Certification Practice Statement PKIo

Datum : 22 augustus 2017
Versie : 1.11
OID : 2.16.528.1.1003.1.5.8

Document Controle Pagina

Title	Certification Practice Statement PKIoverheid
Creator	Marcel A. Wendt
Date	19 mei 2011
Type	Text
Format	Word
Identifier	CPS v1.11 Certification Practice Statement PKIoverheid.docx
Source	N/A
Language	Dutch
Rights	Copyright “Digidentity”

Wijzigingshistorie

Version	Date	Changed by	Changes made
1.0	22-01-11	Marcel A. Wendt	Definitieve uitgave
1.1	07-09-11	Marcel A. Wendt	Definitieve uitgave met SSL
1.2	18-04-12	Marcel A. Wendt	Toevoeging beroepscertificaten
1.3	24-04-2013	Nour Riyad	Intrekking en opschorting certificaten
1.4.1	13-12-2013	Tom Bakker/Nour Riyad	Nieuwe opzet conform RFC3647. Geen inhoudelijke wijzigingen.
1.5	18-02-2015	Tom Bakker	Verwijderen beroepsprofielen
1.6	30-08-2016	Eva Bosch	Tekstuele en redactionele wijzigingen
1.7	12-01-2017	Eva Bosch	Tekstuele en redactionele wijzigingen
1.8	03-04-2017	Eva Bosch	Beschrijving van Geldigheid certificaten verduidelijkt naar 2020. (Geldigheid CA) + wijziging van CSP naar TSP
1.9	20-04-2017	Eva Bosch	Aanpassing WEH → eIDAS.
1.10	02-06-2017	Eva Bosch	Update CA structuur G2
1.11	22-08-2017	Tom Bakker	- §3.2 Initiële identiteitsvalidatie - Toegevoegd WHOIS als domein validatie methode (RFC-PvE 365) - Tekstuele en redactionele wijzigingen n.a.v. interne audit

Inhoudsopgave

1.Introductie

1.1 Overview

De PKI Overheid is een initiatief van de Nederlandse overheid en vormt een raamwerk met eisen en afspraken die het gebruik van een elektronische Handtekening, elektronische authenticatie en vertrouwelijke elektronische communicatie mogelijk maakt. Dit is gebaseerd op certificaten met een hoog betrouwbaarheidsniveau.
De eisen die, aan de Trusted Service Provider (TSP) worden, gesteld voor het uitgeven en beheren van deze certificaten, zijn beschreven in het Programma van Eisen PKI voor de overheid. Zie https://www.logius.nl

Digidentity BV (Digidentity), opgericht in 2008, is een aanbieder van certificaten. Digidentity is in Nederland als TSP gecertificeerd en tevens toegetreden tot de PKI voor de overheid.
De infrastructuur van de PKI Overheid waaraan Digidentity deelneemt, bestaat uit een hiërarchie met meerdere niveaus. Op elk niveau worden diensten geleverd conform strikte normen om de betrouwbaarheid van de gehele PKI voor de overheid zeker te stellen.
De Policy Authority (PA) PKIoverheid is verantwoordelijk voor het beheer van de centrale infrastructuur. De PA van PKI Overheid heeft het afsprakenstelsel beschreven in haar Programma van Eisen (PvE) en het bijbehorende Certificaat Policy (CP).

De PKI overheid is zo opgezet dat overheidsorganisaties en marktpartijen als certificatiedienstverlener (Trusted Service Provider – TSP) onder voorwaarden toe kunnen treden tot de PKI Overheid. Digidentity is als CPS verantwoordelijk voor de dienstverlening binnen de PKI overheid. De PA ziet toe op het handhaven van de afspraken en daarmee op de betrouwbaarheid van de gehele PKI voor de overheid. Digidentity heeft zich aan het PvE geconformeerd.

Digidentity conformeert zich tevens aan de huidige versie van de Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates zoals gepubliceerd op https://www.cabforum.org. Mocht er een inconsistentie aanwezig zijn tussen het PKI Overheid Programma van Eisen deel 3b en de betreffende Baseline Requirements, waardoor niet tenminste tegemoet wordt gekomen aan de hierin beschreven minimale eisen, dit ter beoordeling door de PA, dan prevaleert hetgeen gesteld is in de Requirements.

De totale dienst wordt verleend door twee gescheiden afdelingen binnen Digidentity, te weten; 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 diens online identiteit en (teken) bevoegdheid. Digidentity CA verzorgt onder andere de afgifte, wijziging, vernieuwing en intrekking van de certificaten. Voor dat deze handelingen verricht kunnen worden, worden eerst de handelingen tot registratie door Digidentity RA uitgevoerd. De registratie handelingen zijn elders in dit document beschreven.

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. Deze onderaannemers zijn voor IT: KPN Cybercenter en Data Centre Rotterdam (DCR). Voor ID checks: ID-Checker.

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. Voor het domein Organisatie worden certificaten onder de handelsnaam MachtigingOnline uitgegeven en certificaten binnen het domein Burger onder de handelsnaam Digidentity.

1.2 Documentnaam en identificatie

Voor u ligt het PKIoverheid Certification Practice Statement (CPS) van Digidentity. Dit document beschrijft de procedures en maatregelen die Digidentity in acht neemt bij het uitgeven van certificaten in het domein Burger, Organisatie en Services van de PKI voor de overheid. Deze maatregelen zijn in overeenstemming met de eisen uit ETSI EN 319 411-1, ETSI EN 319 411-2, de aanvullende eisen uit de eIDAS verordening betreffende vertrouwensdiensten en het Programma van Eisen PKIoverheid delen 3a, 3b, 3c en 3e.

1.3 PKI Deelnemende partijen

1.3.1 Certification Authorities

1.3.1.1 Centrale Infrastructuur PKIoverheid

De centrale infrastructuur van de PKI voor de overheid wordt namens de Staat der Nederlanden beheerd door Logius en bestaat uit de volgende componenten:
• Staat der Nederlanden Root Certification Authority
• Staat der Nederlanden Domein Certification Authority - Organisaties

1.3.1.2 Digidentity TSP Certification Authority (TSP-CA)

De Digidentity TSP-CA wordt beheerd in het beveiligde datacenters van Digidentity in Amsterdam en Rotterdam deze geeft de certificaten uit ten behoeve van certificaathouders binnen de PKI voor de overheid en in overeenstemming met dit CPS. Een overzicht van certificaten die worden uitgegeven is opgenomen in hoofdstuk 1.4 Certificaatgebruik van dit CPS.

1.3.2. Registration Authorities

1.3.2.1 Digidentity Registration Authority (Digidentity RA)

De Digidentity RA in Den Haag verzorgt de identificatie en registratie van de certificaathouder en de certificaatbeheerder en verzorgt de intrekkingen van uitgegeven certificaten.

1.3.3. Eindgebruikers

1.3.3.1 Abonnee

Een abonnee is een natuurlijke persoon dan wel een rechtspersoon die met dit TSP een overeenkomst sluit namens één of meer certificaathouders voor het laten certificeren van de publieke sleutels. Een abonnee kan tevens een certificaathouder zijn.

1.3.3.2 Certificaathouder

Bij de persoonlijke certificaten is de 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. De abonnee accordeert bij de aanvraag dat de certificaathouder een certificaat mag ontvangen met daarin de organisatiegegevens van de abonnee.
Bij de Services certificaten is de certificaathouder een apparaat of een systeem (een niet-natuurlijke persoon), bediend door de abonnee of door een daartoe aangewezen certificaatbeheerder.

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 persoonsgebonden certificaat in het domein Organisatie is de organisatie de abonnee en is de certificaathouder een natuurlijke persoon binnen de organisatorische entiteit. Namens de abonnee is een daartoe aangewezen certificaatbeheerder verantwoordelijk voor het beheren van de certificaten.

1.3.3.3 Certificaatbeheerder

Voor het uitvoeren van de operationele handelingen ten behoeve van het systeemcertificaat (o.a. de aanvraag, installatie en beheer, intrekking) is de tussenkomst door een natuurlijke persoon vereist. De abonnee kan dit zelf uitvoeren of wijst hiertoe een functionaris aan, de certificaatbeheerder. In dat geval verleent de abonnee aan de

certificaatbeheerder de expliciete toestemming om de operationele handelingen uit te voeren.

1.3.4. Vertrouwende Partijen

Een Vertrouwende Partij is een natuurlijke of rechtspersoon die ontvanger is van een Certificaat en die handelt in vertrouwen op dat Certificaat.

1.4 Certificaatgebruik

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

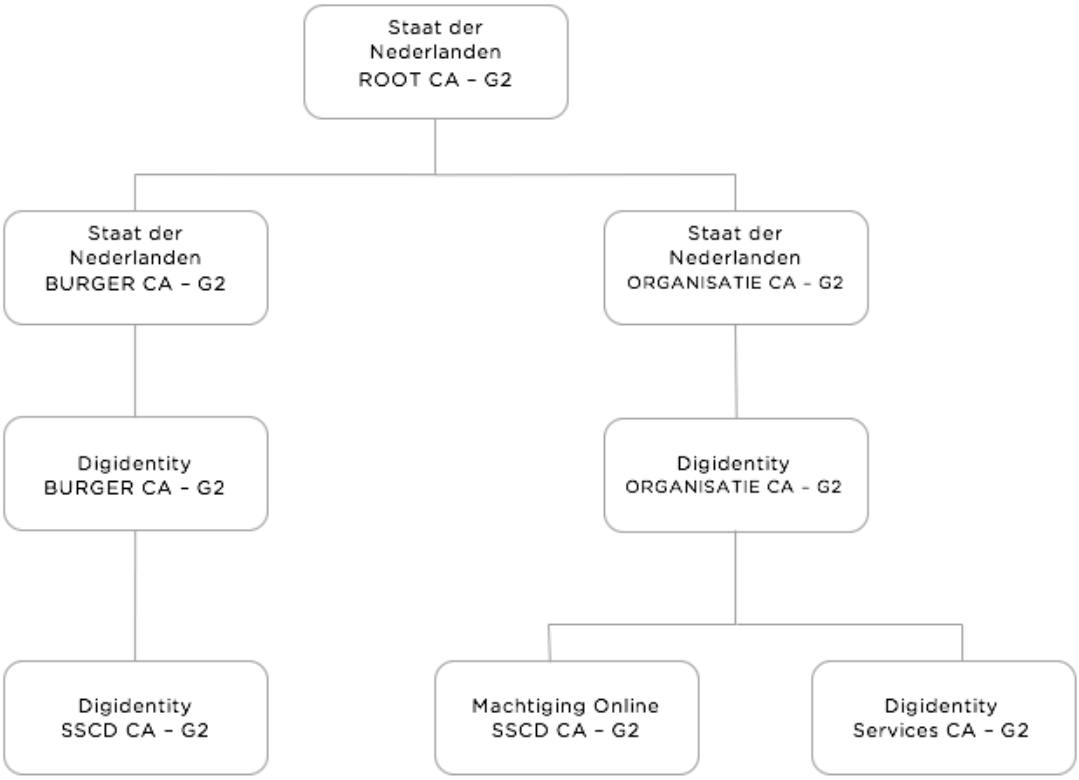
Certificaten voor Personen (Persoonlijke certificaten): Digidentity geeft de volgende certificaten uit aan personen. Een persoon ontvangt de volgende certificaten, opgeslagen op een veilig middel (SSCD):

- Een **Onweerlegbaarheidscertificaat** dat onder dit CPS wordt uitgegeven kan worden gebruikt om een elektronische handtekening te verifiëren, die “dezelfde rechtsgevolgen heeft 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 is een gekwalificeerd certificaat zoals bedoeld in artikel 1.1, lid ss van de Telecomwet;
- Een **Authenticiteitcertificaat** dat onder dit CPS wordt uitgegeven kan worden gebruikt voor het langs elektronische weg betrouwbaar identificeren en authentiseren van een persoon als behorende bij een organisatorische entiteit;
- Een **Vertrouwelijkheidscertificaat** dat onder dit CPS wordt uitgegeven, kan 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.

Servicescertificaten (Systeem): Digidentity geeft daarnaast de volgende niet-persoonlijke certificaten uit (voor systemen).

- Een Server certificaat, dat onder dit CPS worden uitgegeven kan worden gebruikt voor het beveiligen van een verbinding tussen een bepaalde cliënt en een server die behoort bij de organisatorische entiteit (abonnee) die wordt genoemd in het betreffende certificaat.
- Een Service certificaat (authenticatie), dat onder dit CPS worden uitgegeven kan 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, alsmede het versleutelen van data.
- Een Service certificaat (vertrouwelijkheid), dat onder dit CPS wordt uitgegeven, kan worden gebruikt voor het beschermen van de vertrouwelijkheid van gegevens, die worden uitgewisseld en/of opgeslagen in elektronische vorm.

De CA-structuur en de typen certificaten die Digidentity uitgeeft zijn inzichtelijk gemaakt in onderstaand figuur.



Figuur 1.1: Overzicht van de certificaat policies CA - G2

1.5 Beleid beheer

Dit CPS wordt periodiek gereviewd door de documentverantwoordelijke. Dit gebeurt aan de hand van een auditplanning en na eventule PvE PKIo wijzigingen en wijzigingen in de dienstverlening. Na het verwerken van de wijzigingen en het reviewen en goedkeuren van de aangebrachte wijzigingen gaat de documentverantwoordelijke over tot het uitgeven van een nieuwe versie. Deze wordt gepubliceerd op de website.

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 allen tijde worden ingediend en worden direct, doch uiterlijk binnen vier 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/L4/burger/latestCRL.crl
- pki.digidentity.eu/L4/organisatie/latestCRL.crl
- pki.digidentity.eu/L4/sscd-mo/latestCRL.crl
- pki.digidentity.eu/L4/sscd-digidentity/latestCRL.crl
- pki.digidentity.eu/L4/services/latestCRL.crl

De locatie van de OCSP (Online Certificate Status Protocol) responders worden weergegeven in het veld van de betreffende Certificaatprofielen welke zijn opgenomen in dit CPS.

Informatie over dit CPS en voorgenomen wijzigingen daarop kan worden verkregen via onderstaande contactgegevens:

Digidentity B.V.
Waldorpstraat 17p
2521 CA 's Gravenhage

Tel: +31 (0)887 78 78 78
Website: https://www.digidentity.eu
E-mail: info@digidentity.eu

2. Publicatie en verantwoordelijkheid voor elektronische opslagplaats

2.1 Elektronische opslagplaats

Digidentity heeft een elektronische opslagplaats die bereikbaar is via: https://www.digidentity.eu

Toegang tot gepubliceerde informatie

De toegangscontrole tot de elektronische opslagplaats is zodanig ingericht dat alleen leesrechten zijn toegekend voor derden die deze informatie raadplegen.
Uitsluitend Digidentity heeft schrijfrechten op de elektronische opslagplaats.
De elektronische opslagplaats is 24 uur per dag, 7 dagen per week voor een ieder beschikbaar, met uitzondering van systeemdefecten of onderhoudswerkzaamheden. In geval van onvoorziene on-beschikbaarheid, wordt de beschikbaarheid van de elektronische opslagplaats (dissemination service) hersteld binnen 24 uur.

2.2 Publicatie van TSP-informatie

De opslagplaats maakt de volgende zaken toegankelijk:

- CPS
- Algemene Voorwaarden
- Certificaten van certificaathouders die beperkt beschikbaar zijn tot de certificaathouder
- Certificate Revocation List (CRL)

De locatie van de Elektronische opslagplaats en Online Certificate Status Protocol (OCSP) responders worden tevens weergegeven in het toepasselijke veld van de betreffende Certificaatprofielen welke zijn opgenomen in de bijlage bij dit CPS.

De unieke nummers (OID's) die refereren naar de toepasselijke Certificate Policies zijn:

2.2.1 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, - welke 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.

2.2.2 Certificaatgebruik organisatie

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

2.2.3 Certificaatgebruik organisatie gebruiker certificaten

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] Authenticiteitscertificaten, 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, -welke 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.

2.2.4 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] Authenticiteitscertificaten, die onder deze CP worden uitgegeven, kunnen worden gebruikt voor het langs de 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 cliënt en een server die behoort bij de organisatorische entiteit die als abonnee wordt genoemd in het betreffende certificaat.

2.3 Frequentie van publicatie

De informatie in de elektronische opslagplaats wordt zo snel als mogelijk is gepubliceerd en/of geactualiseerd.

Digidentity conformeert zich aan de huidige versie van de Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates zoals gepubliceerd op http://www.cabforum.org. Mocht er een inconsistentie aanwezig zijn tussen het PKIoverheid Programma van Eisen deel 3b en de betreffende Requirements, waardoor niet tenminste tegemoet wordt gekomen aan de hierin beschreven minimale eisen, dit ter beoordeling door de PA, dan prevaleert het gestelde in de Requirements.

Het authenticiteitscertificaat is niet in de Wet op de IDentificatieplicht (WID) als identiteitsdocument opgenomen en kan derhalve niet worden gebruikt voor het identificeren van personen in gevallen waarbij de wet vereist dat de identiteit van personen met een in de Wet op de identificatieplicht aangewezen document wordt vastgesteld. Het authenticiteitscertificaat kan niet worden gebruikt bij het afnemen van overheidsdiensten waarbij de wet vereist dat de identiteit van personen met een in de WID aangewezen document wordt vastgesteld.

3. Identificatie en Authenticatie (I&A)

3.1 Naamgeving

3.1.1 Soorten naamformaten

De naam in het subject veld van het certificaat moet de Certificaathouder duidelijk identificeren en weergegeven zijn in een leesbare en begrijpelijke vorm, in overeenstemming met de X.500 standaard voor Distinguished Names (DN).
Elke certificaathouder moet een unieke en direct identificeerbare X.501 DN hebben. Deze DN kan bestaan uit de volgende attributen:

- Land (C)
- Organisatie (O)
- Organisatorische eenheid (OU)
- Common name (CN)
- SerialNumber

3.1.2 Noodzaak gebruik betekenisvolle namen

De naamgeving in de uitgegeven certificaten is betekenisvol, ondubbelzinnig en uniek en stelt elke vertrouwende partij in de gelegenheid de identiteit van de certificaathouder vast te stellen.
De inhoud van het Certificaat moet een betekenisvolle associatie hebben met de naam van de betreffende persoon, organisatie of het apparaat. In het geval van personen moet de naam bestaan uit de eerste voornaam, overige voorletters en achternaam. Voor organisaties moet de naam op een betekenisvolle manier de naam van de geregistreerde juridische entiteit (van de abonnee) weergeven en in geval van een apparaat tevens de geregistreerde domeinnaam van de organisatie (abonnee) weergeven die verantwoordelijk is voor dat apparaat.

3.1.3. Pseudoniemen

Het gebruik van anonieme certificaten of pseudoniemen is niet toegestaan.

3.1.4. Regels voor interpreteren verschillende naamvormen

De regels voor interpretatie van naamvormen worden teruggevonden in de International Telecommunication (ITU) en Internet Engineering Task Force (IETF) standaarden, zoals de ITU-T X.500 serie van standaarden en toepasbare IETF RFCs.

3.1.5 Uniciteit van namen.

De DistinguishedName van de Certificaathouder in een certificaat dat onder dit CPS is uitgegeven, is te allen tijde uniek voor deze Certificaathouder en wordt niet uitgegeven aan een andere Certificaathouder. Het is de taak van de Digidentity RA te verifiëren dat de DistinguishedName van de certificaathouder nog niet is opgenomen in de elektronische opslagplaats voor certificaten (de Digidentity X.500 serie standaard).

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

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

Elk Certificaat krijgt verder een uniek serienummer toegewezen dat een eenduidige en unieke identificatie van Certificaathouders mogelijk maakt.

3.1.6 Erkenning, authenticatie en de rol van handelsmerken

Voor zover de naam van een organisatie voorkomt in een algemeen erkend openbaar register, een oprichtingsakte, een instellingsbesluit of in een ander wettelijk erkend document ter identificatie van organisaties, zal in het Certificaat deze naam van de organisatie worden opgenomen.

3.1.7. Geschillen

In het geval van geschillen over de op te nemen naamgeving in een certificaat, beslist Digidentity op basis van een belangenafweging welke naam opgenomen wordt.

3.2 Initiële identiteitsvalidatie

Digidentity waarborgt dat de abonnee het CSR (Certificate Signing Request) op een veilige manier aanlevert. Het op een veilige manier aanleveren vindt als volgt plaats:

Het invoeren van het CSR op de HTTPS website van de Digidentity die gebruikt maakt van een PKIoverheid SSL certificaat of gelijkwaardig of;

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

1. Verificatie door Digidentity (deze stap wordt niet toegepast bij eenmalige SSL aankopen)
    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. mobiel telefoonnummer
    - de gebruiker ontvangt een SMS code op het mobiel telefoonnummer, deze dient in het registratieproces ingevoerd te worden;
    e. afgeleide verificatie door middel van € 0,01 betaling met iDeal
    - hiermee controleren we de naam en woonplaats van de gebruiker.

2. Verificatie door AuSO (Authenticatie Service Organisatie):
    a. Achternaam
    b. Eerste voornaam met initialen
    c. Indien van toepassing tussenvoegsels
    d. Geslacht
    e. Geboortedatum
    f. Geboorteplaats
    g. Postcode en huisnummer
    h. Type identiteitsbewijs, nummer en expiratiedatum

3. Zo daartoe aanleiding bestaat wordt door een AuSO gecontroleerd of een aangeboden identiteitsbewijs is aangemeld als vermist of gestolen. Indien de controle een zogenoemde 'HIT' oplevert worden de relevante instanties geïnformeerd.

4. Face to Face controle van gebruiker.

5. Het ontvangen kopie legitimatiebewijs wordt onderzocht op eventuele fraude kenmerken.

6. Geaccepteerde legitimatiebewijzen zijn: geldig paspoort, geldig ID-kaart. Digidentity controleert overeenkomstig Nederlandse wet- en regelgeving de identiteit en, indien van toepassing de specifieke eigenschappen van de certificaatbeheerder.

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

1. Verificatie organisatie middels KvK
    a. Verificatie naam;
    b. Verificatie nummer;
    c. Verificatie bestuurders;

2. Verificatie FQDN
    a. De domeinnaam wordt gecontroleerd bij erkende registers als SIDN (Stichting Internet Domeinregistratie Nederland) en IANA (Internet Assigned Numbers Authority;
    b. gecontroleerd wordt of de desbetreffende domeinnaam eigendom is van de aanvragende organisatie bij 'WHOIS';
    c. wildcards in de domeinnamen worden niet geaccepteerd

Door de abonnee wordt middels een machtiging één of meerdere certificaatbeheerders aangewezen. Deze certificaatbeheerder is verplicht om een authenticatie certificaat binnen het domein Organisatie te hebben om zodanig op te treden. Indien een certificaatbeheerder niet over een Digidentity account beschikt zal bij elke aanvraag een identiteitscontrole op locatie plaatsvinden. Ter autorisatie van de Certificaathouder en Certificaatbeheerder wordt in elk geval vastgelegd dat de certificaatbeheerder gerechtigd is voor een certificaathouder een certificaat te ontvangen namens de

rechtspersoon of andere organisatorische entiteit. Op basis van de aangeleverde formulieren en bewijsmiddelen verifieert Registration Authority dat de certificaathouder geautoriseerd is om namens de abonnee een certificaat te ontvangen dat deze authentiek is en dat de, in dit bewijs, genoemde naam en identiteitskenmerken overeenkomen met de vastgestelde identiteit van de certificaathouder.

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 wordt op papier dan wel langs de elektronische weg aangeleverd.

Digidentity verifieert dat de domeinnaam niet voorkomt op een spam- en/of phishing blacklist. Hiervoor wordt http://www.phishtank.com gebruikt. Wanneer er sprake is van een domeinnaam die voorkomt op phishtank of eventueel de Digidentity blacklist die geraadpleegd is, zal Digidentity tijdens het verificatieproces extra zorgvuldig omgaan met de aanvraag van het betreffende services server certificaat.

Abonnee is een rechtspersoon (organisatie gebonden certificaten):
Relevante wijzigingen in het certificaat dienen door de abonnee, met onmiddellijke ingang, kenbaar gemaakt te worden aan Digidentity doormiddel van een intrekkingsverzoek. Schorsing van een certificaat is niet mogelijk.

3.3 Identificatie en Authenticatie bij vernieuwing van een Certificaat

Een verzoek tot vernieuwing van een Persoonsgebonden Certificaat moet worden gedaan door de gebruiker. Dit resulteert te allen tijde in een nieuw sleutelpaar nadat alle gegevens (doormiddel van een checklist) 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.

Voor Service certificaten moet het aanvraagproces geheel opnieuw worden doorlopen.

3.4 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 allen tijde zijn certificaten intrekken. Als alternatief kan de gebruiker telefonisch zijn certificaten laten intrekken door Digidentity. Indien men toch weer certificaten en smartcard wil hebben moet de registratie procedure in zijn geheel en opnieuw worden doorlopen. 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.

Voor het intrekken van Server certificaten kan de certificaatbeheerder van de abonneeorganisatie die beschikt over een Digidentity hier online opdracht toe geven. Digidentity heeft hiervoor een proces ingericht die ze de zekerheid kan geven dat het verzoek geverifieerd kan worden. Dit proces wordt automatisch verwerkt en is niet herroepbaar. Voor certificaatbeheerders van de abonneeorganisatie die niet beschikken over een Digidentity is 24x7 een intrekkingsnummer operationeel. Dit nummer is: +31 (0)887 78 78 00. Hierna zal Digidentity er zorg voor dragen dat het certificaat binnen vier uur wordt ingetrokken. Om buiten kantoortijden de mogelijkheid tot intrekking te garanderen is er voor de RA2 Officer een piketdienst ingesteld.

4 Operationele eisen

4.1. Certificaataanvraag

Digidentity doet een aanbod op haar website, https://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 te starten. Als de authenticatie positief is verlopen, produceert Digidentity het gevraagde certificaat en verstrekt deze vervolgens aan de certificaathouder. Dit CPS is beschikbaar voor de gebruiker via de website van Digidentity.

Digidentity sluit, voorafgaand aan de uitgifte van een **services server** certificaat, een overeenkomst af met de abonnee en ontvangt een, door de certificaatbeheerder ondertekende, certificaataanvraag.
De overeenkomst voldoet aan de volgende voorwaarden:

1 Digidentity stelt aan Abonnee PKI Overheid certificaten beschikbaar tegen de navolgende voorwaarden;
2 voor PKI Overheid certificaten kan de Certificaatbeheerder de certificaataanvraag aan Digidentity aanleveren op basis van een door hem in eigen beheer gegenereerde private sleutel. Ook is het mogelijk dat Digidentity de private sleutel in een beveiligde omgeving voor de Abonnee genereert;
3 de Abonnee verklaart hierbij bevoegd te zijn voor het ondertekenen van deze overeenkomst;
4 de Abonnee verklaart hierbij dat voor iedere private sleutel compenserende maatregelen worden getroffen. De Abonnee verklaart passende maatregelen te nemen om de private sleutel en de daarbij behorende publieke sleutel in het betreffende services server certificaat toegangsinformatie onder zijn controle te nemen, geheim te houden en te beschermen. Digidentity heeft het recht om een controle uit te voeren naar de getroffen maatregelen;
5 de Abonnee en/of de Certificaatbeheerder is gehouden om, alvorens een toegekend certificaat in gebruik te nemen, de opgenomen gegevens op juistheid en volledigheid te controleren en verklaart dat de gegevens die worden verstrekt volledig en juist zijn. Onjuistheden in een certificaat dat niet is ingetrokken, komen voor rekening en risico van de Abonnee. De Abonnee is gehouden onjuistheden direct, maar in ieder geval *voor* de derde dag *na* ontvangst van het certificaat, aan Digidentity te melden, bij gebreke(n) waarvan Digidentity nimmer aansprakelijk kan worden gehouden voor enige tekortkomingen. Het melden van onjuistheden kan via de helpdesk van Digidentity. Abonnee zal niet het services server certificaat installeren voordat het op juistheid en volledigheid is gecontroleerd;
6 voorts verklaart de Abonnee dat de Certificaatbeheerder geautoriseerd, of gemachtigd, is om de aanvraag te doen en de daarbij behorende private sleutel te beheren;
7 de Abonnee wordt verplicht gesteld Digidentity direct te informeren indien de persoon die de rol van Certificaatbeheerder vervult wijzigt;

8 de Abonnee draagt er zorg voor dat bij het retour zenden van dit contract, aan Digidentity, een kleuren kopie van het identiteitsdocument van de Abonnee en/of Certificaatbeheerder worden toegevoegd. Een aangevraagd certificaat zal pas operationeel worden na ontvangst van deze overeenkomst, getekend door de daartoe bevoegde persoon, alsmede de hiervoor bedoelde documenten;

9 de Abonnee kan te allen tijde het certificaat intrekken;

10 de Abonnee verklaart dat indien de domeinnaam (FQDN) zoals vermeld in een services server certificaat identificeerbaar en adresseerbaar is via het internet, dat het services server certificaat alleen op een server wordt gezet die ten minste bereikbaar is met een van de FQDN's in dit services server certificaat;

11 de Abonnee verklaart dat het services server certificaat alleen wordt gebruikt in overeenstemming met de regelgeving die op haar bedrijfsvoering van toepassing is en alleen in relatie met de werkzaamheden van de abonnee en in overeenstemming met de bepalingen van de voorliggende overeenkomst;

12 de Abonnee verklaart het services server certificaat niet te installeren als duidelijk is dat de gegevens in het services server certificaat onjuist of onvolledig zijn of als er aanwijzingen zijn dat de private sleutel, behorend bij de publieke sleutel van het betreffende services server certificaat, gecompromitteerd is geraakt;

13 de Abonnee verklaart per direct geen gebruik meer te maken van het services server certificaat als duidelijk is dat de gegevens in het services server certificaat onjuist en/of onvolledig zijn of als er aanwijzingen zijn dat de private sleutel, behorend bij de publieke sleutel van het betreffende services server certificaat, gecompromitteerd is geraakt;

14 de Abonnee verklaart dat het per direct geen gebruik meer zal maken van de private sleutel, behorend bij de publieke sleutel van het betreffende services server certificaat, als de geldigheid van het services server certificaat is verlopen of als het services server certificaat is ingetrokken;

15 de Abonnee verklaart te reageren op instructies van de Digidentity binnen de door de Digidentity gestelde termijn in geval van aantasting van de private sleutel en/of certificaatmisbruik;

16 de Abonnee aanvaardt dat Digidentity gerechtigd is om het certificaat in te trekken indien de abonnee de gebruikersovereenkomst heeft geschonden of Digidentity heeft ontdekt dat het certificaat wordt gebruikt voor criminele activiteiten zoals phishing, fraude en/of het verspreiden van malware;

17 op deze overeenkomst zijn de meest recente versies van de Algemene Voorwaarden en CPS van Digidentity, te vinden op de website van Digidentity, van toepassing. De Abonnee verklaart hierbij dat hij van eerder genoemde stukken kennis heeft genomen en zich met de inhoud daarvan akkoord verklaart;

18 voor het certificaat is een fysieke identiteitscontrole verplicht. Voor de fysieke identiteitscontrole afspraak op het adres van de Abonnee worden er éénmalig administratiekosten van €125,- excl. BTW in rekening gebracht aan de Abonnee. Wanneer de fysieke identiteitscontrole bij Digidentity op kantoor plaatsvindt bedragen de kosten €25,- excl. BTW. De Abonnee informeert Digidentity minimaal 24 uur van te voren over een annulering of een wijziging van de afspraak voor een fysieke identiteitscontrole, anders is Digidentity

gerechtigd om de kosten van de geannuleerde afspraak aan de Abonnee in rekening te brengen naast de kosten van een nieuwe afspraak. Betaling van de factuur dient te geschieden vóór de op de factuur vermelde vervaldatum (veertien dagen na dagtekening);

19 op deze overeenkomst is het Nederlandse recht van toepassing. In het geval van een geschil zal, indien Partijen niet binnen redelijke tijd tot een minnelijke oplossing komen, uitsluitend een bevoegde rechter te Den Haag competent zijn om over het geschil te oordelen;

20 Digidentity conformeert zich aan de huidige versie van de Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates zoals gepubliceerd op https://www.cabforum.org. Mocht er een inconsistentie aanwezig zijn tussen het PKIoverheid Programma van Eisen deel 3b en de betreffende Requirements, waardoor niet tenminste tegemoet wordt gekomen aan de hierin beschreven minimale eisen, dit ter beoordeling door de PA, dan prevaleert het gestelde in de Requirements.

4.2. Verwerken Certificaataanvraag

De abonnee dient, voor verwerking van de certificaataanvraag, de bijbehorende overeenkomst en addendum door abonnee ondertekend aan Digidentity op te sturen.

De abonnee dient een volmacht af te geven voor de Certificaatbeheerder via het formulier Volmacht Certificaatbeheerder en deze aan Digidentity op te sturen.

Voor Persoonlijke Certificaten vindt vervolgens bij de Registration Authority de procedure plaats ter identificatie en authenticatie van de Certificaathouder(s) conform hoofdstuk 3.2 van dit CPS. Hierbij worden de door abonnee ingestuurde formulieren/documenten en accountgegevens gehanteerd.
Voor Systeemcertificaten vindt bij de Registration Authority de procedure plaats ter identificatie en authenticatie van de Certificaatbeheerder conform hoofdstuk 3.2 van dit CPS. Hierbij wordt het door Certificaatbeheerder ingestuurde of in het account ge-upload ID document/gegevens en het door abonnee ingestuurde formulier Volmacht Certificaatbeheerder gehanteerd.

4.3 Certificaatuitgifte

4.3.1 Proces

Voor **Persoonsgebonden certificaten** in het domein Burger en/of Organisatie wordt tijdens de identificatie en authenticatieprocedure met tussenkomst van de Certificaathouder een SSCD gegenereerd.
Aanvullende informatie over de Technische beveiligingsmaatregelen is opgenomen in hoofdstuk 6 van dit CPS.
Voor Services Server certificaten wordt door de Certificaatbeheerder een Certificate Signing Request (CSR) gegenereerd en ingestuurd via het zakelijke account. Deze CSR wordt door de Registration Officer 1 geverifieerd aan de hand van de ingezonden specificaties en vervolgens wordt het Services Server certificaat gegenereerd. Het certificaat kan na goedkeuring van de totale aanvraagprocedure en check van de

vereiste documenten, door de Certificaatbeheerder worden gedownload en worden opgeslagen op een drager. Aanvullende informatie over de Technische beveiligingsmaatregelen is opgenomen in hoofdstuk 6 van dit CPS.

4.3.2 Uitgifte van Services Server certificaten

Voor deze certificaten wordt door de Certificaatbeheerder de certificaat aanvraag (CSR) ingegeven in het zakelijk account, waarbij de private sleutel in eigen beheer is gegenereerd. In plaats van gebruik te maken van een hardware matige private sleutel opslag en generatie mogen de sleutels, van een services certificaat, softwarematig worden beschermd indien compenserende maatregelen worden getroffen in de omgeving van het systeem dat de sleutels bevat. De compenserende maatregelen moeten van een deugdelijke kwaliteit zijn dat het praktisch onmogelijk is de sleutels ongemerkt te stelen of te kopiëren. De compenserende maatregelen zijn verantwoordelijkheid van de abonneeorganisatie. De contactpersoon van de abonnee organisatie ondertekend een overkoepelend contract, waarin bij uitgifte van elke certificaat, wordt aangeven dat compenserende maatregelen dienen te worden getroffen en dat Digidentity het recht heeft een controle uit te voeren naar de getroffen maatregelen.

Digidentity voert de volgende controles uit:
- betreft het een externe domeinnaam;
- worden er geen wildcards gebruikt in de domeinnaam;
- is de abonneeorganisatie de eigenaar van de domeinnaam;
- er wordt telefonische navraag gedaan bij de contactpersoon van de abonneeorganisatie over de juistheid van de aanvraag;
- de identiteitsgegevens van zowel de contactpersoon als de certificaatbeheerder van de abonneeorganisatie worden gecontroleerd. Deze laatste controle vindt plaats doormiddel van een Face-to-Face controle bij de Abonnee op locatie of op het kantoor van Digidentity.

4.3.3 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 en/of voor 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 (SSL-store) van Digidentity en is beschikbaar voor de gebruiker in zijn Digidentity account. 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 het authenticatie/onweerlegbaarheid

certificaat te gebruiken. De private keys zijn alleen in de HSM operationeel en zijn alleen na expliciete toestemming van de gebruiker in staat om een operatie uit te voeren. Toestemming wordt verleend door invoer van de ontvangen geheime eenmalig door de HSM gegenereerde code en door de Abonnee gekozen PIN. Op deze manier is het gegarandeerd dat het gebruik van de private sleutel alleen ter beschikking wordt gesteld aan de geautoriseerde personen.

4.3.4 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 uitgeven door Digidentity, is 1, 2 óf 3 jaar vanaf het moment van uitgifte ÓF tot de maximale geldigheid van het certificaat van de uitgevende CA (Maart 2020). Voor Server certificaten is de geldigheidsduur 1, 2 óf 3 jaar vanaf het moment van uitgifte ÓF tot de maximale geldigheid van het certificaat van de uitgevende CA (Maart 2020).

4.3.5 Validatie van ingetrokken Certificaten

Alle informatie met betrekking tot de uitgifte van certificaten, waaronder met name de informatie over de intrekking van certificaten (Revocation Status Information) is beschikbaar middels de gepubliceerde CRL en middels het Online Certificate Status Protocol (OCSP).

4.4. Acceptatie van Certificaten

Acceptatie van certificaten heeft geacht te hebben plaatsgevonden na afronding van de Certificaatuitgifte.
Voorafgaand aan de acceptatie van het certificaat heeft de abonnee reeds aangegeven via ondertekening van de overeenkomst of de certificaten voor publicatie in de elektronische opslagplaats zijn vrijgegeven. De abonnee geeft daarvoor zijn expliciete toestemming.
Met de acceptatie van het certificaat en het gebruik daarvan gaat de Certificaathouder/de Certificaatbeheerder akkoord met:

- Hetgeen bepaald is in dit CPS
- De Algemene Voorwaarden
- De plicht om (toegang tot) de private sleutel die correspondeert met de publieke sleutel opgenomen in het Certificaat adequaat te beveiligen, het SSCD op een zorgvuldige wijze te gebruiken en om redelijke voorzorgsmaatregelen te treffen om verlies, diefstal, modificatie en/of ongeautoriseerd gebruik van de private sleutel te voorkomen.

De Certificaathouder/Certificaatbeheerder is voorafgaand aan acceptatie van het certificaat gehouden de in het Certificaat opgenomen gegevens te controleren op juistheid. Indien het Certificaat niet geheel accuraat blijkt te zijn dan dient de Certificaathouder/Certificaatbeheerder opnieuw een certificaat aanvraag te doen. Als achteraf blijkt dat de gegevens in het certificaat onjuist zijn dan dient er een verzoek tot

intrekking plaats te vinden. De acceptatie van het Certificaat bevestigt de Abonnee of Certificaathouder middels de afronding van de uitgifte procedure.

4.5 Sleutelpaar en Certificaatgebruik

4.5.1 Verplichtingen van de Certificaathouder

Binnen PKIoverheid mag een Certificaathouder de private sleutel en corresponderende publieke sleutel in het Certificaat alleen gebruiken voor het daartoe bestemde gebruik. Bij acceptatie van het Certificaat gaat de Certificaathouder enerzijds akkoord met de Certificaathouderovereenkomst en stemt anderzijds daarmee in het Certificaat te gebruiken op een manier die overeenkomt met de in het Certificaatprofiel opgenomen Key-Usage field extensions.

De gebruiker garandeert dat;

1. de gegevens zoals overgenomen van het Identiteitsbewijs in het Certificaat te allen tijde juist en volledig zijn;
2. bij wijzigingen in de gegevens deze wijziging zo spoedig mogelijk wordt verwerkt door de informatie in het account aan te passen;
3. het Certificaat wordt gebruikt in overeenstemming met de toepasselijke wet- en regelgeving (zoals onder andere; privacywetgeving, het Burgerlijk Wetboek, Telecommunicatie wetgeving);
4. het Certificaat gebruikt wordt overeenkomstig het bepaalde in dit CPS, de Algemene Voorwaarden en de overeenkomsten waarvan dit CPS deel kan uitmaken en die met dit CPS verband houden;
5. het in dit CPS en in de contractuele afspraken, waarvan dit CPS deel kan uitmaken, bepaalde deugdelijk door de certificaathouder(s) wordt nageleefd;
6. er redelijke zorg uitgeoefend wordt tegen onbevoegd gebruik van zijn of haar privé-sleutel;
7. 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 (doormiddel van gebruikersnaam /wachtwoord of PUK brief), en/of
    c. onjuistheid of wijzigingen in de inhoud van het certificaat, zoals gemeld aan de abonnee;
8. gebruiker delegeert alleen een SSCD aan organisaties die additionele maatregelen nemen zodat SSCD's met secondary credentials alleen voor het doel waarvoor zij zijn gedelegeerd worden ingezet, bijvoorbeeld; 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 allen 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 communicatiesystemen, 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:

1. zo spoedig mogelijk na beëindiging van het dienstverband het certificaat wordt ingetrokken;
2. machtigingen conform verleende bevoegdheden worden uitgereikt en tijdig worden ingetrokken;
3. 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;
4. 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;
5. hij additionele maatregelen neemt zodat SSCD's alleen voor het doel waarvoor zij zijn gedelegeerd worden ingezet;
6. voor Services Server certificaten wordt door de certificaatbeheerder de certificaat aanvraag aangeleverd waarbij de private sleutel in eigen beheer is gegenereerd. In plaats van gebruik te maken van een hardware matige private sleutel opslag en generatie mogen de sleutels van een services certificaat softwarematig worden beschermd indien compenserende maatregelen worden getroffen in de omgeving van het systeem dat de sleutels bevat. De compenserende maatregelen moeten van een dusdanige kwaliteit zijn dat het praktisch onmogelijk is de sleutels ongemerkt te stelen of te kopiëren. De compenserende maatregelen is voor verantwoordelijkheid van de abonneeorganisatie.

4.5.2 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 dient 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 gestelde 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 allen tijde eigendom van Digidentity. De gebruiker verkrijgt slechts het recht het Certificaat, tezamen met het sleutelpaar, te gebruiken conform de gestelde eisen in dit CPS.

4.5.3 Verplichtingen van 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:

1. de geldigheid zoals deze blijkt uit het certificaat is geverifieerd;
2. de volledige keten van certificaten tot aan het stamcertificaat van de Staat der Nederlanden geldig is;
3. het Certificaat niet is ingetrokken, te raadplegen in de CRL of via het OCSP-protocol;
4. kennis genomen is van de beperkingen betreffende het gebruik van het Certificaat zoals vermeld in dit CPS;
5. 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.

4.5.4 Verplichtingen van Digidentity

Alle - in het kader van dit CPS en de overeenkomsten waarvan dit CPS deel uitmaakt - door Digidentity verrichte werkzaamheden worden voortvarend, met inachtneming van de procedures die van toepassing zijn en conform de relevante wet- en regelgeving uitgevoerd. Digidentity conformeert zich tevens aan het 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 EN 319 411-1, ETSI EN 319 411-2 en de Richtlijn nr. 1999/93/EG. Deze richtlijnen worden ook in acht genomen wanneer Digidentity, als onderdeel van haar dienstverlening, een AuSO als derde partij inschakelt.

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.

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 gecertificeerde instelling die kan aantonen dat Digidentity en de door haar ingeschakelde entiteiten voldoen aan de gestelde eisen. De conformiteit aan de gestelde eisen wordt aangetoond doormiddel van de certificering. Tevens is Digidentity verantwoordelijk voor het niveau en kwaliteit van de beschikbaar gestelde middelen.

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 dit CPS.

4.5.5 Certificaat hiërarchie

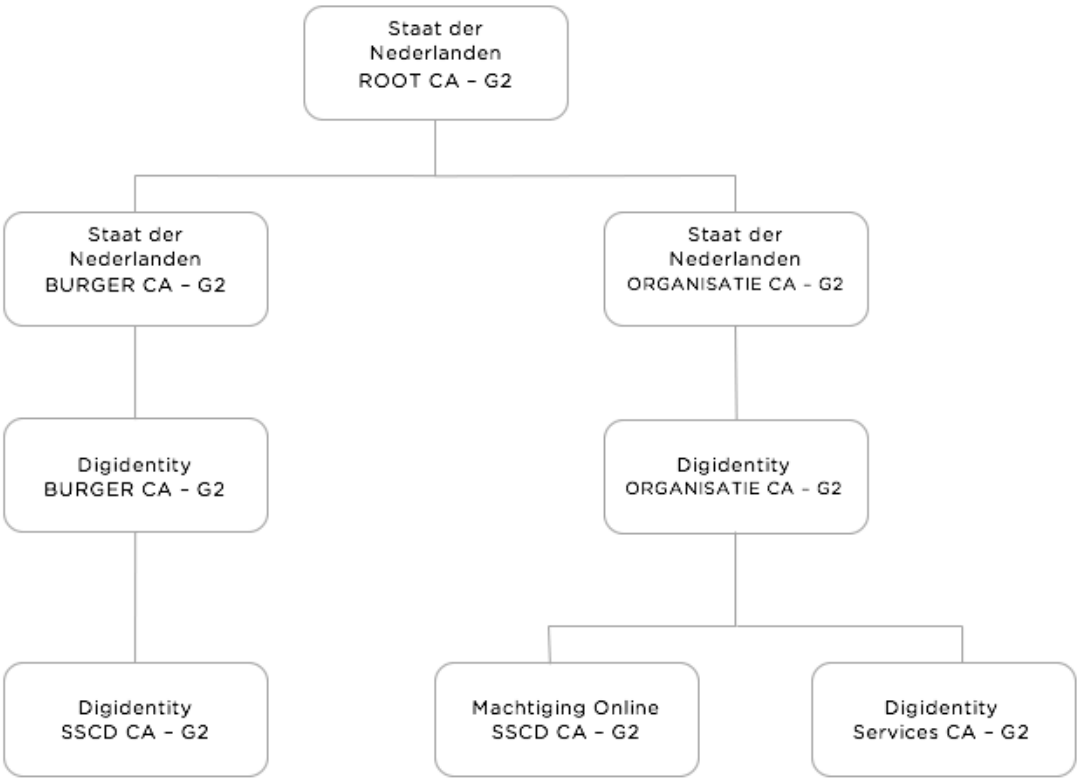
De Certificaten worden niet onmiddellijk door het Nederlandse stamcertificaat getekend. De Public Key Infrastructuur van Nederland is geïmplementeerd in een 'four-level certification hierarchy'.

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
TSP	3
Domein Organisatie	3 in domein burger 5 in domein organisatie
Digidentity	2 in domein burger 8 in domein organisatie

OID voor Digidentity
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



Figuur 1.1: Overzicht van de certificaat policies CA - G2

4.6 Certificaatvernieuwing

Certificaatvernieuwing zonder verandering van de publieke sleutel die in het Certificaat is opgenomen wordt onder dit CPS niet door Digidentity ondersteund. Een nieuw Certificaat is altijd gebaseerd op een nieuw sleutelpaar.

4.7 Certificaat Re-Key

Voorafgaand aan het verstrijken van de geldigheidsduur van certificaten, wordt de Certificaathouder hiervan in kennis gesteld en dienen nieuwe certificaten te worden uitgegeven conform de initiële uitgifte procedure.

4.8 Certificaat Aanpassing

Noodzakelijke aanpassingen in de inhoud van een Certificaat, leidt tot de uitgifte van een nieuw certificaat conform de procedure voor een in initiële uitgifte.

4.9 Procedure voor een verzoek tot intrekking

De Abonnee of de certificaathouder kan zelf een certificaat intrekken via de Digidentity website.

4.9.1 Omstandigheden die leiden tot intrekking

De volgende omstandigheden leiden tot intrekking van een Certificaat:

- Wettelijk voorschrift;
- Bij verlies of mogelijke diefstal van de PUK code;
- Bij verlies of mogelijke diefstal van de mobiele telefoon;
- Bij verlies of mogelijke diefstal van de SIM kaart;
- Het certificaat is niet meer correct, de kwalificaties/gegevens zijn niet meer juist;
- Bij compromittering van de private sleutel;
- Wanneer de Abonnee aangeeft dat het oorspronkelijke verzoek voor een certificaat niet was toegestaan en met terugwerkende kracht ook geen toestemming verleent;
- Wanneer de Abonnee niet aan zijn verplichtingen voldoet zoals verwoord in dit CPS en het bijbehorende contract;
- Wanneer Digidentity op de hoogte wordt gesteld of anderszins zich bewust wordt van een wezenlijke verandering in de informatie die in het certificaat staat;
- Wanneer Digidentity bepaalt dat het certificaat niet is uitgegeven in overeenstemming met dit CPS;
- Wanneer Digidentity bepaalt dat de informatie in het certificaat niet juist of misleidend is;
- Wanneer Digidentity haar werkzaamheden staakt en de CRL en OCSP dienstverlening niet wordt overgenomen door een andere TSP;

- Wanneer de PA van PKIoverheid vaststelt dat de technische inhoud van het certificaat een onverantwoord risico met zich meebrengt voor abonnees, vertrouwende partijen en derden (b.v. browserpartijen);
- Wanneer Digidentity beschikt over voldoende bewijs dat de private sleutel van de Abonnee (die overeenkomt met de publieke sleutel in het certificaat) is aangetast of wanneer er het vermoeden is van compromittering, of er sprake is van inherente beveiligingszwakheid, of dat het certificaat op een andere wijze is misbruikt. Een sleutel wordt als aangetast beschouwd in geval van ongeautoriseerde toegang of vermoede ongeautoriseerde toegang tot de private sleutel, verloren of vermoedelijk verloren private sleutel, SSCD of SUD, gestolen of vermoedelijk gestolen sleutel, SSCD of SUD of vernietigde sleutel of SUD;
- Wanneer Digidentity op de hoogte wordt gesteld of anderszins zich bewust wordt dat het gebruik van de domeinnaam in het certificaat niet langer wettelijk toegestaan is (b.v. door een uitspraak van een rechter);
- Wanneer Digidentity op de hoogte wordt gesteld of anderszins zich bewust wordt van een wezenlijke verandering in de informatie, die in het certificaat staat. Voorbeeld daarvan is: verandering van de naam van de certificaathouder (service);
- Wanner de Abonnee een “code signing” certificaat gebruikt om “hostile code” (waaronder spyware, malware, trojans etc.) digitaal te ondertekenen.

Specifieke omstandigheden bij een Services Server Certificaat:

Wanneer Digidentity op de hoogte wordt gesteld of anderszins zich bewust wordt dat het gebruik van de domeinnaam in het certificaat wettelijk niet langer is toegestaan.

4.9.2 Intrekkingsbevoegdheid

Onderstaande personen zijn bevoegd om een certificaat in te trekken.

- de gebruiker of zijn wettelijke vertegenwoordiger;
- een door de certificaathouder vertegenwoordigde derde waarvan de vertegenwoordiging blijkt uit een afgegeven machtiging in machtiging online;
- de abonnee;
- Digidentity
- ieder andere, naar het oordeel van dit TSP, belanghebbende partij/persoon.

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 de intrekking verzorgt dient hij of zij hierbij de reden van intrekking te vermelden. Het intrekken van een certificaat gebeurt te allen tijde binnen 4 uur.

Bij een compromittering van de CA zullen alle uitstaande certificaten worden ingetrokken door Digidentity.

4.9.3 Procedure voor een verzoek tot intrekking

De reden van intrekking wordt door Digidentity vastgelegd. Zie hoofdstuk 3.4. Digidentity maakt gebruik van een OCSP en CRL om de certificaatstatus informatie beschikbaar te stellen.

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.

Relatie tussen de verschillende CA domeinen

Alle RA functionarissen zijn in bezit van eigen Digidentity organisatie certificaten.

Alle gebruikers hebben een account van Digidentity.

4.9.4 Tijdsduur voor verwerking intrekkingsverzoek

De maximale vertraging tussen de ontvangst van een intrekkingsverzoek of intrekkingsrapportage en de wijziging van de revocation status information is gesteld op 4 uur.

4.9.6 Controlevoorwaarden bij raadplegen certificaat statusinformatie

Een eindgebruiker die de certificaat statusinformatie raadpleegt, dient de authenticiteit van deze informatie te verifiëren door de elektronische handtekening waarmee de informatie is getekend en het bijbehorende certificatiepad te controleren.

4.9.7 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 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 direct na intrekken van het certificaat 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 7 jaar, ook na afloop van de geldigheid, op de CRL vermeld.

4.9.8 Online intrekkings-/statuscontrole beschikbaarheid

Naast de CRL raadpleging is de status van het certificaat te controleren via het OCSP. Voor de informatie op het OCSP gelden dezelfde beschikbaarheid en actualiteit als voor de CRL.

De geldigheid van een PKIoverheid certificaat moet door een vertrouwende partij online gecontroleerd worden, gebruik makend van de CRL of van het Online Certificate Status Protocol. OCSP is ingericht conform RFC 2560. Responses worden digitaal ondertekend door de private sleutel van de Digidentity TSP-CA , ofwel door een door de Digidentity gehanteerde OCSP-responder die beschikt over een OCSP-Signing Certificaat dat voor dit doel is uitgegeven door de Digidentity TSP-CA.

Digidentity maakt bij OCSP geen gebruik van zogenaamde precomputed responses.
De OCSP service wordt tenminste één keer in de vier kalenderdagen bijgewerkt. De maximale vervaltermijn van het OCSP response is tien kalenderdagen.
Voor de informatie op het OCSP gelden dezelfde standaarden voor actualiteit en betrouwbaarheid als voor de CRL, zoals in dit CPS beschreven
Certificaat status informatie is bovendien ten minste zes maanden beschikbaar na het tijdstip waarop de geldigheid van het Certificaat is verlopen of, indien dat tijdstip eerder valt, na het tijdstip waarop de geldigheid door intrekking is beëindigd.

4.9.9 Omstandigheden die leiden tot opschorting

Digidentity ondersteunt bij haar dienstverlening binnen de PKI overheid geen opschorting of schorsing van certificaten.

4.10 Certificaatstatus diensten

De status van certificaten, uitgegeven binnen PKIoverheid, zijn gepubliceerd in een CRL of worden beschikbaar gesteld door middel van het OCSP.

4.11 Beëindiging van dienstverlening aan abonnee

De certificatiedienstverlening activiteiten van Digidentity kunnen, met in achtneming van de wettelijke bepalingen, eenzijdig door Digidentity worden stopgezet. Een voorgenomen stopzetting wordt, tenminste 2 maanden vóór de stopzetting, aan zowel de ACM, Logius en 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 ACM) geregistreerde dienstverlener worden overgenomen. Ingeval de activiteiten niet door een andere certificatiedienstverlener worden overgenomen, worden alle uitgegeven certificaten ingetrokken.

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 allen tijde voldoende financiële middelen veiliggesteld om na beëindiging van de dienstverlening aan deze verplichting te voldoen. Deze zekerheid wordt verkregen door deze contractuele verplichting aan een derde partij over te dragen.

4.12 Sleutelbewaring en herstel (escrow)

Digidentity geeft haar TSP-CA sleutels niet in escrow uit bij een onafhankelijke derde. Key recovery diensten voor het terug halen van private decryptiesleutels van eindgebruikers worden door Digidentity onder dit CPS niet aangeboden.

5 Management, operationele en fysieke beveiligingsmaatregelen

5.1 Fysieke en Technische beveiliging

5.1.1 Infrastructuur

De infrastructuur van de informatiebeveiliging, die nodig is voor het beheren van de beveiliging binnen Digidentity, zal te allen tijde in stand worden gehouden, elke verandering die van invloed kan zijn op het beveiligingsniveau dient te worden goedgekeurd door het Digidentity managementteam. De beheersmaatregelen gericht op beveiliging en de operationele procedures voor Digidentity faciliteiten, systemen en informatiemiddelen waarmee de certificatiediensten worden geleverd, zijn gedocumenteerd, geïmplementeerd en worden onderhouden.

5.1.2 Logs en Protocollen
Zie ook 5.4.2

De volgende gebeurtenissen worden automatisch met datum en tijd gelogd:

- alle gegevens relevant voor het aanmelden van een gebruiker in het systeem;
- alle gegevens van authenticatie via het systeem;
- de generatie van CA sleutelparen;
- alle gebeurtenissen relevant bij het registratieproces van een Certificaat;
- alle gegevens relevant voor de publicatie van de Digitale Certificaten;
- alle gegevens relevant voor de publicatie van intrekkingslijsten;
- alle herroeping details van een Certificaat, inclusief de reden van intrekking;
- alle netwerkverkeer van en naar vertrouwde machines;

Daarnaast worden de volgende gebeurtenissen onder protocol gebracht:

- verandering in de rolverdeling;
- melding van verdenking van sleutelmisbruik;
- melding van incidenten;
- alle gebeurtenissen relevant bij beheer van de beveiligde omgeving;
- alle wijzigingen in de configuratie van de back-up;
- alle gebeurtenissen relevant bij het back-upproces;
- alle aspecten van de installatie van nieuwe of bijgewerkte software;
- alle aspecten van hardware updates;
- 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.

5.1.3 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.

5.1.4 Netwerk technische 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.

Digidentity beheert en implementeert op passende wijze de fysieke beveiligingsmaatregelen om toegang tot de hardware en software, gebruikt voor de CA-operaties, te beperken.

5.1.5 Vestigingslocatie operationele CA-dienstverlening

Digidentity voert haar operationele CA-diensten uit vanaf beveiligde datacenters, gevestigd in een gebouwencomplex te Amsterdam en Rotterdam. Deze datacenters houden zich aan de strikte regels en hoge beveiligingsstandaarden opgesteld door een onafhankelijk gecertificeerde partij. Beide datacenters zijn ISO 27001:2013 gecertificeerd.

5.1.6 Fysieke toegang

Digidentity staat fysieke toegang tot haar beveiligde operationele omgeving enkel toe aan daartoe bevoegde personen. De fysieke verplaatsingen van personen binnen de beveiligde omgeving worden opgeslagen in een log-file en worden periodiek geëvalueerd. Fysieke toegang tot de beveiligde omgeving wordt gecontroleerd door een combinatie van toegangspassen en biometrische identificatie.

5.1.7 Afval verwerking

Papieren documenten en magnetische media welke vertrouwelijke Digidentity of commercieel gevoelige informatie bevatten, worden beveiligd vernietigd door middel van:
In het geval van magnetische media:

- Toebrengen van onherstelbare fysieke schade of gehele vernietiging van de betreffende informatiedrager;
- Gebruik van een daarvoor geschikt apparaat voor het wissen of overschrijven van de informatie.

In het geval van gedrukte informatie, wordt het document versnipperd of vernietigd op een daarvoor geschikte wijze.

5.1.8 Externe back-up

Een externe locatie wordt gebruikt voor de opslag van back-up software en data. De externe locatie:

- is 24 uur per dag en 7 dagen per week beschikbaar voor geautoriseerd personeel, met als doel het terughalen van software en data;
- beschikt over adequate fysieke beveiligingsmaatregelen (software en data zijn bijvoorbeeld opgeslagen in vuurvaste kluizen en de opslag bevindt zich achter deuren met toegangscontrole, in een omgeving die alleen toegankelijk zijn voor daartoe geautoriseerd personeel).

5.2 Procedurele Beveiliging

5.2.1 Vertrouwelijke rollen

Alle medewerkers van Digidentity hebben een vertrouwelijke rol. Om zeker te stellen dat een enkel persoon de beveiliging niet kan omzeilen, zijn de verantwoordelijkheden verdeeld over meerdere rollen en personen. Dit is onder andere bewerkstelligd door het creëren van separate rollen en accounts op de verschillende componenten van het CA-systeem en elke rol heeft daarbij beperkte autorisaties. Toezicht kan alleen worden uitgevoerd door een persoon die niet direct betrokken is bij de uitgifte van certificaten (bijvoorbeeld een Security Officer die systeem records of audit logs bekijkt om zeker te stellen dat andere personen handelen binnen diens verantwoordelijkheden en binnen het toepasselijke beveiligingsbeleid).
De toepasselijke rollen zijn:

- **Certification Authority Officers** die verantwoordelijk zijn voor CA hardware en software en de generatie en ondertekening van uitgifte CA sleutels.
- **Registration Authority Officers** die verantwoordelijk zijn voor het verrichten van functies van de Registration Authority en de interface met Digidentity.
- **Digidentity Security Officer** die verantwoordelijk is voor het verifiëren van de integriteit van de Digidentity TSP-CA en de configuratie en operations daarvan.
- **Auditor** die verantwoordelijk is voor het houden van toezicht en het geven van een onafhankelijk oordeel over de wijze waarop de bedrijfsprocessen zijn ingericht en over de wijze waarop aan de eisen ten aanzien van de betrouwbaarheid wordt voldaan.
- **Systeembeheerder** die verantwoordelijk is voor het beheer van de Digidentity systemen, inclusief het installeren, configureren en onderhouden van de systemen.

Digidentity heeft functiescheidingen ingericht tussen medewerkers die de uitgifte van een certificaat controleren en medewerkers die de uitgifte van een certificaat goedkeuren.

5.2.2 Aantal personen vereist per operationele handeling

Er zijn tenminste twee personen toegewezen per vertrouwelijke rol om altijd adequate ondersteuning te waarborgen, met uitzondering van de interne Auditor rol. Sommige rollen zijn toegewezen aan verschillende personen om ervoor te zorgen dat er geen belangenverstrengelingen kan optreden. Tevens om de mogelijkheid tot abusievelijke of bewuste compromittering van enig component van de CA infrastructuur te voorkomen met name de private sleutel van de Digidentity TSP-CA.

CA-sleutelpaargeneratie en initialisatie vereist per geval de actieve participatie van ten minste twee Vertrouwelijke Rollen. Dergelijk gevoelige handelingen vereisen tevens de actieve participatie en toezicht van hoger management.

5.2.3 Identificatie en authenticatie voor elke rol

Elk individu dat een van de vertrouwelijke rollen vervult, gebruikt een door Digidentity uitgegeven certificaat, opgeslagen op een SSCD, teneinde zichzelf voor operationele handelingen te identificeren aan de diverse systemen die gebruikt worden voor het uitgeven en beheren van PKIoverheid certificaten.

5.2.4 Risico analyse

Digidentity voert minimaal jaarlijks een risicoanalyse uit. Wanneer PA hier opdracht toe geeft, of op advies van het NCSC voert Digidentity de risicoanalyse opnieuw. Op basis van deze analyse ontwikkeld Digidentity een informatiebeveiligingsplan, implementeert, onderhoudt, handhaaft en evalueert deze.

De risicoanalyse raakt alle PKIoverheid processen die onder de verantwoordelijkheid van Digidentity vallen.

Dit plan beschrijft een samenhangend geheel van passende administratieve, organisatorische, technische en fysieke maatregelen alsmede procedures waarmee Digidentity de beschikbaarheid, exclusiviteit en integriteit van alle PKIoverheid processen (aanvragen en de gegevens die daarvoor worden gebruikt) waarborgt.

5.2.5 Audits

Naast een (externe) audit uitgevoerd door een geaccrediteerd auditor kan zo nodig Digidentity een audit uitvoeren bij zijn externe leveranciers van PKIoverheid kerndiensten. Om er zeker van te zijn dat deze leveranciers de relevante eisen van het PVE van PKIoverheid conform de wensen van Digidentity en rekening houdend met zijn bedrijfsdoelstellingen, -processen en -infrastructuur hebben geïmplementeerd en geoperationaliseerd.
Digidentity is vrij in de keuze om zelf een eigen audit uit te (laten) voeren dan wel gebruik te gaan maken van reeds bestaande audit resultaten zoals die van de formele certificeringsaudits, de diverse interne en externe audits, Third party mededelingen (TPM's) en compliancy rapportages.
Digidentity is gerechtigd om inzage te verkrijgen in het onderliggende bewijsmateriaal zoals audit dossiers en overige, al dan niet systeem-, documentatie.
Uiteraard beperkt zich het bovenstaande tot de bij de leveranciers gehoste Digidentity, -systemen en –infrastructuur voor PKIo kerndiensten.

5.3 Personele Beveiliging

5.3.1 Geheimhoudingsverklaring

Het openbaar worden van vertrouwelijke informatie kan grote gevolgen hebben voor (onder andere; de betrouwbaarheid van) Digidentity. Om het vertrouwelijk houden en behouden van deze informatie, laat Digidentity al haar werknemers, en ingehuurde derden, een geheimhoudingsverklaring tekenen.

5.3.2 Antecedentenonderzoek

Voor het inschakelen van een persoon, bij één of meerdere kerndiensten van PKIoverheid, verricht Digidentity, of een externe leverancier die een deel van deze werkzaamheden, een controle uit naar identiteit en de betrouwbaarheid van deze werknemer.
De personen die de Vertrouwelijke Rollen vervullen moeten een toepasselijke screening procedure hebben ondergaan. De Vertrouwende Rollen in Nederland beschikken over een Verklaring omtrent het Gedrag (VOG) van het ministerie van Veiligheid en Justitie. Digidentity is niet aansprakelijk voor het gedrag van werknemers dat buiten de uitoefening van de functie ligt en waarover Digidentity derhalve geen controle heeft, inclusief, maar niet beperkt tot (bedrijfs-)spionage, sabotage en misdadig gedrag.

5.3.3 Vakkennis, ervaring en kwalificaties

Digidentity biedt haar werknemers professionele en on-the-job training aan om de geschikte en vereiste niveaus van competentie te onderhouden en om de verantwoordelijkheden van de functie uit te voeren.

Alvorens tot uitgifte van services server certificaten kan worden overgegaan heeft Digidentity:

- al het personeel dat zich bezighoudt met het controleren en goedkeuren van een services server certificaat een training laten ondergaan waarbij algemene kennis over PKI, authenticatie en verificatie policies en procedures met betrekking tot het controle- en goedkeuringsproces en dreigingen waaronder phishing en andere social engineering tactieken, aan bod komen;
- al het personeel een intern examen afgenomen dat succesvol moet worden afgerond;
- een administratie bijgehouden van de training(en) en het examen en kan Digidentity waarborgen dat de vaardigheden van het betreffende personeel op het juiste niveau blijft.

Ongeautoriseerde handelingen van het personeel kan resulteren in het opleggen van disciplinaire maatregelen door het Management van Digidentity. De noodzaak tot het opleggen van deze maatregelen en de inhoud ervan wordt per incident vastgesteld door het management.

Digidentity voorziet haar personeel van alle benodigde handleidingen, procedurebeschrijvingen en trainingsmaterialen die nodig zijn om de functie en rol te kunnen vervullen.

5.4 Procedures ten behoeve van beveiligingsaudits

5.4.1 Vastleggen van gebeurtenissen

De diverse soorten data die door Digidentity worden geregistreerd omvatten, maar zijn niet beperkt tot;

- Routers, firewalls en netwerk systeem componenten;
- Database activiteiten en events;
- Transacties;
- Operating systemen;
- Access control systemen;
- Mail servers.

Digidentity legt de volgende events vast:

- CA key life cycle management;
- Certificate life cycle management;
- Bedreigingen en risico's zoals:
    - Succesvolle en niet succesvolle aanvallen op het PKI systeem;
    - Activiteiten van medewerkers op het PKI systeem;
    - Lezen, schrijven en verwijderen van gegevens;
    - Profiel wijzigingen (Access Management);
    - Systeem uitval, hardware uitval en andere abnormaliteiten;
    - Firewall en router activiteiten;
    - Betreden van en vertrekken uit de ruimte van de CA.

Daarnaast wordt het volgende geregistreerd:

- Bron adressen (IP adressen indien voorhanden);
- Doel adressen (IP adressen indien voorhanden);
- Tijd en datum;
- Gebruikers ID's (indien voorhanden);
- Naam van de gebeurtenis;
- Beschrijving van de gebeurtenis.

5.4.2 Bewaartermijn van audit logs

Digidentity bewaart logbestanden voor gebeurtenissen met betrekking tot:

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

Logs worden voor 7 jaar en worden daarna verwijderd.

Digidentity bewaart logbestanden voor gebeurtenissen met betrekking tot:

- Bedreigingen en risico's;

Logs worden voor 18 maanden en worden daarna verwijderd.

De logbestanden zijn zodanig opgeslagen, dat de integriteit en toegankelijkheid van de data gewaarborgd is.

5.5 Archivering van documenten

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

- de logging van het authenticatie proces;
- de logging van de levenscyclus van het Certificaat;
- de logging van het gebruik van de private sleutels;
- de logging van de mutaties in de registratie informatie.

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

- audit logs;
- certificaataanvragen en alle daaraan gerelateerde handelingen en formulieren;
- inhoud van uitgegeven Certificaten;
- bewijs van Certificaatacceptatie en ondertekende overeenkomsten
- intrekkingsverzoeken en alle gerelateerde handelingen en vastleggingen;
- gepubliceerde intrekkingslijsten van certificaten;
- auditbevindingen zoals besproken binnen dit CPS.

De archieven worden adequaat beschermd tegen modificatie of vernietiging. Tevens wordt dit systeem uitsluitend gebruikt als intern systeem De toegang tot het archief is beperkt. Het gehele systeem is alleen voor CA medewerkers, de Digidentity Chief Security Officer en auditoren inzichtelijk. De inhoud van de archieven wordt alleen in diens geheel vrijgegeven wanneer dit een vereiste is op basis van, wet- en regelgeving, op last van een rechtelijk bevel of door een andere (juridische bevoegde) instantie. Digidentity kan beslissen om logging van individuele transacties vrij te geven, wanneer de abonnee of diens vertegenwoordigers hierom vragen. Een redelijke tegemoetkoming in de administratieve kosten per verzoek wordt hiervoor in rekening gebracht.

Digidentity handhaaft en implementeert back-up procedures als zodanig dat, in het geval van het verlies of de vernietiging van de primaire archieven, per direct een volledige reeks reserve-exemplaren beschikbaar is.
Digidentity ondersteunt timestamping voor al haar gegevens. Alle gelogde gebeurtenissen die binnen de dienstverlening van Digidentity worden vastgelegd omvatten de datum en het tijdstip van het moment waarop de gebeurtenis plaatsvond. Deze datum en tijd zijn gebaseerd op de systeemtijd waarop het Digidentity TSP-CA systeem werkt. Digidentity gebruikt procedures om te waarborgen dat alle systemen die binnen de PKIoverheid omgeving operationeel zijn, vertrouwen op een betrouwbare tijdbron.

5.6 Wijziging van de publieke sleutel

De wijziging van de publieke sleutel van de CA gebeurt aan de hand van een daarvoor opgestelde procedure. Tegen het eind van de levensduur van de CA private sleutel, stopt Digidentity het gebruik van deze private sleutel voor het ondertekenen van publieke sleutels en gebruikt de expirerende private sleutel uitsluitend nog om CRL's en OSCP-responder Certificaten, verbonden met die private sleutel, te ondertekenen.
Er wordt een nieuw CA signing sleutelpaar uitgegeven en vervolgens worden alle vanaf dat moment uitgegeven Certificaten en CRL's ondertekend met de nieuwe private sleutel.

5.7 Compromitteren en Continuïteit

Een securitry breach binnen PKIoverheid is "een inbreuk op de TSP kerndiensten". Te weten; registration service, certificate generation service, subject device provisioning service, dissemination service, revocation management service en revocation status service. Dit is in ieder geval, maar niet limitatief:

- het ongeoorloofd uitschakelen of onbruikbaar maken van een kerndienst;
- ongeautoriseerde toegang tot een kerndienst t.b.v. het afluisteren, onderscheppen en of veranderen van berichtenverkeer;
- ongeautoriseerde toegang tot een kerndienst t.b.v. het ongeoorloofd verwijderen, wijzigen of aanpassen van computergegevens.

Digidentity stelt de PA, het NCSC en de auditor onmiddellijk op de hoogte van een security breach en/of calamiteit, na analyse en vaststelling en houdt de PA, het NCSC en de auditor van het verdere verloop op de hoogte.

Digidentity informeert de PA onmiddellijk over de risico's, gevaren of gebeurtenissen die op enigerlei wijze de betrouwbaarheid van de dienstverlening en/of het imago van de PKI voor de overheid kunnen bedreigen of beïnvloeden. Hieronder vallen in ieder geval ook, maar niet uitsluitend, security breaches en/of calamiteiten met betrekking tot andere, door Digidentity uitgevoerde, PKI diensten, niet zijnde PKIoverheid.

Digidentity heeft een Business Continuity Plan (BCP) opgesteld voor minimaal de kerndiensten dissemination service, revocation management service en revocation status service met als doel, in het geval zich een security breach of calamiteit voordoet, het informeren en redelijkerwijs beschermen en continueren van onze dienstverlening ten behoeve van abonnees, vertrouwende partijen en derden (waaronder browserpartijen). Digidentity test jaarlijks, beoordeelt en actualiseert het BCP jaarlijks. De gestelde eisen aan inwerkingtreding;

- noodprocedure/uitwijkprocedure;
- eisen aan het herstarten onze dienstverlening;
- onderhoudsschema en testplan welke voorziet in het jaarlijks testen, beoordelen en actualiseren van het BCP;
- bepalingen over het onder de aandacht brengen van het belang van business continuity;
- taken, verantwoordelijkheden en bevoegdheden van betrokken actoren;

- beoogde hersteltijd oftewel Recovery Time Objective (RTO);
- vastleggen van de frequentie van back-ups van kritische bedrijfsinformatie en software;
- vastleggen van de afstand van de uitwijkfaciliteit tot de hoofdvestiging van Digidentity;
- het vastleggen van procedures voor het beveiligen van de faciliteiten gedurende de periode na een security breach of calamiteit en voor de inrichting van een beveiligde omgeving bij de hoofdvestiging of de uitwijkfaciliteit.

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

Wanneer Digidentity genoodzaakt is de dienstverlening te beëindigen, dan zullen de negatieve gevolgen van deze beëindiging tot een minimum worden beperkt.
Digidentity specificeert de procedures die worden gevolgd bij het beëindigen van het leveren van certificaatdiensten. De procedures moeten minimaal tot doel hebben:

- dat iedere vorm van onderbreking, veroorzaakt door de beëindiging van de Digidentity certificatiedienstverlening, tot een minimum is beperkt;
- dat gearchiveerde documenten van Digidentity worden behouden;
- dat er onmiddellijke berichtgeving wordt verstrekt aan abonnees; Certificaathouders, vertrouwende partijen en andere relevante partijen binnen de PKI voor de overheid;
- dat het intrekkingsproces van alle certificaten die zijn uitgegeven door Digidentity, ten tijde van beëindiging operationeel blijft;
- relevante overheidsinstanties, waaronder de PA PKIoverheid, in het kader van toepasselijke wet- en regelgeving, op de hoogte te stellen.

Indien mogelijk wordt de intrekking van certificaten gepland in samenhang met de geplande uitgifte van nieuwe certificaten door een TSP die de activiteiten van Digidentity binnen de PKI voor de overheid overneemt.
Indien mogelijk dient de TSP die de activiteiten van Digidentity binnen de PKI voor de overheid overneemt gelijksoortige procedures, richtlijnen en verplichtingen te hanteren als die Digidentity hanteerde. De TSP die de activiteiten van Digidentity binnen de PKI voor de overheid overneemt dient verder certificaten uit te geven aan alle Certificaathouders wiens certificaten zijn ingetrokken. Dit kan met zich meebrengen dat de abonnee en de Certificaathouders zich in de opvolgende situatie zich dienen te conformeren aan de procedures en vereisten van de nieuwe TSP. De nieuwe TSP draagt in elk geval zorg voor het gedurende zes maanden beschikbaar stellen van de certificaat status informatie, het operationeel houden van de revocatie management dienst (intrekkingsfaciliteit) en het bewaren van de gearchiveerde documenten inzake registratie.

6 Technische beveiligingsmaatregelen

6.1 Generatie en installatie van het sleutelpaar

6.1.1 Sleutelpaar generatie

De sleutel van de Digidentity TSP-CA is gegenereerd en opgeslagen binnen een cryptografische module (HSM) die minimaal voldoet aan de standaarden FIPS 140-2 level 3 en/of Common Criteria EAL4 AUGMENTED (EAL4+). De sleutels voor de autoriserende Registratie Officers worden gegenereerd op een Signature Creation Device (SSCD), een veilig middel voor het genereren van een elektronische handtekening.
Het sleutelmateriaal voor Systeemcertificaten wordt gegenereerd door de Certificaatbeheerder.

6.1.2 Levering van de private sleutel aan de certificaathouder

De private sleutel die op een SSCD gegenereerd is, blijft te allen tijde in de met een PIN beveiligde omgeving op het SSCD opgeslagen. Dit is het geval voor de Persoonlijk- en Systeem certificaten voor authenticatie en vertrouwelijkheid.

De private sleutel van de certificaathouder wordt geleverd aan de certificaathouder, indien van toepassing via de abonnee, op een zodanige wijze dat de vertrouwelijkheid en integriteit van de sleutel niet kan worden aangetast en, eenmaal geleverd aan de certificaathouder, alleen de certificaathouder toegang heeft tot zijn private sleutel.

6.1.3 Levering van een publieke sleutel aan Digidentity

Publieke sleutels voor Persoonlijke en Systeemcertificaten die binnen een SSCD worden gegenereerd, worden door middel van een PKCS#10 request ter certificatie aangeboden aan de Digidentity TSP-CA. Publieke sleutels voor Systeemcertificaten (SSL) die niet binnen de SSCD, maar op locatie worden gegenereerd, moeten worden aangeleverd op een veilige en betrouwbare manier, zoals door middel van een Certificate Signing Request (PKCS#10).

6.1.4 Distributie CA publieke sleutel aan vertrouwde partijen

De publieke sleutels van de Digidentity TSP-CA binnen de PKI voor de overheid, alsmede de Domein CA en de Root CA van de Staat der Nederlanden worden op de SSCD vastgelegd. De Root CA van de Staat der Nederlanden is als stamcertificaat van de PKI voor de Overheid opgenomen in de populaire browsers en/of in de besturingssystemen.

6.1.5 Sleutellengte

De Digidentity TSP-CA maakt gebruik van een 4.096 bit sleutellengte op basis van sha256WithRSAEncryption.
De Persoonlijke en Systeemcertificaten maken gebruik van minimaal 2048 bits sleutels op basis van sha256WithRSAEncryption
Voor de overige informatie over de uitgegeven certificaten verwijzen wij naar de certificaatprofielen, die zijn opgenomen in hoofdstuk 7.

De lengte van de cryptografische sleutels van de certificaathouders voldoen aan de eisen, die daaraan zijn gesteld in de lijst van cryptografische algorithms en sleutellengtes, zoals gedefinieerd in ETSI TS 102 176-1.

6.1.6 Publieke sleutel parameter generatie en kwaliteitscontrole

Voor certificaathouders: De kwaliteit van de parameters, welke wordt gebruikt voor de aanmaak van publieke sleutels, wordt bepaald door de gebruikte SSCD en door de gebruikte programmatuur van de Certificaathouder.

6.1.7 Doeleinden voor sleutel gebruik (Vanaf X.509 V3 sleutel gebruiksvelden)

Sleutels mogen uitsluitend worden gebruikt voor doeleinden zoals beschreven in Hoofdstuk 7 inzake Certificaatprofielen. De Digidentity TSP-CA private sleutel mag uitsluitend worden gebruikt voor het ondertekenen van publieke sleutels (certificaten) en CRL's/OCSP responses.

6.2 Private sleutel bescherming

6.2.1 Standaarden en controles van de cryptografische module (HSM)

De private sleutels van Digidentity TSP-CA zijn gegenereerd en opgeslagen in een cryptografische module welke voldoet aan de FIPS 140-2 level 3 en/of EAL 4 beveiligingsstandaarden.
De HSM-modules worden altijd opgeslagen in een beveiligde omgeving en zijn onderhevig aan strikte beveiligingsprocedures gedurende de gehele levenscyclus.

6.2.2 Private key controle

Toegang tot de HSM's is beperkt tot personen in Vertrouwende Rollen en geschiedt op basis van private keys. Dergelijke vereiste aanwezigheid van meerdere personen alvorens toegang te verkrijgen zorgt ervoor dat niet één enkel persoon de totale controle kan voeren over een kritiek component binnen de infrastructuur.

6.2.3 Escrow van de private sleutel

Digidentity geeft haar TSP-CA sleutels niet in escrow uit bij een onafhankelijke derde.

6.2.4 Private sleutel back-up

De Private Sleutel wordt in versleutelde staat geback-upt, on-site onderhouden en daarnaast in een beveiligde off-site locatie bewaard.
Private sleutels van Certificaathouders worden door Digidentity niet geback-upt. Het is niet toegestaan een back-up te maken van de private sleutel voor de elektronische handtekening.

6.2.5 Archivering van de private sleutel

Digidentity archiveert in geen geval private sleutels van Certificaathouders.
Digidentity biedt geen diensten aan voor het bewaren en terughalen van private decryptiesleutels (key recovery voor vertrouwelijkheidsleutels).

6.2.6 Toegang tot private sleutels in cryptografische module

De sleutels van de Digidentity TSP-CA worden opgeslagen in een HSM (zie 6.2.1). Ze worden daarbinnen opgeslagen in versleutelde staat (waarbij gebruik wordt gemaakt van een encryptie sleutel om een “cryptografische verpakking” te maken voor de sleutel). De private sleutels mogen nooit in plaintext vorm bestaan buiten de cryptografische module. Wanneer de private sleutel moet worden getransporteerd tussen twee cryptografische modules, wordt deze gedecodeerd overgebracht van de ene naar de andere module, onder strikte beveiligingsmaatregelen. Toegang tot het sleutelmateriaal is uitsluitend door aanwezigheid van meerdere personen in Vertrouwende Rollen te verkrijgen, zoals beschreven in hoofdstuk 6.2.2.

6.2.7 Private sleutelopslag op een cryptografische module

De private sleutels die op een cryptografische module zijn opgeslagen, zijn beveiligd gedurende hun gehele levenscyclus.

6.2.8 Activeringsmethoden voor een private sleutel

De activering van de private sleutels van de Digidentity TSP-CA is beschreven in hoofdstuk 6.2.2. De private sleutels van de Certificaathouders worden geactiveerd door middel van een pincode.

6.2.9 Methoden voor deactivatie van de private sleutel

De Private sleutel van de operationele Digidentity TSP-CA wordt normaliter niet gedeactiveerd, maar blijft in productie in de beveiligde omgeving. Overige cryptografische modules worden na gebruik gedeactiveerd, bijvoorbeeld, door middel van een handmatige logout procedure of een passieve time-out. Cryptografische Modules die niet in gebruik zijn worden verwijderd en opgeslagen.

6.2.10 Methode voor de vernietiging van de private sleutel

Private sleutels worden vernietigd wanneer zij niet meer nodig zijn, of wanneer de Certificaten waarmee zij corresponderen zijn verlopen of ingetrokken.
Alle Certificaathouders/Certificaatbeheerders hebben de verplichting om hun private sleutels tegen misbruik te beschermen. Private sleutels worden vernietigd op een wijze die verlies, diefstal, wijziging, onbevoegde onthulling of onbevoegd gebruik voorkomt. Wanneer de geldigheidsduur van een sleutelpaar afloopt, of in andere gevallen waarin vernietiging vereist is, zal het daartoe geautoriseerde personeel van Digidentity de private sleutel vernietigen (bijvoorbeeld door re-initialisering of zeroization van de Cryptografische Module.

6.2.11 Cryptografische classificatie van de module en SSCD's

De cryptografische modules die door de Digidentity TSP-CA worden gebruikt, zijn gecertificeerd op basis van de standaard FIPS 140-2 level-3 en/of Common Criteria EAL 4. De veilige middelen die Digidentity verschaft aan Certificaathouders voor het aanmaken van elektronische handtekeningen (de SSCD, zowel de processor als het operating system), zijn gecertificeerd op basis van de standaard FIPS 140-2 level 3 (wat gelijkwaardig is aan certificatie op basis van Common Criteria EAL4+ (AUGMENTED).

6.3 Overige aspecten van sleutelpaar management

6.3.1 Archivering van het publieke sleutelpaar

De publieke sleutels in certificaten zullen worden geregistreerd en worden gearchiveerd in de elektronische opslagplaats. De sleutels blijven in het archief voor de duur van ten minste 7 jaar gerekend vanaf het verstrijken van de geldigheid ervan. Er wordt geen afzonderlijk archief van publieke sleutels onderhouden.

6.3.2 Gebruiksduur van sleutels en certificaten

Gebruiksperiodes voor de publieke- en private sleutels zijn gelijk aan de gebruiksperiode van het Certificaat welke de publieke sleutel verbindt aan een Certificaathouder.
De maximum geldigheidsperiodes voor certificaten binnen de PKI voor de overheid zijn als volgt:

- De geldigheid van de Digidentity TSP-CA eindigt op 23-03-2020.
- De geldigheidsduur van de PKIoverheid Persoonlijke en Systeemcertificaten in domein Burger en in domein Organisatie is 1/2 óf 3 jaar.
- De geldigheid van services server certificaten is 1/2 óf 3 jaar.

Op het moment van uitgifte van het eindgebruikerscertificaat is de resterende geldigheidsduur van de Digidentity TSP-CA altijd langer dan de gespecificeerde geldigheidsduur van het certificaat voor de Certificaathouder.

6.4 Activeringsgegevens

6.4.1 Activatiedata - generatie en installatie

Een unieke persoonlijke identificatiecode (PIN) wordt geforceerd afgedwongen bij het in gebruik nemen van de SSCD met als doel de private sleutel te beschermen.

6.4.2 Activatiedata bescherming

Activeringsgegevens voor Persoonlijke certificaten dienen door de Certificaathouder/Certificaatbeheerder altijd strikt persoonlijk te worden gehouden.

6.5 Computerbeveiliging

6.5.1 Technische maatregelen inzake computerbeveiliging

Digidentity hanteert en onderhoudt een informatiebeveiligingsbeleid waarin wordt gedocumenteerd wat het Digidentity beleid, de normen en de richtlijnen met betrekking tot informatiebeveiliging zijn. Dit beleid is goedgekeurd door het Digidentity management en medegedeeld aan alle werknemers.
Technische maatregelen inzake computerbeveiliging omvatten onder andere, maar zijn niet beperkt tot:

- Toegangscontrole tot de CA diensten en PKI rolverdeling, zie hoofdstuk 5.1
- Gedwongen scheidingen van de autorisaties en rollen, zie hoofdstuk 5.2
- De identificatie en de authenticatie procedures van personeel dat in Vertrouwelijke Rollen opereert, zie hoofdstuk 5.3
- Het gebruik van cryptografie voor sessiecommunicatie en database beveiliging, wederzijdse authenticatie en versleuteling door middel van SSL/TLS wordt gebruikt voor alle communicatie
- Archivering van de audit logs, zie hoofdstuk 5.4 en 5.6
- Gebruik van x.509 certificaten voor alle administrators

Digidentity gebruikt multi-factor authenticatie voor het systeem of de gebruiker accounts waarmee uitgifte of goedkeuring van certificaten kan worden verricht. Multi-factor authenticatie tokens worden niet op een permanente of semipermanente wijze aangesloten op het systeem.

Digidentity stelt deze eis zowel voor de productie omgeving als voor de uitwijk omgeving.

6.5.2 Classificatie van de computerbeveiliging

De classificatie van de Digidentity computerveiligheid is uitgewerkt in het informatiebeveiligingsbeleid en wordt bereikt door real-time monitoring en analyse, maandelijkse beveiligingscontrole door de Digidentity Chief Security Officer en jaarlijkse beveiligingscontroles door externe auditoren.

6.6 Beheersmaatregelen technische levenscyclus

6.6.1 Beheersmaatregelen ten behoeve van systeemontwikkeling

Software die door Digidentity is ontwikkeld en wordt ingezet voor gebruik in de dienstverlening binnen de PKI voor de overheid, wordt ontwikkeld in een gecontroleerde omgeving welke voldoet aan strikte veiligheidseisen. De software die binnen Digidentity zelf is ontwikkeld en wordt ingezet binnen een van de PKI-kerndiensten, dient te voldoen aan de toepasselijke eisen voor betrouwbare systemen zoals opgenomen in CEN Workshop Agreement (CWA) 14167-1.

6.6.2 Beveiligingsmaatregelen van de levenscyclus

Alle hard- en software die ten behoeve van de Digidentity dienstverlening binnen de PKI voor de overheid wordt ingezet, moeten op een zodanige wijze worden aangekocht en geleverd dat het risico op ongeautoriseerde handelingen tot een minimum wordt beperkt.
Gedurende de operations gebruikt Digidentity een configuratie management procedure voor de installatie en het doorlopend onderhoud van de CA-systemen. Wanneer de CA-software voor het eerst wordt geladen, levert deze een methode voor het verifiëren van de software op het systeem, met daarbij de volgende garanties:

- Afkomstig van de softwareontwikkelaar/-leverancier
- Is niet gewijzigd voorafgaand aan de installatie
- Betreft de versie die is bestemd voor gebruik

De Digidentity Chief Security Officer verifieert periodiek de integriteit van de CA's software en houdt toezicht op de configuratie van de CA systemen.

6.7 Beveiligingsmaatregelen van het netwerk

Alle toegang tot Digidentity informatie en documentatie via een netwerk is beveiligd door middel van firewalls en routers. Firewalls en routers die worden gebruikt voor apparatuur van Digidentity beperkt de beschikbare diensten van en de toegang tot het Digidentity materiaal tot diegenen die dit voor de uitoefening van de functie nodig hebben.
Alle ongebruikte netwerkpoorten en -diensten zijn uitgeschakeld om ervoor te zorgen dat apparatuur van Digidentity is beveiligd tegen het toebrengen van schade op het netwerk. Alle netwerksoftware die aanwezig is op Digidentity apparaten is benodigd voor het functioneren van de applicatie.

Digidentity draagt er zorg voor dat alle PKIoverheid ICT systemen met betrekking tot de registration service, certificate generation service, subject device provision service, dissemination service, revocation management service en revocation status service:

- zijn voorzien van de laatste updates en;
- de webapplicatie alle invoer van gebruikers controleert en filtert en;
- de webapplicatie de dynamische uitvoer codeert en;
- de webapplicatie een veilige sessie met de gebruiker onderhoudt en;
- de webapplicatie op een veilige manier gebruik maakt van een database.

Digidentity gebruikt hiervoor de “Checklist beveiliging webapplicaties4” van het NCSC als guidance. Daarnaast heeft Digidentiy alle overige aanbevelingen uit de laatste versie van de whitepaper “Raamwerk Beveiliging Webapplicaties” van het NCSC geïmplementeerd.

Digidentity voert maandelijks, met behulp van een audit tool (OpenVas), een security scan uit op haar PKIoverheid infrastructuur. Digidentity documenteert het resultaat van elke security scan en de maatregelen die hierop zijn genomen.

6.8 Timestamping

Digidentity biedt geen timestamping services.

7. Certificaat, CRL en OCSP profielen

7.1 Certificaat Profielen

De onderstaande certificaatprofielen leveren een overzicht van de certificaatprofielen die worden uitgegeven in overeenstemming met het PKIoverheid Programma van Eisen, deel 3a, 3b, 3c en 3e.

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.

7.1.1 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 1, 2 óf 3 jaar vanaf het moment van uitgifte ÓF tot de maximale geldigheid van het certificaat van de uitgevende CA (Maart 2020). 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 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.

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 eindgebruikers certificaten, welke worden uitgeven door Digidentity, is 1, 2 óf 3 jaar vanaf het moment van uitgifte ÓF tot de maximale geldigheid van het certificaat van de uitgevende CA (Maart 2020).

7.1.2 MachtigingOnline

Werknemers gebonden authenticiteit certificaat

OID: 2.16.528.1.1003.1.2.5.1

Het werknemers gebonden 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 werknemers gebonden authenticatiecertificaat is 1, 2 óf 3 jaar vanaf het moment van uitgifte ÓF tot de maximale geldigheid van het certificaat van de uitgevende CA (Maart 2020). 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.

Werknemers gebonden handtekeningcertificaat

OID: 2.16.528.1.1003.1.2.5.2

Het werknemers gebonden 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 eindgebruikers certificaten, welke worden uitgeven door Digidentity, is 1, 2 óf 3 jaar vanaf het moment van uitgifte ÓF tot de maximale geldigheid van het certificaat van de uitgevende CA (Maart 2020).

7.1.3 MachtigingOnline SSL

Services - Authenticiteit certificaat

OID: 2.16.528.1.1003.1.2.5.4

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

Services - Vertrouwelijkheid certificaat

OID: 2.16.528.1.1003.1.2.5.5

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

Services - Server certificaat

OID 2.16.528.1.1003.1.2.5.6

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

7.1.4 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 allen tijde uniek zijn voor deze Certificaathouder en niet worden uitgegeven aan een andere Certificaathouder. Pseudoniemen zijn nimmer toegestaan.

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

2. 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 na afweging van de betrokken belangen, voor zover hierin niet wordt voorzien door dwingend Nederlands recht of overige toepasselijke regelgeving.

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	Authenticiteit Vertrouwelijkheid Server

Digidentity SSCD CA - G2	Authenticatie certificaat Onweerlegbaarheid certificaat – qc Encryptie certificaat

De geldigheid van eindgebruikers certificaten, welke worden uitgeven door Digidentity, is 1, 2 óf 3 jaar vanaf het moment van uitgifte ÓF tot de maximale geldigheid van het certificaat van de uitgevende CA (Maart 2020). Voor Server certificaten is de geldigheidsduur 1, 2 óf 3 jaar vanaf het moment van uitgifte ÓF tot de maximale geldigheid van het certificaat van de uitgevende CA (Maart 2020).

7.1.5 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

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	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	UTF8String	Verplicht ingeval van hiërarchie organisatie.
Subject. organizationalUnitName	O	Voor certificaten in domein Burger certificaten wordt gebruik van organizationalUnitName niet toegestaan, bevat de orgnaisatie naam in het domein organisatie		
Subject. serialNumber	O	Door de TSP te bepalen nummer. De combinatie van CommonName en Serialnumber MOET binnen de context van de TSP uniek zijn.	Printable String	Conform aanlevering RA. Numeriek 10 getallen, met voorloopnullen. Verplicht, tenzij het een services certificaat betreft.
Subject. title	O	.		
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 TSP/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.

Attribuut		Beschrijving	Type	Toelichting
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.		http://pki.digidentity.eu/L4/xxxxx/latestCRL.crl
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.
rfc822Name	O			e-mail adres

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.
authorityinfoAccess	O	MOET de URLvan het OCSP responder bevatten.		http://ocsp.digidentity.eu/L4/services/ocsp

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 TSP 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	PrintableStri ng	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/validatie

Alle CA's conformeren zich aan onderstaand 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 TSP 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 organisatieonderdeel. 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 Attributes

Attribuut		Beschrijving	Type	Toelichting
AuthorityKey Identifier	V		BitString	De waarde moet de SHA-1 hash van de authorityKey (publieke sleutel van de TSP/CA) bevatten
CRLNumber	V	Dit attribuut MOET een oplopend nummer bevatten dat het bepalen van de volgorde van CRL's ondersteunt (de TSP voorziet de CRL van de nummering).	Integer	
CRLReason	O	Optioneel	UTF8String	Reden van intrekking

OID Nummers

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

	CA Profiel	OID	KeyUsage	Qc_statement
Digidentity Organisatie CA - G2	TSP-Organisatie	oid: 2.16.528.1.1003.1.3.5.8.1		
Digidentity burger CA - G2	TSP-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	0,2,4	
	SSCD-O-Organisatie	2.16.528.1.1003.1.2.5.2	-	Ja
	SSCD-E-Organisatie	2.16.528.1.1003.1.2.5.3	0,4	
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,	-	
	SSCD-O- Burger	2.16.528.1.1003.1.2.3.2	-	Ja
	SSCD-E- Burger	2.16.528.1.1003.1.2.3.3.	-	

Legenda key usage

nummer	betekenis
0	Any keyusage
1	SSL server
2	SSL client
4	email beveiliging

8 Compliance Audit en andere beoordelingen

8.1. Audits en frequentie

Digidentity is een TSP (certificatiedienstverlener) in de zin van de Telecomwet en is als zodanig geregistreerd bij de ACM.
Het managementsysteem van Digidentity inzake het uitgeven van gekwalificeerde certificaten aan het publiek is gecertificeerd op basis van ETSI EN 319 411-1 en ETSI EN 319 411-2. Digidentity verkreeg in 2011 het conformiteitscertificaat hiervoor met nummer ETS-015, afgegeven door de geaccrediteerde certificatie-instelling BSI Management Systems B.V. (BSI) te Amsterdam. Daarbij is tevens aangegeven dat Digidentity tevens voldoet aan de aanvullende eisen zoals neergelegd in het Besluit Elektronische Handtekeningen. Het conformiteitscertificaat heeft een geldigheid van 3 jaar en is tussentijds onderhevig aan tussentijdse controle-audits (na 12 en 24 maanden).

8.2 Kwalificatie Auditor

Certificatie audits worden uitgevoerd door BSI. BSI is geaccrediteerd door de Raad van Accreditatie.

8.3. De verhouding van de auditor met de beoordeelde entiteit

De auditor en Digidentity welke wordt ge-audit, mogen geen relatie hebben die de auditors onafhankelijkheid aantast en objectiviteit volgens Generally Accepted Auditing Standards. Tot deze relaties behoren, financieel, wettelijk, sociaal of andere relaties welke tot een conflict kunnen leiden.

8.4. Scope van de audit

De scope van de certificatie-audit betreft de volgende onderwerpen en processen:

- Registration Service;
- Certificate Generation Service;
- Revocation Management Service;
- Revocation Status Service
- Dissemination Service;
- Subject Device Provision Service.

8.5. Acties ondernomen vanwege deficiënties

Ingeval tijdens een audit non-conformiteiten zijn geconstateerd, wordt door Digidentity een Corrective Action Plan (CAP) opgesteld waarin corrigerende maatregelen worden voorgesteld om de non-conformiteiten weg te nemen. De certificerende instelling dient goedkeuring te verlenen aan het CAP.
Tussentijds worden door Digidentity interne audits uitgevoerd waarin de opvolging van de corrigerende acties worden gecontroleerd.

Tenslotte wordt bij een volgende certificatie-audit de implementatie van de corrigerende maatregel door de certificerende instelling gecontroleerd.

8.6. Publicatie accreditaties en registraties

De registratie van Digidentity als certificatiedienstverlener is gepubliceerd op de website van Agentschap Telecom:
https://www.agentschaptelecom.nl/onderwerpen/zakelijk-gebruik/eidas-elektronische-vertrouwensdiensten/trust-service-providers

Een lijst met certificatiedienstverleners die certificaten uitgeven binnen de PKI voor de overheid vindt u hier:
https://www.logius.nl/ondersteuning/pkioverheid/

Overige accreditaties van Digidentity is raadpleegbaar op de volgende locatie:
https://www.digidentity.eu/nl/home/#accreditations

9. Algemene en juridische bepalingen

9.1 Tarieven

Alle tarieven van Digidentity zijn beschikbaar via de website https://www.digidentity.eu

9.2. Financiële verantwoordelijkheid en aansprakelijkheid

Digidentity is verantwoordelijk voor het beheren van haar financiële boekhouding en vastleggingen op commercieel redelijke wijze en zal gebruik maken van de diensten van een accountantsbureau voor financiële diensten, waaronder periodieke controles.

Voor zover niet expliciet anders overeengekomen, stelt Digidentity geen beperkingen aan de waarde van de transacties waarvoor gekwalificeerde certificaten kunnen 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 één miljoen euro. Het eerdergenoemde laat onverlet de mogelijkheden tot verhaal op degene aan wie de schade toe te rekenen valt.

9.3. Vertrouwelijkheid van bedrijfsgevoelige gegevens

9.3.1. Toepassingsgebied vertrouwelijke informatie

Enige persoonlijke- of bedrijfsinformatie in het bezit van Digidentity, gerelateerd aan de aanvraag van de Certificaathouder en de uitgifte van Certificaten, wordt als vertrouwelijk beschouwd en zal niet worden vrijgegeven zonder voorafgaande toestemming van de betreffende Certificaathouder, tenzij anders vereist door wetgeving of om aan de vereisten van dit CPS te voldoen.

9.3.2. Gegevens die als niet-vertrouwelijk worden beschouwd

Informatie in Certificaten of deze is opgeslagen in de elektronische opslagplaats wordt niet als vertrouwelijk beschouwd, tenzij statuten of speciale overeenkomsten dit voorschrijven.

9.3.3. Verantwoordelijkheid vertrouwelijke informatie te beschermen

Digidentity, Abonnees, Certificaathouders, vertrouwende partijen en alle anderen zijn verantwoordelijk voor de bescherming van vertrouwelijke bedrijfsinformatie die in hun bezit is.

9.4. Vertrouwelijkheid van persoonlijke informatie

Digidentity voldoet aan de eisen van de Wet Bescherming Persoonsgegevens. Digidentity heeft zich geregistreerd bij het College Bescherming Persoonsgegevens als zijnde verantwoordelijk voor het verwerken van persoonsgegevens ten behoeve van de Certificatiedienstverlening.

9.4.1. Vertrouwelijke informatie

Digidentity, Registratieautoriteiten, Abonnees, Certificaathouders, vertrouwende partijen en alle anderen die gebruik maken of toegang hebben tot persoonsgegevens, zullen zich houden aan relevante wet- en regelgeving inzake de bescherming van persoonsgegevens.

9.4.2. Vertrouwelijk behandelde informatie

Alle informatie betreffende Certificaathouders die niet publiekelijk beschikbaar is door middel van de inhoud van uitgegeven Certificaten, CRL's of van de elektronische opslagplaats worden vertrouwelijk behandeld.
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.

9.4.2.1. Registratievastleggingen

Alle registratievastleggingen zullen als vertrouwelijke informatie beschouwd en behandeld worden.

9.4.2.2. Certificaatintrekking

Met uitzondering van de intrekkingsredenen opgenomen in een CRL wordt de gedetailleerde reden voor de intrekking van een Certificaat gezien als vertrouwelijke informatie, met als enige uitzondering de intrekking van het certificaat van de Digidentity TSP-CA:

- De compromittering van de private sleutel van de Digidentity TSP-CA, in welk geval er een openbaarmaking mag worden gepubliceerd dat de private sleutel is gecompromitteerd;
- De opheffing van de Digidentity TSP-CA binnen de PKI voor de overheid, in welk geval er voorafgaande openbaarmaking mag worden gepubliceerd van de opheffing.

9.4.3. Niet-vertrouwelijke informatie

9.4.3.1. Certificaatinhoud

De inhoud van Certificaten, uitgegeven door Digidentity, is publieke informatie en dient niet als vertrouwelijk te worden beschouwd.

9.4.3.2. Certificaat intrekkingslijst

Certificaten welke gepubliceerd zijn in de elektronische opslagplaats worden niet als vertrouwelijke informatie beschouwd.

9.4.3.3. CPS

Het CPS van Digidentity is een publiekelijk document bevat geen vertrouwelijke informatie en zal niet als zodanig worden behandeld.

9.4.4. Verantwoordelijkheid om vertrouwelijke informatie te beschermen

Informatie die aan Digidentity wordt verstrekt door handelingen beschreven in dit CPS wordt als vertrouwelijk aangemerkt. Digidentity zal om geen enkele reden persoonlijke Certificaathouderinformatie verstrekken aan enige derde partij, tenzij dit wordt vereist door wet- en regelgeving of op last van een rechterlijk bevel.

9.4.5. Melding van- en instemming met het gebruik van persoonsgegevens

Tijdens het acceptatie proces van een Certificaat stemt de gebruiker in met de verwerking en het gebruik, door en namens Digidentity, van diens persoonlijke gegevens zoals verstrekt tijdens het registratieproces.
De eindgebruiker krijgt de mogelijkheid om af te zien van het gebruik van diens persoonlijke gegeven voor bepaalde doeleinden.
Tevens dienen zij, al dan niet overeengekomen, bepaalde persoonlijke informatie zichtbaar te maken in de elektronische opslagplaats en voor verstrekking aan derden.

Certificaathouders stemmen nadrukkelijk in met de verplaatsing van persoonlijke gegevens, in de vorm van gegevens die zijn opgenomen in de Certificaatvelden, buiten Nederland en stemmen al dan niet in met de publicatie van het Certificaat in de elektronische opslagplaats die de Certificaatinformatie publiekelijk toegankelijk maakt voor vertrouwende partijen die met de toepasselijke query string zoeken binnen de elektronische opslagplaats. Persoonlijke gegevens, verkregen tijdens het registratieproces die niet zijn opgenomen in het Certificaat, zullen niet worden verplaatst buiten Nederland.

9.4.6. Overhandiging van gegevens op last van een rechterlijke instantie

Digidentity zal geen vertrouwelijke gegevens, welke in haar bezit zijn, vrijgeven aan opsporingsinstanties of –ambtenaren. Tenzij de Nederlandse wet- en regelgeving hier toe dwingt middels een gerechtelijk bevel.

9.5 Intellectuele eigendomsrechten

Alle intellectuele eigendomsrechten, inclusief alle auteursrechten, op Certificaten en Digidentity documenten (elektronisch of in iedere andere vorm) zijn permanent eigendom van Digidentity. Om verwarring te voorkomen worden documenten, die zijn ondertekend of versleuteld, met een Digidentity Certificaat niet aangemerkt als Digidentity documenten in relatie tot deze paragraaf. Derhalve is Digidentity niet verantwoordelijk voor de inhoud van dergelijke documenten en/of aantekeningen. Private en publieke sleutels zijn eigendom van de Abonnee en de Certificaathouder. Digidentity garandeert jegens haar Abonnees en Certificaathouders dat de door haar uitgegeven certificaten en dragers van de private en publieke sleutel, inclusief de daarbij behorende en geleverde apparatuur en documentatie, geen inbreuk maken op intellectuele eigendomsrechten. Waaronder auteursrechten, merkenrechten en gebruikte programmatuur waarvan deze berusten bij haar (toe)leveranciers.

9.6. Aansprakelijkheid en garanties

9.6.1. Aansprakelijkheid van de TSP

Digidentity verklaart hierbij dat:

a) zij redelijke stappen heeft ondernomen om de informatie die is opgenomen in een Certificaat te verifiëren op accuraatheid ten tijde van de uitgifte
b) certificaten zullen worden ingetrokken indien Digidentity vermoedt, of erop is gewezen, dat de inhoud van een Certificaat niet meer accuraat is of, dat de sleutel geassocieerd met een Certificaat, op enige wijze is gecompromitteerd.

Digidentity is alleen aansprakelijk jegens Certificaathouders of vertrouwende partijen voor onmiddellijk verlies voortvloeiend uit het door Digidentity schenden van bepalingen uit dit CPS of van enige andere aansprakelijkheid uit overeenkomst, onrechtmatige daad of anders, inclusief de aansprakelijkheid voor nalatigheid tot een in hoofdstuk 9.2. opgenomen maximum bedrag, voor enige gebeurtenis of reeks verwante gebeurtenissen (in een periode van 12 maanden).
Dit TSP sluit alle aansprakelijkheid uit voor schade die ontstaat indien het Certificaat niet wordt gebruikt conform het beoogde Certificaatgebruik, zoals beschreven in paragraaf 1.4 van dit CPS.

Digidentity kan, op aanwijzen van de PA van de PKI voor de overheid, in het handtekeningcertificaat beperkingen ten aanzien van het gebruik ervan opnemen, mits de betreffende beperkingen duidelijk zijn voor derden. Digidentity is niet aansprakelijk voor schade als gevolg van gebruik van een handtekeningcertificaat in strijd met een dergelijk opgenomen beperking.
Digidentity accepteert geen enkele vorm van aansprakelijkheid voor geleden schade van vertrouwende partijen, met daarop de volgende uitzonderingen:

- Digidentity is in beginsel aansprakelijk overeenkomstig artikel 6.19b, eerste tot en met derde lid, van het Burgerlijk Wetboek, met dien verstande dat:
    - voor “een gekwalificeerd certificaat als bedoeld in artikel 1.1. onderdeel ss Telecommunicatiewet” gelezen wordt: “een authenticiteitscertificaat”
    - voor “ondertekenaar” gelezen wordt: “certificaathouder”;
    - voor “elektronische handtekeningen” gelezen wordt: “authenticiteitskenmerken”.
- Digidentity is in beginsel aansprakelijk overeenkomstig artikel 6.19b, eerste tot en met derde lid, van het Burgerlijk Wetboek, met dien verstande dat:
    - voor “een gekwalificeerd certificaat als bedoeld in artikel 1.1. onderdeel ss Telecommunicatiewet” gelezen wordt: “een vertrouwelijkheidscertificaat”;
    - voor “ondertekenaar” gelezen wordt: “certificaathouder”;
    - voor “aanmaken van elektronische handtekeningen” gelezen wordt: “aanmaken van vercijferde data”;
    - voor “verifiëren van elektronische handtekeningen” gelezen wordt: “ontcijferen van vercijferde data”.
    - voor “een gekwalificeerd certificaat als bedoeld in artikel 1.1. onderdeel ss Telecommunicatiewet” gelezen wordt: “een servercertificaat”;
    - voor “ondertekenaar” gelezen wordt: “certificaathouder”;
    - voor “aanmaken van elektronische handtekeningen” gelezen wordt: “verifiëren van authenticiteitskenmerken een aanmaken van vercijferde data”;
    - voor “verifiëren van elektronische handtekeningen” gelezen wordt: “ontcijferen van authenticiteitskenmerken en vercijferde data”.

In het kader van de afgifte van Gekwalificeerde certificaten stelt Digidentity zich aansprakelijk conform de eisen van de eIDAS verordening (EU nr 910/2014). Tevens is de Nederlandse wetgeving, 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:

1. 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;

2. 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;

3. 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 4.5.1 van dit CPS. Digidentity is voor deze aansprakelijkheid verzekerd.

9.6.2.Aansprakelijkheid van Abonnees en Certificaathouders

Certificaathouders garanderen dat:

- de private sleutel beschermd is en er nooit toegang is geweest voor een ander persoon
- alle representaties, die door de Certificaathouder zijn gemaakt, juist zijn
- alle informatie in het Certificaat juist en accuraat is
- het Certificaat wordt gebruikt conform de bedoelde, geautoriseerde en rechtmatige gebruik overeenkomstig dit CPS
- zij onmiddellijk intrekking verzoeken van het Certificaat in het geval dat: (a) enige informatie, opgenomen in het Certificaat, incorrect of inaccuraat is of wordt, of (b) de private sleutel die correspondeert met de publieke sleutel in het Certificaat (vermoedelijk) is misbruikt of gecompromitteerd.

9.6.3.Aansprakelijkheid Vertrouwende Partijen

Vertrouwende Partijen garanderen dat:

- zij voldoende informatie zullen verzamelen over een Certificaat en zijn houder om een besluit op basis van goede informatie te maken over in hoeverre er op een Certificaat vertrouwd kan worden.
- zij zijn als enige verantwoordelijk voor het maken van de beslissing te vertrouwen op een Certificaat (met uitzondering van het genoemde in hoofdstuk 9.6.1)
- zij de juridische consequenties dragen als gevolg van het nalaten van het handelen overeenkomstig de verplichtingen van vertrouwende partijen conform dit CPS.

9.7. Uitsluiting van garanties

Voor zover toegestaan door de toepasbare wetgeving zal deze CPS, de Certificaathouderovereenkomst en enig andere contractuele documentatie, toepasselijk binnen de PKI voor de overheid, garanties van Digidentity uitsluiten.

9.8. Beperking van aansprakelijkheid

9.8.1. Beperkingen van aansprakelijkheid van Digidentity

Digidentity zal in geen geval verantwoordelijk zijn voor het verlies van winst, verlies van verkoop of omzet, verlies of schade aan reputatie, verlies van contracten, verlies van klanten, verlies van het gebruik van enige software of data, verlies of gebruik van enige computer of andere apparatuur (tenzij direct het gevolg door breuk van dit CPS), verspilde tijd van management of ander personeel, verliezen of aansprakelijkheden met betrekking tot of in samenhang met andere contracten, indirecte schade of verlies, gevolgschade of –verlies, speciaal verlies of schade, en binnen deze paragraaf betekent "verlies" zowel een gedeeltelijk verlies van of daling in waarde als volledig of totaal verlies.
De aansprakelijkheid van Digidentity richting een bepaald persoon betreffende schade die op enige wijze optreedt onder, uit naam van, binnen of gerelateerd aan deze CPS, Certificaathouderovereenkomst, het toepasselijke contract of gerelateerde overeenkomst, hetzij in contract, garantie, onrechtmatige daad of enig andere wettelijke theorie, is, onderworpen aan wat verderop uiteen is gezet, beperkt zijn tot daadwerkelijke schade die door deze persoon is geleden. Digidentity zal niet aansprakelijk zijn voor indirecte, gevolg-, incidentele, speciale, voorbeeld- of bestraffende schade met betrekking tot enige persoon, zelfs als Digidentity is gewezen op de mogelijkheid van dergelijke schade, ongeacht hoe dergelijke schade of verantwoordelijkheid is opgetreden, hetzij in onrechtmatige daad, achteloosheid, rechtvaardigheid, contract, statuut, gewoonterecht of anderzijds. Als voorwaarde aan deelname binnen de PKI voor de overheid (inclusief, zonder beperking, het gebruik van of vertrouwen op Certificaten) stemt iedere persoon die binnen de PKI voor de overheid deelneemt onherroepelijk in dat zij geen aanspraak wil maken op, of op andere wijze zoeken naar, voorbeeld-, gevolg-, speciale, incidentele of bestraffende schade en bevestigt onherroepelijk aan Digidentity de aanvaarding van het voorgaande als een conditie en aansporing om deze persoon toe te staan deel te nemen binnen de PKI voor de overheid.

9.8.2. Uitgesloten aansprakelijkheid

Digidentity zal op geen enkele wijze aansprakelijk zijn voor enig verlies betreffende of voortkomende uit een (of meerdere) van de volgende omstandigheden of oorzaken:

- Als het Certificaat, gehouden door de eisende partij of op andere wijze onderwerp van enige eis, is gecompromitteerd door ongeautoriseerde onthulling of gebruik van het Certificaat, of enig wachtwoord of activeringsgegevens die de toegang hiertoe controleren;
- Als het Certificaat, gehouden door de eisende partij of op andere wijze onderwerp van enige eis uitgegeven is als gevolg van onjuiste voorstelling, fout of feit, of nalatigheid van enige persoon, entiteit of organisatie;
- Als het Certificaat, gehouden door de eisende partij of op andere wijze onderwerp van enige eis is verlopen of ingetrokken voor de datum van omstandigheden die leiden tot enige claim;
- Als het Certificaat, gehouden door de eisende partij of op andere wijze onderwerp van enige eis is gewijzigd of op enige wijze is veranderd of op een andere manier

is gebruikt dan toegestaan door de voorwaarden van deze CPS en/of de relevante Certificaathouderovereenkomst of enige toepasbare wet- of regelgeving;
- Als de private sleutel, die correspondeert met het Certificaat, gehouden door de eisende partij of op andere wijze onderwerp van enige eis, is gecompromitteerd;
- Als het Certificaat, gehouden door de eisende partij, uitgegeven is op een wijze die in overtreding is met enige toepasbare wet- of regelgeving;
- Computer hardware of software, of mathematische algoritmen, zijn ontwikkeld die de neiging hebben publieke sleutelcryptografie of asymmetrische cryptosystemen onzeker te maken, op voorwaarde dat Digidentity commercieel redelijke praktijen gebruikt om te beschermen tegen schendingen van beveiliging als gevolg van dergelijke hardware, software of algoritmen;
- Stroomuitval, stroomonderbreking, of andere onderbrekingen van elektriciteit, op voorwaarde dat Digidentity commercieel redelijke methoden gebruikt om te beschermen tegen dergelijke storingen;
- Uitval van een of meerdere computersystemen, communicatie-infrastructuur, verwerking, of opslagmedia of –mechanismen of enig sub component van voorgaande, niet onder exclusieve controle van Digidentity en/of diens onderaannemers; of
- Een of meer van de volgende gebeurtenissen: een natuurramp of overmacht (inclusief, zonder beperking, overstroming, aardbeving, of andere natuurlijke of weer gerelateerde oorzaak); een arbeidsstoring; oorlog, opstand of openlijke militaire vijandigheden; tegenstrijdige wetgeving of overheidsactie, verbod, embargo of boycot; rellen of burgerlijke ongeregeldheden; vuur of explosie; catastrofale epidemie; handelsembargo; beperking of beletsel (met inbegrip van, zonder beperking, exportcontroles); enig gebrek aan beschikbaarheid of integriteit van telecommunicatie; wettelijke dwang, met inbegrip van enige beslissing, gemaakt door een hof van bekwame jurisdictie, waaraan Digidentity onderworpen is; en
- enige gebeurtenis, omstandigheid of reeks omstandigheden die buiten de controle van Digidentity vallen.

9.8.3. Beperking van aansprakelijkheid Digidentity

Digidentity heeft een aantal maatregelen geïntroduceerd om haar aansprakelijkheden te verminderen of te beperken in het geval dat beschermingsmiddelen voor het beschermen van bronnen er niet in slagen om:
- misbruik van deze bronnen door geautoriseerd personeel te voorkomen
- toegang tot deze bronnen door ongeautoriseerde individuen te verbieden

Deze maatregelen omvatten, maar zijn niet beperkt tot:
- het identificeren van onvoorziene gebeurtenissen en toepasselijke herstelacties in een bedrijfscontinuïteitsplan en Disaster Recovery Plan (IT uitwijk);
- het regelmatig uitvoeren van back-ups van systeemdata;
- het uitvoeren van een back-up van de huidige werkende software en bepaalde software configuratie-files;
- het opslaan van alle back-ups in beveiligde lokale en gedecentraliseerde opslag;
- het handhaven van beveiligde gedecentraliseerde opslag van overig materiaal, benodigd voor rampenherstel;

- het periodiek testen van lokale en gedecentraliseerde back-ups om zeker te stellen dat de informatie her winbaar is in het geval van een storing;
- het periodiek beoordelen van het bedrijfscontinuïteitsplan en Disaster Recovery Plan, inclusief de identificatieanalyse, evaluatie en prioritering van risico's; en
- het periodiek controleren van ononderbroken voeding.

9.8.4.1. Notificatieperiode

Digidentity zal geen verplichtingen hebben overeenkomstig enige eis voor breuk van haar verplichtingen tenzij de eisende partij Digidentity binnen negentig (90) dagen nadat de eisende partij wist of redelijkerwijs had moeten weten van de claim, en in geen geval meer dan 3 jaar na afloop van het Certificaat die de eisende partij hield, hiervan op de hoogte stelt.

9.8.4.2. Beperkende handelingen en onthulling van ondersteunende informatie

Als voorwaarde voor uitbetaling van Digidentity betreffende enige eis onder de voorwaarden van dit CPS zal een eisende partij alle verdere handelingen uitvoeren. Alle dergelijke overeenkomsten, instrumenten en documenten uitvoeren en aanleveren die Digidentity redelijkerwijs verzoekt om een claim van verlies, gemaakt door de eisende partij, te kunnen onderzoeken.

9.9. Schadeloosstelling

De bepalingen en verplichtingen betreffende schadevergoedingen zijn opgenomen in de relevante contractuele documentatie.

9.10. Geldigheidstermijn CPS

9.10.1. Termijn

Dit CPS is geldig vanaf het moment van publicatie op de Digidentity website. Herzieningen op dit CPS zijn geldig vanaf het moment van publicatie op de Digidentity website.

9.10.2. Beëindiging

Dit CPS zal geldig blijven tot deze is herzien of verplaatst door een andere versie.

9.10.3. Effect van beëindiging en overleving

De bepalingen binnen dit CPS zullen de beëindiging of terugtrekking van een Certificaathouder of vertrouwende partij binnen de PKI voor de overheid overleven, met betrekking tot alle handelingen gebaseerd op het gebruik van, of het vertrouwen op, een Certificaat of andere deelname binnen de PKI voor de overheid. Enige dergelijke beëindiging of terugtrekking zal niet zo optreden om enig recht op actie of remedie te benadelen of beïnvloeden die gevolg waren aan enig persoon tot en met de datum van terugtrekking of beëindiging.

9.11. Individuele kennisgeving en communicatie met betrokken partijen

Elektronische post, brievenbuspost en webpagina's zullen beschikbare middelen zijn die Digidentity gebruikt om enig van de berichten, vereist door dit CPS, aan te bieden, tenzij op specifiek andere wijze aangeboden. Elektronische post en brievenbuspost zullen allebei geldige middelen zijn om enige berichtgeving, vereist overeenkomstig dit CPS, aan Digidentity te verstrekken tenzij specifiek op andere wijze aangeboden (bijvoorbeeld met betrekking tot intrekking procedures).

9.12. Wijziging

Wijzigingen aan dit CPS zullen in de vorm van een gewijzigd CPS of vervangend CPS zijn. Bijgewerkte versies van deze CPS zullen aangewezen of tegenstrijdige bepalingen van de vermelde versie van het CPS vervangen.
Er zijn twee mogelijke soorten van beleidsverandering:

- de uitgifte van een nieuwe CPS; of
- een verandering of aanpassing van een beleid in het bestaande CPS.

De enige veranderingen die mogen worden gemaakt aan dit CPS zonder berichtgeving zijn; redactionele of typografische correcties die geen consequenties hebben voor enige participanten binnen de PKI voor de overheid.

Indien er een voornemen is de CA-structuur te veranderen, dient Digidentity informatie hieromtrent voor te leggen aan de PA.

Bij veranderende marktvoorwaarden, veiligheidseisen, wetswijzigingen etc., behoudt Digidentity 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.

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.

9.13. Geschillenbeslechting

Op de website van Digidentity is de klachtenprocedure gepubliceerd.
In geval van klachten betreffende diensten geleverd in het kader van dit CPS kan de klacht via deze website, per email (info@digidentity.eu) of per telefoon (+31 (0)887 78 78 78) ingediend worden bij Digidentity. Dit zal de Digidentity klachtenprocedure in werking stellen.

Enige controversie of eis tussen twee of meer deelnemers binnen de PKI voor de overheid (met Digidentity als deelnemer binnen de PKI voor de overheid), voortkomend uit of gerelateerd aan dit CPS zal deze worden voorgelegd aan de gewone rechter in het arrondissement waar Digidentity is gevestigd.

Alle overeenkomsten tussen de gebruiker Digidentity vallen onder het Nederlands recht.

9.14. Van toepassing zijnde wetgeving

Op alle overeenkomsten die door Digidentity worden afgesloten is het Nederlands recht van toepassing, tenzij anders is bepaald.

9.15. Naleving relevante wetgeving

Digidentity is een Certificatiedienstverlener ingevolge de Telecommunicatiewet. Digidentity conformeert zich aan de toepasselijke wet- en regelgeving die betrekking heeft op haar rol als Certificatiedienstverlener.

9.16. Overige bepalingen

Enige bepaling binnen dit CPS die ongeldig of onuitvoerbaar wordt verklaard, zal buiten werking treden. Dit laat onverlet de toepasselijkheid van de resterende bepalingen in dit CPS.

Bijlage A – Definities

Aanvrager: een natuurlijke of rechtspersoon die een aanvraag tot uitgifte van een Certificaat indient bij Digidentity. De Aanvrager hoeft niet dezelfde partij te zijn als de Abonnee of de Certificaathouder, maar is wel één van beide.

Abonnee: de natuurlijke persoon of rechtspersoon die zich aanmeldt bij Digidentity om uitgifte van PKIoverheid Certificaten aan door hem aangewezen Certificaathouders te bewerkstelligen.

Accreditatie: Procedure waarbij een autoriteit bezittende organisatie een formele erkenning uitspreekt dat een entiteit bekwaam is specifieke taken uit te voeren

Algemene Voorwaarden: de Algemene Voorwaarden PKIoverheid Certificaten, zoals van toepassing op alle bij de uitgifte en het gebruik van PKIoverheid Certificaten betrokken partijen.

Algoritme: Een verzameling instructies die stap voor stap uitgevoerd dienen te worden om een rekenkundig proces uit te voeren of een specifiek type problemen op te lossen.

Asymmetrisch Sleutelpaar: een Publieke Sleutel en Private Sleutel binnen de publieke sleutelcryptografie die wiskundig zodanig met elkaar zijn verbonden dat de publieke sleutel en de private sleutel elkanders tegenhanger zijn. Wordt de ene sleutel gebruikt om te versleutelen, dan móet de andere gebruikt worden om te ontsleutelen en omgekeerd.

Authenticatie:
1. Het controleren van een identiteit voordat informatieoverdracht plaatsvindt;
2. het controleren van de juistheid van een boodschap of afzender.

Authentificatie: zie Authenticatie.

Autoriseren: Het verlenen van een bevoegdheid tot het verrichten van handelingen (zoals inzien, aanpassen of bewerken) op informatie of middelen.

Beschikbaarheid: Het aanwezig zijn en het toegankelijk zijn van de relevante gegevens. Wat betreft infrastructuur: de mate waarin een systeem bruikbaar is op het moment dat hier een behoefte aan bestaat.

CA-Certificaat: een Certificaat van een Certification Authority.

Calamiteit (Engels: Disaster) Een ongeplande situatie waarbij verwacht wordt dat de duur van het niet beschikbaar zijn van één of meer diensten de afgesproken drempelwaarden zal overschrijden.

Certificaat: de Publieke Sleutel van een Eindgebruiker, samen met aanvullende informatie. Een Certificaat is vercijferd met de Private Sleutel van de Certification Authority die de Publieke Sleutel heeft uitgegeven, waardoor het Certificaat onvervalsbaar is.

Certificaataanvraag: de door een Aanvrager ingediend verzoek om uitgifte van een Certificaat door Digidentity.

Certificaatbeheerder: een natuurlijke persoon die bevoegd is om namens de Abonnee en ten behoeve van de Certificaathouder een Servercertificaat of Groepscertificaat aan te vragen, te installeren, te beheren en/of in te trekken. De Certificaatbeheerder voert handelingen uit waartoe de Certificaathouder zelf niet in staat is.

Certificaat & kaart management: De procedures met betrekking tot het beheer van de certificaten en smartcards.

Certificaatgeldigheidsduur (Engels: Certificate validity period): Het tijdsinterval gedurende welke de Certification Authority de bruikbaarheid van het certificaat garandeert. De Certification Authority houdt tot tenminste 6 maanden na het verlopen van de geldigheidsduur informatie bij betreffende de status van een certificaat.

Certificaathouder: een entiteit die geïdentificeerd wordt in een Certificaat als de houder van de Private Sleutel behorende bij de Publieke Sleutel die in het Certificaat gegeven wordt.

Certificaatprofiel: een beschrijving van de inhoud van een Certificaat. Ieder soort Certificaat (handtekening, vertrouwelijkheid, en dergelijke) heeft een eigen invulling en daarmee een eigen beschrijving – hierin staan bijvoorbeeld afspraken omtrent naamgeving.

Certificate Policy (CP): een benoemde 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 Abonnees 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.

Certificate Revocation List (CRL): een openbaar toegankelijke en te raadplegen lijst van ingetrokken Certificaten, ondertekend en beschikbaar gesteld door de uitgevende TSP.

Certificatie: Een brede (zowel technisch als niet-technisch) evaluatie van de beveiligingseigenschappen van een informatiesysteem of, zoals in het kader van de PKI voor de overheid, een managementsysteem. Certificatie wordt uitgevoerd als een onderdeel van een proces, waarbij wordt nagegaan in welke mate een managementsysteem overeenkomt met een vastgestelde verzameling van eisen (ETSI TS 319 411-1/ETSI EN 319 411-2). De regels voor de certificering zijn vastgelegd in een schema: Scheme for Certification of Certification Authorities against ETSI 319 411-2.

Certificatie Autoriteit (CA): een organisatie die Certificaten genereert en intrekt. Het functioneren als CA is een deelactiviteit die onder de verantwoordelijkheid van de TSP wordt uitgevoerd. In dit verband opereert Digidentity derhalve als CA.

Certificatiediensten: het afgeven, beheren en intrekken van Certificaten door Certificatiedienstverleners.

Certification Practice Statement (CPS): een document dat de door een TSP gevolgde procedures en getroffen maatregelen ten aanzien van alle aspecten van de dienstverlening beschrijft. Het CPS beschrijft daarmee op welke wijze de TSP voldoet aan de eisen zoals gesteld in de van toepassing zijnde Certificate Policy.

Certification Practice Statement PKIoverheid (CPS PKIoverheid): de onderhavige Certification Practice Statement, zoals van toepassing op de uitgifte door Digidentity van PKIoverheid Certificaten alsmede het gebruik daarvan.

Certificatiedienstverlener: een natuurlijke persoon of rechtspersoon die als functie heeft het verstrekken en beheren van Certificaten en sleutelinformatie, met inbegrip van de hiervoor voorziene dragers (SSCD, SUD). De Certificatiedienstverlener heeft tevens de eindverantwoordelijkheid voor het leveren van de certificatiediensten waarbij het niet uit maakt of hij de feitelijke werkzaamheden zelf uitvoert of deze uitbesteedt aan anderen.

CommonName – CN: Een aanduiding van de certificaathouder, in het geval van een persoonsgebonden certificaat bestaande uit: achternaam, voorna(a)m(en) en eventueel voorletters. Ook de certificaatuitgever kan worden aangeduid met een CommonName, in dat geval zal deze meestal bestaan uit een bedrijfsnaam aangevuld met het van toepassing zijnde domein van de PKI voor de overheid.

Cryptografische module: De verzameling van hardware, software, firmware, of enige combinatie hiervan die cryptografische processen implementeert, inclusief cryptografische algoritmen en die bevat is binnen de cryptografische grenzen van de module.

Digitale Handtekening: zie Geavanceerde Elektronische Handtekening.

Directory Dienst: een dienst van (of met medewerking van) een TSP die de door de CA uitgegeven Certificaten online beschikbaar en toegankelijk maakt ten behoeve van raadplegende of vertrouwende partijen.

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.

Eindgebruiker: een natuurlijke persoon of rechtspersoon die binnen de PKI voor de overheid één of meer van de volgende rollen vervult: Abonnee, Certificaathouder of Vertrouwende Partij. Gezien het geringe onderscheidende vermogen van deze term wordt ze in dit CPS niet gebruikt, behalve daar waar het de voorgeschreven structuur van het document betreft (headings en dergelijke)

Eindgebruikercertificaat (Engels: End user certificate): Een certificaat uitgegeven door een Certification Service Provider aan een entiteit, zoals een persoon, een computer of een stukje informatie, die zelf geen certificaten kan uitgeven. Omdat naar de eindgebruiker die een certificaat van een Certification Service Provider ontvangt, vaak wordt verwezen als zijnde de cliënt, wordt dit certificaat ook wel een cliënt-certificaat genoemd. Ook wordt soms de term “Gebruikercertificaat” gehanteerd.

Elektronische Handtekening: elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie. De Elektronische Handtekening wordt ingezet om ervoor te zorgen dat elektronische correspondentie en transacties op twee belangrijke punten kunnen wedijveren met de aloude “handtekening op papier”. Door het plaatsen van een Elektronische Handtekening staat vast dat iemand die zegt een document te hebben ondertekend, dat ook daadwerkelijk heeft gedaan.

Elektronische identiteit: De gegevens in elektronische vorm die worden toegevoegd aan of op logische wijze verbonden met andere elektronische gegevens en fungeren als uniek kenmerk van de identiteit van de eigenaar. Soms wordt de term “Digitale identiteit” gebruikt.

Encryptie: Een proces waarmee gegevens met behulp van een wiskundig algoritme en een cryptografische sleutel worden vercijferd, zodat deze onleesbaar worden voor onbevoegden. De betrouwbaarheid van de encryptie hangt af van het algoritme, de implementatie daarvan, de lengte van de cryptografische sleutel en de gebruiksdiscipline. Bij symmetrische encryptie wordt bij het vercijferen en ontcijferen gebruik gemaakt van één en dezelfde, geheime, sleutel. Bij asymmetrische encryptie wordt gebruik gemaakt van een sleutelpaar. De ene sleutel, de private sleutel, is slechts bekend bij de eindgebruiker van deze sleutel en moet strikt geheim worden gehouden. De andere, de publieke sleutel, wordt verspreid onder communicatiepartners. Wat met de private sleutel is vercijferd, kan alleen met de bijbehorende publieke sleutel worden ontcijferd en omgekeerd.

Elektronische Opslagplaats: locatie waar relevante informatie ten aanzien van de dienstverlening van Digidentity is te vinden. Zie: https://www.digidentity.eu

Escrow (Key-escrow): Een methode om tijdens uitgifte van een certificaat een kopie te genereren van de Private Sleutel ten behoeve van toegang tot versleutelde gegevens door daartoe bevoegde partijen, alsmede de beveiligde bewaarneming daarvan.

European Electronic Signature Standardization Initiative – EESSI: Een workshop op Europees niveau met als taak het vormgeven van de concretisering via standaardisatieafspraken van de Europese Richtlijn 1999/93/EG voor elektronische handtekeningen.

European Telecommunications Standards Institute – ETSI: Een organisatie die verantwoordelijk is voor het bepalen van standaarden en normen op telecommunicatiegebied die geldig zijn voor geheel Europa.

Europese Richtlijn: In het kader van PKI wordt hiermee bedoeld het document 1999/93/EG van het Europees parlement en de Raad, d.d.13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (Publicatieblad nr.L013 d.d. 19/01/2000, p.12-20).

Evaluation Assurance Level – EAL: Een pakket bestaande uit betrouwbaarheidscomponenten uit ISO/IEC 15408 Deel 3 die een punt vertegenwoordigen op de betrouwbaarheidsschaal zoals die is gedefinieerd in de Common Criteria.

Extended Normalized Certificate Policy – NCP+: Een Certificate Policy voor niet-gekwalificeerde certificaten die hetzelfde kwaliteitsniveau geeft als voor gekwalificeerde certificaten geldt (in de QCP), maar buiten de werking van de Europese Richtlijn. Deze wordt gebruikt in situaties waar het gebruik van een SUD nodig wordt geacht.

Federal Information Processing Standard – FIPS: Een officiële standaard voor de Verenigde Staten en uitgegeven door de NIST. In het kader van PKI zijn vooral FIPS 140 (“Security Requirements for Cryptographic Modules”) en FIPS 186-2 (“Digital Signature Standard”) van belang.

FQDM - Fully Qualified Domain Name

Geavanceerde Elektronische Handtekening: een Elektronische Handtekening die voldoet aan de volgende eisen:

1. Zij is op unieke wijze aan de ondertekenaar verbonden;
2. Zij maakt het mogelijk de ondertekenaar te identificeren;
3. Zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
4. Zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;

Gegevens voor het aanmaken van Elektronische Handtekeningen: zie Signature Creation Data.

Gegevens voor het verifiëren van een Elektronische Handtekening: zie Signature Verification Data.

Gekwalificeerd Certificaat: een Certificaat dat voldoet aan de eisen, gesteld krachtens artikel 18.15, tweede lid van de Telecommunicatiewet, en is afgegeven door een Certificatiedienstverlener die voldoet aan de eisen gesteld krachtens artikel 18.15, eerste lid van de Telecommunicatiewet. Het Certificaat dient tevens te strekken tot toepassing van de Gekwalificeerde Elektronische Handtekening.

Gekwalificeerde Elektronische Handtekening: een elektronische handtekening die voldoet aan de volgende eisen:
1. Zij is op unieke wijze aan de ondertekenaar verbonden;
2. Zij maakt het mogelijk de ondertekenaar te identificeren;
3. Zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
4. Zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;
5. Zij is gebaseerd op een Gekwalificeerd Certificaat als bedoeld in artikel 1.1 onderdeel dd van de Telecommunicatiewet;
6. Zij is gegenereerd door een veilig middel voor het aanmaken van Elektronische Handtekeningen als bedoeld in artikel 1.1 onderdeel gg van de Telecommunicatiewet.

Groepscertificaat: een op een SUD opgeslagen combinatie van twee Niet-Gekwalificeerde Certificaten die tezamen de functies van vertrouwelijkheid en authenticiteit ondersteunen en die voldoen aan de volgende vereisten:
1. Ze zijn uitgegeven aan een dienst of een functie door Digidentity, en
2. Ze zijn uitgegeven op basis van de binnen de PKI voor de Overheid geldende ‘Certificate Policy Services’ (PvE deel 3b)

Hardware Security Module (HSM): De randapparatuur dat wordt gebruikt aan de server kant om cryptografische processen te versnellen en om cryptografisch sleutelmateriaal veilig te bewaren. Hier dient met name gedacht te worden aan het aanmaken van sleutels.

Hashfunctie: Een functie die een bericht van willekeurige lengte omzet in een reeks met een vaste lengte en voldoet aan de volgende voorwaarden:
1. Het is praktisch onuitvoerbaar om voor een gegeven uitvoer een invoer te vinden die
2. deze uitvoer als resultaat heeft (“one-way”);
3. Het is praktisch onuitvoerbaar om voor een gegeven invoer een tweede invoer te vinden die dezelfde uitvoer als resultaat heeft (“zwak collision-free”);
4. Het is praktisch onuitvoerbaar om twee willekeurige berichten te vinden die dezelfde
5. uitvoer als resultaat hebben (“sterk collision-free”).

Hiërarchisch model: De PKI voor de overheid gaat uit van een hiërarchisch model. Dat betekent dat het vertrouwen in een keten doorgegeven wordt. Een eindgebruiker kan daarmee alle Certification Authorities vertrouwen die onder dezelfde stam-CA vallen.

Identificatie: Het vaststellen van de identiteit van een persoon (of zaak). Geaccepteerde legitimatiebewijzen zijn: geldig -paspoort, -ID kaart, -rijbewijs (alleen plastic).

Identiteit en Authenticiteit Certificaat: Zie “Authenticiteitcertificaat”.

Identiteitcertificaat: Zie “Authenticiteitcertificaat”.

Incident: Een gebeurtenis die geen onderdeel uitmaakt van de standaardwerking van een dienst en die een onderbreking van, of een reductie in, de kwaliteit van die dienst veroorzaakt of kan veroorzaken.

Integriteit: De zekerheid dat gegevens volledig zijn en niet zijn gewijzigd, ongeacht of dat opzettelijk, niet opzettelijk door menselijk toedoen of anderszins is gebeurd.

Internet Engineering Task Force – IETF: Een internationale organisatie die zich in wil zetten voor de ontwikkeling van de internet architectuur vanuit technisch-wetenschappelijk oogpunt.

Lightweight Directory Access Protocol – LDAP: Een open protocol dat applicaties in staat stelt om informatie uit directories te verkrijgen, zoals bijvoorbeeld e-mail adressen en sleutels.

Lokale Registratie Autoriteit (LRA): de organisatie-eenheid of functie aan wie de uitvoering van de taak van Registratie Autoriteit is opgedragen en die fysiek de identificatie gegevens van een aanvrager verzamelt, controleert, registreert en doorstuurt ten behoeve van de Certificaat uitgifte.

Middel voor het vervaardigen van handtekeningen: zie Signature Creation Device.

Niet-Gekwalificeerd Certificaat: een Certificaat dat niet voldoet aan de voor een Gekwalificeerd Certificaat gestelde eisen.

Non-repudiation (NL: Onloochenbaarheid, Onweerlegbaarheid): De eigenschap van een bericht om aan te tonen dat bepaalde gebeurtenissen of handelingen hebben plaatsgevonden, zoals het verzenden en ontvangen van elektronische documenten. Binnen de PKI voor de overheid wordt non-repudiation (van de inhoud van een bericht) bewezen door middel van het handtekeningcertificaat.

Object Identifier: een rij van getallen die op unieke wijze en permanent een object aanduidt.

Ondertekenaar (Engels: Signatory): (Voor de toepassing van de Telecommunicatiewet) *Degene die een middel voor het aanmaken van elektronische handtekeningen als bedoeld in artikel 1.1, onderdeel uu Telecommunicatiewet gebruikt.* [eIDAS]
In het kader van de PKI voor de overheid wordt onder de certificaathouder van het handtekeningcertificaat de ondertekenaar verstaan en wordt de term ‘ondertekenaar’ zelf niet gehanteerd.

Online Certificate Status Protocol (OCSP): een methode om de geldigheid van Certificaten online (en real time) te controleren. Deze methode kan worden gebruikt als alternatief voor het raadplegen van de CRL.

Onweerlegbaarheid: de eigenschap van een bericht om aan te tonen dat bepaalde gebeurtenissen of handelingen hebben plaatsgevonden, zoals het verzenden en ontvangen van elektronische documenten.

Overheids-CA: een CA die binnen de hiërarchie van de PKI voor de overheid de stam-CA is. Ze vormt in technische zin het centrale punt voor het vertrouwen binnen de hiërarchie en wordt aangestuurd door de Overheids-Policy Authority.

Overheids-Policy Authority: de hoogste beleidsbepalende autoriteit binnen de hiërarchie van de PKI voor de overheid die de regie over de Overheids-CA voert.

Overheid/Bedrijven en Organisatie: Binnen de PKI voor de overheid bestaan de domeinen Overheid/Bedrijven en Organisatie uit alle organisaties binnen overheid en bedrijfsleven.

Personal Unlock Key (PUK): een code die wordt gebruikt om cryptografische modules vrij te geven of te maken

Persoonlijk Certificaat: een op een SSCD opgeslagen combinatie van twee Niet-Gekwalificeerde Certificaten die tezamen de functies van authenticiteit en vertrouwelijkheid ondersteunen, alsmede een Gekwalificeerd Certificaat dat de functie van onweerlegbaarheid ondersteunt, en die voldoen aan de volgende vereisten:

1. Ze zijn uitgegeven aan een natuurlijke persoon door Digidentity, en
2. Ze zijn uitgegeven op basis van de binnen de PKI voor de Overheid geldende ‘Certificate Policy Domein Overheid en Bedrijven” (PvE deel 3a).

PKI voor de overheid: een afsprakenstelsel dat generiek en grootschalig gebruik mogelijk maakt van de Elektronische Handtekening, en faciliteert voorts identificatie op afstand en vertrouwelijke communicatie. Het afsprakenstelsel is eigendom van de Minister van Binnenlandse Zaken en Koninkrijksrelaties en wordt beheerd door de Policy Authority PKIoverheid.

PKIoverheid Certificaat: een onder de PKI voor de Overheid door Digidentity uitgegeven Persoonlijk Certificaat en Servercertificaat.

PKI voor de overheid: de Public Key Infrastructure van de Staat der Nederlanden. Policy Authority PKIoverheid – PA PKIoverheid: De Policy Authority (PA) voor de hiërarchie van de PKI voor de overheid. De PA ondersteunt de minister van Binnenlandse Zaken en Koninkrijksrelaties bij het beheer over de PKI voor de overheid. De dienstverlening van de PA is onder te verdelen in het beheren van de bovenste lagen van de infrastructuur, het toelaten van TSP’s tot de infrastructuur en het houden van toezicht op de betrouwbaarheid van de PKI voor de overheid. Zie ook het plaatje bij *“Hiërarchisch model”.*

Policy Management Authority: de organisatorische entiteit binnen Digidentity die verantwoordelijk is voor ontwikkelen, onderhouden en formeel vaststellen van aan de dienstverlening verwante documenten, inclusief dit CPS.

Private key (Nederlands: Private Sleutel): de sleutel van een asymmetrisch sleutelpaar die alleen bekend dient te zijn bij de houder ervan en strikt geheim moet worden gehouden. In het kader van de PKI voor de overheid wordt de Private Sleutel door de Certificaathouder gebruikt om zich elektronisch te identificeren, zijn Elektronische Handtekening te zetten of om een vercijferd bericht te ontcijferen.

Public key cryptografie: Het systeem waarbij een mechanisme van publieke sleutels en private sleutels wordt gebruikt. Dit houdt in dat er twee sleutels worden gebruikt. Eén sleutel wordt geheim gehouden (de private sleutel) en de andere sleutel mag publiekelijk worden verspreid (de publieke sleutel). Alles wat met de publieke sleutel vercijferd wordt is alleen met de private sleutel te ontcijferen en andersom. Het is een vorm van asymmetrische encryptie.

Public Key Cryptography Standard – PKCS: Een standaard op het gebied van public key cryptografie, ontwikkeld door RSA-laboratories. In het kader van de PKI voor de overheid zijn vooral PKCS#7 (Cryptographic Message Syntax Standard), PKCS#11 (Cryptographic Token Interface Standard), PKCS#12 (Personal Information Exchange Syntax Standard) en PKCS#15 (Cryptographic Token Information Format Standard) van belang.

Public Key Infrastructure – PKI: Een samenstelling 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.

Public Key (Nederlands: Publieke sleutel): De sleutel van een asymmetrisch sleutelpaar die publiekelijk kan worden bekendgemaakt. De publieke sleutel wordt gebruikt voor de controle van de identiteit van de eigenaar van het asymmetrisch sleutelpaar, voor de controle van de elektronische handtekening van de eigenaar van het asymmetrisch sleutelpaar en voor het vercijferen van informatie voor een derde.

Qualified Certificate Policy (QCP): Een Certificate Policy die een uitwerking van de vereisten bevat die zijn omschreven in artikel 18.15, eerste en tweede lid van de Telecommunicatiewet.

Registratie Autoriteit (RA): een Registratie Autoriteit zorgt voor de verwerking van Certificaataanvragen en alle daarbij behorende taken waarbij de verificatie van de identiteit van de Certificaathouder de belangrijkste is. In dit verband opereert Digidentity als RA.

Request for Comments – RFC: Een voorstel voor een standaard afkomstig van de IETF. Hoewel een RFC niet de formele status van een standaard heeft, worden in praktijk de RFC's normaliter gevolgd.

Revocation management service: Een dienst die verzoeken, die te maken hebben met intrekking van certificaten, behandelt en rapporteert, om zo de te nemen maatregelen te bepalen. De resultaten worden verspreid door middel van de Revocation Status Service.

Revocation service: Een dienst van een TSP waarbij deze certificaten intrekt bij beëindiging van de overeenkomst, constatering van fouten in het certificaat of bij compromittatie van de private sleutel die hoort bij de in het certificaat opgenomen publieke sleutel. De ingetrokken certificaten worden opgenomen in de Certificate Revocation List.

Root: het centrale gedeelte van een (PKI-)hiërarchie waaraan de gehele hiërarchie en haar betrouwbaarheidsniveau is opgehangen.

Root Certificate: zie Stamcertificaat.

Root Certification Authority (Root-CA): een Certificatie Autoriteit die het centrum van het gemeenschappelijk vertrouwen in een PKI-hiërarchie is. Het Certificaat van de Root-CA (de Root Certificate of Stamcertificaat) is self-signed, waardoor het niet mogelijk is de bron van de handtekening op dit Certificaat te authenticeren, alleen de integriteit van de inhoud van het Certificaat. De Root-CA wordt echter vertrouwd op basis van bijvoorbeeld de CP en andere documenten. De Root-CA hoeft niet noodzakelijkerwijs aan de top van een hiërarchie te zijn gepositioneerd.

Rivest-Shamir-Adleman algoritme – RSA-algoritme: Een cryptografische methode die gebruik maakt van een tweeledige sleutel. De private sleutel wordt bewaard door de eigenaar; de publieke sleutel wordt gepubliceerd. Data wordt vercijferd met de publieke sleutel van de ontvanger en kan alleen ontcijferd worden met de private sleutel van de ontvanger. Het RSA-algoritme is rekenintensief, waardoor het vaak wordt gebruikt om een digitale envelop te maken, die een met RSA vercijferde DES sleutel bevat en met DES vercijferde data.

Root-signing: Het ondertekenen van het certificaat van de Root-CA – het stamcertificaat – door de Root- CA zelf. Zie ook het plaatje bij “Hiërarchisch model”.

Secure Hash Algorithm – SHA: Een bepaald algoritme dat een concrete invulling geeft voor een Hashfunctie. Het nog veel gebruikte SHA-1 is ontwikkeld door de Amerikaanse overheid en maakt een Message Digest van 160 bits aan. De Advanced Encryption Standard en SHA-2 zijn opvolgers hiervan.

Secure Signature Creation Device (SSCD): een middel voor het aanmaken van Elektronische Handtekeningen dat voldoet aan de eisen gesteld krachtens artikel 18.17, eerste lid van de Telecommunicatiewet. Dit kan bijvoorbeeld een (bij Digidentity virtuele) smartcard of een USB token zijn.

Secure User Device (SUD): Een middel dat de gebruikers private sleutel(s) bevat, deze sleutel(s) tegen compromitteren beschermt en elektronische ondertekening, authenticatie of ontcijfering uitvoert namens de gebruiker.

Servercertificaat: een binnen de Veilige Omgeving van de Abonnee opgeslagen combinatie van twee Niet-Gekwalificeerde Certificaten die tezamen de functies van authenticiteit en vertrouwelijkheid ondersteunen en die voldoen aan de volgende vereisten:

1. Ze zijn door Digidentity uitgegeven aan een server, en
2. Ze zijn uitgegeven op basis van de binnen de PKI voor de Overheid geldende 'Certificate Policy Services' (PvE deel 3b).

Services Certificaat: een Servercertificaat of een Groepscertificaat.

Signature Creation Data: unieke gegevens, zoals codes of private cryptografische sleutels, die door de ondertekenaar worden gebruikt om een Elektronische Handtekening te maken.

Signature Creation Device: geconfigureerde software of hardware die wordt gebruikt voor het implementeren van de gegevens voor het aanmaken van Elektronische Handtekeningen.

Signature Verification Data: gegevens, zoals codes of cryptografische publieke sleutels, die worden gebruikt voor het verifiëren van een Elektronische Handtekening.

Secure Sockets Layer – SSL: Een protocol gecreëerd door Netscape voor het beheer van de veiligheid van bericht verzendingen in een netwerk en de toegang tot web servers. Het woord sockets verwijst hierbij naar de methode om data heen en weer tussen een client en een server programma te sturen in een netwerk of tussen programmalagen in dezelfde computer.

Security policy: De verzameling van regels, neergelegd door de beveiligingsautoriteit, die het gebruik van en de maatregelen ten aanzien van beveiligingsdiensten en faciliteiten regelen.

Self-signed certificaat: Een certificaat voor een Certification Authority, getekend door die Certification Authority zelf. Dit kan alleen bij het stamcertificaat van een hiërarchie.

Services certificaat: Een certificaat waarmee een dienst, functie of apparaat, bijvoorbeeld een server, wordt gekoppeld aan een rechtspersoon of andere organisatie. In het geval van een server wordt het certificaat aangeboden aan een browser, die toegang zoekt tot de server. Hierdoor kan deze vertrouwende partij zekerheid krijgen omtrent de identiteit van de eigenaar van de server. Een services certificaat is geen gekwalificeerd certificaat.

Sessiesleutel: Een symmetrische sleutel die één keer wordt gebruikt voor een berichtenuitwisseling of een telefoongesprek (een sessie). Na afloop van de berichtenuitwisseling of het telefoongesprek wordt de sleutel weggegooid.

SHA-2-RSA encryptie: Signing algoritme(versleuteling/unieke afscherming) voor alle certificaten en CRL's

Signing key (NL: Tekensleutel): De private sleutel die wordt gebruikt om een elektronische handtekening te zetten. Er kan onderscheid worden gemaakt tussen een signing key van een Certification Authority en een signing key van een eindgebruiker. Met de signing key van de eindgebruiker plaatst deze diens elektronische handtekening. Met de signing key van de Certification Authority worden onder andere de uitgegeven certificaten en de Certificate Revocation List getekend.

Sleutelpaar: In een asymmetrisch cryptografische systeem is dit een private sleutel en zijn wiskundig verbonden publieke sleutel. Deze hebben de eigenschap dat met behulp van de publieke sleutel een elektronische handtekening kan worden geverifieerd die met een private sleutel is gemaakt. In het geval van encryptie betekent deze eigenschap dat informatie die met de publieke sleutel is vercijferd met behulp van de private sleutel kan worden ontcijferd (of andersom).

Smartcard: Een plastic kaart ter grootte van een creditcard die in een chip elektronica bevat, inclusief een microprocessor, geheugenruimte en een voedingsbron. De kaarten kunnen worden gebruikt om informatie op te slaan en zijn makkelijk mee te nemen. Bij Digidentity is sprake van een virtuele smartcard die in de HSM ligt opgeslagen.

Stamcertificaat: het Certificaat van de Root-CA. Dit is het Certificaat behorend bij de plek waar het vertrouwen in alle binnen de PKI voor de overheid uitgegeven Certificaten zijn oorsprong vindt. Er is geen hoger liggende CA waaraan het vertrouwen wordt ontleend. Dit Certificaat wordt door de Certificaathouder (binnen de PKI voor de overheid is dat de Overheids-CA) zelf ondertekend. Alle onderliggende Certificaten worden uitgegeven door de houder van het stamcertificaat.

Subordinate CA – Sub CA: Een Certification Authority welk onderdeel is van een Certificatiedienstverlener of die onder verantwoordelijkheid van de Certificatiedienstverlener handelt. Bij de PKI voor de overheid wordt het certificaat van de Sub CA getekend met de signing key van de TSP Certification Authority. Zie verder “Certification Authority” en zie ook het plaatje bij “Hiërarchisch model”.

Token: Een beveiligd stukje hard- of software waarin de private sleutels van de eindgebruiker opgeslagen worden. Een hardware token kan ook cryptografische berekeningen uitvoeren. Voorbeelden van hardware tokens zijn een smartcard en een USB-token.

Trusted Service Provider - TSP (NL: Vertrouwende partij): Een natuurlijke of rechtspersoon die certificaten afgeeft of andere diensten in verband met elektronische handtekeningen verleent. [eIDAS] In het kader van de PKI voor de overheid kan de TSP ook diensten verlenen in verband met identiteit en vertrouwelijkheid. Een TSP heeft als functie het verstrekken en beheren van certificaten en sleutelinformatie, met inbegrip van de hiervoor voorziene dragers (bijvoorbeeld smartcards). De TSP heeft tevens de eindverantwoordelijkheid voor het leveren van de certificatiediensten. Daarbij maakt het niet uit of de TSP de feitelijke werkzaamheden zelf uitvoert of deze uitbesteedt aan anderen. Het is bijvoorbeeld niet ondenkbaar dat een TSP de CA-functie en/of de RA-functie uitbesteedt. Zie ook het plaatje bij “Hiërarchisch model”.

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.

USB-token: Een USB-token is een token vergelijkbaar met een smartcard, maar heeft een andere vorm. Het is een medium om certificaten op te slaan. Het verschil is dat voor een USB-token geen extra smartcardreader hoeft te worden geïnstalleerd. Daarentegen is het niet mogelijk om eindgebruikerskenmerken op de USB-token op de nemen, zoals een foto of persoonsgegevens.

Validity data (NL: Geldigheidsgegevens): Aanvullende gegevens, verzameld door de ondertekenaar en/of de controlerende partij, benodigd om de juistheid en geldigheid van een elektronische handtekening te controleren om zo aan de vereisten van de Certificate Policy te voldoen.

Veilig middel voor het aanmaken van Elektronische Handtekeningen: zie Secure Signature Creation Device.

Veilige Omgeving: De omgeving van het systeem dat de sleutels van de Servercertificaten bevat. Binnen deze omgeving is het toegestaan de sleutels softwarematig te beschermen, in plaats van in een SUD. De compenserende maatregelen hiervoor moeten van dusdanige kwaliteit zijn dat het praktisch onmogelijk is de sleutels ongemerkt te stelen of te kopiëren. Bij compenserende maatregelen moet bijvoorbeeld worden gedacht aan een combinatie van fysieke toegangsbeveiliging, logische toegangsbeveiliging, logging, audit en functiescheiding.

Vertrouwelijkheid: De garantie dat gegevens daadwerkelijk en uitsluitend terechtkomen bij degene voor wie zij zijn bedoeld, zonder dat iemand anders ze kan ontcijferen. Buiten de private sector wordt hiervoor ook wel de term “exclusiviteit” gebruikt.

Vertrouwelijkheidcertificaat: Certificaat waarin de Publieke Sleutel wordt gecertificeerd van het sleutelpaar dat voor vertrouwelijkheidsdiensten wordt gebruikt.

Vertrouwende partij: de natuurlijke persoon of rechtspersoon die ontvanger is van een Certificaat en die handelt in vertrouwen op dat Certificaat.

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.

X.509: een ISO standaard die een basis voor de elektronische opmaak van Certificaten definieert.

Bijlage B - Afkortingen

AuSO	Authenticatie Service Organisatie: De partij met wie Digidentity samenwerkt voor de face-to-face controle.
CA	Certificatie Autoriteit (Certification Authority)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DID	Een digitale representatie van een natuurlijke of rechtspersoon, welke bij Digidentity altijd uniek is
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunication Standardisation Institute
FQDN	Fully Qualified Domain Name
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
ACM	Autoriteit Consument & Markt (Toezichthouder)
PIN	Personal Identification Number (Nederlands; Persoonlijk Identificatie Nummer)
PKI	Public Key Infrastructure
PA	Policy Authority
PUK	Personal Unlock Code
QCP	Qualified Certificate Policy
RA	Registratie Autoriteit (Registration Authority)
SSCD	Secure Signature Creation Device
SUD	Secure User Device
TSP	Trusted Service Provider
TTP	Trusted Third Party
VIS	Verificatie Identificatie Systeem
VPN	Virtual Private Network
WBP	Wet Bescherming Persoonsgegevens
WID	Wet op de Identificatieplicht