digidentity.eu™

Certification Practice Statement
OID: 2.16.528.1.1003.1.5.8

Datum : 22 februari 2011
Versie : 1.0

Document Controle Pagina

Title	Certification Practice Statement
Creator	Marcel A. Wendt
Date	22 februari 2011
Type	Text
Format	Word
Identifier	CPS v10 Certification Practice Statement PKIo.doc
Source	N/A
Language	Dutch
Rights	Copyright "Digidentity"

Version number	1.0
Date	22 februari 2011
Modified by	Marcel A. Wendt
Comments	Definitieve uitgave

Wijzigingshistorie

Version	Date	Changed by	Changes made
1.0	22-01-11	Marcel A. Wendt	Definitieve uitgave

Distributielijst

Naam	**Bedrijf**	**Afdeling**

Inhoudsopgave

Begrippenlijst

Begrip	Definitie
Audit (EDP)	EDP audit is de onafhankelijke beoordeling van de geautomatiseerde informatievoorziening. De afkorting EDP staat voor 'Electronic Data Processing'.
AuSO	Authenticatie Service Organisatie: De partij met wie Digidentity samenwerkt voor de face-to-face controle.
Authenticatie	Controle of een persoon in kwestie inderdaad degene is voor wie hij zich uitgeeft.
Autorisatie	Het verstrekken van een of meer bevoegdheden na identificatie en authenticatie.
CA	Certification Authority. Betrouwbare entiteit die de identiteit van een gebruiker (al dan niet) bevestigt.
CP	Een schriftelijk vastgelegde verzameling regels die de toepasbaarheid van een certificaat aangeeft voor een bepaalde gemeenschap en/of toepassingsklasse met gemeenschappelijke beveiligingseisen. Met behulp van een CP kunnen eindgebruikers en vertrouwende partijen bepalen hoeveel vertrouwen zij kunnen stellen in het verband tussen de publieke sleutel en de identiteit van de houder van de publieke sleutel.
CPS	Certificate Practice Statement: een document dat de door Digidentity gevolgde procedures en getroffen maatregelen over alle aspecten van de dienstverlening beschrijft.
CRL	Certificate Revocation List: een openbare lijst van ingetrokken Certificaten.
CSP	Certification Service Provider: Een natuurlijke of rechtspersoon die certificaten afgeeft of andere diensten in verband met elektronische handtekeningen verleent (Definitie uit Wet Elektronische Handtekeningen).
DID	Een digitale representatie van een natuurlijke of rechtspersoon, welke bij Digidentity altijd uniek is.
Distinguished Name	unieke naam die aan de Certificaathouder van een Gekwalificeerd certificaat wordt toegekend,
EFQM / INK	EFQM is de European Foundation for Quality Management, eind jaren '80 opgericht door 14 grote ondernemingen. INK is het Instituut voor Nederlandse Kwaliteit. Het Instituut heeft het internationale EFQM model overgenomen. Door trainingen en ondersteunende publicaties geeft het INK in Nederland verdere bekendheid aan het model.
ETSI	European Telecom Standard Institute: een onafhankelijk instituut voor standaardisatie binnen de Telecommunicatie.
Firewall	Hard- en/of softwarematige oplossing om ongeautoriseerde toegang op een netwerk te voorkomen.
FQDN	Fully Qualified Domain Name
Identificatie	Het vaststellen van de identiteit van een persoon.
LDAP	Lightweight Directory Access Protocol: het door Digidentity onderhouden bestand waarin de door Digidentity afgegeven Certificaten zijn opgenomen.
OID	Object Identifier: een rij van getallen die op unieke wijze en permanent een object aanduidt.
OSCP	Online Status Certificate Protocol: het standaard protocol dat gebruikt wordt om Certificaten online (en realtime) te controleren.
PKI	Public Key Infrastructure: een samenstel van architectuur, techniek, organisatie, procedures en regels, gebaseerd op public key cryptografie. Het doel is het hiermee mogelijk maken van betrouwbare elektronische communicatie en betrouwbare elektronische dienstverlening.
PUK	Personal Unlock Key: een code die wordt gebruikt om cryptografische modules vrij te geven of te maken.
QCP	Qualified Certificate Policy: Een Certificate Policy die een uitwerking van de vereisten bevat die zijn omschreven in artikel 18.15, eerste en tweede lid van de Telecommunicatiewet.
RA	Registration Authority: een Registration Authority zorgt voor de verwerking van certificaataanvragen en alle daarbij behorende taken.

Begrip	Definitie
SHA-2-RSA encryptie	Signing algoritme(versleuteling/unieke afscherming) voor alle certificaten en CRL's.
SSCD	Secure Signature Creation Device. Een middel voor het aanmaken van elektronische handtekeningen dat voldoet aan de eisen gesteld in artikel 18.17, eerste lid van de Telecommunicatiewet..
TTP	Trusted Third Party: Organisatie die zich bij elektronische transacties en berichtenverkeer opwerpt als onafhankelijke derde tussen de betrokken partijen, en sleutels en certificaten afgeeft als bewijs van de authenticiteit van een transactie of bericht.
VIS	Verificatie Identificatie Systeem. VIS is een geautomatiseerd informatiesysteem dat informeert over de unieke nummers van gestolen, vermiste of anderszins ongeldig verklaarde identiteits- en reisdocumenten uit binnen- en buitenland.

1. Doel, dienstverlening en organisatie

1.1. Inleiding

De enorme toename in digitale communicatie en transacties heeft geleid tot een even zo grote vraag naar een digitale identiteit (DID). Tot op heden is er geen uniforme DID en moeten alle aanbieders van diensten zelf deze DID regelen. Gebruikers moeten daarom vele verschillende DID beheren en onthouden bij voorkeur zonder aantekening ervan met alle gevolgen van dien (kosten, verlies, onoverzichtelijkheid e.d.). Gesproken wordt in dit verband van een "digitale sleutelbos" die almaar groter wordt.

Voor het veilig communiceren en veilig doen van transacties is het cruciaal voor alle betrokkenen dat de afwezigheid van fysiek contact wordt ondervangen door een uniforme en betrouwbare digitale identiteit. Anders gezegd hoe kan de digitale identiteit worden geauthentiseerd en kan dit zo worden gedaan dat het overal het zelfde wordt toegepast zodat je weet waar je aan toe bent en dat authenticatie een voorspelbare en doodgewone stap wordt in het digitale verkeer. De dienstverlening van Digidentity geeft hiervoor de oplossing.

1.2. Organisatie

De totale dienst wordt verleend door twee gescheiden afdelingen binnen Digidentity BV, t.w. Digidentity CA en Digidentity RA.

Digidentity CA is eindverantwoordelijk voor de technische realisatie van de aangeboden en verleende services en voor haar werkzaamheden als Certification Authority. Digidentity CA geeft partijen de zekerheid over hun identiteit en bevoegdheid. Digidentity CA verzorgt onder andere de afgifte, wijziging, vernieuwing en intrekking van de certificaten. Alvorens tot deze handelingen over te gaan worden de door Digidentity RA in dit document beschreven handelingen aangaande registratie verricht.

Digidentity RA is eindverantwoordelijk voor de identiteit controle en voor haar werkzaamheden als Registration Authority (RA). Voor een aantal processtappen maakt Digidentity gebruik van onderaannemers, Digidentity is echter eindverantwoordelijk.

Digidentity heeft interne goedkeuringsprocedures en een wijziging advies raad. Deze raad geeft advies aan de directie die gewenste aanpassing goedkeurt.

1.3. Doel van dit Certification Practice Statement

Digidentity opereert volgens QCP public + SSCD, een Gekwalificeerd Certificaat Beleid (QCP) voor gekwalificeerde certificaten waarbij een veilig middel, SSCD, wordt gebruikt voor het aanmaken van elektronische handtekeningen. Hiermee maakt Digidentity mogelijk dat de afwezigheid van fysiek contact wordt ondervangen door een uniforme en betrouwbare digitale identiteit. Digitaal communiceren en digitale transacties zijn daarmee beveiligd volgens de standaard ETSI TS 101 456.

Digidentity treedt hier op, in termen van ETSI TS 101 456, als een Trusted Third Party (TTP) en verzorgt als Certificate Service Provider (CSP) de service die een Public Key Infrastructure (PKI) in de praktijk bruikbaar maakt. Digidentity opereert binnen de Europese en Nederlandse wet- en regelgeving en conformeert zich aan de Europese richtlijn elektronische handtekeningen (1999/93/EG) en de Wet- en het besluit elektronische handtekeningen en bijbehorende richtlijnen en de Wet op de identificatieplicht.

Dit document geeft een beschrijving van de activiteiten van Digidentity, de organisatie voor gekwalificeerde certificaten en is voor deze certificaten het Certification Practice Statement (CPS) van Digidentity, overeenkomstig de standaard ETSI TS 101 456.

Digidentity

Digidentity geeft certificaten uit binnen de hiërarchie van PKIoverheid met de volgende Certificate policies certificaten uit.

Domein Burger:

Authenticiteit	2.16.528.1.1003.1.2.3.1
Onweerlegbaarheid	2.16.528.1.1003.1.2.3.2
Vertrouwelijkheid	2.16.528.1.1003.1.2.3.3

MachtigingOnline

MachtigingOnline geeft certificaten uit binnen de hiërarchie van PKIoverheid met de volgende Certificate policies certificaten uit.

Domein Organisatie:

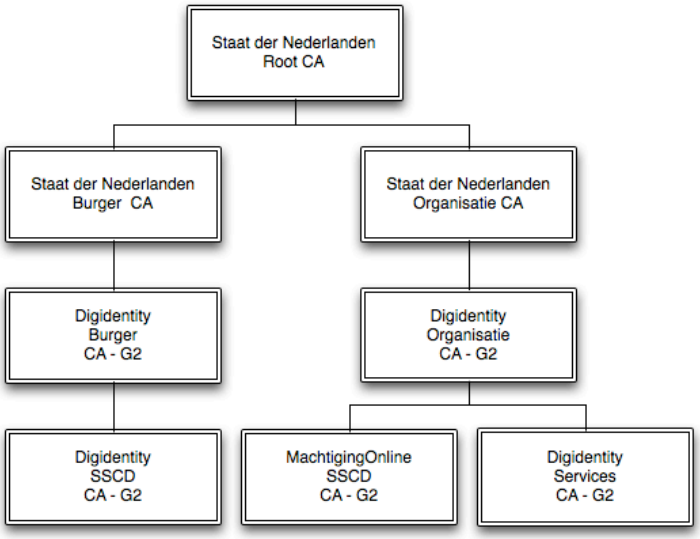
Authenticiteit	2.16.528.1.1003.1.2.5.1
Onweerlegbaarheid	2.16.528.1.1003.1.2.5.2
Vertrouwelijkheid	2.16.528.1.1003.1.2.5.3
Services - Authenticiteit	2.16.528.1.1003.1.2.5.4
Services - Vertrouwelijkheid	2.16.528.1.1003.1.2.5.5
Services - Server	2.16.528.1.1003.1.2.5.6

Certificaten vallen binnen de hiërarchie van PKIoverheid, deze certificaten zijn gelijkgesteld aan een juridisch rechtsgeldige digitale handtekening (gekwalificeerde elektronische handtekening).

Certificaten voor vertrouwelijkheid kunnen technisch worden gegenereerd maar zullen in de praktijk niet worden uitgegeven. Beroepsgebonden certificaten worden niet uitgegeven.

Voor het domein organisatie worden certificaten onder de handelsnaam machtiging online uitgegeven en certificaten binnen het domein burger onder de handelsnaam Digidentity.

Digidentity hanteert in het kort de volgende CA hiërarchie de profielen van deze CA's zijn beschikbaar in appendix A:



1.4. Beschikbaarheid en onderhoud CPS

Het CPS van Digidentity is opgesteld en wordt periodiek onderhouden door:

Digidentity BV
Postbus 19148
2500 CC Den Haag

Telefoon : +31 (0)887 78 78 78
E-mail : info@digidentity.eu
Web : www.digidentity.eu

Digidentity draagt er zorg voor dat dit CPS 24x7 beschikbaar is via de website van Digidentity behoudens het geval van systeemdefecten, serviceactiviteiten of andere factoren die buiten het bereik van Digidentity liggen. In het laatste geval maakt Digidentity zich er sterk voor dat de storing niet langer duurt dan 24 uur. Intrekkingsverzoeken kunnen te alle tijde worden ingediend en worden direct, doch uiterlijk binnen 4 uur verwerkt en op de gepubliceerde CRL geplaatst.

Tevens zal Digidentity voor alle CA onder zijn beheer de volgende CRL's publiceren en 24x7 beschikbaar stellen.

- pki.digidentity.eu/PKIoverheid/burger/latest.crl
- pki.digidentity.eu/PKIoverheid/organisatie/latest.crl
- pki.digidentity.eu/PKIoverheid/sscd-mo/latest.crl
- pki.digidentity.eu/PKIoverheid/sscd-Digidentity/latest.crl
- pki.digidentity.eu/PKIoverheid /services/latest.crl

1.5. Audit

Digidentity zal bij wijziging in beleid en procedures, maar minimaal een keer per jaar, door middel van een internationaal gestandaardiseerde zelfevaluatie (EFQM / INK) toetsen of wordt voldaan aan alle eisen zoals de standaard ETSI TS 101 456 die stelt aan een certificatiedienstverlener die gekwalificeerde diensten aanbiedt, zowel in beleidsmatig opzicht als in de operationele uitvoering. Digidentity zal in dit verband ook bij derden die betrokken zijn in de operationele uitvoering, toetsen of wordt voldaan aan alle eisen zoals de standaard ETSI TS 101 456 die stelt aan een certificatiedienstverlener die gekwalificeerde diensten aanbiedt, zowel in beleidsmatig opzicht als in de operationele uitvoering.

Een door het ministerie van EL&I aangewezen certificerende instelling, zal jaarlijks bij Digidentity, inclusief de door haar ingeschakelde derde partijen, nagaan en vaststellen of wordt voldaan aan de vereisten als gesteld in dit CPS, de wettelijke voorschriften, de bijlagen bij dit CPS, de overeenkomsten waarvan dit CPS deel kan uitmaken alsmede het beveiligingsbeleid.

1.6. Aanpassingen van het CPS

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

Bij veranderende marktvoorwaarden, veiligheidseisen, wetswijzigingen etc., behoudt Digidentity BV zich het recht voor om wijzigingen en aanpassingen in deze documentatie aan te brengen. Voorgenomen wijzigingen worden tijdig op de internetsite van Digidentity aangekondigd inclusief ingangsdatum waarop de herziende versie van dit CPS van kracht wordt. Indien van toepassing zullen ook de wijzigingen worden doorgevoerd in de algemene voorwaarden, die van toepassing zijn op de dienstverlening van Digidentity en die gepubliceerd worden via de internetsite van Digidentity.

Bij het inloggen wordt het nieuwe CPS getoond en dient deze expliciet goedgekeurd te worden door de gebruiker. Indien een gebruiker door eigen doen of nalaten geen kennis neemt of kan nemen van de gewijzigde documenten, komt dit geheel voor rekening van de gebruiker. Digidentity kan daarvoor geen aansprakelijkheid aanvaarden evenmin als voor de nadelige gevolgen die dit voor gebruiker met zich kan brengen.

Gebruikers kunnen commentaar geven op dit CPS met betrekking tot de inhoud. De bevoegdheid om al dan niet wijzigingen aan te brengen in de documentatie blijft voorbehouden aan Digidentity BV.

Veranderingen van dit CPS of het CP van PKIoverheid waarbij Digidentity verplicht is gebruikers hiervan in kennis te stellen geschiedt, door het plaatsen van een mededeling op de Digidentity website en vindt plaats ten minste 30 dagen voorafgaand aan het toepasselijk verklaren van het nieuwe CPS.

2. Registratie, identificatie en authenticatie

2.1. Wijze van aanvragen

Digidentity doet een aanbod op haar website, www.digidentity.eu. Bij de acceptatie van dit aanbod door een aankomende certificaathouder ontstaat de verplichting van Digidentity een certificaataanvraag in behandeling te nemen en een verificatie-procedure zoals in 2.3 beschreven te starten. Als de Authenticatie positief is verlopen, produceert Digidentity het gevraagde certificaat en geeft dit de certificaathouder in gebruik. Dit CPS is beschikbaar voor de gebruiker via de website van Digidentity.

2.2. Processtappen

- het registratie proces waarbij de identiteit van de aanvrager wordt opgetekend en waarbij Digidentity optreedt als Registration Authority (RA);
- het authenticatieproces waarbij de identiteit van de aanvrager wordt geverifieerd, waarbij Digidentity optreedt als Registration Authority;
- het certificaatgeneratieproces conform de eisen die ETSI TS 101 456 stelt, waarbij Digidentity optreedt als Certification Authority (CA).

2.3. Verificatie

Om de identiteit van de gebruiker vast te stellen worden de volgende gegevens van de gebruiker of abonnee vastgesteld:

a) Verificatie door Digidentity
   a. Gebruikersnaam
      - gecontroleerd wordt dat de gebruikersnaam maar één keer voorkomt;
   b. Wachtwoord
      - controle op de sterkte van het wachtwoord;
   c. e-Mail adres
      - de gebruiker ontvangt een e-mail met een verificatielink op het e-mail adres zodat na het klikken op de link het e-mail adres gecontroleerd is;
   d. Mobiele telefoonnummer
      - de gebruiker ontvangt een SMS code op het mobile telefoonnummer, deze dient in het registratieproces ingevoerd te worden;
   e. afgeleide verificatie d.m.v. € 0,01 betaling met iDeal
      - hiermee controleren we de naam en woonplaats van de gebruiker.

b) Verificatie door AuSO
   a. Achternaam
   b. Eerste voornaam met initialen
   c. Geboortedatum
   d. Geboorteplaats
   e. Postcode en huisnummer
   f. Burgerservicenummer
   g. Type identiteitsbewijs en nummer

c) Zo daartoe aanleiding bestaat wordt door VIS gecontroleerd of een aangeboden identiteitsbewijs is aangemeld als vermist of gestolen. Indien de VIS controle een zgn. HIT oplevert worden de relevante instanties geïnformeerd.

d) Face to Face controle van gebruiker.

e) Het ontvangen kopie legitimatiebewijs wordt onderzocht op eventuele fraude kenmerken.

Voor het aanvragen van een certificaat in het domein organisatie is een certificaat in het domein burger verplicht en worden door MachtigingOnline worden de volgende extra gegevens vastgesteld:

f) Verificatie organisatie middels kvk
    a. Verificatie naam;
    b. Verificatie nummer;
    c. Verificatie bestuurders;
    d. Indien een organisatie niet in het KvK is geregistreerd zou een wet, oprichtingsakte of een algemene maatregel van bestuur ook kunnen volstaan;
    e. Indien voor EV wordt het insolventie register van de internetsite van de Rechtspraak en de Hoge Raad der Nederlanden geraadpleegd.

g) Verificatie FQDN
    a. De domeinnaam wordt gecontroleerd bij erkende registers als SIDN (Stichting Internet Domeinregistratie Nederland) en IANA (Internet Assigned Numbers Authority;
    - gecontroleerd wordt of de desbetreffende domeinnaam eigendom is van de aanvragende organisatie.

h) Voor het aanvragen van een Services certificaat binnen het domein organisatie is een authenticatie certificaat binnen het domein organisatie verplicht.

2.4. Doel en soorten certificaten

Digidentity kan conform vereisten die PKIoverheid stelt vertrouwelijkheids-certificaten uitgeven. In de praktijk worden deze niet uitgeven anders dan voor server certificaten. Naast dat encryptie certificaten in beginsel niet worden uitgegeven, vindt ook geen escrow van de private key plaats. Berichten die versleuteld zijn met de private key zullen zijn verloren indien deze kwijt raakt of defect raakt. Schade die kan ontstaan uit een dergelijke situatie valt geheel onder de verantwoordelijkheid van de houder van de private key.

Daarnaast wordt door Digidentity geen beroepsgebonden certificaten uitgegeven of beroepgebonden registers geraadpleegd alvorens een certificaat uit te geven.

Tevens kan een gebruiker een SSCD creëren naast zijn bestaande SSCD met secundaire credentials en het gebruik van deze alternatieve SSCD delegeren.

2.4.1. Digidentity

Persoonsgebonden authenticiteit certificaat

OID: 2.16.528.1.1003.1.2.3.1

Het persoonsgebonden authenticiteit certificaat bevat de publieke sleutel ten behoeve van de identificatie en authenticatie van een persoon. Deze kan worden gebruikt voor het betrouwbaar identificeren en authentiseren van personen langs elektronische weg. Dit betreft zowel de identificatie van personen onderling als tussen personen en geautomatiseerde middelen. De geldigheid van het persoonsgebonden authenticatiecertificaat is vijf jaar. Bij het gekwalificeerde authenticiteit certificaat de houder zich persoonlijk gelegitimeerd bij de CA en kan zich alleen digitaal authentiseren met behulp van een beveiligd SMS bericht en een wachtwoord. Authenticiteit certificaten die onder deze CPS worden uitgegeven kunnen niet worden gebruikt voor het identificeren van personen in gevallen waarbij de wet vereist dat de identiteit van personen alleen met een in de Wet op de identificatieplicht aangewezen document mag worden vastgesteld.

Persoonsgebonden handtekeningcertificaat

OID: 2.16.528.1.1003.1.2.3.2

Het persoonsgebonden handtekeningcertificaat, bevat de publieke sleutel ten behoeve van de gekwalificeerde elektronische handtekening. Deze elektronische handtekening heeft dezelfde rechtsgevolgen als een handgeschreven handtekening, zoals aangegeven in artikel 15a, eerste en tweede lid, in Titel 1 van Boek 3 van het Burgerlijk Wetboek onder afdeling 1A en zijn gekwalificeerde certificaten zoals bedoeld in artikel 1.1, lid ss van de Telecom wet. De geldigheid van het persoonsgebonden handtekeningcertificaat is vijf jaar.

2.4.2. MachtigingOnline

Werknemersgebonden authenticiteit certificaat

OID: 2.16.528.1.1003.1.2.5.1

Het persoonsgebonden authenticiteit certificaat bevat de publieke sleutel ten behoeve van de identificatie en authenticatie van een werknemer binnen een bedrijf. Deze kan worden gebruikt voor het betrouwbaar identificeren en authentiseren van werknemers langs elektronische weg. Dit betreft zowel de identificatie van werknemers onderling als tussen werknemers en geautomatiseerde middelen. De geldigheid van het werknemersgebonden authenticatiecertificaat is vijf jaar. Authenticiteit certificaten die onder dit CPS worden uitgegeven kunnen niet worden gebruikt voor het identificeren van personen in gevallen waarbij de wet vereist dat de identiteit van personen alleen met een in de Wet op de identificatieplicht aangewezen document mag worden vastgesteld.

Werknemersgebonden handtekeningcertificaat

OID: 2.16.528.1.1003.1.2.5.2

Het werknemersgebonden handtekeningcertificaat, bevat de publieke sleutel ten behoeve van de gekwalificeerde elektronische handtekening. Deze elektronische handtekening heeft dezelfde rechtsgevolgen als een handgeschreven handtekening, zoals aangegeven in artikel 15a, eerste en tweede lid, in Titel 1 van Boek 3 van het Burgerlijk Wetboek onder afdeling 1A en zijn gekwalificeerde certificaten zoals bedoeld in artikel 1.1, lid ss van de Telecom wet. De geldigheid van het persoonsgebonden handtekeningcertificaat is vijf jaar.

2.4.3. MachtigingOnline SSL

Werknemersgebonden authenticiteit certificaat

OID: 2.16.528.1.1003.1.2.5.4
2.16.528.1.1003.1.2.5.5
2.16.528.1.1003.1.2.5.6

Onder het domein van PKIoverheid SSL certificaten

2.5. Controle certificaat door 'vertrouwende partijen'

Digidentity registreert alle gegenereerde en ingetrokken certificaten. Ingetrokken certificaten worden gepubliceerd in een CRL voor zogeheten 'relying parties' ofwel 'vertrouwende partijen' ter verificatie.

2.6. Uniciteit van namen

De Distinguished Name (unieke naam) die aan de Certificaathouder van een Gekwalificeerd certificaat voor een CA van Digidentity waarop dit CPS van toepassing is, wordt toegekend, zal te alle tijde uniek zijn voor deze Certificaathouder en niet worden uitgegeven aan een andere Certificaathouder. Pseudoniemen zijn nimmer toegestaan.

a) de schrijfwijze van een Persoonsnaam moet met de schrijfwijze in het legitimatiebewijs overeenkomen en mag niet met leestekens, bijvoorbeeld trema's, gewijzigd zijn.

b) indien dezelfde naam vaker voorkomt, wordt met Subject.serialNumber, een numeriek achtervoegsel, het onderscheid kenbaar gemaakt.

In gevallen waarin partijen het oneens zijn over het gebruik van de opgenomen namen in het certificaat welke de certificaathouder identificeren, beslist uitsluitend Digidentity BV na afweging van de betrokken belangen, voor zover hierin niet wordt voorzien door dwingend Nederlands recht of overige toepasselijke regelgeving.

2.7. Certificaathouder

Een certificaathouder is 'subject' van een certificaat, een entiteit gekenmerkt als de houder van de private sleutel die is verbonden met de publieke sleutel die in het certificaat is opgenomen. Een certificaathouder kan zich, binnen de grenzen van de toepasselijke regelgeving, met behulp van de Digidentity certificaten identificeren en authentiseren.

Een natuurlijk persoon die certificaathouder is, is in de praktijk bij Digidentity tevens de gebruiker. Als zodanig is hij/zij contractpartij van Digidentity en verkrijgt, middels de voorgeschreven controles en procedures, het recht zijn/haar certificaat samen met het sleutelpaar conform dit CPS te gebruiken. Bij een MachtigingOnline certificaat is de organisatie de certifcaathouder en de natuurlijke persoon de gebruiker.

Een natuurlijk persoon kan ook een secundairy credential voor een certificaat aanmaken en te alle tijde weer intrekken. In dat geval kan het sleutelgebruik expliciet gedelegeerd worden. Per secundairy credential wordt een aparte SSCD gecreëerd. Deze SSCD wordt dan alleen nog maar voor het doel gebruikt. Een SSCD met secundairy credential is voor persoonlijk gebruik, de gebruiker is vrij in de toepassing er van. Een SSCD met secundairy credential kan ook worden gedelegeerd, de SSCD wordt dan alleen voor de gedelegeerde doeleinden gebruikt.

3. Verplichtingen

3.1. Verplichtingen van Digidentity

Alle, in het kader van dit CPS en de overeenkomsten waarvan dit CPS deel kan uitmaken, door Digidentity verrichte werkzaamheden worden voortvarend met inachtneming van de van toepassing zijnde procedures en conform de van toepassing zijnde wet- en regelgeving uitgevoerd. Digidentity conformeert zich tevens aan de genoemde CPS van de PKIoverheid.

Digidentity zal, in het kader van haar TTP dienstverlening, haar apparatuur, programmatuur, telecommunicatiefaciliteiten, systeembeheer en procedures inrichten volgens de richtlijnen van ETSI TS 101 456 en de Richtlijn nr. 1999/93/EG.

Digidentity opereert binnen de Europese en Nederlandse wet- en regelgeving en conformeert zich aan Europese richtlijn elektronische handtekeningen (1999/93/EG) en de Wet en besluit elektronische handtekeningen en bijbehorende richtlijnen en Wet op de identificatieplicht.

Digidentity zal, waar zij als onderdeel van haar dienstverlening, een AuSO als derde partij inschakelt, er op toezien dat ook zij haar TTP dienstverlening, haar apparatuur, programmatuur, telecommunicatiefaciliteiten, systeembeheer en procedures inricht volgens de richtlijnen van ETSI TS 101 456 en de Richtlijn nr. 1999/93/EG. In het kader van de identificatie zal Digidentity persoonsgegevens uitwisselen met haar onderaannemers om de identificatie te kunnen volbrengen. Digidentity en haar onderaannemers nemen bij opname, verwerking en archivering van persoonsgegevens de relevante wet- en regelgeving stipt in acht.

Digidentity zal zich jaarlijks laten beoordelen door een certificerende instelling die kan aantonen dat Digidentity en de door haar ingeschakelde entiteiten voldoen aan de genoemde eisen.

Digidentity is verantwoordelijk voor het niveau en kwaliteit van de beschikbaar gestelde middelen. De conformiteit aan de gestelde eisen wordt aangetoond middels de certificering.

Digidentity is verantwoordelijk voor de keuze van de gebruikte systemen en apparatuur en vrijwaart de abonnee of burger voor schendingen van het intellectueel eigendom door CPS.

3.2. Certificaat hiërarchie

De Certificaten worden niet onmiddellijk door het Nederlandse stamcertificaat getekend. De Public Key Infrastructuur van Nederland is geïmplementeerd in een 'four-level certification hierarchy'.

Op het hoogste niveau tekent het Nederlandse stamcertificaat, 'Staat der Nederlanden Root CA – G2' het Staat der Nederlanden Domein (Organisatie of Burger) CA. Dit CA certificaat tekent vervolgens het Digidentity CA certificaat. Met dit Certificaat tekent Digidentity CA de Certificaten van haar gebruikers. 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 van PKIoverheid.

De basis is het volgende nummer dat door het Normaliseringinstituut aan Digidentity is toegekend. Het OID is als volgt opgebouwd:

Categorie	Nummer
JOINT-ISO-ITU-IT	2
Country	16
Netherlands	528
Organisation	1
Overheid	1003
PKIoverheid	1
CSP	3
Domein Organisatie	3 5
Digidentity	2 in domein burger 8 in domein organisatie

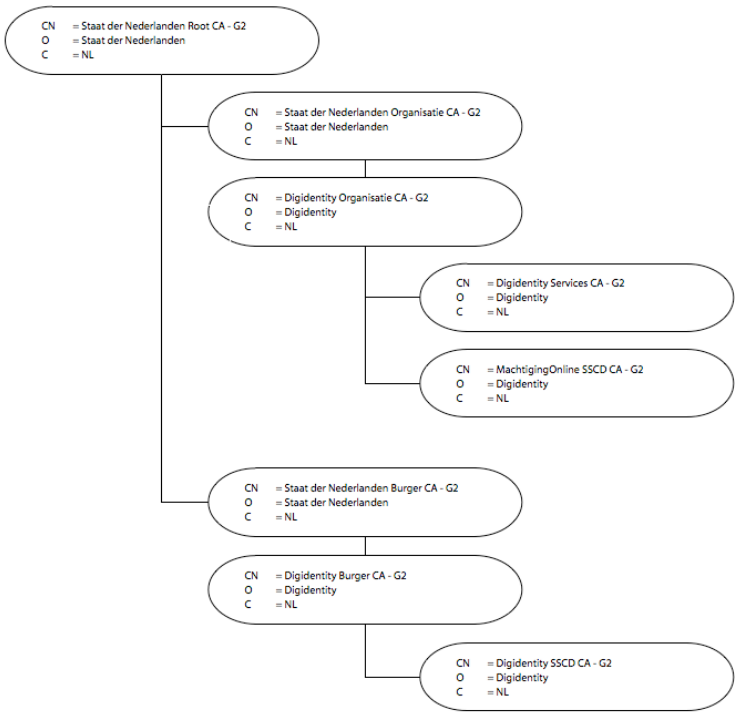
Dus:

2.16.528.1.1003.1.3.5.8 voor het domein organisatie

en

2.16.528.1.1003.1.3.3.2 voor het domein burger

Hiërarchie Digidentity



3.3. Verplichtingen van de gebruiker en abonnee

Juistheid van gegevens en veilig gebruik

De gebruiker staat ervoor in dat:

a) de gegevens zoals overgenomen van het Identiteitsbewijs in het Certificaat te alle tijde juist en volledig zijn;
b) bij wijzigingen in de gegevens deze wijziging zo spoedig mogelijk wordt verwerkt door de informatie in het account aan te passen;
c) het Certificaat wordt gebruikt in overeenstemming met de toepasselijke wettelijke en andere regelgeving (zoals privacywetgeving, het Burgerlijk Wetboek, Telecommunicatie wetgeving e.d.);
d) het Certificaat gebruikt wordt overeenkomstig het bepaalde in dit CPS en de overeenkomsten waarvan dit CPS deel kan uitmaken en die met dit CPS verband houden;
e) het in dit CPS, en in de contractuele afspraken waarvan dit CPS deel kan uitmaken, bepaalde deugdelijk door de certificaathouder(s) wordt nageleefd;
f) er redelijke zorg uitgeoefend wordt tegen onbevoegd gebruik van zijn of haar prive-sleutel;
g) de CA in kennis gesteld wordt zonder enige vertraging, als een van de volgende events optreden tot het einde van de geldigheidsduur van het certificaat:
    a. van de abonnee de privé-sleutel is verloren en/of gestolen, of
    b. de controle over de abonnees private sleutel verloren is gegaan door compromittering van de activering gegevens (bv. gebruikersnaam /wachtwoord of PUK brief), en / of
    c. onjuistheid of wijzigingen in de inhoud van het certificaat, zoals gemeld aan de abonnee;
h) gebruiker delegeert alleen een SSCD aan organisaties die additionele maatregelen nemen zodat SSCDs met secundairy credentials alleen voor het doel waarvoor zij zijn gedelegeerd worden ingezet, bijv. Mass-Signing. De gebruiker dient een separate SSCD aan te vragen voor het doel Mass-Signing. Dit certificaat is expliciet bedoeld voor Mass-Signing en kan te alle tijde door de gebruiker in de Digidentity omgeving worden ingetrokken. De gebruiker blijft eindverantwoordelijk voor het zorgvuldig omgaan met zijn certificaat.

De gebruiker betracht goed huisvaderschap omtrent de keuze en (fysieke) beveiliging van zijn programmatuur, apparatuur en telecommunicatie faciliteiten en is alsmede zelf verantwoordelijk voor de beschikbaarheid van zijn informatie- en communicatie-systemen, waarmee hij het elektronische berichten verkeer tot stand brengt. De gebruiker zal adequate maatregelen nemen ter bescherming van zijn systeem tegen virussen en andere programmatuur oneigenlijke elementen.

De abonnee staat er voor dat:

a) zo spoedig mogelijk na beëindiging van het dienstverband het certificaat wordt ingetrokken;
b) machtigingen conform verleende bevoegdheden worden uitgereikt en tijdig worden ingetrokken;
c) de apparatuur waar de private sleutel voor ssl certificaten wordt gegenereerd en gebruikt adequaat de toegang tot de private sleutel afschermt, conform PKIoverheid richtlijnen en vereisten;
d) voor alle aanvragen voor ssl certificaten de domeinen en merken in eigendom zijn of dat hiervan gebruiksrecht wordt genoten, en dat op aanvraag hiervoor de bewijzen ter beschikking kunnen worden gesteld;
e) hij additionele maatregelen neemt zodat SSCDs met secundairy credentials alleen voor het doel waarvoor zij zijn gedelegeerd worden ingezet.

Beperkingen in het gebruik

De gebruiker zal zich houden aan de toepasselijke Nederlandse, Europese en overige (inter)nationale wet- en regelgeving en de bepalingen van dit CPS met betrekking tot het doel waarvoor hij het Certificaat wenst te gebruiken, de keuze van de wederpartij met wie hij elektronische berichten en/of transacties uitwisselt en meer in het bijzonder de inhoud van het berichten- en/of transactieverkeer dat hij met gebruikmaking van het Certificaat wenst te verrichten waaronder, voor zover van toepassing, de door hem gesloten overeenkomsten met andere Partijen en de eventuele uitvoering daarvan. Het is de gebruiker en de Certificaathouder(s) verboden om het Certificaat te gebruiken buiten de door het CP, dit CPS of in het Certificaat aangegeven doeleinden.

Overschrijdingen

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

Eigendomsrecht van het Certificaat

Het Certificaat blijft te alle tijde eigendom van Digidentity BV. De gebruiker verkrijgt slechts het recht het Certificaat tezamen met het sleutelpaar te gebruiken conform het bepaalde in dit CPS.

3.4. Verplichtingen van de vertrouwende partijen

Een vertrouwende partij is iedere natuurlijke of rechtspersoon die handelt in vertrouwen op een ontvangen certificaat. Een vertrouwende partij zal het Certificaat uitsluitend vertrouwen indien:

a) de geldigheid zoals deze blijkt uit het certificaat is geverifieerd;

b) de volledige keten van certificaten tot aan het stamcertificaat van de Staat der Nederlanden geldig is;

c) het Certificaat niet is ingetrokken;

d) kennis genomen is van de beperkingen betreffende het gebruik van het Certificaat zoals vermeld in dit CPS;

e) bij het raadplegen van de Certificaat statusinformatie, de authenticiteit van deze informatie is geverifieerd door de elektronische handtekening waarmee de informatie is getekend en het bijbehorende certificatie-pad te controleren.

3.5. Aansprakelijkheid

In het kader van de afgifte van Gekwalificeerde certificaten stelt Digidentity zich aansprakelijk conform de eisen van de richtlijn Elektronische handtekeningen, 1999/93/EG. Tevens zijn de Nederlandse wetgeving (WEH) en het PvE van PKIoverheid van toepassing. Dit houdt in dat Digidentity aansprakelijk kan zijn voor schade die natuurlijke of rechtspersonen ondervinden terwijl zij in redelijkheid op dit Certificaat mochten vertrouwen, in samenhang met:

a) 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 dergelijke Certificaat voorgeschreven gegevens;

b) 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;

c) de garantie dat de gegevens voor het aanmaken van de handtekening en die voor het verifiëren van de handtekening complementair kunnen worden gebruikt.

Een en ander tenzij Digidentity bewijst dat zij niet nalatig heeft gehandeld en voorts aantoont dat de gebruiker niet voldaan heeft aan het bepaalde in artikel 3.3 van dit CPS. Digidentity is voor deze aansprakelijkheid verzekerd.

3.6. Financiële verantwoordelijkheid en aansprakelijkheid

Voor zover niet expliciet anders overeengekomen, stelt Digidentity geen beperkingen aan de waarde van de transacties waarvoor gekwalificeerde certificatenkunnen worden gebruikt.

Behoudens voor zover Digidentity aantoont dat zij niet aansprakelijk kan worden gehouden en voorts behoudens het overigens in dit CPS gestelde, aanvaardt Digidentity aansprakelijkheid voor zowel directe als indirecte schade per schadeveroorzakende gebeurtenis of serie van schadeveroorzakende gebeurtenissen tot een bedrag van maximaal een miljoen euro. Het vorenstaande laat onverlet de mogelijkheden tot verhaal op degene aan wie de schade toe te rekenen valt.

3.7. Vertrouwelijkheid

De informatie, die Certificaathouders aan Digidentity verstrekken, zal niet zonder de toestemming van de eindgebruiker dan wel ingeval van 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.

Indien en voor zover van toepassing draagt Digidentity er zorg voor dat de vereisten van de geldende privacy wet- en regelgeving worden nageleefd. De activiteiten en administratie van Digidentity zijn aangemeld bij het College Bescherming Persoonsgegevens onder nummer m1451668.

3.8. Handhaving

Op de website van Digidentity wordt de klachtenprocedure gepubliceerd.
In geval van klachten betreffende diensten geleverd in het kader van dit CPS kan de klacht via deze website ingediend worden bij Digidentity. Dit zal de Digidentity klachtenprocedure in werking stellen.

Geschillen kunnen worden voorgelegd aan de gewone rechter in het arrondissement waar Digidentity BV is gevestigd. Alle overeenkomsten tussen de gebruiker Digidentity vallen onder het Nederlands recht.

3.9. Beëindiging van de service

De certificatiedienstverlening activiteiten van Digidentity kunnen, met in achtneming van de wettelijke bepalingen, eenzijdig door Digidentity BV worden stopgezet. Een voorgenomen stopzetting wordt tenminste 2 maanden vóór de stopzetting, aan zowel de OPTA, Logius, alsmede aan alle betrokkenen medegedeeld. Bij het stopzetten van de certificatiedienstverlening activiteiten zal de CRL nog tot 6 maanden na stopzetting van de activiteiten raadpleegbaar blijven voor relying parties.

Indien Digidentity 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. Ingeval de activiteiten niet door een andere certificatiedienstverlener worden overgenomen, worden alle uitgegeven certificaten geblokkeerd.

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

De CRL en de archieven worden tot 7 jaar na het vervallen van het laatste certificaat beschikbaar gehouden. Digidentity heeft hiervoor te alle tijde voldoende financiële middelen veiliggesteld om na beëindiging van de dienstverlening aan deze verplichting te voldoen. Deze zekerheid wordt verkregen hetzij door deze contractuele verplichting aan een derde partij over te dragen dan wel via een garantie verklaring van een derde die deze verplichting afdekt.

4. Operationeel management

4.1. Certificaatmanagement

Uitgifte van certificaten

Na acceptatie van de aanvraag wordt een certificaat geproduceerd door de Certification Authority (CA) van Digidentity. Dit certificaat is in een SAAS (Signing as a Service) model beschikbaar. De Private Key van de gebruiker blijft veilig bewaard op de Digidentity servers en kan op afstand vrijgegeven worden voor een authenticatie, onweerlegbaarheid.

Onmiddellijk na het aanmaken van het Certificaat, staat het Certificaat ter beschikking van de gebruiker. De CA zal het Certificaat publiceren in de interne certificatendatabank van Digidentity en is beschikbaar voor de gebruiker in zijn Digidentity kluis. De gebruiker draagt zelf zorg voor publicatie en verspreiding van zijn certificaat.

Na het eerste gebruik van de opgegeven gebruikersnaam en wachtwoord krijgt de gebruiker toegang tot zijn sleutelparen om authenticatie, onweerlegbaarheid uit te voeren. De private keys zijn alleen in de HSM operationeel en zijn alleen na expliciete toestemming van de gebruiker instaat om een operatie uit te voeren. Toestemming wordt verleend door invoer van de ontvangen geheime eenmalig gegenereerde code. Op deze manier is het gegarandeerd dat het gebruik van de private sleutel alleen ter beschikking wordt gesteld aan geautoriseerde personen.

Aanvaarding

Het Certificaat wordt geacht door de gebruiker te zijn aanvaard op het tijdstip van afgifte. Het certificaat wordt op het scherm getoond en gebruiker kan na controle de correctheid van de inhoud bevestigen. Slechts na bevestiging van de inhoud komt het certificaat beschikbaar voor gebruik.

De gebruiker tevens Certificaathouder is gehouden om, alvorens het Certificaat in gebruik te nemen, de daarin opgenomen gegevens op juistheid te controleren.
Onjuistheden in een Certificaat die niet is ingetrokken, komen voor rekening en risico van de gebruiker. De gebruiker is gehouden onjuistheden onverwijld, maar in ieder geval op de 3^{e} dag na ontvangst van het Certificaat, aan Digidentity te melden, bij gebreke waarvan Digidentity nimmer aansprakelijk kan worden gehouden voor zulke tekortkomingen.

De gebruiker dient zich er bewust van te zijn dat het Certificaat alleen gebruikt kan worden voor het zetten van een elektronische handtekening en authenticatie al naar gelang het type zulks met inachtneming van de overige beperkingen die aan de gebruiker zijn kenbaar gemaakt.

Geldigheidsduur

De geldigheidsduur van een certificaat wordt in het certificaat zelf aangegeven. De certificaathouder is verantwoordelijk voor het tijdig aanvragen van nieuwe respectievelijk vervangende certificaten. Digidentity stelt zijn gebruikers tijdig op de hoogte zodra de vervaldatum nadert. De geldigheid van eindgebruikers certificaten welke worden uitgegeven door Digidentity is 5 jaar vanaf het moment van uitgifte of tot maximaal de geldigheid van de certificaat van de uitgevende CA.

Wijziging en vernieuwing

Een verzoek tot vernieuwing van een Certificaat moet worden gedaan door de gebruiker. Dit resulteert te alle tijde in een nieuw sleutelpaar nadat alle gegevens zijn vergeleken met het oude certificaat. Het verzoek kan alleen elektronisch met het oude nog geldige certificaat worden gedaan voor hetzelfde domein en/of organisatie op hetzelfde niveau. Indien het certificaat is ingetrokken of verlopen dan dient de registratie procedure in zijn geheel en opnieuw doorlopen te worden.

Validatie van ingetrokken Certificaten

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 middel de gepubliceerde CRL.

Schorsing en intrekking van Certificaten

Onder dit CPS uitgegeven certificaten kunnen niet worden geschorst.

Onder dit CPS uitgegeven certificaten kunnen worden ingetrokken. Onder intrekking van een Certificaat wordt verstaan dat het Certificaat permanent buiten werking is gesteld en dat daarop niet meer kan worden vertrouwd.

Intrekking van een Certificaat dient via de Digidentity website door een bevoegd persoon te worden aangevraagd. De gebruiker kan na inloggen te alle tijde zijn middel en daarmee zijn certificaten intrekken. Als alternatief kan de gebruiker telefonisch zijn kluis deactiveren met behulp van de ter beschikking gestelde PUK en PIN code bij activatie. Een kluis kan ook weer actief worden gemaakt nadat de registratie procedure in zijn geheel en opnieuw is doorlopen. Echter, het middel en de certificaten zijn dan reeds ingetrokken en moeten opnieuw worden aangevraagd. De certificaathouder ontvangt een bevestiging per e-mail over de status wijziging.

Wanneer men niet meer beschikt over een PUK en/of telefoon en wachtwoord kan intrekking van een certificaat ook aangevraagd worden op het hoofdkantoor van Digidentity. De eigenaar van het certificaat dient zich dan met een geldig identiteitsbewijs te legitimeren. Tijdens dit intrekkingsverzoek zal een Digidentity medewerker de reden van intrekking vastleggen. Als alternatief kan men ook zijn identiteitsbewijs e-mailen onder vermelding van zijn gebruikersnaam.

Omstandigheden die leiden tot intrekking

De volgende omstandigheden leiden tot intrekking van een Certificaat:

a) Wettelijk voorschrift;
b) Verlies of mogelijke diefstal van de PUK code;
c) Verlies of mogelijke diefstal van de mobiele telefoon;
d) Verlies of mogelijke diefstal van de SIM kaart;
e) Het certificaat is niet meer correct, de kwalificaties/gegevens zijn niet meer juist;
f) compromittering van de private key.

Intrekkingsbevoegdheid

De intrekking van een Certificaat kan worden gelast door:

a) de gebruiker of zijn wettelijke vertegenwoordiger;
b) een door de certificaathouder vertegenwoordigde derde waarvan de vertegenwoordiging blijkt uit een afgegeven machtiging in machtiging online;
c) de abonnee;
d) Digidentity BV.

Digidentity RA is verplicht om een Certificaat in te trekken indien mededeling is gedaan van overlijden van de gebruiker en/of Certificaathouder en daarbij afdoende bewijsstukken zijn overlegd.

Indien een daartoe bevoegde medewerker van Digidentity B.V. de intrekking verzorgt dient hij of zij hierbij de reden van intrekking te vermelden.

Overigens is noch de RA noch de CA van Digidentity, tot intrekking op eigen initiatief verplicht, doch zal na melding en verzoek van intrekking, anders dan middels de daartoe geëigende elektronische faciliteiten, van de certificaathouder en na identificatie Digidentity tot intrekking overgaan, doch niet te alle tijde binnen de gestelde 4 uur.
Bij een compromittering van de CA zullen alle uitstaande certificaten worden ingetrokken door Digidentity.

Herroepen van een intrekking

Een intrekking van een Certificaat is definitief en kan niet worden herroepen.
Een Certificaat wordt geacht te zijn ingetrokken zodra de intrekking op de Digidentity website is gepubliceerd. Dit is uiterlijk 4 uur nadat het verzoek tot intrekking is gedaan.

Relatie tussen de verschillende CA domeinen

Alle RA functionarissen zelf Digidentity organisatie certificaten.

Alle gebruikers hebben een account van Digidentity. Deze zijn rand voorwaardelijk voor MachtigingOnline account.

Een MachtigingOnline account is rand voorwaardelijk voor een machtiging voor het aanvragen van SSL certificaten.

4.2. CRL beschikbaarheid en uitgifte frequentie

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 Digidentity liggen, zal Digidentity al het mogelijke doen om ervoor te zorgen dat deze informatie niet langer dan 4 uur niet beschikbaar is.

De Revocation status informatie wordt tenminste iedere vier uur ververst in de Certificate Revocation List. De CRL kan via de LDAP server op elk moment van de dag worden ingezien. Opname van een Certificaat in de CRL is de definitieve bevestiging van een blokkering/intrekking. Certificaten worden minstens tot zeven jaar, ook na afloop van de geldigheid, op de CRL vermeld.

4.3. Archivering van documenten

Digidentity zal alle registratie informatie vastleggen, met inbegrip van het volgende:

a) de logging van het authenticatie proces;
b) de logging van de levenscyclus van het Certificaat;
c) de logging van het gebruik van de private sleutels;
d) de logging van de mutaties in de registratie informatie.

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

4.4. Fysieke en Technische beveiliging

Infrastructuur

De infrastructuur van de informatiebeveiliging, die nodig is voor het beheren van de beveiliging binnen de CSP Digidentity, zal te alle tijde in stand worden gehouden, iedere verandering die invloed kan hebben op het beveiligingsniveau dient te worden goedgekeurd door het Digidentity managementteam. 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.

Logs en Protocollen

De volgende gebeurtenissen worden automatisch met datum en tijd gelogd:

a) alle gegevens relevant voor het aanmelden van een gebruiker in het systeem;
b) alle gegevens van authenticatie via het systeem;
c) de generatie van CA sleutelparen;
d) alle gebeurtenissen relevant bij het registratieproces van een Certificaat;
e) alle gegevens relevant voor de publicatie van de Digitale Certificaten;
f) alle gegevens relevant voor de publicatie van intrekkingslijsten;
g) alle herroeping details van een Certificaat, inclusief de reden van intrekking;
h) alle netwerkverkeer van en naar vertrouwde machines;

Daarnaast worden de volgende gebeurtenissen onder protocol gebracht:

a) verandering in de rolverdeling;
b) melding van verdenking van sleutelmisbruik;
c) melding van incidenten;
d) alle gebeurtenissen relevant bij beheer van de beveiligde omgeving;
e) alle wijzigingen in de configuratie van de back-up;
f) alle gebeurtenissen relevant bij het back-upproces;
g) alle aspecten van de installatie van nieuwe of bijgewerkte software;
h) alle aspecten van hardware updates;
i) alle aspecten van shutdown en restart.

Logs en Protocollen worden beveiligd online bewaard. Alleen geautoriseerd personeel heeft toegang tot deze bestanden. Er worden regelmatig back-ups gemaakt. Na enige tijd worden de bestanden op CD gearchiveerd. Deze CD's worden 7 jaar in een beveiligde ruimte bewaard. Alle uitgegeven publieke sleutels worden 7 jaar na beëindiging van het certificaat in de administratie gehouden.

Identiteitsbewijzen

Het kopie van het identiteitsbewijs inclusief de handtekening van de certificaathouder worden zowel fysiek in een afgesloten kast alsook beveiligd online bewaard. Alleen geautoriseerd personeel heeft toegang tot deze bestanden. Er worden regelmatig back-ups gemaakt. Na enige tijd worden de bestanden op CD gearchiveerd. Deze CD's worden 7 jaar in een beveiligde kluis bewaard.

Netwerktechnische veiligheidsmaatregelen

De gebruikte firewall en computersystemen corresponderen met de actuele stand van de techniek. Alle systemen zijn minimaal geconfigureerd, alleen de meest noodzakelijke software is geïnstalleerd. De configuratie van de systemen en de firewall worden regelmatig door een onafhankelijke instantie gecontroleerd. Alle opgeslagen data staan per gebruiker uniek versleuteld in de database.

Appendix A

De onderstaande tabel geeft de profielen weer die actief zijn op de bovenstaande CA's

CA CN=	Profielen actief
Staat der Nederlanden Root CA - G2	
Staat der Nederlanden Organisatie CA - G2	
Digidentity Organisatie CA - G2	CA certificaat
Staat der Nederlanden Burger CA – g2	-
Digidentity burger CA - G2	CA certificaat
Machtiging Online SSCD CA - G2	Authenticatie certificaat Onweerlegbaarheid certificaat – qc Encryptie certificaat
Digidentity Services CA - G2	SSL certificaat PKIoverheid Authenticiteit Vertrouwelijkheid Server EV server
Digidentity SSCD CA - G2	Authenticatie certificaat Onweerlegbaarheid certificaat – qc Encryptie certificaat

De geldigheid van eindgebruikers certificaten welke worden uitgegeven door een CA is 5 jaar vanaf het moment van uitgifte of tot maximaal de geldigheid van de certificaat van de uitgevende CA.

Certificate Generation Component

Slechts de sleutels die encryptie SHA-256-RSA, 2048 bit RSA, gebruiken worden toegestaan. Voor alle (sub) CA's geldt een sleutellengte van 4096 bit RSA.

Basis attributen voor Alle User Certificaten

Attribuut		Beschrijving	Type	Toelichting
Version	V	MOET ingesteld worden op 2 (X.509v3).	Integer	Beschrijft de versie van het certificaat, de waarde 2 staat voor X.509 versie 3.
SerialNumber	V	Een serienummer dat op unieke wijze het certificaat binnen het uitgevende CA domein MOET identificeren.	Integer	-
Signature	V	MOET worden ingesteld op het algoritme, zoals deze door de PA is bepaald.	OID	Moet gelijk zijn aan het veld signatureAlgorithm. Ten behoeve van maximale interoperabiliteit wordt alleen SHA-256 met RSA encryptie toegestaan.
Issuer	V	Moet een Distinguished Name (DN) bevatten. Veld heeft de onderstaande attributen:		Andere attributen dan hieronder genoemd MOETEN NIET worden gebruikt. De attributen die worden gebruikt MOETEN gelijk zijn aan de gelijknamige attributen in het Subject veld van het CSP certificaat (ten behoeve van validatie).
Issuer .countryName	V	Moet de landcode bevatten van het land waar de uitgevende organisatie van het certificaat is gevestigd.	Printable String	C = NL
Issuer. OrganizationName	V	Volledige naam conform geaccepteerd document of basisregistratie	UTF8String	O=Digidentity BV
Issuer. commonName	V	Dient de naam van de CA te bevatten conform geaccepteerd document of basisregistratie, optioneel aangevuld met de Domein aanduiding en/of de typen certificaat die worden ondersteund	UTF8String	Conform tabel CA's
Validity	V	MOET de geldigheidsperiode (validity) van het certificaat definiëren volgens RFC 5280.	UTCTime	Max 5 jaar of tot geldigheid van CA
Subject	V	De attributen die worden gebruikt om het subject (eindgebruiker) te beschrijven MOETEN het subject op unieke wijze benoemen. Veld heeft de onder- staande attributen:		Moet een Distinguished Name (DN) bevatten. Andere attributen dan hieronder genoemd MOETEN NIET worden gebruikt.
Subject. countryName	V	Vaste waarde: C=NL, conform ISO 3166	PrintableStri ng	C=NL
Subject. commonName	V	Het commonName attribuut dient te worden ingevoerd conform de paragraaf Naamconventie Subject.commonName hierboven.	UTF8String	Identiek aan MRZ data uit WID of Als de service een DNS naam heeft MOET deze in de common-Name vermeld worden als "fully-qualified domain name"
Subject. organizationName	O	Voor certificaten in domein burger wordt gebruik van organizationName niet toegestaan, bevat de organisatie naam in het domein organisatie	UTF8String	Verplicht ingeval van hiërarchie organisatie.

Attribuut		Beschrijving	Type	Toelichting
Subject. organizationalUnitName	O	Voor certificaten in domein Burger wordt gebruik van organizationalUnitName niet toegestaan, bevat de orgnaisatie naam in het domein organisatie		
Subject. serialNumber	O	Door de CSP te bepalen nummer. De combinatie van CommonName en Serialnumber MOET binnen de context van de CSP uniek zijn.	Printable String	Conform aanlevering RA. Numeriek 10 getallen, met voorloopnullen. Verplicht, tenzij het een services certificaat betreft.
subjectPublicKeyInfo	V	Bevat o.a. de publieke sleutel.		Bevat de publieke sleutel, identificeert het algoritme waarmee de sleutel kan worden gebruikt.

Standaard extensies

Attribuut		Beschrijving	Type	Toelichting
authorityKeyIdentifier	V	Het algoritme om de AuthorityKey te genereren MOET worden ingesteld op een algoritme zoals door de PA is bepaald.	BitString	De waarde moet de SHA-1 hash van de authorityKey (publieke sleutel van de CSP/CA) bevatten.
SubjectKeyIdentifier	V	Het algoritme om de subjectKey te genereren MOET worden ingesteld op een algoritme zoals door de PA is bepaald.	BitString	De waarde moet de SHA-1 hash van de subjectKey (publieke sleutel van de certificaathouder) bevatten.
KeyUsage	V	Dit attribuut extensie specificeert het beoogde doel van de in het certificaat opgenomen sleutel. In de PKI voor de overheid zijn per certificaatsoort verschillende bits opgenomen in the keyUsage extensie. In authenticiteitcertificaten moet het digitalSignature bit zijn opgenomen en zijn aangemerkt als essentieel. Geen ander keyUsage mag hiermee worden gecombineerd. In certificaten voor de elektronische handtekening moet het non-repudiation bit zijn opgenomen en zijn aangemerkt als essentieel. Geen ander keyUsage mag hiermee worden gecombineerd.	BitString	Conform beschrijving
CertificatePolicies	V	MOET de OID bevatten van de certificate policy (CP), de URI van het certification practice statement (CPS), en een gebruikersnotitie. Het te gebruiken OID schema in de PKI voor de overheid wordt beschreven in de CP.	OID, String, String	Conform beschrijving
SubjectAltName	V	MOET worden gebruikt en voorzien zijn van een persoonlijk wereldwijd uniek nummer.		Moet een unieke identifier bevatten in het othername attribuut. Andere attributen dan hieronder genoemd MOETEN NIET worden gebruikt.
SubjectAltName. otherName	V	MOET worden gebruikt met daarin een uniek nummer dat de certificaathouder identificeert.	Microsoft UPN	OID-UUID UUID is uniek voor elke certificaat.
CRLDistributionPoints	V	MOET de URI van een CRL distributiepunt bevatten.		Wordt in het certificaat profiel tabel gedefinieerd.
ExtKeyUsage	O	Wordt niet gebruikt.		Wordt in certificaten in domein Burger niet gebruikt. Dit veld wordt ook wel enhancedKeyUsage genoemd. Wordt in het certificaat profiel tabel gedefinieerd.

Private extensies

Attribuut		Beschrijving	Type	Toelichting
QcStatement	O	Certificaten voor de elektronische handtekening MOETEN aangeven dat deze certificaten worden uitgegeven als gekwalificeerde certificaten die overeenstemmen met de Europese Richtlijn. Deze overeenstemming wordt aangegeven door het opnemen van de id-etsi-qcs-QcCompliance statement in deze extensie. De certificaten voor authenticiteit en de certificaten voor vertrouwelijkheid mogen deze extensie NIET gebruiken.	OID	De OID van het id-etsi-qcs-QcCompliance statement is 0.4.0.1862.1.1 Is alleen van toepassing op onweerlegbaarheid c.q. non-repudation certificaten.

Basis attributen voor Alle CA profielen

Attribuut		Beschrijving	Type	Toelichting
Version	V	MOET ingesteld worden op 2 (X.509v3).	Integer	Beschrijft de versie van het certificaat, de waarde 2 staat voor X.509 versie 3.
SerialNumber	V	Een serienummer dat op unieke wijze het certificaat binnen het uitgevende CA domein MOET identificeren.	Integer	-
Signature	V	MOET worden ingesteld op het algoritme, zoals deze door de PA is bepaald.	OID	Moet gelijk zijn aan het veld signatureAlgorithm. Ten behoeve van maximale interoperabiliteit wordt alleen SHA-256 met RSA encryptie toegestaan.
Issuer	V	Moet een Distinguished Name (DN) bevatten. Veld heeft de onderstaande attributen:		Andere attributen dan hieronder genoemd MOETEN NIET worden gebruikt. De attributen die worden gebruikt MOETEN gelijk zijn aan de gelijknamige attributen in het Subject veld van het CSP certificaat (ten behoeve van validatie).
Issuer .countryName	V	Moet de landcode bevatten van het land waar de uitgevende organisatie van het certificaat is gevestigd.	Printable String	C = NL
Issuer. OrganizationName	V	Volledige naam conform geaccepteerd document of basisregistratie	UTF8String	O=Digidentity BV
Issuer. commonName	V	Dient de naam van de CA te bevatten conform geaccepteerd document of basisregistratie, optioneel aangevuld met de Domein aanduiding en/of de typen certificaat die worden ondersteund	UTF8String	Conform tabel CA's
Validity	V	MOET de geldigheidsperiode (validity) van het certificaat definiëren volgens RFC 5280.	UTCTime	Conform tabel CA's

Attribuut		Beschrijving	Type	Toelichting
Subject	V	De attributen die worden gebruikt om het subject (eindgebruiker) te beschrijven MOETEN het subject op unieke wijze benoemen. Veld heeft de onder- staande attributen:		Moet een Distinguished Name (DN) bevatten. Andere attributen dan hieronder genoemd MOETEN NIET worden gebruikt.
Subject. countryName	V	Vaste waarde: C=NL, conform ISO 3166	PrintableString	C=NL
Subject. commonName	V	Het commonName attribuut dient te worden ingevoerd conform de paragraaf Naamconventie Subject.commonName hierboven.	UTF8String	Conform tabel CA's
Subject. organizationName	O	Voor certificaten in domein burger wordt gebruik van organizationName niet toegestaan, bevat de orgnaisatie naam in het domein organisatie	UTF8String	O=Digidentity BV
subjectPublicKeyInfo	V	Bevat o.a. de publieke sleutel.		Bevat de publieke sleutel, identificeert het algoritme waarmee de sleutel kan worden gebruikt.

Standaard extensies voor CA profielen

Attribuut		Beschrijving	Type	Toelichting
SubjectKeyIdentifier	V	Het algoritme om de subjectKey te genereren MOET worden ingesteld op een algoritme zoals door de PA is bepaald.	BitString	De waarde moet de SHA-1 hash van de subjectKey (publieke sleutel van de certificaathouder) bevatten.
BasicContraint		Het "CA" veld MOET op "True" staan of worden weggelaten. Pathlen=-1		
KeyUsage	V	Dit attribuut extensie specificeert het beoogde doel van de in het certificaat opgenomen sleutel. In de PKI voor de overheid zijn per certificaatsoort verschillende bits opgenomen in the keyUsage extensie. In authenticiteitcertificaten moet het digitalSignature bit zijn opgenomen en zijn aangemerkt als essentieel. Geen ander keyUsage mag hiermee worden gecombineerd. In vertrouwelijkheidcertificaten moeten keyEncipherment en dataEncipherment bits zijn opgenomen en zijn aangemerkt als essentieel. Optioneel kan dit worden gecombineerd met het keyAgreement bit. Geen ander keyUsage mag hiermee worden gecombineerd. In certificaten voor de elektronische handtekening moet het non-repudiation bit zijn opgenomen en zijn aangemerkt als essentieel. Geen ander keyUsage mag hiermee worden gecombineerd.	BitString	CRL Signer, Certificate Signer.
CertificatePolicies	V		OID, String, String	Policy: 2.5.29.31.0 http://pki.digidenity.eu/policy-pkio

Alle CA's conformeren zich aan onderstaande CRL profiel

Attribuut		Beschrijving	Type	Toelichting
Version	V	MOET ingesteld worden op 2 (X.509v3).	Integer	Beschrijft de versie van het certificaat, de waarde 2 staat voor X.509 versie 3.
Signature	V	MOET worden ingesteld op het algoritme, zoals deze door de PA is bepaald.	OID	Moet gelijk zijn aan het veld signatureAlgorithm. Ten behoeve van maximale interoperabiliteit wordt alleen SHA-256 met RSA encryptie toegestaan.
Issuer	V	Moet een Distinguished Name (DN) bevatten. Veld heeft de onderstaande attributen:		Andere attributen dan hieronder genoemd MOETEN NIET worden gebruikt. De attributen die worden gebruikt MOETEN gelijk zijn aan de gelijknamige attributen in het Subject veld van het CSP certificaat (ten behoeve van validatie).
Issuer .countryName	V	Moet de landcode bevatten van het land waar de uitgevende organisatie van het certificaat is gevestigd.	Printable String	C = NL
Issuer. OrganizationName	V	Volledige naam conform geaccepteerd document of basisregistratie	UTF8String	O=Digidentity BV
Issuer. commonName	V	Dient de naam van de CA te bevatten conform geaccepteerd document of basisregistratie, optioneel aangevuld met de Domein aanduiding en/of de typen certificaat die worden ondersteund	UTF8String	Conform tabel CA's
Issuer.organizationalUnitName	O	Optionele aanduiding van een organi-satieonderdeel. Dit veld MAG NIET een functieaanduiding of dergelijke bevatten. Wel eventueel de typen certificaten die worden ondersteund.	ETSI TS 102280: 5.2.4	Is een mogelijk toekomstige uitbreiding
ThisUpdate	V		UTCTime	Uitgave datum van CRL
NextUpdate	V		UTCTime	Dit is het uiterste tijdstip waarop een update verwacht mag worden, eerdere update is mogelijk. (4uur vanaf thisupdate)
RevokedCertificates	V		Serialnumber,UTCTime	

CRL

Attribuut		Beschrijving	Type	Toelichting
CRLNumber	V	Dit attribuut MOET een oplopend nummer bevatten dat het bepalen van de volgorde van CRL's ondersteunt (de CSP voorziet de CRL van de nummering).	Integer	

OID Nummers

Elke CP wordt uniek geïdentificeerd door het OID, overeenkomstig de volgende tabel.

	CA Profiel	OID	KeyUsage	Qc_statement
Digidentity Organisatie CA - G2	CSP-Organisatie	oid: 2.16.528.1.1003.1.3.5.8.1		
Digidentity burger CA - G2	CSP-Burger	oid: 2.16.528.1.1003.1.3.3.2.1		
Machtiging Online SSCD CA - G2		oid: 2.16.528.1.1003.1.3.5.8.2		
	SSCD-A-Organisatie	2.16.528.1.1003.1.2.5.1	2,4	
	SSCD-O-Organisatie	2.16.528.1.1003.1.2.5.2	-	Yes
	SSCD-E-Organisatie	2.16.528.1.1003.1.2.5.3	4	
Digidentity Services CA - G2		oid: 2.16.528.1.1003.1.3.5.8.3		
	SSL-A-Organisatie	2.16.528.1.1003.1.2.5.4	2,4	
	SSL-V-Organisatie	2.16.528.1.1003.1.2.5.5	2,4	
	SSL-S-Organisatie	2.16.528.1.1003.1.2.5.6	1,2,4	
Digidentity SSCD CA - G2		oid: 2.16.528.1.1003.1.3.3.2.2		
	SSCD-A- Burger	2.16.528.1.1003.1.2.3.1,	2,4	
	SSCD-O- Burger	2.16.528.1.1003.1.2.3.2	-	yes
	SSCD-E- Burger	2.16.528.1.1003.1.2.3.3.	4	

Legenda key usage

nummer	betekenis
1	SSL server
2	SSL client
4	email beveiliging

Certificaat gebruik burger

Het gebruik van certificaten uitgegeven onder deze CP heeft betrekking op communicatie van certificaathouders op persoonlijke titel.

[2.16.528.1.1003.1.2.3.1] Authenticiteit certificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het betrouwbaar identificeren en authentiseren van personen langs elektronische weg. Dit betreft zowel de identificatie van personen onderling als tussen personen en geautomatiseerde middelen.

[2.16.528.1.1003.1.2.3.2] Handtekeningcertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt om elektronische handtekeningen te verifiëren, die “dezelfde rechtsgevolgen hebben als een handgeschreven handtekening”, zoals wordt aangegeven in artikel 15a, eerste en tweede lid, in Titel 1 van Boek 3 van het Burgerlijk Wetboek onder afdeling 1A en zijn gekwalificeerde certificaten zoals bedoeld in artikel 1.1, lid ss van de Telecomwet.

Certificaatgebruik organisatie

Het gebruik van certificaten uitgegeven onder deze CP heeft betrekking op communicatie van certificaathouders in de hoedanigheid van employee van de abonnee.

Certificaatgebruik organisatie gebruikercertificaten

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

[2.16.528.1.1003.1.2.5.1] Authenticiteit certificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het betrouwbaar identificeren en authentiseren van personen, organisaties en middelen langs elektronische weg. Dit betreft zowel de identificatie van personen onderling als tussen personen en geautomatiseerde middelen.

[2.16.528.1.1003.1.2.5.2] Handtekeningcertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt om elektronische handtekeningen te verifiëren, die "dezelfde rechtsgevolgen hebben als een handgeschreven handtekening", zoals wordt aangegeven in artikel 15a, eerste en tweede lid, in Titel 1 van Boek 3 van het Burgerlijk Wetboek onder afdeling 1A en zijn gekwalificeerde certificaten zoals bedoeld in artikel 1.1, lid ss van de Telecomwet.

Certificaatgebruik services

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

[2.16.528.1.1003.1.2.5.4] Authenticiteit certificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het langs elektronische weg betrouwbaar identificeren en authentiseren van de service als behorende bij de organisatorische entiteit, die verantwoordelijk is voor de betreffende service.

[2.16.528.1.1003.1.2.5.5] Vertrouwelijkheidcertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het beschermen van de vertrouwelijkheid van gegevens, die worden uitgewisseld en/of opgeslagen in elektronische vorm.

[2.16.528.1.1003.1.2.5.6] Servercertificaten die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het beveiligen van een verbinding tussen een bepaalde client en een server die behoort bij de organisatorische entiteit die als abonnee wordt genoemd in het betreffende certificaat.