PKI DISCLOSURE STATEMENT

Datum: 22 augustus 2017
Versie : 1.3

Be Verified
Digidentity BV | Waldorpstraat 17p | 2521 CA 's-Gravenhage | NL | +31 (0)88 778 78 78 | info@digidentity.com
IBAN NL35RABO0102420173 | BIC RABONL2U | VAT- NL 8196.96.079.B.01 | KVK Den Haag 27322631

PKI Disclosure Statement

Het PDS (PKI Disclosure Statement) is geen vervanging óf aanpassing van het Digidentity CP/CPS (Certificate Policy/Certification Practice Statement). Het CP/CPS dient gelezen te worden op de website alvorens een u een aanvraag doet, of vertrouwt op een Digidentity BV uitgegeven certificaat.

Het PDS vangt de belangrijkste zaken van het CP/CPS samen. Het PDS heeft geen contractuele relatie tussen Digidentity en enig ander.

De huidige versie van het PDS is goedgekeurd door Digidentity en heeft alleen betrekking tot Digidentity en haar producten. Het PDS wordt van tijd tot tijd geauditeerd eventuele aanpassing zijn conform de eis.

Versie historie

Datum	Auteur	Versie	Opmerking/wijziging
30-09-2016	Digidentity EB	1.0	Gebaseerd op ETSI EN 319 411-1 Annex A
12-01-2017	Digidentity EB	1.1	Tekstuele review
05-03-2017	Digidentity EB	1.2	Vervanging van CSP naar TSP
22-08-2017	Digidentity TB	1.3	- Tekstuele en redactionele wijzigingen n.a.v. interne audit - Hoofdstuk 11 Logo's ETSI TS 102 042/ETSI EN 319-411-2 vervangen door gecombineerd logo ETSI EN 319-411-1/ETSI EN 319-411-2

Inhoudsopgave

1. TSP-contact informatie

Digidentity BV

Bezoekadres;	*Postbus*
Waldorpstraat 17p	Postbus 19148
2521 CA 's-Gravenhage (The Hague)	2500 CC 's-Gravenhage (The Hague)
Nederland	Nederland

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

Voor intrekking van een door Digidentity uitgegeven certificaat verwijzen wij u naar de website.

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 kantoor 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 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.

CPS §3.4 Schorsing en intrekking van Certificaten

2. Certificaat type, validatie, procedure en gebruik

Onderstaand overzicht geeft de certificaattypes weer van Digidentity;

Domein: Burger

Persoonsgebonden authenticiteit certificaten:	2.16.528.1.1003.1.2.3.1
Persoonsgebonden onweerlegbaarheid certificaten:	2.16.528.1.1003.1.2.3.2
Persoonsgebonden vertrouwelijkheid certificaten:	2.16.528.1.1003.1.2.3.3

Domein: Organisatie

Persoonsgebonden authenticiteit certificaten:	2.16.528.1.1003.1.2.5.1
Persoonsgebonden onweerlegbaarheid certificaten:	2.16.528.1.1003.1.2.5.2
Persoonsgebonden vertrouwelijkheid certificaten:	2.16.528.1.1003.1.2.5.3

Domein: Services

Services authenticiteit certificaten:	2.16.528.1.1003.1.2.5.4
Services vertrouwelijkheid certificaten:	2.16.528.1.1003.1.2.5.5
Services server certificaten:	2.16.528.1.1003.1.2.5.6

Certificaten uitgeven door Digidentity zijn van toepassing op

- het digitaal ondertekenen van documenten (onweerlegbaarheid)
- het authentiseren van een gebruiker bij diensten (authenticatie)

3. Beperkingen in de betrouwbaarheid

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.

CPS §4.5.2 Beperkingen in het gebruik

4. Verplichtingen van abonnees

De abonnee 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, waar dit CPS deel van 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. onjuistheden 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 telecommunicatiefaciliteiten 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 ervoor 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 PKI overheid 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.

CPS §4.5.1 Verplichtingen van de Certificaathouder

5. Verplichtingen van vertrouwende partijen met betrekking tot het controleren van de certificaatstatus

Als een Vertrouwende Partij redelijkerwijs geacht wordt een certificaat te vertrouwen dient deze:

- er voor te zorgen dat het gebruik van certificaten uitgegeven onder de Certificate Policy is beperkt tot het toegestane gebruik (zie Digidentity PKIo CPS).
- te controleren of de geldigheid van het certificaat niet is verstreken.
- er voor te zorgen dat het certificaat niet is geschorst of ingetrokken door toegang tot de huidige intrekkingsstatus informatie die beschikbaar en gespecificeerd is in het betreffende Certificaat.
- te bepalen dat een dergelijk certificaat voldoende waarborgen biedt voor het beoogde gebruik.

6. Gelimiteerde garantie/disclaimer en aansprakelijkheid

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.

CPS §9.8.1. Beperkingen van aansprakelijkheid van Digidentity

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.

CPS §9.8.3. Uitgesloten aansprakelijkheid

7. Toepasselijke overeenkomsten CPS

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/ondersteuning/pkioverheid/aansluiten-als-tsp/programma-van-eisen/

8. Privacy Beleid

Het privacy beleid, samen met de Algemene Voorwaarden, beschrijft hoe Digidentity uw privacy beschermt en hoe Digidentity gebruik maakt van de door u verstrekte persoonlijke informatie voor de levering van de Digidentity Identity Service aan u.

Digidentity gelooft erin dat uw gegevens tot niemand anders dan u alleen behoren. Dat is de kern van onze service. Digidentity gebruikt uw gegevens alleen om uw identiteit mee te verifiëren. Digidentity deelt uw gegevens niet met derden. Digidentity staat niemand toe om uw gegevens te gebruiken en/of om toegang te krijgen tot uw gegevens, voor andere doeleinden dan bedoeld voor de levering van de Digidentity Identity Service aan u.

https://www.digidentity.eu/nl/home/#privacy-policy

9. Terugbetalingsbeleid

Er is geen terugbetaling of terugbetalingsbeleid bij Digidentity BV.

10. Toepasselijk wetgeving, klachten- en geschillenbeslechting

10.1 Toepasselijke wetgeving

Abonnees en vertrouwende partijen zullen de, door Digidentity BV, uitgegeven certificaten alleen gebruiken met de toepasbare wet- en regelgeving. Digidentity behoudt het recht om certificaten te weigeren en/of in te trekken wanneer de, naar redelijke mening, toepasselijke wet- en regelgeving niet gehanteerd wordt.

Digidentity committeert naar Nederlandse wet- en regelgeving, de Telecommunicatiewet.

10.2 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 en Digidentity vallen onder het Nederlands recht.

11. CA, bewaarplaats licenties, trust marks en audits

Digidentity wordt periodiek onderworpen aan compliance audits conform ETSI EN 319-411-1 (voorheen ETSI TS 102 042), ETSI EN 319-411-2 en ISO27001. Dit gebeurt jaarlijks en na significante wijzigingen in de procedures en infrastructuur.