Belgian eID
PKI Disclosure Statement

Company:	*Certipost*
Version:	*1.0*
Status:	*Final*
Rel. Date:	*07/09/2017*

Document Control

Date	Version	Editor	Change
30/08/2017	1.0	Cristof Fleurus / Don Giot	German Translation

Haftungsausschluss:

Diese rechtlichen Hinweise gelten für das "Certificate Practice Statement" (CPS) und das "PKI Disclosure Statement" (PDS). Dieses Dokument ist eine Übersetzung ins Deutsche des ursprünglichen Englischen Dokuments, das auf der Website https://repository.eid.belgium.be veröffentlicht wird. Dieses Deutschsprachige Dokument dient als Informationsquelle. Die Englische Version des CPS-Dokuments ist die einzige offizielle Version des CPS und ist das einzige Dokument, das rechtlich verbindliche Verpflichtungen schaffen kann. Für den Fall, dass dieses Niederländische Dokument aus dem Englischen CPS unterscheidet, im Fall von Zweifeln, oder wenn dieses Dokument eine ältere Version der Englischen CPS-Publikation ist, wird immer die meist rezent publizierte Version der Englischen CPS vorherrschen.

Inhaltsverzeichnis

1 Zusammenfassung

Der Zweck dieser PKI Disclosure Statement (PDS) ist es, die Kernpunkte der Zertifizierungsrichtlinie (Certification Practice Statement - CPS) und die Sonderbestimmungen in eine lesbarere und verständlichere Fassung für die Zertifikatnehmer und auf die Zertifikate vertrauende Dritte zusammenzufassen und zu präsentieren.

Dieser PDS tritt nicht anstelle der Zertifizierungsrichtlinie (CPS), unter der die digitalen Zertifikate ausgegeben sind. Der Leser muss die CPS auf https://repository.eid.belgium.be lesen, bevor er ein Zertifikat anwendet oder auf dieses vertraut.

Die Struktur des vorliegenden Dokuments wurde auf ETSI TS 101 456 Annex B.2 "The PDS Structure“ abgestimmt.

2 CA Kontaktinformation

Fragen zu diesem PDS sind an folgende Anschrift zu richten:

Certipost nv / sa
Policy administration – Citizen / Foreigner CA
Centre Monnaie
1000 Brüssel

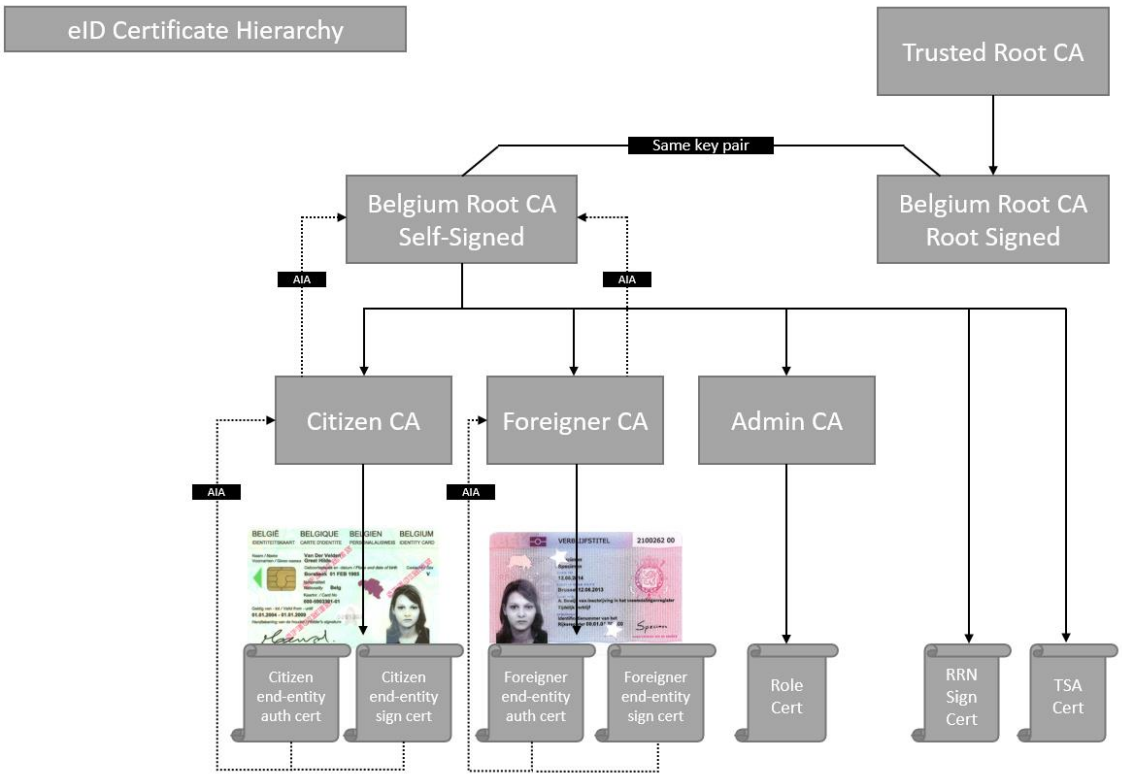
3 Zertifikatstypen, Validierungsverfahren und Zertifikatverwendung

Die belgische PKI sieht mehrere Zertifizierungsstellen für CA-Zertifikate vor (exkl. die belgischen Root-CA). Jede CA-Zertifizierungsstelle kann nur digitale Zertifikate mit den für diese Stelle genehmigten Profilen für digitale Zertifikate (https://stage-pki.belgium.be/resources/) ausstellen. Für jedes digitale Zertifikat, das ausgestellt wird, gibt es eine kurze Beschreibung des Registrierungsverfahrens, der Validierung und der Verwendung. Die unterstehende Übersicht zeigt die zwei verschiedenen CA-Zertifizierungsstellen und die Zertifikate, die diese ausstellen:

- Citizen CA
  - Bürgerauthentifizierungszertifikat
  - Elektronisches Bürgersignaturzertifikat
- Foreigner CA
  - Ausländeridentitätszertifikat
  - Elektronisches Ausländersignaturzertifikat

3.1 Die eID-Hierarchie

Die Struktur der eID-PKI-Hierarchie ist:



3.2 Erste Registrierung: Für einen elektronischen Personalausweis

Das National Register (RRN) fungiert als Registrierungsstelle (RA) zusammen mit den belgischen Gemeinden, die die lokalen Registrierungsstellen (LRA) sind. Wenn das Subjekt (Der Bürger oder Ausländer) einen elektronischen Personalausweis (eID) beantragt, führt die LRA die Identifizierung des Betreffens nach den für die Lieferung von eID geltenden Verfahren und Vorschriften durch. Dieser Identifizierungsprozess erfordert, dass das Subjekt physisch an der LRA vorhanden ist.

Nach der Identifizierung, die LRA's Anfrage Zertifikate für die Themen. Dies ist ein integraler Bestandteil des angewandten Registrierungsprozesses für den elektronischen Personalausweis. Nach dieser ersten Zertifikatsanforderung werden private Schlüssel auf sichere Signatur-Smartcards nach europäischem und belgischem Signaturgesetz erstellt. Der Kartenhersteller ist für die Sicherung der Chipkarte verantwortlich, auf der sich das qualifizierte Signaturerstellungsgerät (QSCD) mit einer persönlichen Identifikationsnummer (PIN) befindet.

Nach der Genehmigung der Zertifikatsanwendung sendet die RA eine Zertifikatausgabeanforderung an die CA. Wenn die Voraussetzungen für die Zertifizierungsrichtlinie erfüllt sind (CPS), gibt die CA das Zertifikat aus und liefert sie an die RA

Die RA fordert den Kartenhersteller auf, die ausgestellten Zertifikate auf dem elektronischen Personalausweis zu laden. Der Kartenhersteller liefert die elektronische Identitätskarte sicher mit den Zertifikaten an die LRA, danach kann das Thema seine eID-Karte mit der LRA abrufen.

3.3 Zweck des Zertifikats:

In diesem Abschnitt beschreiben wir den Zweck der Anwenderzertifikate innerhalb der belgischen eID:

- (Bürger/Ausländer) Authentifizierungszertifikat: Das Authentifizierungszertifikat wird verwendet, um den Bürger in Online-Anwendungen mit TLS Client Authentication zu authentifizieren
- (Bürger/Ausländer): Elektronisches Signaturzertifikat: Das elektronische Signaturzertifikat wird für die Nichtabweisung verwendet und kann eine qualifizierte elektronische Signatur erstellen.

Für eine ausführlichere Beschreibung verweisen wir auf die Zertifizierungsrichtlinie der jeweiligen Zertifizierungsstelle.

4 Einschränkung der Haftungsfunktion von Zertifikaten (Haftungshöchstgrenze)

Die Haftung der TSP gegenüber dem Zertifikatnehmer oder einem vertrauenden Dritten wird auf die Zahlung einer Schadensvergütung von höchstens 2500 € pro Transaktion begrenzt, wobei die Art der Vorfälle im nachstehenden Abschnitt aufgelistet ist.

5 Verpflichtungen für Zertifizierungsnehmer

Außer wenn in der vorliegenden PDS oder die veröffentlichte Citizen / Foreigner Zertifizierungsrichtlinie anders angegeben, gelten für das Subjekt folgende Pflichten:

- Von der Manipulierung eines Zertifikats absehen;
- Zertifikate nur zu gesetzlichen und zugelassenen Zwecken gemäß dem CPS benutzen.
- Einen neuen elektronischen Personalausweis (und also Bürgerzertifikate und Ausländerzertifikat) im Falle einer Änderung der im Zertifikat veröffentlichten Information beantragen;
- Von der Nutzung des öffentlichen Schlüssels in einem ausgestellten Bürgerzertifikat / Ausländerzertifikat für die Ausstellung anderen Zertifikate absehen;
- Die Gefährdung, den Verlust, die Enthüllung, Änderung oder jeden anderen unzulässigen Gebrauch seiner Privatschlüssel vorbeugen;
- Die Polizei, die Gemeindeverwaltung oder den RA-Helpdesk benachrichtigen, um die Aussetzung eines Zertifikats bei einem (vermutlichen) Zwischenfall, der das Zertifikat materiell beschädigen könnte, zu beantragen; Zu den Zwischenfällen gehören Verlust, Diebstahl, Änderung, unbefugte Offenlegung oder andere Gefährdungen des privaten Schlüssels eines Bürgerzertifikats / Ausländerzertifikats oder beider Bürgerzertifikate / Ausländerzertifikate;
- Die Polizei, die Gemeindeverwaltung oder den RA-Helpdesk benachrichtigen, um die Aussetzung eines Zertifikats bei einem (vermutlichen) Zwischenfall, der die Integrität des Zertifikats beschädigt. Zu den Zwischenfällen gehören Verlust, Diebstahl, Änderung, unbefugte Offenlegung oder andere Gefährdungen des privaten Schlüssels eines Bürgerzertifikats / Ausländerzertifikat oder beider Bürgerzertifikate / Ausländerzertifikate oder auch der Kontrollverlust über den privaten Schlüssel aufgrund der Gefährdung der Aktivierungsdaten (z. B. PIN-Code);

- Verpflichtung zu angemessener Sorgfalt, um unerlaubte Handlungen mit dem privaten Schlüssel des Zertifikatnehmers zu vermeiden.
- Infolge der Gefährdung, der Verpflichtung nachkommen, die Nutzung des privaten Schlüssels unverzüglich und vollständig auszusetzen;
- Die Verpflichtung, den RA-Helpdesk unverzüglich zu benachrichtigen, wenn die Sicherheit des privaten Schlüssels aufgrund einer Gefährdung der Aktivierungsdaten (z. B. PIN-Code verloren) nicht mehr gewährleistet werden kann.

6 Verpflichtung vertrauender Dritter zur Überprüfung des Zertifikatstatus

Die Partei, die auf ein CA-Zertifikat vertraut:

- Wird über die Nutzung von elektronischen Zertifikaten und PKI ausreichend informiert;
- Wird über die Bedingungen des Bürger-/Ausländer Zertifizierungsrichtlinie sowie über die für die vertrauenden Dritten damit verbundenen Bedingungen informiert und erklärt sich mit diesen einverstanden;
- Wird ein Zertifikat mit Hilfe einer CRL-, Delta CRL-, OCSP- oder Web-basierten Zertifikatsbestätigung und in Übereinstimmung mit dem Validierungsprozess des Zertifizierungspfads bestätigen;
- Vertraut nur dann der Gültigkeit des Zertifikats, wenn dieses nicht gesperrt oder widerrufen worden ist;
- Vertraut einem Zertifikat auf einen den Umständen entsprechenden Weise.

Für den Zugang zu den Informationen in den CA-Dateien und auf der Website und für das Vertrauen in diese Daten und der Bestätigung haftet ausschließlich die vertrauende Drittpartei.

Wenn eine vertrauende Partei feststellt oder vermutet, dass ein privater Schlüssel gefährdet ist, muss sie den RA-Helpdesk unmittelbar benachrichtigen.

7 Haftungsausschlüsse und - Begrenzungen

Die Haftung der TSP gegenüber dem Zertifikatnehmer oder einem vertrauenden Dritten wird auf die Zahlung einer Schadensvergütung von höchstens 2500 € pro Transaktion begrenzt, wobei die Art der Vorfälle im nachstehenden Abschnitt aufgelistet ist.

7.1 Qualifizierte Zertifikate

Die Ausstellung qualifizierter elektronischer Bürgersignaturzertifikate wird von Artikel 14 des Gesetzes über die elektronischen Unterschriften und die Haftung der TSP geregelt.

Gemäß dieser Bestimmung haftet die TSP für den Schaden, den eine Institution, eine natürliche oder juristische Person erleidet, die vernünftigerweise auf das Zertifikat vertraut:

a) die Richtigkeit aller im qualifizierten Zertifikat aufgenommenen Informationen am Datum, wo es ausgestellt wurde, und das Vorhandensein aller für ein qualifiziertes Zertifikat vorgeschriebenen Angaben in diesem Zertifikat;

b) die Garantie, dass zum Zeitpunkt der Ausstellung des qualifizierten Zertifikats der in diesem Zertifikat identifizierte Unterzeichner den privaten Schlüssel besaß, der dem im Zertifikat angegebenen oder identifizierten öffentlichen Schlüssel entspricht;

c) die Garantie, dass der Privatschlüssel und der öffentliche Schlüssel komplementär benutzt werden können;

Der TSP haftet für jeden Schaden, der einer Institution, einer natürlichen bzw. juristischen Person entsteht, die dem Zertifikat vernünftigerweise vertraut haben, sofern der Widerruf des Zertifikates nicht registriert wurde, es sei denn der TSP kann beweisen, dass sie nicht nachlässig gewesen ist.

7.2 Zertifikate, die nicht als qualifizierte Zertifikate zu betrachten sind

Die allgemeinen Haftungsregeln sind auf jeden Schaden anwendbar, der einer Institution oder natürlichen bzw. juristischen Person entsteht, die vernünftigerweise einem von dem TSP ausgestellten Zertifikat vertraut.

Die TSP lehnt ausdrücklich jede Haftung gegenüber vertrauenden Dritten in allen Fällen ab, wenn das Authentifizierungszertifikats im Kontext von Anwendungen benutzt wurde, die die Benutzung des Identitätszertifikats zur Generierung von elektronischen Unterschriften ermöglichen.

7.3 Haftung ausgeschlossen

Die TSP übernimmt keine Haftung für Verluste jeder Art, die sich aus einem Umstand oder mehreren der folgenden Umstände ergeben:

- Sofern die Sicherheit des elektronischen Zertifikats der klagenden Partei oder sofern der Gegenstand einer Klage aufgrund der unbefugten Offenlegung oder nichtgestatteten Verwendungen des elektronischen Zertifikats, des Passworts oder der zugangsprüfenden Aktivierungsdaten nicht mehr gegeben ist;
- Sofern das elektronische Zertifikat der klagenden Partei oder der Gegenstand einer Klage auf falsche Darstellungen, Fakten oder auf Fehler, Versäumnisse einer Person, Einheit oder Organisation beruhen;
- Sofern das elektronische Zertifikat der klagenden Partei oder der Gegenstand einer Klage vor dem Datum der Umstände, die einen Anspruch erheben, abgelaufen ist oder zurückgezogen wurde;
- Sofern das elektronische Zertifikat der klagenden Partei oder der Gegenstand einer Klage geändert wurden oder nicht gemäß den Bedingungen dieser CA CP/CPS-Zertifizierungsstelle und/oder gemäß dem zuständigen Zertifikatinhabervertrag oder gemäß jeder geltenden Gesetzgebung oder Vorschrift geändert wurde;
- Sofern der zum elektronischen Zertifikat gehörende Privatschlüssel der klagenden Partei oder der Gegenstand der Klage gefährdet worden sind;
- Sofern das elektronische Zertifikat der klagenden Partei in einer Weise ausgegeben wurde, die gegen geltende Gesetze und Regeln verstößt;
- Unter der Voraussetzung, dass Certipost kommerziell vertretbare Maßnahmen zum Schutz gegen Sicherheitslücken bei der Hardware, Software und bei den Algorithmen ergreift, ist darauf hinzuweisen, dass bestimmte Rechner-Hardware oder -Software sowie mathematische Algorithmen mit dem Ziel entwickelt werden, die

Verschlüsselung öffentlicher Schlüssel oder asymmetrische Verschlüsselungssysteme zu gefährden;

- Unter der Voraussetzung, dass Certipost alle kommerziell angemessenen Maßnahmen gegen Strompannen, Stromunterbrechungen und andere Probleme veranlasst;
- Der Absturz eines Rechnersystems oder mehrerer, der Kommunikationsinfrastruktur, der Abläufe, der Speicherträger oder -mechanismen oder aller Subkomponenten der vorherigen, nicht unter exklusiver Kontrolle von Certipost und/oder seiner Subunternehmer oder Serviceanbieter stehenden Systeme;
- Einen der folgenden Vorfälle oder mehrere: Naturkatastrophe (einschl. und ohne Ausschluss Überschwemmungen, Erdbeben oder andere natur- und wetterbedingte Ursachen); ein Arbeitsstreik, Kriege, Aufstände, Rebellion, oder häufige militärische Feindseligkeiten, widrige Gesetze oder Regierungsmaßnahmen, Verbot, Embargo oder Boykott, Krawalle oder zivile Unruhen, Feuer oder Explosion; Epidemien mit katastrophalem Ausmaß; Handelsembargo; Einschränkungen oder Behinderungen (einschl. und ohne Einschränkung Exportkontrollen); Telekommunikationsmängel oder -störungen; rechtliche Verpflichtungen einschl. aller Urteile eines Gerichts oder einer zuständigen Gerichtsbarkeit, dem/der Certipost unterliegt oder unterliegen könnte sowie jeder Vorfall, jede Gelegenheit oder jeder Umstand oder jede Folge von Umständen, die außerhalb der Kontrolle von Certipost liegen.

8 Anwendbare Verträge, CPS, Zertifikatsrichtlinie

Diese PKI Disclosure Statement dient als Zusammenfassung des CPS und bezieht sich auf andere Betriebsunterlagen, in denen die Anfrage- und Validierungsverfahren bestätigt werden.

9 Datenschutz

Der TSP zielt darauf ab, die ISO 27001 & ISO 27002-Sicherheitsrichtlinien für die Festlegung und Umsetzung von operativen Kontrollen einzuhalten.

10 Rückerstattungsanweisungen

Nicht Zutreffend.

11 Geltendes Gesetz und Beilegung von Streitklauseln

Die vorliegenden Allgemeinen Geschäftsbedingungen unterliegen ausschließlich dem belgischen Recht.

12 CA und Zertifikatsverzeichnis Lizenzen, Vertraulichkeits-Warenzeichen und Audit

In Bezug auf qualifizierte Zertifikate für elektronische Signatur-Formate beruft sich die CPS auf die EU-Richtlinie 910/2014, die den gesetzlichen Rahmen für elektronische Unterschriften in Belgien festlegt.

Die TSP genügt den Forderungen, die in den ETSI-Policy-Dokumenten festgelegt sind, die sich auf den qualifizierten Zertifikaten beziehen, einschließlich:

- 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

Die TSP erklärt sich mit Übereinstimmungsaudits einverstanden, um zu garantieren, dass sie den Forderungen, Normen, Prozeduren und Service Levels gemäß diesen vertraglichen Anforderungen und Industriestandards genügt. Die TSP erklärt sich mit der Überprüfung ihrer Praktiken und Prozeduren einverstanden, soweit diese nicht gegen bestimmte Bedingungen wie die Vertraulichkeit der Information, Geschäftsgeheimnisse usw. verstößt. Solche Audits können direkt oder über einen Beamten folgender Behörden erfolgen:

- Die Behörde, die die Zertifizierungsdienstleister in Belgien beaufsichtigt und im Namen der belgischen Regierung handelt.
- Die belgische Regierung oder eine von der belgischen Regierung angewiesene Drittpartei.

Die TSP bewertet die Ergebnisse dieser Audits, bevor sie diese ausführt.

13 Abkürzungen und Begriffe

CA	Zertifizierungsbehörde
CM	Kartenhersteller
CPS/CP	Zertifizierungsrichtlinie
CRL	Zertifikatwiderrufliste
RA	Registrierungsstelle
TSP	Trust Service Provider