bevoegd door DigiNotar vastgelegde registratie-informatie, individuele transacties en andere op hen betrekking hebbende informatie op te vragen.

4. Identificatie en authenticatie

4.1 Wijze van aanvragen

Om de identiteit van (de vertegenwoordiger van) de Abonnee persoonlijk te kunnen vaststellen, dient de aanvraag van een eerste Certificaat altijd schriftelijk te worden gedaan. De aanvraag wordt geïnitieerd door of namens de certificaathouder of door de Abonnee. Eventuele vervolgaanvragen kunnen zowel schriftelijk als elektronisch worden gedaan, voor zover dit, met in achtneming van het CPS en de door DigiNotar opgestelde beleidsregels, door DigiNotar wordt toegestaan.

4.2 De Registration Authority (RA)

De RA is verantwoordelijk voor het verifiëren van de identiteit van de Abonnee en de Certificaathouder en overige in het Certificaat op te nemen gegevens, onverminderd de aansprakelijkheid van DigiNotar als CSP. Aanvragen van Certificaten dienen dan ook bij een voor de afgifte van gekwalificeerde certificaten binnen het Domein Overheid en Bedrijven van PKI overheid toegelaten RA te worden ingediend.

De RA neemt de aanvraag slechts in behandeling, indien van de identiteit van de Abonnee en/of de in het Certificaat genoemde Certificaathouder en waar nodig van diens bevoegdheid genoegzaam is gebleken. De RA is bevoegd om bij de verrichte controles gebleken kennelijke verschrijvingen, vergissingen of omissies bij het invullen van de gevraagde gegevens te verbeteren, voor zover deze verbeteringen niet de inhoud van de aanvraag betreffen.

De RA is gerechtigd een verzoek tot de afgifte, vernieuwing, wijziging of intrekking van een Certificaat te weigeren indien de uitkomst van de onder verantwoordelijkheid van de RA uitgevoerde verificatie- en controleprocedure onvoldoende is.

In dat geval zal met bekwame spoed contact worden opgenomen met de Abonnee.

4.3 Initiële registratie - Verificatie

Vóór afgifte van het eerste Certificaat voor een persoon die als ondertekenaar in het Gekwalificeerd certificaat zal worden aangeduid worden, onafhankelijk van het soort Certificaat, de volgende controlehandelingen verricht:

De RA stelt de identiteit van de persoon die als ondertekenaar in het Gekwalificeerd certificaat wordt aangeduid, vast met in achtneming van het bepaalde in artikel 4.8.

De volgende gegevens worden gecontroleerd:

- Achternaam met tussenvoegsels;
- Eerste voornaam (voluit);
- Geboortedatum;
- Geboorteplaats;
- Nummer identiteitsbewijs;
- Uitgifteplaats identiteitsbewijs;
- Geldigheid identiteitsbewijs

Bij twijfel omtrent de geldigheid van het identiteitsbewijs en voorzover mogelijk, wordt aan de hand van het VIS (verificatiesysteem voor identiteitsbewijzen) geverifieerd:

- of het aangeboden legitimatiebewijs als vermist of gestolen is aangemeld.

In aanvulling op het bovenstaande worden van in het Certificaat op te nemen organisaties de volgende gegevens gecontroleerd:

Aan de hand van een uittreksel uit het register van de Kamer van Koophandel (hierna: KvK) waar de Abonnee staat ingeschreven dan wel, in geval van niet KvK geregistreerde organisaties, bij de daartoe geëigende registraties casu quo op basis van relevante documenten:

- Bevoegdheid tot vertegenwoordiging van de Abonnee;
- Handelsnaam;
- Statutaire naam (uitsluitend voor statutair geregelde organisaties);
- Adres (vestigingsadres (fysiek adres) en postadres);
- Statutaire vestigingsplaats (uitsluitend voor statutair geregelde organisaties);
- Inschrijvingsnummer Kamer van Koophandel (uitsluitend voor KvK geregistreerde organisaties);

Indien de Certificaathouder en de rechtsgeldig vertegenwoordiger van de Abonnee niet dezelfde zijn wordt van de rechtsgeldig vertegenwoordiger van de Abonnee eenmalig dezelfde identiteitsvaststelling gedaan als van de Certificaathouder op de wijze als beschreven in artikel 4.7 met dien verstande dat fysieke verschijning optioneel is, ter keuze van de RA. Bij een tweede of

latere aanvraag hoeft van dezelfde persoon niet wederom een identiteitsvaststelling te worden uitgevoerd.

4.4 Uniciteit van namen

De Distinguished Name die aan de Certificaathouder van een Gekwalificeerd certificaat onder de Root van DigiNotar waarop dit CPS van toepassing is, wordt toegekend, zal te allen tijde uniek zijn voor deze Certificaathouder en niet worden uitgegeven aan een andere Certificaathouder.

4.5 Geschillen inzake naam-claims

In gevallen waarin partijen het oneens zijn over het gebruik van in het certificaat opgenomen namen welke de certificaathouder identificeren, en voor zover hierin niet wordt voorzien door Nederlands recht of overige toepasselijke regelgeving, beslist DigiNotar B.V. na zorgvuldige afweging van de belangen van de betrokkenen.

Verder geldt de geschillen regeling zoals in dit CPS 3.6.4 is opgenomen.

4.6 Erkenning, authenticatie en de rol van handelsmerken

Voor zover een organisatie voorkomt in een algemeen erkend openbaar register zal in het Certificaat worden opgenomen de/een naam van deze organisatie zoals deze wordt genoemd in het uittreksel van dit register.

4.7 Methode om bezit van de private sleutel aan te tonen

Indien en voor zover het sleutelpaar waarvoor een Gekwalificeerd certificaat wordt aangevraagd niet door DigiNotar is gegenereerd, dient de (aanstaande) Certificaathouder aan te tonen dat hij in het bezit is van de private sleutel, die behoort bij de voor certificatie aangeboden publieke sleutel.

Tevens dient hij, aan te tonen dat het sleutelpaar is gegenereerd met een veilig middel (SSCD).

4.8 Authenticatie van organisatorische entiteit

Alvorens een certificaat wordt afgegeven binnen het Domein – Overheid en Bedrijven van PKIoverheid zal de RA, dan wel DigiNotar onderzoeken of de betreffende organisatorische entiteit in de zin zoals die volgt uit het CP Domein – Overheid en Bedrijven past binnen dit Domein.

Hierbij zal DigiNotar/de RA de conformiteit voor het domein toetsen aan de van toepassing zijnde definities in het CP Domein – Overheid en Bedrijven.

Bij verschil van inzicht tussen de RA en DigiNotar is de mening van DigiNotar doorslaggevend.

Het geschil kan voorgelegd worden aan de Policy Authoriteit PKI overheid. RA en DigiNotar zullen zich conformeren aan een definitief oordeel van de Policy Authoriteit.

Ten einde te kunnen verifiëren of de door de Abonnee aangemelde organisatienaam juist en volledig is, kan de CSP van de Abonnee verlangen dat deze een geautoriseerde verklaring overlegt.

Ten einde te kunnen verifiëren of de Abonnee bevoegd is namens een organisatorische entiteit te handelen, kan de CSP van de Abonnee en/of de organisatorische entiteit verlangen dat deze een geautoriseerd stuk overlegt waaruit dit blijkt.

4.9 Authenticatie van persoonlijke identiteit

DigiNotar controleert overeenkomstig de Nederlandse wet- en regelgeving en met name aan de hand van de bij artikel 1 van de Wet op de Identificatieplicht aangewezen geldige documenten, de identiteit en, indien van toepassing, specifieke eigenschappen van de persoon aan wie Certificaten worden uitgegeven.

Bewijs van de identiteit wordt gecontroleerd aan de hand van fysieke verschijning van de persoon zelf, hetzij direct, hetzij indirect met behulp van middelen waarmee dezelfde zekerheid kan worden verkregen als bij persoonlijke aanwezigheid. Het bewijs van identiteit kan op papier dan wel langs elektronische weg worden aangeleverd.

5. Operationele eisen

5.1 Uitgifte van certificaten - Afgifte

Na verificatie en akkoordbevinding van de informatie zoals deze door de Abonnee en/of Certificaathouder is verstrekt, draagt de RA zorg voor het doen vervaardigen van het Certificaat. Het Certificaat kan op de volgende wijzen worden aangeboden.

Indien DigiNotar het bij het Certificaat behorende sleutelpaar genereert wordt het Certificaat geactiveerd met behulp van een aan de Certificaathouder toe te kennen PINcode, dan wel of eventueel aangevuld met (een) andere beveiligingsmethode(n) die de Certificaathouder onder zijn uitsluitende controle kan houden, zoals biometrie. De PINcode wordt per aangetekende post met de aantekening “strikt persoonlijk” aan de Certificaathouder in gesloten – niet voor anderen dan (na opening) de Certificaathouder leesbare – toestand toegezonden. Hierbij wordt gebruik gemaakt van een zogenaamde “Pinmailer”.

Het SSCD wordt aan de Abonnee per post, verzonden. Onder het onderhavige CPS worden sleutelparen altijd geplaatst op een SSCD. De PINcode wordt nimmer tegelijk met het SSCD naar hetzelfde adres verzonden.

Op verzoek kan de Certificaathouder het SSCD en/of de betreffende Pinmailer persoonlijk bij de RA of een onder diens verantwoordelijkheid werkende derde in ontvangst nemen onder overlegging van een identiteitsbewijs zoals bedoeld in artikel 1 van de Wet op de Identificatieplicht.

Het moment waarop DigiNotar een Certificaat aanmaakt, geldt als de datum en het tijdstip van afgifte van het Certificaat. Deze datum en dit tijdstip van afgifte van het Certificaat blijken uit de logbestanden van het afgifteproces die door DigiNotar worden aangehouden, welke logbestanden tussen DigiNotar en/of RA en/of de Abonnee en/of jegens derden dienen tot bewijs. De datum en het tijdstip van het activeren van het Certificaat is niet relevant voor het bepalen van het moment van afgifte.

Onmiddellijk na het aanmaken van het Certificaat, staat het Certificaat, afhankelijk van hetgeen is overeengekomen, ter beschikking van de Abonnee, dan wel de Certificaathouder.

De CA zal het Certificaat publiceren in de certificatendatabank van DigiNotar (LDAP Directory).

5.2 Aanvaarding

Het Certificaat wordt geacht door de Abonnee te zijn aanvaard op het tijdstip van afgifte. De Abonnee en Certificaathouder zijn gehouden om, alvorens het

Certificaat in gebruik te nemen, de daarin opgenomen gegevens op juistheid te controleren.

De Abonnee dan wel de Certificaathouder is gehouden om, wanneer een onjuistheid in het afgegeven Certificaat dan wel de afgifteprocedure wordt geconstateerd, per omgaande een verzoek tot wijziging te doen.

Onjuistheden in een Certificaat dat niet is ingetrokken komen voor rekening en risico van de Abonnee, zulks onverminderd de eventuele aansprakelijkheid van de CA en de RA wegens aan hen toe te rekenen tekortkomingen.

De Abonnee zal ervoor zorgdragen dat de Certificaathouders, die gebruik gaan maken van een door de Abonnee voor hen aangevraagd Certificaat, bekend zijn en akkoord gaan met het CPS. De Abonnee is naast de Certificaathouder verantwoordelijk voor de juiste naleving hiervan.

5.3 Geldigheidsduur

Het Certificaat wordt afgegeven voor een geldigheidsduur welke staat aangegeven in het Certificaat.

Onverminderd de eigen verantwoordelijkheid van de Abonnee voor het tijdig aanvragen van een nieuw Certificaat zal de Certificaathouder, uiterlijk 60 dagen van tevoren via standaard e-mail op het in het Certificaat vermelde e-mail adres worden gewezen op het verstrijken van de geldigheidsduur van het Certificaat; voor zover de Abonnee en de Certificaathouder niet dezelfde zijn, is de Certificaathouder gehouden de Abonnee hiervan eveneens in kennis te stellen.

5.4 Wijziging en vernieuwing

Een verzoek tot wijziging of vernieuwing van een Certificaat moet worden gedaan door de Abonnee. Het verzoek kan zowel per elektronisch, met een Gekwalificeerd Certificaat ondertekend, bericht als schriftelijk aan de RA worden gedaan.

Alvorens tot honorering van een verzoek tot wijziging of vernieuwing over te gaan controleert de RA of de identiteitsgegevens en andere kenmerken van de Certificaathouder nog steeds geldig en actueel zijn.

De RA honoreert het verzoek tot wijziging of vernieuwing niet, indien naar zijn uitsluitend oordeel de verrichte controles niet het gewenste resultaat hebben opgeleverd. Van dit laatste wordt met bekwame spoed mededeling gedaan aan de Abonnee.

Voor een aangepaste aanvraag is de procedure voor een nieuwe aanvraag van overeenkomstige toepassing.

Wordt het Certificaat gewijzigd of vernieuwd dan worden een nieuw Sleutelpaar en Certificaat gegenereerd en afgegeven.

5.5 Validatie van ingetrokken Certificaten:

5.5.1 Algemeen

Door DigiNotar wordt een lijst van ingetrokken Certificaten gepubliceerd. De in de gepubliceerde DigiNotar CRL opgenomen informatie over ingetrokken Certificaten kan op verschillende wijzen worden geraadpleegd. De vertrouwende partij is verantwoordelijk voor de wijze waarop hij besluit Certificaten te valideren.
De vertrouwende partij dient, indien hij een CRL raadpleegt, tevens de elektronische handtekening van DigiNotar en het het certificatiepad te controleren.

De volgende validatie methoden worden aangeboden:

A. Website validatie

B. OCSP validatie

C. CRL validatie

5.5.2 Website validatie

Website validatie is de via de DigiNotar website www.diginotar.nl voor *iedereen* beschikbare informatie over ingetrokken Certificaten welke op de website wordt gepubliceerd, waarbij de belanghebbende het Certificaat kan Valideren (op de status daarvan) door het oproepen van de gegevens van het betreffende Certificaat met een op de DigiNotar website aangeboden zoekmethode. De website publicatie is te allen tijde actueel en is maatgevend voor het tijdstip van intrekking.

5.5.3 OCSP validatie

OCSP validatie is een online validatie methode waarbij DigiNotar aan de afnemer van deze dienst een elektronisch ondertekend elektronisch bericht (OCSP response) verstuurt waarin de door afnemer opgevraagde status van het Certificaat (het al dan niet ingetrokken zijn van het Certificaat) wordt weergegeven. De, zonder geldige overeenkomst, via de OCSP validatie verstrekte informatie over het al dan niet ingetrokken zijn van een Certificaat is ten minste gelijk aan, en even actueel als, de informatie die op basis van CRL validatie wordt gepubliceerd.

Indien OCSP validatie wordt aangeboden op basis van een door afnemer met DigiNotar afgesloten daartoe strekkende overeenkomst is de verstrekte

informatie over het al dan niet ingetrokken zijn van een Certificaat gelijk aan, en even actueel als, de informatie die via de DigiNotar website wordt gepubliceerd.

Een OCSP respons is altijd een door DigiNotar verzonden en ondertekend bericht; blijft een OCSP response om enigerlei (al dan niet technische reden) uit dan kan daaraan geen gevolgtrekking worden verbonden omtrent de status van het Certificaat.

5.5.4 CRL validatie

CRL validatie is een validatie methode waarbij op basis van een, op een bepaald tijdstip door DigiNotar aangemaakte kopie of uittreksel van de gepubliceerde DigiNotar CRL kan worden bekeken of een Certificaat is ingetrokken.

De kopie of het uittreksel van de DigiNotar CRL bevat uit haar aard niet de meest actuele informatie omtrent uitgegeven certificaten.

De voor de CRL validatie beschikbaar gestelde kopie CRL wordt minimaal eens per 24 uur ververst.[2]

Het actualiteitsrisico komt voor rekening van degene die gebruik maakt van de CRL validatie.

Deze standaard CRL validatie wordt aangeboden op basis van een door afnemer met DigiNotar afgesloten daartoe strekkende overeenkomst.

Op basis van een door de afnemer met DigiNotar af te sluiten overeenkomst kan een meer actuele CRL frequent (bijvoorbeeld eens in de 4 uur) worden verstrekt middels een daartoe door DigiNotar aangeboden methode.

5.6 Schorsing, intrekking en validatie van Certificaten

5.6.1 Schorsing en intrekking: algemeen

Onder dit CPS uitgegeven certificaten kunnen *niet* worden geschorst.

Onder schorsing van een Certificaat wordt verstaan dat het Certificaat tijdelijk buiten werking is gesteld en dat daarop tijdelijk niet kan worden vertrouwd.

Onder dit CPS uitgegeven certificaten kunnen worden ingetrokken.

[2] Conform overige CRL's die door DigiNotar via de website ter beschikking worden gesteld, is de geldigheid van de CRL 48 uur. Dit wordt weergegeven als "next update".

Onder Intrekking van een Certificaat wordt verstaan dat het Certificaat permanent buiten werking is gesteld en dat daarop niet meer kan worden vertrouwd.

5.6.2 Verzoek tot intrekking: algemeen

Aan de Certificaathouder wordt een bij het Certificaat behorende Revocation Passphrase ter beschikking gesteld.

Met behulp van deze Revocation Passphrase kan zelfstandig een verzoek tot intrekking worden gedaan met betrekking tot het aan hem verstrekte Certificaat.

Hiertoe dient het betreffende formulier op de DigiNotar website te worden ingevuld. Op dit verzoek worden geen nadere controles uitgevoerd. Certificaathouder is gehouden de Revocation Passphrase strikt persoonlijk te behandelen, met dien verstande dat indien Certificaathouder en Abonnee niet dezelfde zijn en Abonnee het Certificaat voor Certificaathouder heeft aangevraagd, Abonnee het recht heeft van Certificaathouder een kopie van de Revocation Passphrase te ontvangen voor zover hij niet reeds in het bezit daarvan is.

De revocation management services waarbij gebruik gemaakt wordt van het met het Certificaat meegeleverde Revocation Passphrase zijn 24 uur per dag beschikbaar, 7 dagen per week. De intrekking wordt, behoudens het gestelde in de volgende volzin, binnen een uur op de website van DigiNotar gepubliceerd tenzij het websiteformulier ten behoeve van de intrekking om enigerlei reden niet beschikbaar is, in welk geval de intrekking maximaal 4 uur na het intrekkingsverzoek op de website van DigiNotar zal worden gepubliceerd. In geval van systeemdefecten, service-activiteiten, of andere factoren die buiten het bereik van DigiNotar liggen, zal DigiNotar al het mogelijke doen om ervoor te zorgen dat deze dienst niet langer niet beschikbaar is dan vier (4) uur.

De overige revocation management services zijn beschikbaar op werkdagen van 09.00 uur tot 16.30 uur Nederlandse tijd.

Een intrekkingsverzoek dat niet op bovenstaande wijze wordt gedaan, dient gemotiveerd schriftelijk, per telefax of via e-mail getekend op basis van een door de RA als voldoende betrouwbaar geachte handtekening c.q. geldig Certificaat van de tot intrekking bevoegde persoon te worden gedaan en kan worden gericht aan DigiNotar of de RA.

Indien het verzoek wordt gedaan aan DigiNotar zal laatstgenoemde het verzoek onmiddellijk ter hand stellen van een RA ten einde het verzoek te behandelen.

In geval van een schriftelijk of middels telefax gedaan verzoek dient bij het verzoek een kopie legitimatiebewijs van de verzoeker gevoegd te worden en indien van toepassing een bewijs van vertegenwoordigingsbevoegdheid. Tevens dienen bij ieder verzoek tot intrekking dat wordt gedaan, anders dan met

behulp van de Revocation Passphrase te worden overgelegd alle bescheiden welke noodzakelijk zijn om het verzoek te kunnen beoordelen. Een verzoek tot intrekking kan eerst in behandeling worden genomen zodra alle noodzakelijke bescheiden bij de RA zijn aangeleverd.

De RA heeft te allen tijde de bevoegdheid nadere bewijzen ter adstructie van het verzoek te vragen.

De RA honoreert het verzoek tot intrekking niet, indien naar zijn uitsluitend oordeel de verrichte controles niet het gewenste resultaat hebben opgeleverd. Van dit laatste wordt met bekwame spoed mededeling gedaan aan de indiener van het verzoek en aan de Certificaathouder.

Van een te honoreren verzoek tot intrekking geeft de RA onmiddellijk kennis aan de CA met het verzoek met bekwame spoed, van de intrekking melding te maken op de DigiNotar CRL.

Een compleet verzoek tot intrekking, van een RA anders dan op basis van de Revocation Passphrase, zal door de CA uitsluitend op Werkdagen tijdens kantooruren binnen maximaal drie uur na ontvangst van het complete verzoek en alle benodigde aanvullende documenten worden verwerkt en vervolgens binnen één uur op de DigiNotar website worden gepubliceerd. Op werkdagen na 15.00 uur Nederlandse tijd of buiten kantooruren of Werkdagen ontvangen verzoeken tot intrekking van een Certificaat worden geacht bij aanvang van de eerst daarop volgende Werkdag te zijn ontvangen.

Van de intrekking van een Certificaat zal aan de Certificaathouder en voor zover van toepassing de Abonnee terstond mededeling worden gedaan middels een schriftelijke of elektronische mededeling.

Deze mededeling zal geschieden aan het laatste bij DigiNotar bekende adres of e-mail adres.

Voor intrekking op andere wijze dan met gebruikmaking van de Revocation Passphrase kunnen kosten in rekening worden gebracht.

5.6.3 Tot (het doen) intrekken bevoegden

De Abonnee alsmede de in het Certificaat genoemde Certificaathouder zijn te allen tijde bevoegd een verzoek tot intrekking te doen ten aanzien van een op zijn verzoek casu quo ten behoeve van hem afgegeven Certificaat. Aan een verzoek tot intrekking door de Abonnee of Certificaathouder wordt gelijkgesteld het verzoek door een daartoe gevolmachtigde van de Abonnee of Certificaathouder dan wel een erfgenaam van de betreffende persoon of de persoon die op andere wijze krachtens de Wet de certificaathouder of Abonnee vertegenwoordigt zoals bijvoorbeeld een curator of bewindvoerder.

Een Certificaat kan worden ingetrokken conform de in artikel 5.7.5. van het CPS genoemde gronden.

Tevens zijn bevoegd tot intrekking:

- DigiNotar en de RA;
- DigiNotar en/of de RA namens de Abonnee en/of Certificaathouder.

5.6.4 Verplichting tot intrekking: Abonnee, Certificaathouder, RA

De Abonnee of de Certificaathouder is in ieder geval verplicht een verzoek tot intrekking te doen conform dit CPS, indien:

a) de gegevens in het Certificaat dienen te worden gewijzigd op grond van onvolledigheid, onjuistheid of verandering van omstandigheden;

b) een Private sleutel en/of de benodigde toegangscode tot de Private sleutel verloren is gegaan, ter kennis is gekomen van een onbevoegde of de Elektronische handtekening anderszins onvoldoende waarborgen meer biedt voor de beveiliging van het door hem te verrichten elektronische berichtenverkeer.

Het behoort tot de verantwoordelijkheid van de Abonnee om de door hem aangewezen Certificaathouders te verplichten een omstandigheid als hierboven genoemd onverwijld aan hem te melden.

Een RA is verplicht om een Certificaat in te trekken indien hem mededeling is gedaan van het overlijden van een Certificaathouder en daarbij afdoende bewijsstukken zijn overlegd.

Indien niet tot intrekking bevoegde personen omstandigheden die tot intrekking zouden kunnen leiden melden aan de CA of RA, kan de CA of RA een onderzoek naar de omstandigheid instellen. De melding kan leiden tot een intrekkingsverzoek door de CA.

Overigens is noch de RA noch de CA tot intrekking op eigen initiatief verplicht.

5.6.5 Gronden (verzoek tot) schorsing of intrekking: RA, CA

De RA is verplicht om op eerste verzoek van Abonnee een door hem afgegeven Certificaat in te doen trekken indien de met Abonnee gesloten overeenkomst eindigt vóórdat de in het Certificaat vermelde geldigheidsduur is verstreken.

De RA is gerechtigd in de volgende gevallen een verzoek tot intrekking te doen en/of de met de Abonnee gesloten overeenkomst buiten rechte geheel of gedeeltelijk te ontbinden:

a) indien de Abonnee of de Certificaathouder onjuiste of onvolledige informatie heeft verstrekt over zijn identiteit of bevoegdheden;

b) indien het een Certificaat betreft waarvan de inhoud niet (meer) strookt met de gegevens die zijn ingeschreven in een Erkend Register

c) indien van toepassing indien dit wordt verzocht door de houder van het Erkend Register;

d) indien het bevoegd gezag, op grond van een wettelijk voorschrift dan wel rechterlijke uitspraak, toegang krijgt tot een eventueel in escrow gegeven encryptiesleutel van Certificaathouder;

e) indien de Abonnee zonder toestemming van de RA zijn rechten en verplichtingen uit de met de RA gesloten overeenkomst overdraagt aan een derde;

f) indien de Abonnee of Certificaathouder tekortschiet in de nakoming van enige op hem rustende verplichting uit hoofde van het CP, dit CPS of van met Abonnee en/of Certificaathouder gemaakte contractuele afspraken;

g) indien de Abonnee of Certificaathouder anderszins zodanig handelt dat het zorgvuldig gebruik van het Certificaat naar het oordeel van de RA niet langer gewaarborgd is;

h) indien DigiNotar haar werkzaamheden als CSP beëindigt, zulks met inachtneming van de bepalingen van het CP, de Wet en Europese Richtlijn;

i) indien er op grond van technische overwegingen geen sprake meer is van voldoende veiligheid;

j) indien de met Abonnee gesloten overeenkomst eindigt vóórdat de in het Certificaat vermelde geldigheidsduur is verstreken.

Iedere voor het uitgeven van gekwalificeerde certificaten toegelaten RA, alsmede de CA is tot intrekking als bedoeld in dit artikel bevoegd, met uitzondering van de gevallen sub e. en j. waarvoor uitsluitend de RA die de overeenkomst heeft gesloten en de CA bevoegd zijn..

De reden van intrekking wordt door de RA vastgelegd en gearchiveerd voor tenminste 7 jaar.

5.6.6 Intrekking Certificaten, externe werking

Een Certificaat wordt geacht te zijn ingetrokken zodra de intrekking op de DigiNotar website is gepubliceerd. De intrekking heeft eerst vanaf dat moment externe werking.

Een ingetrokken Certificaat kan niet worden hersteld.

5.6.7 Beëindigen gebruik na intrekking

De Certificaathouder is gehouden na intrekking van een Certificaat het gebruik ervan tezamen met het eraan verbonden Sleutelpaar te staken. Handelt de Certificaathouder in strijd met dit verbod dan zal de RA de Abonnee en/of de Certificaathouder kunnen bevestigen dat deze in gebreke is en hem sommeren zich te onthouden van een verdere schending van het verbod. Geeft de Abonnee en/of de Certificaathouder geen gevolg aan deze sommatie dan verbeurt hij een direct opeisbare boete per overtreding, gelijk aan tienmaal de DigiNotar adviesprijs verbonden aan de afgifte van het soort Certificaat dat is ingetrokken, zulks onverminderd het recht van de RA om volledige vergoeding te vorderen van de ten gevolge van de overtreding geleden schade.

5.6.8 CRL-uitgiftefrequentie

Revocation status information is 24 uur per dag, 7 dagen per week via de website beschikbaar. In geval van systeemdefecten, service-activiteiten, of andere factoren die buiten het bereik van DigiNotar liggen, zal DigiNotar al het mogelijke te doen om ervoor te zorgen dat deze informatie niet langer niet beschikbaar is dan 4 uur.

De Revocation status informatie wordt tenminste ieder half uur ververst.

5.7 Archivering van documenten

DigiNotar casu quo de betreffende RA zullen alle registratie-informatie vastleggen, met inbegrip van het volgende:

- het type document dat door de aanvrager wordt overlegd ten behoeve van de registratie;
- unieke identificatiegegevens, getallen of een combinatie hiervan, van de identiteitsbewijzen, indien van toepassing;
- de opslaglocatie van kopieën van aanvragen en identiteitsbewijzen, met inbegrip van de ondertekende overeenkomst met de Abonnee;
- alle specifieke keuzes in de overeenkomst met de Abonnee (bijvoorbeeld toestemming tot publicatie van het Certificaat);
- identiteit van de entiteit die de aanvraag accepteert;
- de methode die is gebruikt voor het valideren van de identiteitsbewijzen, indien van toepassing;

- de naam van de ontvangende CA en/of toeleverende RA, indien van toepassing.

DigiNotar casu quo de betreffende RA garanderen ieder voor zover het ieder aangaat en onverminderd het overigens in dit CPS gestelde omtrent aansprakelijkheid, dat de records met betrekking tot certificaten minimaal bewaard blijven gedurende een periode van 7 jaar na het einde van de geldigheidsduur van het betreffende Certificaat.

Door het aangaan van de overeenkomst en/of het feitelijk in gebruik nemen van het Certificaat is de Abonnee, respectievelijk de Certificaathouder akkoord met het vorenstaande.

5.8 Calamiteiten

DigiNotar staat er voor in dat in geval van een calamiteit waarbij is inbegrepen de aantasting van de Private sleutel van DigiNotar waarmee certificaten worden ondertekend, de activiteiten zo snel mogelijk weer doorgang vinden.

DigiNotar heeft daartoe een bedrijfscontinuïteitsplan (of calamiteitenplan).

In het geval van aantasting van de Private sleutel van DigiNotar waarmee certificaten worden ondertekend, zal DigiNotar minimaal het volgende doen:

- alle Abonnees en vertrouwende partijen en andere CSP's waarmee DigiNotar overeenkomsten heeft of andere vormen van reguliere samenwerking, over de aantasting informeren;

- aangeven dat Certificaten en Revocation status information uitgegeven met deze sleutel mogelijkerwijs niet langer geldig zijn.

5.9 Beëindiging van de dienstverlening

Indien DigiNotar de dienstverlening beëindigt maakt zij zich er sterk voor dat de door haar uitgegeven gekwalificeerde certificaten door een andere (bij de OPTA) geregistreerde dienstverlener worden overgenomen welke dienstverlener in staat is aan de verplichtingen uit het onderhavige CPS en het CP te voldoen.

Indien dit redelijkerwijs niet mogelijk is zal zij de door haar uitgegeven gekwalificeerde certificaten uiterlijk op het tijdstip dat de dienstverlening wordt beëindigd intrekken en de Certificaathouders daarvan in kennis stellen.

De Revocation status information zal, indien de Certificaten niet worden overgenomen door een geregistreerde certificatiedienstverlener, door de Stichting Continuïteit Certificaten DigiNotar gevestigd te Beverwijk op tot dan

toe gebruikelijke wijze worden gepubliceerd tot ten minste 6 maanden nadat de dienstverlening is beëindigd.

Bij beëindiging van de dienstverlening garandeert DigiNotar dat mogelijke verstoringen voor Abonneeen en vertrouwende partijen zo minimaal mogelijk blijven.

Voordat de dienstverlening wordt beëindigd zullen minimaal:

- alle Abonnees, vertrouwende partijen en andere CSP's waarmee overeenkomsten bestaan of andere vormen van reguliere samenwerking, worden geïnformeerd;

- alle autorisaties van onderaannemers die namens DigiNotar werkzaam zijn in het proces van het uitgeven van certificaten worden beëindigd;

- voor zover nog nodig al het nodige worden ondernomen om de verplichtingen over te dragen voor het handhaven van registratie-informatie en de gearchiveerde logbestanden gedurende de periode, zoals aangegeven aan de Abonnee en vertrouwende partij, zo mogelijk aan een geregistreerde certificatendienstverlener en zo dit niet mogelijk is bij de Stichting Continuïteit Certificaten DigiNotar;

- de Private sleutels van DigiNotar worden vernietigd of buiten gebruik gesteld op een zodanige wijze dat zij niet meer kunnen worden teruggehaald of wederom in gebruik genomen.

6. Fysieke, procedurele en personele beveiliging

DigiNotar kent een orgaan van hoog niveau, dat verantwoordelijk is voor het opstellen van het informatiebeveiligingsbeleid van DigiNotar en voor het garanderen van publicatie en communicatie van dit beleid naar alle werknemers op wie dit beleid betrekking heeft.

De infrastructuur van de informatiebeveiliging, die nodig is voor het beheren van de beveiliging binnen de CSP DigiNotar, zal te allen tijde in stand worden gehouden, iedere verandering die invloed zal hebben op het beveiligingsniveau dient te worden goedgekeurd door dit DigiNotar CSP-managementorgaan.

De beheersmaatregelen gericht op beveiliging en de operationele procedures voor CSP-faciliteiten, systemen en informatiemiddelen waarmee de certificatiediensten worden geleverd, zijn gedocumenteerd, geïmplementeerd en worden onderhouden.

7. Technische beveiliging

7.1 Archivering van sleutels

7.1.1 Escrow van Private sleutel

- Escrow van het Authenticiteitcertificaat en het Handtekeningcertificaat is niet toegestaan.

- Escrow van het Vertrouwelijkheidcertificaat is toegestaan.

- De bewaarneming kan te allen tijde op verzoek van de Abonnee worden beëindigd. Een verzoek hiertoe dient schriftelijk of per elektronisch ondertekende e-mail te worden gedaan.

7.1.2 Verstrekken Private sleutel voor Encryptie

De Abonnee die de aanvraag heeft gedaan en de Certificaathouder zijn te allen tijde bevoegd om tegen betaling een kopie van de Private sleutel voor Encryptie, zoals die in kopie in bewaring is genomen, op te vragen. De RA c.q. DigiNotar zal deze kopie slechts aan de Abonnee, de Certificaathouder of hun gevolmachtigde afgeven.

De Abonnee, de Certificaathouder dan wel de gevolmachtigde dienen zich ter zake van deze aanvraag op eenzelfde wijze te legitimeren als is voorgeschreven voor de aanvraag van een Gekwalificeerd certificaat onder het onderhavige CPS.

Indien de RA casu quo DigiNotar de bij DigiNotar in bewaring genomen Private sleutel voor Encryptie op grond van enig wettelijk voorschrift of gerechtelijke uitspraak dient te verstrekken aan het bevoegd gezag, zal hij daarvan onverwijld kennis geven aan de Abonnee, tenzij dit ingevolge het betreffend voorschrift of de betreffende rechterlijke uitspraak niet is toegestaan.

7.1.3 Bewaartermijn

De Private sleutel voor Encryptie zal, tenzij anders met de Abonnee is overeengekomen, in bewaring worden genomen voor een periode van drie jaar. Aan het einde van deze periode kan de termijn, in onderling overleg en voor een alsdan te bepalen periode, worden verlengd. DigiNotar is gerechtigd om op grond van notariële of technische redenen te besluiten van verlenging van de bewaringstermijn af te zien.

8. Specificatie van onderhoud op CPS

8.1 Wijzigingsprocedure voor de CPS

8.1.1 Onderdelen die kunnen wijzigen zonder bekendmaking

Wijzigingen in deze CPS van redactionele aard of correcties van kennelijke schrijf en/of spelfouten kunnen zonder voorafgaande bekendmaking in werking treden.

8.1.2 Onderdelen die kunnen wijzigen waarbij bekendmaking verplicht is

Bij elk wijzigingsvoorstel betreffende een onderdeel of een bepaling van deze CPS dient, behoudens de in 8.1.1 genoemde gevallen, een redelijke implementatieperiode te worden opgenomen. Een wijziging van een onderdeel of een bepaling van deze CPS treedt, behoudens de in 8.1.1 genoemde gevallen, niet eerder in werking dan drie maanden na de bekendmaking van deze wijziging.

Een wijziging van een onderdeel of bepaling van deze CPS mag in afwijking van het in de vorige volzin bepaalde één maand na de bekendmaking hiervan in werking treden als de materiële gevolgen van deze wijziging gering zijn.

DigiNotar beslist zonodig of een wijziging leidt tot het toewijzen van een nieuwe OID.

8.1.3 Procedure voor het bekendmaken van wijzigingen

Wijzigingsvoorstellen die vallen onder de bepalingen van 8.1.2 worden schriftelijk en/of elektronisch aan de Abonnees medegedeeld.

8.1.4 Procedure voor het geven van commentaar

Abonnees kunnen commentaar geven op de wijzigingsvoorstellen door contact op te nemen met DigiNotar.

Hierbij geldt een reactietermijn van 45 dagen na publicatie van het wijzigingsvoorstel, voor wijzigingen met geringe materiële gevolgen geldt een reactietermijn van 15 dagen na publicatie.

DigiNotar beslist op welke wijze het commentaar verwerkt zal worden.

8.1.5 Acceptatie wijzigingen CPS

Indien een wijziging voor een Abonnee niet acceptabel is, dient deze dit schriftelijk of elektronisch via getekende mail vóór de inwerkingtreding bij DigiNotar te melden en zullen diens Certificaten worden ingetrokken.

Bij gebreke van een dergelijke melding wordt de Abonnee geacht de nieuwe voorwaarden te hebben geaccepteerd.

Intrekking om reden als gemeld in dit artikel kan niet leiden tot verval van de lopende verplichtingen tenzij DigiNotar kennelijk onredelijk heeft gehandeld.

8.1.6 Overige omstandigheden

Waar is dit hoofdstuk een beslissing dient te worden genomen door DigiNotar, gebeurt dit door de directie van DigiNotar op voordracht van het CSP-management orgaan als bedoeld in hoofdstuk 6 van dit CPS.

9. Rechten van intellectuele en industriële eigendom

De rechten van intellectuele en industriële eigendom, waaronder auteursrechten en merkenrechten, die in samenhang met de DigiNotar Certificate Services worden gebruikt, of in de DigiNotar Certificate Services zijn vervat, waaronder uitdrukkelijk valt de programmatuur voor het aanmaken en activeren van Certificaten met Sleutelparen, als ook documentatie, handboeken en vertalingen daarbij, berusten bij DigiNotar dan wel bij haar toeleveranciers. Indien de intellectuele eigendomsrechten bij een toeleverancier van de CA respectievelijk RA rusten, garandeert de CA respectievelijk RA, ieder voor zover het hem aangaat, dat hij gerechtigd is de licentie voor het gebruik van de programmatuur te verlenen onder de betreffende licentievoorwaarden.

De Abonnee casu quo de Certificaathouder verkrijgt uitsluitend de gebruiksrechten en bevoegdheden die bij deze voorwaarden of anderszins uitdrukkelijk gedurende de looptijd van deze overeenkomst worden toegekend en voor het overige zal hij de programmatuur of andere materialen niet verveelvoudigen of daarvan kopieën vervaardigen. Bij de beëindiging of ontbinding van de overeenkomst dient de Abonnee casu quo de Certificaathouder (de dragers van) de programmatuur, als ook documentatie, handboeken en vertalingen daarbij, te retourneren.

Het is de Abonnee casu quo de Certificaathouder niet toegestaan enige aanduiding omtrent auteursrechten, merken, handelsnamen of andere rechten van intellectuele of industriële eigendom uit de programmatuur, apparatuur of materialen te verwijderen of te wijzigen, daaronder begrepen aanduidingen omtrent het vertrouwelijk karakter en geheimhouding van de programmatuur.