Belgian eID
PKI Disclosure Statement

Company:	*Certipost*
Version:	*2.0*
Status:	*FINAL*
Rel. Date:	*07/09/2017*

Document Control

Date	Version	Editor	Change
13/02/2017	1.0	Bart Eeman	Initial version
30/08/2017	2.0	Cristof Fleurus / Don Giot	eIDAS Update

Disclaimer:

Deze disclaimer is van toepassing op de “Certification Practice Statement” en de “PKI Disclosure Statement”. Dit document is een vertaling naar het Nederlands van het originele, Engelstalige document gepubliceerd op https://repository.eid.belgium.be/. Dit Nederlandstalige document dient als een informatieve bron. De Engelstalige versie van het CPS document is de enige officiële versie van de CPS en is het enige document dat juridisch bindende verplichtingen kan creëren. In het geval dit Nederlandstalig document afwijkt van de Engelstalige CPS, in het geval van twijfel, of in het geval dit document een oudere versie van de gepubliceerde Engelstalige CPS bevat, zal steeds de laatst gepubliceerde versie van het Engelstalige CPS voorrang hebben.

Inhoudstafel

1 Samenvatting

Het doel van deze PKI Disclosure Statement (PDS) is om de hoofdelementen van de Certification Practice Statement en de bijzondere voorwaarden in een beter leesbaar en begrijpelijk formaat samen te vatten en te presenteren, voor de abonnees en de vertrouwende partijen (ook “relying parties” genoemd”).

Deze PDS vervangt geenszins de Certification Practice Statements, waaronder certificaten worden uitgegeven.

Vooraleer een certificaat aan te vragen of er op te vertrouwen, moet de lezer eerst de op http://repository.eid.belgium.be/ gepubliceerde CPS (i.e. Verklaring met betrekking tot de certificatiepraktijk) lezen.

De structuur van dit document stemt overeen met ETSI TS 101 456 Annex B.2 "De PDS-structuur".

2 Contactinformatie CA

Gelieve vragen over deze PKI Disclosure Statement te richten aan:

Certipost nv
Administratief Beheer – Citizen / Foreigner CA
Muntcentrum
1000 Brussel

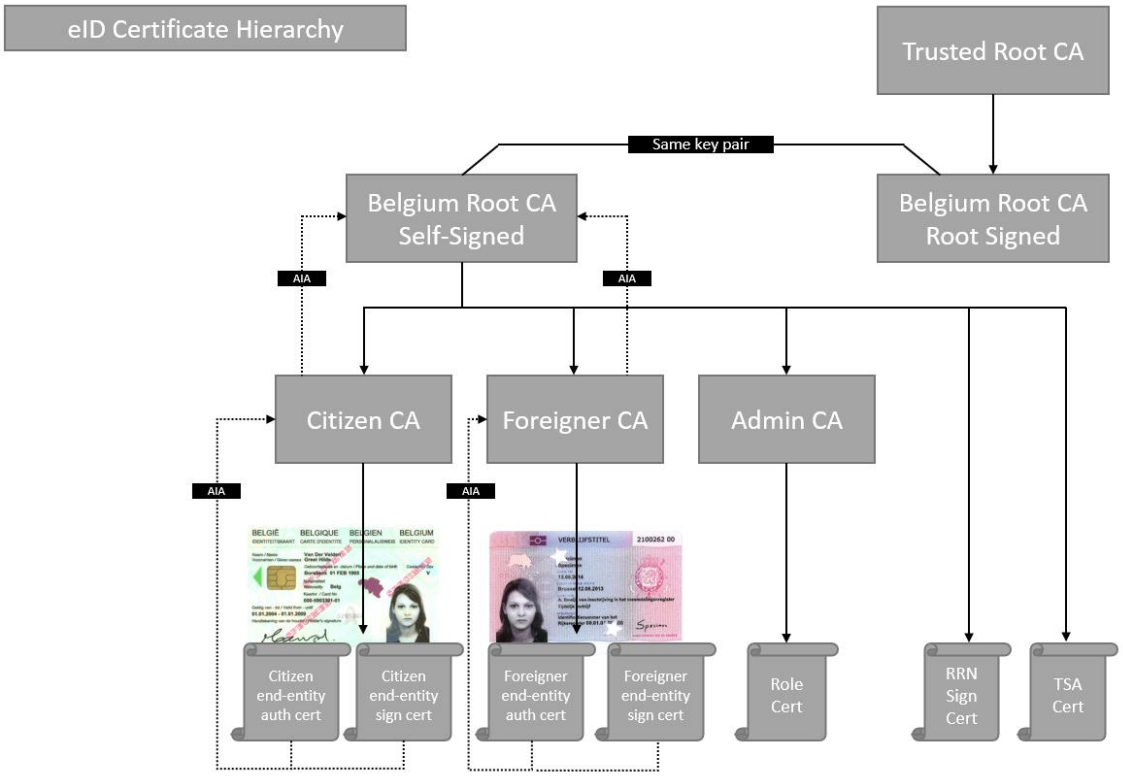
3 Soorten certificaten, procedures voor validatie en gebruik van certificaten

Binnen de Belgische eID PKI zijn er meerdere types uitgevende Certificaatautoriteiten (CA) (zonder de Belgische Root-CA's). Elk type uitgevende CA mag enkel certificaten met goedgekeurde certificaatprofielen uitgeven (https://stage-pki.belgium.be/resources/) voor dat toegestane type. Voor elk type certificaat dat wordt uitgegeven, wordt een korte beschrijving gegeven over de registratie, de validatie en het gebruik. Hieronder vindt u een overzicht van twee types uitgevende CA's, met de types certificaten die zij kunnen uitgeven:

- Citizen CA
  - Citizen authenticatie certificaat
  - Citizen elektronische handtekening certificaat
- Foreigner CA
  - Foreigner authenticatie certificaat
  - Foreigner elektronische handtekening certificaat

3.1 De eID-Hiërarchie

De structuur van de eID PKI-hiërarchie is als volgt:



3.2 Initiële registratie: voor een elektronische identiteitskaart:

Het Nationaal Rijksregister (RRN) fungeert als Registratieautoriteit (RA) samen met de steden en gemeenten die de Lokale Registratieautoriteiten (LRA) zijn. Wanneer een onderdaan (d.w.z. de burger of buitenlander) een elektronische identiteitskaart (eID) aanvraagt, zal de LRA de identificatie van de onderdaan uitvoeren volgens de procedures en voorschriften die van toepassing zijn op de afgifte van eID's. Dit identificatieproces vereist dat de onderdaan fysiek aanwezig is bij de LRA.

Na de identificatie dient de LRA een aanvraag in voor het aanmaken van de certificaten voor de onderdaan. Dit is een belangrijk onderdeel van het toegepaste inschrijvingsproces voor de eID. Na dit aanvankelijke certificaatverzoek worden geheime sleutels gegenereerd op beveiligde smartcards (Qualified Signature Creation Device (QSCD)) overeenkomstig met de Europese en Belgische handtekeningwetgeving. De kaartfabrikant is verantwoordelijk voor het beveiligen van de smartcard met een persoonlijk identificatienummer (PIN).

Na goedkeuring van de certificaataanvraag stuurt de RA een certificaatuitgifteverzoek aan de CA. Als de vereisten voor het certificaatuitgifteverzoek zijn vervuld (zie CPS), geeft de CA het certificaat uit en levert het aan de RA.

De RA verzoekt de kaartfabrikant om de uitgegeven certificaten op de eID te laden. De kaartfabrikant levert de eID met certificaten veilig aan de LRA, waarna de onderdaan zijn eID-kaart kan ophalen.

3.3 Doel van het certificaat:

In deze sectie bespreken we het doel van de bestaande end-entity-certificaten binnen de Belgische eID:

- (Citizen/Foreigner) Authenticatiecertificaat: Dit certificaat wordt gebruikt door burgers om zich te authenticeren in online toepassingen gebruikmakende van TLS-authenticatie.
- (Citizen/Foreigner) Handtekeningcertificaat: Dit certificaat wordt gebruikt voor niet-ontkenning en maakt het mogelijk gekwalificeerde elektronische handtekeningen te zetten.

Voor een meer gedetailleerde beschrijving, verwijzen we naar de CP/CPS-verklaring voor elke respectievelijke Certificatieautoriteit.

4 Beperking van het gebruik van de vertrouwelijkheid van certificaten

De aansprakelijkheid van de vertrouwensdienstleverancier (Trust Service Provider of TSP) ten opzichte van de abonnee of een vertrouwende partij beperkt zich tot het betalen van een schadevergoeding van €2500 per transactie, beïnvloed door de gebeurtenissen die zijn opgesomd in hoofdstuk 7 van dit document.

5 Verplichtingen voor abonnees

Tenzij anders vermeld in deze PDS, of in de gepubliceerde burger/buitenlander CPS, hebben de onderdanen onder meer de volgende plichten:

- Zich ervan onthouden een certificaat te vervalsen;
- Certificaten alleen gebruiken voor wettelijke en geoorloofde doeleinden, overeenkomstig de CPS;
- Een nieuwe Elektronische Identiteitskaart (en dus Burgercertificaten of Buitenlandercertificaten) aanvragen in geval van wijzigingen aan de informatie die in het certificaat opgenomen is;
- De publieke sleutel van de onderdaan niet gebruiken om in het kader van een gepubliceerd Burgercertificaat/Buitenlandercertificaat andere certificaten te verkrijgen;
- Voorkomen om roekeloos om te gaan met de geheime sleutels en voorkomen dat ze verloren gaan, openbaar gemaakt worden, wijzigingen ondergaan of op ongeoorloofde wijze gebruikt worden;
- De politie, het gemeentebestuur of de RA Helpdesk contacteren voor een aanvraag tot schorsing van een certificaat, ingeval van een gebeurtenis die het vermoeden doet rijzen dat de materiële integriteit van het certificaat in het gedrang gekomen is. Met dergelijke gebeurtenissen wordt onder meer bedoeld: verlies, diefstal, wijziging, ongeoorloofde openbaarmaking of een andere aantasting van de geheime sleutel van een burger-/buitenlandercertificaat (of van beide)

- De politie, het gemeentebestuur of de RA Helpdesk contacteren voor een aanvraag tot intrekking van een certificaat, in geval van een gebeurtenis die het vermoeden doet rijzen dat de materiële integriteit van het certificaat in het gedrang is gekomen. Met dergelijke evenementen wordt onder meer bedoeld: het verlies, de diefstal, de wijziging, de ongeoorloofde openbaarmaking of een andere aantasting van de geheime sleutel van een burger-/buitenlandercertificaat (of van beide), of ingeval de controle over de geheime sleutels niet meer verzekerd is wegens het in gevaar brengen van de activatiegegevens (bv. pincode);
- Verplichting er redelijk zorg voor te dragen dat er geen ongeoorloofd gebruik wordt gemaakt van de geheime sleutel van de abonnee;
- Na in gevaarbrenging, de verplichting om onmiddellijk en definitief elk gebruik van de geheime sleutel te staken;
- Verplichting onmiddellijk te verwittigen indien de controle over de geheime sleutel verloren ging wegens het in gevaar brengen van de activatiegegevens (bv. pincode);

6 Verplichtingen van de partijen die vertrouwen op een CA-certificaat om de status ervan te controleren

Een partij die vertrouwt op een CA-certificaat moet:

- Voldoende geïnformeerd zijn over het gebruik van digitale certificaten en PKI;
- Mededelingen ontvangen en de voorwaarden van de burger/buitenlander CPS en de voorwaarden voor vertrouwende partijen naleven;
- Een certificaat valideren met behulp van een CRL, delta CRL, OCSP of webgebaseerde validatie van een certificaat, overeenkomstig de procedure voor de validatie van een certificaat;
- Enkel tijdens de geldigheidsperiode vertrouwen stellen in een certificaat als het niet geschorst of ingetrokken werd;
- Op een certificaat vertrouwen in de mate dat dat mogelijk is in de gegeven omstandigheden.

Enkel de vertrouwende partijen die toegang hebben tot de informatie in de CA Repository's en op de website, zijn verantwoordelijk voor het inschatten van en het vertrouwen op de erin vervatte informatie.

Indien een vertrouwende partij vaststelt of vermoedt dat de geheime sleutel gecompromitteerd werd, moet hij de RA-helpdesk hiervan onmiddellijk op de hoogte brengen.

7 Toepasselijke wetgeving en bepalingen inzake beperkte aansprakelijkheid

De aansprakelijkheid van de TSP ten opzichte van de abonnee of een vertrouwende partij beperkt zich tot het betalen van een schadevergoeding van €2500 per transactie, beïnvloed door de gebeurtenissen die zijn opgesomd in het hoofdstuk hieronder.

7.1 Gekwalificeerde certificaten

Wat de uitgifte van de gekwalificeerde certificaten betreft, regelt artikel 14 van de Wet op de Elektronische Handtekeningen de aansprakelijkheid van de TSP.

Volgens deze bepaling is de TSP aansprakelijk voor schade die wordt berokkend aan elke instelling, natuurlijk of rechtspersoon die redelijkerwijze vertrouwen stelt in het certificaat, voor wat betreft:

a) de juistheid op het ogenblik van uitgifte van het gekwalificeerd certificaat van alle gegevens die erin opgenomen zijn en het feit dat het certificaat alle voorgeschreven gegevens voor een gekwalificeerd certificaat bevat;

b) de garantie dat, op het ogenblik van uitgifte van het gekwalificeerd certificaat, de in het certificaat geïdentificeerde ondertekenaar houder was van de geheime sleutel die overeenstemt met de openbare sleutel die in het certificaat werd uitgegeven of geïdentificeerd;

c) de garantie dat de geheime sleutel en de publieke sleutel complementair gebruikt kunnen worden.

De TSP is aansprakelijk voor schade toegebracht aan een entiteit, natuurlijk of rechtspersoon die redelijkerwijs rekent op het certificaat, ingeval de intrekking van het certificaat niet geregistreerd werd, tenzij de TSP kan bewijzen dat het niet nalatig geweest is.

7.2 Certificaten die niet als gekwalificeerde certificaten beschouwd kunnen worden

De algemene aansprakelijkheidsregels zijn van toepassing op schade toegebracht aan een entiteit, natuurlijk of rechtspersoon die redelijkerwijs vertrouwen stelt in een certificaat uitgegeven door de TSP.

De TSP wijst uitdrukkelijk elke aansprakelijkheid af ten opzichte van vertrouwende partijen, in alle gevallen waarin het authenticatiecertificaat gebruikt wordt in de context van toepassingen die kunnen gebruikt worden voor het aanmaken van elektronische handtekeningen.

7.3 Uitgesloten Aansprakelijkheid

De TSP zal geenszins aansprakelijk kunnen worden gesteld voor verlies dat betrekking heeft op of voortkomt uit een (of meerdere) van de volgende omstandigheden of oorzaken:

- als het certificaat in het bezit van de eisende partij, of anders het voorwerp van een claim in het gedrang is gekomen door de ongeoorloofde bekendmaking of het ongeoorloofde gebruik van het certificaat of, een wachtwoord of activatiegegevens die worden gebruikt om de toegang hiertoe te controleren;
- als het certificaat in het bezit van de eisende partij, of anders het voorwerp van een claim, werd uitgegeven als gevolg van enige misinterpretatie, feitelijke vergissing of nalatigheid van een persoon, entiteit of organisatie;
- als het certificaat in het bezit van de eisende partij, of anders het voorwerp van een claim, is vervallen of werd ingetrokken vóór de datum van de omstandigheden die aanleiding gaven tot de claim;
- als het certificaat in het bezit van de eisende partij, of anders het voorwerp van een claim, werd gewijzigd of veranderd op welke manier dan ook, of op een andere

manier werd gebruikt dan is toegestaan volgens de voorwaarden van de CP/CPS en/of de relevante overeenkomst met de houder van het certificaat of een toepasbare wet of reglementering;

- indien de geheime sleutel geassocieerd met het certificaat in het bezit van de eisende partij, of anders het voorwerp van een aanspraak, in het gedrang is gekomen;
- als het certificaat in het bezit van de eisende partij werd uitgegeven op een manier die een inbreuk betekent op een toepasbare wet of reglementering;
- computerhardware of -software, of wiskundige algoritmes, zijn ontwikkeld zodat ze publiekesleutelcryptografie of asymmetrische cryptosystemen onveilig maken, op voorwaarde dat Certipost commercieel redelijke praktijken hanteert ter bescherming tegen inbreuken op de beveiliging die voortkomen van dergelijke hardware, software of algoritmen;
- stroompanne, stroomonderbreking of andere stroomstoringen, op voorwaarde dat Certipost commercieel redelijke methodes gebruikt ter bescherming tegen dergelijke storingen;
- panne van een of meerdere computersystemen, communicatie-infrastructuur, verwerking, of opslagmedia of -mechanismen, of een subcomponent van de voorgaande, die niet onder de exclusieve controle van Certipost en/of zijn onderaannemers of dienstverleners vallen;
- een of meerdere van de volgende gebeurtenissen: een natuurramp of overmacht (met inbegrip van en zonder beperkte zijn tot: overstroming, aardbeving, of enige andere natuurlijke of aan het weer gerelateerde omstandigheden); arbeidsverstoringen, oorlog, oproer of openlijke militaire vijandelijkheden; strijdige wetgeving of overheidsactie, verbod, embargo of boycot; onlusten of verstoring van het openbare leven; brand of ontploffing; catastrofale epidemie; handelsembargo; beperking of belemmering (met inbegrip van, maar niet beperkt tot exportcontroles); onbeschikbaarheid of gecompromitteerde integriteit van telecommunicatie; met inbegrip van wettelijke verplichting, alle vonnissen van bevoegde rechterlijke instanties waaraan Certipost onderworpen is of kan zijn; en elke gebeurtenis of omstandigheid of reeks van omstandigheden die buiten de controle van Certipost vallen.

8 Toepasbare akkoorden, verklaring met betrekking tot de certificatiepraktijk, certificatenbeleid

Deze PKI Disclosure Statement doet dienst als een samenvatting voor de Certification Practice Statements (CPS, verklaringen met betrekking tot de certificatiepraktijk), en verwijst naar andere operationele documenten voor meer details over de aanvraag- en valideringsprocedures.

9 Gegevensbescherming

De TSP streeft ernaar de ISO 27001 & ISO 27002-beveiligingsnormen na te volgen voor het definiëren en implementeren van operationele controles voor de informatieveiligheid.

10 Richtlijnen voor terugbetaling

Niet van toepassing.

11 Toepasselijk recht en clausules voor het regelen van geschillen

Alle diensten inzake certificaten worden uitsluitend beheerst door het Belgisch recht.

12 Certificatenautoriteit en licenties voor certificatendirectory, handelsmerk van vertrouwelijkheid en audit

Wat het gekwalificeerd handtekeningcertificaat voor elektronische handtekeningen betreft, gaat de TSP te werk volgens de bepalingen van EU Regelgeving N°910/2014, dat het wettelijk kader bepaalt voor elektronische handtekeningen in België.

De TSP voldoet aan de vereisten die zijn opgesomd in de ETSI-beleidsdocumenten die verwijzen naar gekwalificeerde certificaten, waaronder:

- EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;

  Part 2: Requirements for trust service providers issuing EU qualified certificates;
- EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles;

  Part 5: QcStatements

De TSP aanvaardt nalevingsgerichte controles, om na te gaan of de vereisten, procedures en dienstniveaus overeenkomstig zijn met de contractuele vereisten en met de relevante industriestandaarden. De TSP aanvaardt deze audits m.b.t. de eigen praktijken en procedures, voor zover dit niet indruist tegen bepaalde voorwaarden zoals de vertrouwelijkheid van de informatie, handelsgeheimen, enz. Dergelijke controles worden hetzij rechtstreeks uitgevoerd, hetzij door bemiddeling van:

- De autoriteit die toezicht houdt op de certificatiedienstverleners in België, handelend onder de autoriteit van de Belgische Federale Overheid.
- De Belgische Federale Overheid of een derde partij aangesteld door de Belgische Federale Overheid.

De TSP evalueert de resultaten van deze audits, vooraleer ze verder in te voeren.

13 Afkortingen en terminologie

CA	**Certification Authority**
CC	Common Criteria
CM	Card Manufacturer
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
RA	Registration Authority
TSP	Trust Service Provider