Belgische Zertifizierungspolitik und Darlegung der Zertifizierungsverfahren für eID PKI-Infrastruktur Foreigner CA

OID: **2.16.56.1.1.1.7**
2.16.56.9.1.1.7
2.16.56.10.1.1.7
2.16.56.12.1.1.7

Firma:	Certipost
Version:	*2.0*
Status:	FINAL
Veröff. am:	07/09/2017

Dokumentkontrolle

Datum	Version	Bearbeitet von	Änderung
04/09/2017	2.0	Don Giot / Cristof Fleurus	Übersetzung

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 Einleitung

Die vorliegende Darlegung der Zertifizierungsrichtlinie (abgekürzt zu „CPS“ für „Certification Practice Statement“) beschreibt die Zertifizierungsverfahren, die auf die digitalen Zertifikate anwendbar sind, die innrhalb Belgiens von dem Trust Service Provider (abgekürzt zu TSP) unter der Bezeichnung „Foreigner CA“ (nachstehend „die CAs“) für Ausländer, die sich in Belgien aufhalten, ausgestellt werden und die auf den elektronischen Chipkarten für Ausländer (nachstehend „die elektronischen Personalausweise“) installiert sind.

Wie oben beschrieben ist das vorliegende CPS eine unilatrale öffentliche Erklärung der Richtlinien, die die „Foreigner CA“ bei der Bereitstellung von Zertifizierungsdiensten einhält, und es wird umfasend beschrieben, wie die „Foreigner CA“ ihre Dienste zur Verfügung stellt.

Erstes Ziel des vorliegenden CPS ist es, die gesetzlichen und vertraglichen Bestimmungen zu präzisieren und alle betreffenden Parteien über die Verfahrensweisen der „Foreigner CA“ zu informieren.

Certipost nv/sa geht konform mit den Grundanforderungen für die Ausstellung und Verwaltung öffentlicher vertrauenswürdiger Zertifikate („Grundanforderunten“), veröffentlicht auf http://www.cabforum.org. Im Fall eines Widerspruchs zwischen dem vorliegenden Dokument und diesen Anforderungen haben diese Anforderungen Vorrang vor dem Dokument.

1.1 Übersicht

Der TSP für die „Foreigner CA„ ist zur Zeit die „CERTIPOST Aktiengesellschaft“ (nachstehend „Certipost“ genannt), deren Sitz Muntcentrum / Centre Monnaie /, in 1000 Brüssel gelegen ist und die zu diesem Zweck von den Belgischen Föderalen Behörden als vertragschließende Behörde für das eID-Projekt unter den folgenden Bedingungen eingesetzt wurde:

CERTIPOST übernimmt die Aufgabe des Trust Service Provider („TSP“) im Sinne des Gesetzes vom 21. Juli 2016, der Europäischen Verordnung Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt. CERTIPOST übernimmt, im Auftrag und für Rechnung der belgischen Behörden, die Aufgabe von CA und TSP für die Foreigner CAs und ist in dieser Eigenschaft verantwortlich für die Ausländerzertifikate, die im Rahmen dieser CAs ausgestellt werden.

Dieses CPS sollte nur im Bereich der CA benutzt werden. Das CPS zielt darauf ab, den Bereich der im Rahmen des CA-Bereichs an Ausländer und vertrauende Parteien geleisteten Zertifizierungsdienste abzugrenzen. Dieses CPS umschreibt ebenfalls die Beziehung zwischen der Zertifizierungsbehörde (CA) und anderen Zertifizierungsbehörden in der PKI-Hierarchie der Belgischen Föderalen Behörde wie die Belgium Root Certification Authority (BRCA). Es beschreibt ebenfalls die Beziehung zwischen dem TSP und den anderen Organisationen, die bei der Ausstellung von Zertifikaten für die belgischen elektronischen Personalausweise (nachstehend „Ausländerzertifikate“) mitarbeiten.

Dieses CPS liefert ebenfalls operationelle Richtlinien für alle Ausländer und vertrauenden Parteien, einschließlich der natürlichen und juristischen Personen in Belgien und im Ausland. Dieses CPS liefert ebenfalls die operationellen Richtlinien (PKI Best Practices) für die

anderen Zertifizierungsdienstleister wie die BRCA, die zur PKI-Hierarchie der Belgischen Förderalen Behörde im juristischen Rahmen der elektronischen Unterschriften und der elektronischen Personalausweise in Belgien gehören. Außerdem beschreibt dieses CPS die Beziehungen zwischen der „Foreigner CA“ und allen anderen Entitäten, die eine Rolle im Kontext des belgischen elektronischen Personalausweises spielen wie etwa der Kartenersteller. Die Belgische Föderale Behörde erwirbt diese Dienste mittels des Rahmenvertrags.

Schließlich sieht dieses CPS Informationen in Sachen Beglaubigung und Aufsicht für Kontrollbehörden, Beglaubigungsorgane, beglaubigte Buchprüfer, usw. in Bezug auf die Verfahren des TSP vor.

Diese „Foreigner CA CPS“ unterschreibt die folgenden Normen und bringt sie zur Ausführung:

- RFC 3647: Internet X.509 Public Key Infrastructure – Zertifikatspolitik und Zertifizierungsverfahren
- RFC 5280: Internet X.509 Public Key Infrastructure – Zertifikat und CRL-Profil.
- RFC 6818: Aktualisierung zur RFC 5280.
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualifiziertes Zertifikatsprofil.
- RFC 6960: X.509 Internet Public Key Infrastructure – Protokoll zur Online-Gültigkeitserklärung von Zertifikaten – OCSP
- ETSI EN 319 411-1: Policy- und Sicherheitsanforderungen für TSP, die Zertifikate ausstellen; Teil 1: Allgemeine Anforderungen
- ETSI EN 319 411-2: Policy- und Sicherheitsanforderungen für TSP, die Zertifikate ausstellen; Teil 2: Anforderungen für TSP, die EU-qualifizierte Zertifikate ausstellen
- ETSI EN 319 412-5: Policy- und Sicherheitsanforderungen für TSP, die Zertifikate ausstellen; Teil 5: QS-Erklärung.
- Die Norm ISO/IEC 27001 in Sachen Sicherheit und Infrastruktur.

Das CPS behandelt detailliert die technischen verfahrens- und organisationsbezogenen Policies und Praktiken der CA für alle angebotenen Zertifizierungsdienste, und dies während der gesamten Gültigkeitsdauer der von der „Foreigner CA“ ausgestellten Zertifikate. Außer dem vorliegenden CPS können andere mit dem Zertifizierungsprozess im Rahmen des belgischen elektronischen Personalausweises verbundene Dokumente berücksichtigt worden sein. Diese Dokumente sind über das CA-Archiv verfügbar (siehe § 2 Haftung in Sachen Veröffentlichung und Archivierung).

Das vorliegende CPS entspricht den formellen Forderungen der Internet Engineering Task Force (IETF) RFC 3647 hinsichtlich des Formats und des Inhalts. Indem gewisse Abschnittstitel gemäß der Struktur vom RFC 3647 eingeschlossen sind, kann es sein, dass das Thema auf die Anwendung der Zertifizierungsdienste der „Foreigner CA“ nicht zutrifft. Solche Abschnitte werden mit der Anmerkung „Abschnitt nicht anwendbar“ gekennzeichnet. Kleine redaktionelle Änderungen der RFC 3647-Vorschriften wurden in das vorliegende CPS inseriert, um die Struktur vom RFC 3647 den Bedürfnissen dieses Anwendungsgebiets besser anzupassen.

Dieses CPS muss ebenfalls als Zertifizierungspolicy (abgekürzt zu „CP“) für die von der „Foreigner CA“-Zertifizierungsbehörde ausgegebenen Zertifikate betrachtet werden.

In Bezug auf die anderen von der belgischen Regierung verwendeten CAs verweisen wir auf folgende Website, auf der eine Verknüpfung zu jedem CPS zu finden ist:

- Gov CA repository.eid.belgium.be
- Citizen CA repository.eid.belgium.be
- Belgium Root CA repository.eid.belgium.be

Hinweis: Diese CAs (Gov & Foreigner) haben jeweils eigene CP/CPS.

1.2 die eid Hierarchie

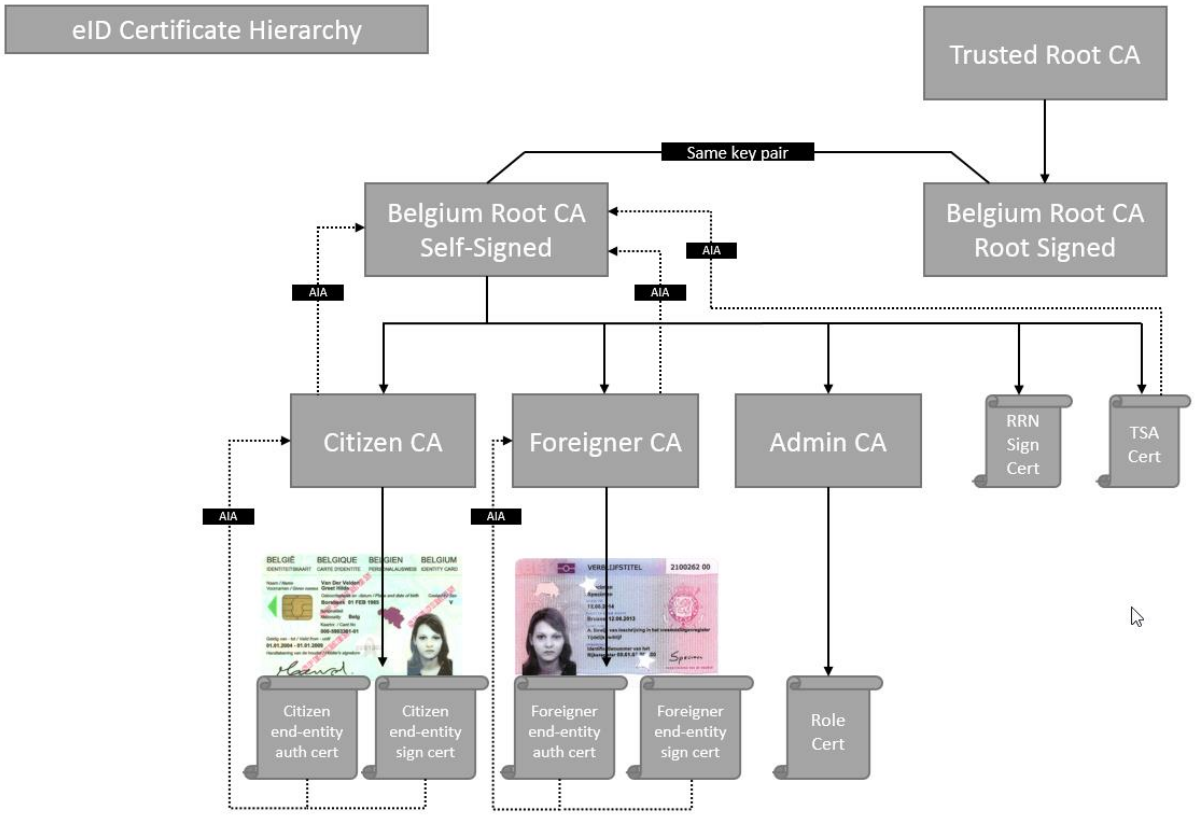

Abbildung: Belgische eID PKI-Hierarchie

1.3 Name und Identifizierung des Dokuments

Name dieses Dokuments	*Belgian Certificate Policy & Certification Practice Statement für eID PKI Infrastruktur-Foreigner CA*
Dokumentversion	*2.16.56.12.1.* **– V1.0** *Diese Zertifikatspolicy wird durch ihren Namen und ihre Versionsnummer identifiziert.*
	Diese Dokument-OID ersetzt folgende OIDs ***2.16.56.1.1*** ***2.16.56.9.1*** ***2.16.56.10.1*** *Diese Foreigner CP/CPS hebt ab dem Datum der Veröffentlichung alle anderen Versionen von Foreigner CP/CPS auf.*
OID, der auf dieses Dokument verweist	*Die Identifizierer unter der Kontrolle von Certipost:* ***BRCA (1)*** *OID: 2.16.56.1.1.1.7 – Foreigner CA* *OID: 2.16.56.1.1.1.7.1 – Foreigner Unterzeichnungszertifikat* *OID: 2.16.56.1.1.1.7.2 – Foreigner Authentifizierungszertifikat*
	BRCA 2 *OID: 2.16.56.9.1.1.7 – Foreigner CA* *OID: 2.16.56.9.1.1.7.1 – Foreigner Unterzeichnungszertifikat* *OID: 2.16.56.9.1.1.7.2 – Foreigner Authentifizierungszertifikat*
	BRCA 3 *OID: 2.16.56.10.1.1.7 – Foreigner CA* *OID: 2.16.56.10.1.1.7.1 – Foreigner Unterzeichnungszertifikat* *OID: 2.16.56.10.1.1.7.2 – Foreigner Authentifizierungszertifikat*
	BRCA 4 *OID: 2.16.56.12.1.1.7 – Foreigner CA* *OID: 2.16.56.12.1.1.7.1 – Foreigner Unterzeichnungszertifikat* *OID: 2.16.56.12.1.1.7.2 – Foreigner Authentifizierungszertifikat*

1.4 PKI-Teilnehmer

Die PKI-Hierarchie besteht aus verschiedenen teilnehmenden Parteien. Die hiernach erwähnten Parteien, einschließlich aller Zertifizierungsstellen, der RA, die LRAs (Gemeindeverwaltungen), die Ausländer und der vertrauenden Parteien werden gemeinsam PKI-Teilnehmer genannt.

1.4.1 Zertifizierungsbehörden

Eine Zertifizierungsbehörde ist eine Organisation, die digitale Zertifikate entsprechend einer digitalen Identität ausstellt und verwaltet.

Die Zertifizierungsbehörde stellt die nötigen Dienste zum Prüfen der Gültigkeit ausgestellter Zertifikate bereit.

CERTIPOST übernimmt, im Auftrag und für Rechnung der belgischen Behörden, die Aufgabe von CA und TSP für die Foreigner CAs und ist in dieser Eigenschaft verantwortlich für die Ausländerzertifikate, die im Rahmen der Foreigner CA ausgestellt werden. Die belgischen Behörden sind als TSP verantwortlich für die „Belgium Root CA“ und für die CA-Zertifikate, die unter den „Belgium Root CA“ ausgestellt werden.

Die „Foreigner CA“ ist eine Zertifizierungsbehörde, die zur Ausstellung von Ausländerzertifikaten ermächtigt ist. Diese Genehmigung wird durch die Belgium Root Certification Authority (hiernach „BRCA“ genannt) gewährt.

Die „Foreigner CA“ garantiert die Verfügbarkeit aller Dienstleistungen in Verbindung mit den Zertifikaten, einschließlich Ausstellung, Widerrufung, Statusüberprüfung und Anbringung von Zeitstempeln, sobald sie bei spezifischen Anwendungen verfügbar oder erforderlich werden.

Die „Foreigner CA“ ist in Belgien ansässig. Sie kann unter der im vorliegenden CPS veröffentlichten Adresse kontaktiert werden. Zur Leistung der CA-Dienste, die die Ausstellung, die Sperrung, die Widerrufung, die Erneuerung und die Statusüberprüfung von Zertifikaten umfasst, operiert die „Foreigner CA“ innerhalb eines gesicherten Systems und sieht ein Hilfezentrum in Belgien vor, um die Kontinuität der CA-Dienste zu gewährleisten.

Das Verantwortungsgebiet der „Foreigner CA“ umfasst die allgemeine Verwaltung der Lebensdauer der Zertifikate, einschließlich:

- Ausstellung;
- Sperrung/Aufhebung der Sperrung;
- Widerrufung;
- Statusüberprüfung (Dienst für Zertifikatstatus);
- Verzeichnisdienste.

1.4.2 Registrierungsbehören oder RA

Das RRN (Nationalregister) und die Gemeindeverwaltungen sind die RA innerhalb des Bereiches der „Foreigner CA“ unter Ausschluss aller anderen. Das RRN ist konstituiert und handelt unter den Verfügungen des Gesetzes über das Nationalregister und unter dem Gesetz über die Personalausweise.

Die Registrierungsbehörde („RA“ für Registration Authority), die im Namen und auf Rechnung des TSP bescheinigt, dass ein gewisser öffentlicher Schlüssel einer bestimmten Entität gehört (zum Beispiel einer Person), indem sie ein digitales Zertifikat ausstellt und dies mit ihrem Privatschlüssel unterzeichnet. Für den belgischen elektronischen Personalausweis übernimmt das belgische Nationalregister, eine öffentliche Verwaltung, die zur Belgischen Föderalen Behörde für den Föderalen Öffentlichen Dienst Inneres gehört, die Rolle der „RA“. Die meisten Registrierungsaufgaben werden von den örtlichen Verwaltungsdiensten, in den Gemeinden übernommen, den so genannten Örtlichen Registrierungsstellen („LRA“ für Local Registration Authority). Auf Basis dieses Prozesses bittet die RA die CA um Ausstellung eines Zertifikats.

Insbesondere sind RA und LRA verantwortlich für:

i. die Identitätsprüfung von Ausländern
ii. die Aufnahme der zu zertifizierenden Angaben,
iii. die Genehmigung zur Ausstellung eines Zertifikats für einen bestimmten Ausländer,
iv. die Garantie, dass die Zertifikate der Ausländer auf der korrekten Identitätskarte gespeichert werden,
v. die Garantie, dass ein Ausländer genau den für ihn bestimmten Ausweis erhält und dass dieser Ausweis nur dann aktiviert wird, wenn er dem richtigen Ausländer ordnungsgemäß zugewiesen wurde,
vi. die SRA (Suspension and Revocation Authority - Sperr - und Widerrufungsbehörde): die Entität, die die Zertifikate unter Berufung auf die ETSI-Normen sperrt und/oder widerruft.

1.4.3 Abonnent & Benutzer

Certipost hat als TSP für die Foreigner CAs eine vertragliche Vereinbarung mit den belgischen Behörden. Insofern können wir den Staat als den „Abonnenten“ der CA-Dienste im „Foreigner CA“-Bereich betrachten.

Die Benutzer der CA-Dienste im „Foreigner CA“-Bereich sind Ausländer, die ihren Wohnsitz in Belgien haben und die Inhaber eines elektronischen Personalausweises mit gemäß dem Gesetz über die Personalausweise aktivierten Zertifikaten sind. Weiter im vorliegenden Dokument kann das Wort „Benutzer“ durch das Wort „Ausländer“ ersetzt werden. Diese Ausländer:

- werden in den beiden Ausländerzertifikaten identifiziert;
- besitzen die Privatschlüssel, die den öffentlichen Schlüsseln entsprechen, die in ihren jeweiligen Ausländerzertifikaten eingetragen sind.

- sind Ausländer, die ihren Wohnsitz in Belgien haben.

Die Ausländer haben das Recht, am Anfang des Antrags auf ihren elektronischen Personalausweis anzugeben, ob sie Ausländerzertifikate möchten. Der elektronische Personalausweis wird den Ausländern mit geladenen Ausländerzertifikaten geliefert. Auf der eID-Karte von Ausländern, die keine Ausländerzertifikate wünschen, kann ein oder kein Zertifikat vorhanden sein Mehr dazu finden Sie in dem Dokument EID-DEL-004 eID PKI Hierarchy certificate profile .

Für Ausländer, die das Alter von 6 Jahren noch nicht erreicht haben, wird das Zertifikat für Authentifizierung nicht installiert. Für Ausländer, die das Alter von 18 Jahren noch nicht erreicht haben, wird das Zertifikat für elektronische Unterschrift nicht installiert.

	Authentifizierungszertifikat	**Unterschriftszertifikat**
0 – 6 Jahre	0	0
6 – 18 Jahre	X	0
+18 Jahre	X	X

Die Tabelle oben beschreibt für jede Alterskategorie die Zertifikate, zu denen sie berechtigt ist.

1.4.4 Vertrauende Parteien

Vertrauende Parteien sind Entitäten, einschließlich natürliche Personen oder Rechtspersonen, die einem Zertifikat und/oder einer digitalen Unterschrift, das/die mittels des öffentlichen Schlüssels, der in das Zertifikat eines Ausländers aufgenommen ist, geprüft werden kann, vertrauen.

1.4.5 Andere Teilnehmer

1.4.5.1 Kartenersteller (Card Manufacturer)

Der Kartenersteller für die „Foreigner CA" ist die „Zetes nv/sa", mit eingetragenem Sitz in 1130 Brüssel 3 Straatsburgstraat/Rue de Strasbourg, die von den belgischen Behörden in ihrer Eigenschaft als Vertragsbehörde für das eID-Projekt mit dieser Aufgabe betraut wurde.

Der Kartenersteller macht intelligente nicht personalisierte Ausweise zu personalisierten elektronischen Personalausweisen, indem er die Identitätsangaben und das Foto des Ausländers auf den Ausweis druckt.

Der Kartenersteller leistet außerdem folgende Dienste:

- Generieren der für den Ausweis erforderlichen Schlüsselpaare;
- Speichern der beiden eID-Ausländerzertifikate auf dem Ausweis;

- Generieren der persönlichen Aktivierungscodes des Antragstellers und der Gemeindeverwaltung und des anfänglichen PIN-Codes des Antragstellers;
- Laden der aktiven Stammzertifikate der Behörde auf den Ausweis;
- Liefern des elektronischen Personalausweises an die Gemeindeverwaltung;
- Liefern des persönlichen Aktivierungscodes und des PIN-Codes an den Antragsteller;
- Aufnehmen der Angaben im Register der Personalausweise.

1.4.5.2 Lieferant des Root Sign-Zertifikats

Der Lieferant des „Root Sign“ Zertifikats garantiert das Vertrauen zur BRCA in weit verbreiteten Browsern und Anwendungen. Der Lieferant des Root Sign-Zertifikats sorgt dafür, dass diese Browser und Anwendungen ihr Vertrauen zu seiner Root-Zertifizierungsbehörde behalten, und benachrichtigt die RA von allen Ereignissen, die das Vertrauen in seine Root-Zertifizierungsbehörde beeinträchtigen. Der Lieferant des Root Sign-Zertifikats aller aktiven BRCAs ist Digicert. Die Digicert-Zertifizierungspolicy und die Zertifikatprofile sind verfügbar auf: https://www.digicert.com/ssl-cps-repository.htm

1.4.5.3 Subauftragnehmer

Certipost beauftragt einen Drittauftragnehmer, den TSP mit operationellen Aufgaben und Verantwortungen zu unterstützen. Der Subauftragnehmer übernimmt die technische Unterstützung für folgende Dienste:

- Ausstellung der Zertifikate
- Widerrufung/Sperrung des Zertifikats
- Prüfung der Zertifikate
    - OCSP
    - CRL & Delta CRL

Zwischen dem Subauftragnehmer, Certipost und dem Staat existiert ein Service Level Agreement (SLA - Dienstleistungsvertrag), der die Qualität der geleisteten Dienste hinsichtlich Performanz und Verfügbarkeit bestimmt. Der Subauftragnehmer erstattet monatlich Bericht über die gemessenen Performanzindikatoren, um die Übereinstimmung mit dem SLA nachzuweisen. Bei Schlüsselzeremonien stellt der Subauftragnehmer auch organisatorische Unterstützung bereit.

1.5 Benutzung der Zertifikate

Die Benutzung der Zertifikate auf dem elektronischen Personalausweis unterliegt gewissen Einschränkungen.

Zwei Arten von elektronischen Zertifikaten werden von der „Foreigner CA“ ausgestellt, jedes mit seinem eigenen Nutzungszweck:

- Authentifizierungszertifikat: Dieses Zertifikat dient zur Authentifizierung für elektronische Transaktionen, die den Zugang zu Websites und anderen Online-Inhalten unterstützen.

- Qualifiziertes elektronisches Unterschriftszertifikat: Dieses Zertifikat wird zum Erstellen qualifizierter elektronischer Unterschriften benutzt.

Jede für einen Ausländer ausgestellte eID kann sowohl ein Authentifizierungszertifikat als auch ein qualifiziertes elektronisches Unterschriftszertifikat enthalten. Aufgrund modernster Sicherheitsanforderungen wird nämlich empfohlen, keine Authentifizierungszertifikate für elektronische Unterschriftszwecke zu benutzen. Die „Foreigner CA“ übernimmt deshalb den vertrauenden Parteien gegenüber in allen Fällen, wo das Authentifizierungszertifikat zur Generierung von elektronischen Unterschriften benutzt wurde, keine Haftung.

1.6 Policy-Verwaltung

1.6.1 Organisation für die Verwaltung des Dokuments

Die Policy-Verwaltung ist CERTIPOST vorbehalten.

- Kontaktdaten: Per Post:

  Certipost nv / sa
  Policy administration - Foreigner CA
  Muntcentrum / Centre Monnaie
  1000 Brüssel

- Per E-Mail:

  An: eid.cps@bpost.be
  Betr.: Policy administration - Foreigner CA

1.6.2 Kontaktperson

Die wichtigste Ansprechperson für alle Fragen zu Foreigner CA CP/CPS finden Sie unter §1.6.1 ORGANISATION FÜR DIE VERWALTUNG DES DOKUMENTS

Alle Bemerkungen, ob positiv oder negativ, sind stets willkommen und an die obige E-Mail-Adresse zu richten, damit sie angemessen und zeitnah behandelt werden können.

1.6.3 Person, die die CPS-Eignung für die Policy bestimmt

Übereinstimmend mit der Norm ETSI EN 319 411-2 zur Unterstützung der europäischen Verordnung (Verordnung 910/2014) übernimmt CERTIPOST die Verwaltung seiner TSP-Aufgaben über ein PKI Management Board (CEPRAC), das über alle erforderlichen Kompetenzen verfügt.

Durch ihre offizielle Teilnahme an den regelmäßigen eID Progress Meetings, auf denen alle vorerwähnten Parteien gehörig vertreten sind, sammelt CERTIPOST alle nötigen Informationen und stellt diesen Parteien alle relevanten Fragen, um ihre Verantwortung als TSP aufzunehmen. Die Probleme und Fragen werden innerhalb des PKI Management Board analysiert. Wenn nötig, werden Vorschläge/Verbesserungen beim Progress Meeting formuliert.

Das PKI Management Board wird, gegenüber dem durch FEDICT geleiteten eID CSP Lenkungsausschuss, jede Angelegenheit mitteilen, die mit Hilfe dieses Verfahrens nicht gelöst werden kann. Der Lenkungsausschuss hat die Möglichkeit, die Dienste von externen Fachleuten in Anspruch zu nehmen, um eine zusätzliche Meinung zu erhalten und die Verantwortung in Sachen Beilegung von Streitfällen zu übernehmen.

1.7 Definitionen und Akronyme

1.7.1 Definitionen

Am Ende dieses CPS finden Sie eine Liste mit Definitionen.

1.7.2 Akronyme

Am Ende dieses CPS finden Sie eine Liste mit Akronymen.

2 Haftung in Sachen Veröffentlichung und Archivierung

2.1 Archive

Die „Foreigner CA“ bewahrt ein aktuelles Online-Archiv der Dokumente, in denen sie gewisse Aktivitäten und Verfahren sowie den Inhalt gewisser Aspekte ihrer Politik, einschließlich ihres CPS, das unter http://repository.eid.belgium.be zugänglich ist, bekannt gibt. Die CA behält sich das Recht vor, Informationen über gewisse Aspekte ihrer Politik in jeder Form, die sie für geeignet hält, zur Verfügung zu stellen und zu veröffentlichen.

Das Archiv ist auf der Website http://repository.eid.belgium.be verfügbar.

2.2 Veröffentlichung von Zertifizierungsinformation

Die CA veröffentlicht ein Archiv, in dem alle ausgestellten digitalen Zertifikate und alle widerrufenen digitalen Zertifikate aufgeführt sind. Der Standort des Archivs und von Beantwortern des Protokolls zur Online Gültigkeitserklärung von Zertifikaten (abgekürzt zu „OCSP“ für Online Certificate Status Protocol) werden in den einzelnen Zertifikatsprofilen angegeben, ausführlicher offenbart in EID-DEL-004 eID PKI Hierarchy certificate profile.Die CA erstellt und pflegt ein Verzeichnis aller Zertifikate auf, die sie ausgestellt hat. Dieses Verzeichnis zeigt auch den Status eines ausgestellten Zertifikats.

Die CA stellt gewisse Unterteile und Elemente von solchen Dokumenten, einschließlich bestimmter Sicherheitskontrollen, Verfahren in Verbindung mit dem Funktionieren unter anderem von Registrierungsbehörden, mit interner Sicherheitspolitik, usw. der Öffentlichkeit nicht zur Verfügung, da diese Elemente sehr empfindlich sind. Jedoch sind solche Dokumente und dokumentierten Aktivitäten bedingt verfügbar zur Kontrolle durch angestellte Parteien, gegenüber denen die CA Verpflichtungen hat.

Die „Foreigner CA“ veröffentlicht Informationen über die Zertifikate in einem oder mehreren öffentlich zugänglichen Online-Archiven unter der Internet-Domain „eid.belgium.be“. Die CA behält sich das Recht vor, Informationen über den Status der Zertifikate in Drittarchiven zu veröffentlichen.

2.3 Zeit oder Häufigkeit der Veröffentlichung

Die PKI-Teilnehmer werden benachrichtigt, dass die CA Informationen, die sie ihr direkt oder indirekt mitteilen, in Verzeichnissen, die der Öffentlichkeit zugänglich sind, veröffentlichen kann, soweit diese Informationen den Status elektronischer Zertifikate betreffen. Die CA veröffentlicht regelmäßig Informationen über den Status von Zertifikaten, so wie im vorliegenden CPS angegeben.

Genehmigte Versionen von Dokumenten, die im Archiv veröffentlicht werden, müssen konform dem Änderungsverwaltungsverfahren hochgeladen werden.

2.4 Kontrolle des Zugangs zu den Archiven

Obwohl die „Foreigner CA“alles einsetzt, damit der Zugang zu den veröffentlichten Angaben kostenlos bleibt, könnte sie im Rahmen ihres Vertrags mit der belgischen Regierung solche Dienste wie die Veröffentlichung von Statusinformationen in Datenbanken von Drittparteien, Privatverzeichnisse, usw. gebührenpflichtig machen.

Der OCSP-Dienst, der Dienst zur Überprüfung des Status der Zertifikate per Webseite, das Zertifikatarchiv und die Zertifikatwiderrufungslisten (CRLs und Delta CRLs) sind für die Öffentlichkeit auf der Webseite der CA und über die Netzwerke der Belgischen Föderalen Behörde verfügbar.

Im Rahmen des Vertrags mit der Belgischen Föderalen Behörde ist der Zugang zu den von der „Foreigner CA“ geleisteten Diensten begrenzt, wie folgt:

- Über die öffentlich verfügbare Schnittstelle zum Verzeichnis der Zertifikate kann nur ein Zertifikat für jeden von jeder Partei, mit Ausnahme der RA, eingereichten Antrag geliefert werden;
- Die CA kann angemessene Maßnahmen zum Schutz gegen die Missbräuche des OCSP-Dienstes, des Dienstes zur Überprüfung des Status per Webseite und des Dienstes zum Herunterladen der CRLs und der Delta CRLs treffen.
- Die CA kann die Verarbeitung von OCSP-Anträgen für eine Partei, die aufgrund ihrer Aktivitäten genötigt ist, den OCSP-Status regelmäßig zu überprüfen, nicht beschränken.

3 Identifizierung und Authentifizierung

3.1 Benennung

Die Regeln bezüglich der Benennung und der Identifizierung der Ausländer für Ausländerzertifikate sind dieselben wie die gesetzlichen Regeln, die auf die Benennung und die Identifizierung der Ausländer für die Personalausweise angewandt werden.

3.1.1 Arten von Namen

Betreff-Feldattribute in Endbenutzerzertifikaten sind in dem Dokument **EID-DEL-004 EID PKI HIERARCHY CERTIFICATE PROFILE** beschrieben.

3.1.2 Notwendigkeit aussagefähiger Namen

Siehe Abschnitt 3.1.1.

3.1.3 Anonymität oder Pseudonymität von Abonnenten

Abschnitt nicht anwendbar.

3.1.4 Regeln zum Interpretieren verschiedener Namensformen

Siehe Abschnitt 3.1.1.

3.1.5 Eindeutigkeit von Namen

Der DN eines Endbenutzerzertifikats muss eindeutig sein.

3.1.6 Erkennung, Authentifizierung und Rolle von Handelsmarken

Abschnitt nicht anwendbar.

3.2 Anfängliche Gültigkeitserklärung der Identität

Die Identifizierung des Ausländers, der einen elektronischen Personalausweis beantragt, erfolgt in Übereinstimmung mit den Verfahren und der Gesetzgebung, die auf die Lieferung der elektronischen Personalausweise anwendbar sind. Die RA spezifiziert die Verfahren, die von den LRAs anzuwenden sind. Die RA spezifiziert die Verfahren, die von den LRAs anzuwenden sind.

Die anwendbaren Verfahren finden Sie auf:

Niederländisch: www.ibz.rrn.fgov.be/nl/identiteitsdocumenten/eid/reglementering/

Französisch: www.ibz.rrn.fgov.be/fr/documents-didentite/eid/reglementation/

Deutsch: www.ibz.rrn.fgov.be/de/identitaetsdokumente/eid/vorschriften/

3.2.1 Verfahren zum Nachweis des Besitzes eines Privatschlüssels

In Übereinstimmung mit dem europäischen und belgischen Signaturgesetz werden Privatschlüssel auf gesicherten Smartcards für Signatur generiert. Der Kartenersteller ist dafür verantwortlich, die Smartcard, auf der sich die qualifizierte Signaturerstellungsvorrichtung (abgekürzt zu „QSCD“ für Qualified Signature Creation

Device) befindet, mit einer persönlichen Identifikationsnummer (PIN) zu sichern. Der Ausländer, der Inhaber des Zertifikats ist, muss die PIN für seine Smartcard geheim halten.

3.2.2 Authentifizierung der Organisationsidentität

Abschnitt nicht anwendbar

3.2.3 Authentifizierung der individuellen Identität

Siehe Abschnitt 3.2.

3.2.4 Nicht überprüfte Abonnenteninformation

Abschnitt nicht anwendbar.

3.2.5 Gültigkeitserklärung der Behörde

Siehe Abschnitt 3.2.

3.2.6 Kriterien für Interoperation

Abschnitt nicht anwendbar.

3.3 Identifizierung und Authentifizierung für Anfragen nach neuen Schlüsseln

Die Identifizierung und Authentifizierung des Ausländers, der eine Neuverschlüsselung anfragt wird ausgeführt entsprechend dem Verfahren, das in der RA spezifiziert und in den LRAs implementiert ist.

Die anwendbaren Verfahren finden Sie auf:

Niederländisch: www.ibz.rrn.fgov.be/nl/identiteitsdocumenten/eid/reglementering/

Französisch: www.ibz.rrn.fgov.be/fr/documents-didentite/eid/reglementation/

Deutsch: www.ibz.rrn.fgov.be/de/identitaetsdokumente/eid/vorschriften/

3.3.1 Identifizierung und Authentifizierung für Routine-Neuverschlüsselung

Siehe Abschnitt 3.3.

3.3.2 Identifizierung und Authentifizierung für Neuverschlüsselung nach Widerrufung

Siehe Abschnitt 3.3.

3.4 Identifizierung und Authentifizierung für Widerrufungsantrag

Die Identifizierung des Ausländers, der eine Sperrung oder Widerrufung seines Ausländerzertifikats beantragt, erfolgt in Übereinstimmung mit den Verfahren und Vorschriften, die für die Ausstellung von elektronischen Personalausweisen gelten.

Die Identifizierung und Authentifizierung von Inhabern, die die Sperrung oder Widerrufung ihrer Ausländerzertifikate beantragen, wird durch die Entität vorgenommen, die den Antrag empfängt. Diese Entitäten können folgende sein:

- Die Gemeindeverwaltung,
- die Polizei,
- DOCSTOP 00800 2123 2123 oder +32 2 518 2123

Diese Entität sendet anschließend alle Widerrufsanträge an die CA über die RA. Die RA ist der einzige Kontaktpunkt, über welchen die CA einen Sperr- oder Widerrufungsantrag empfangen kann.

Die RA sendet den digital unterschriebenen Widerrufungsantrag über ein gesichertes Netzwerk an die CA. Die CA bestätigt die Widerrufung an die RA.

4 Operationelle Erfordernisse Für Die Lebensdauer Eines Zertifikats

Alle Entitäten im Befugnisbereich des TSP, einschließlich der LRAs, Ausländer, vertrauenden Parteien und/oder anderen teilnehmenden Parteien, haben die dauernde Verpflichtung, die RA mittelbar oder unmittelbar von allen Änderungen der Informationen, die in ein Zertifikat aufgenommen sind, auf dem Laufenden zu halten. Dieses gilt für den ganzen operationellen Zeitraum eines solches Zertifikats oder jeder anderen Tatsache, die die Gültigkeit eines Zertifikates materiell beeinflussen kann. Die RA wird in diesem Fall die angepassten Maßnahmen treffen, um zu garantieren, dass die Situation korrigiert wird (z.B. indem sie den Widerruf von bestehenden Zertifikaten und die Generierung von neuen Zertifikaten mit den richtigen Angaben bei der CA beantragt).

Die CA führt die Ausstellung, Widerrufung oder Sperrung von Zertifikaten nur auf Anfrage der RA oder des TSP aus, unter Ausschluss jeder anderen Behörde, es sei denn, dass die RA andere ausdrückliche Anweisungen gibt.

Für die Ausführung seiner Aufgaben nimmt der TSP die Dienste von Dritten in Anspruch. Den Ausländern und vertrauenden Parteien gegenüber nimmt der TSP die volle Verantwortung auf sich für Handlungen oder Versäumnisse jedes Dritten, dessen Dienste er für die Lieferung von Zertifizierungsdiensten in Anspruch nimmt.

4.1 Zertifikatantrag

4.1.1 Wer kann einen Zertifikatantrag stellen?

Das Abonnementverfahren für den Ausländer zur Beantragung der Zertifikate ist ein integraler Bestandteil des angewendeten Einschreibeverfahrens durch die Gemeindeverwaltungen (die LRA also) für den elektronischen Personalausweis. Das Verfahren, das die LRA für die Einschreibung der Ausländer befolgt, wird von der RA vorgesehen.

4.1.2 Einschreibeprozess und Verantwortungen

Nach Genehmigung eines Zertifikatantrags beantragt die RA die Ausstellung eines Zertifikats bei der CA. Die CA überprüft die Vollständigkeit, die Integrität und die Einmaligkeit der von der RA eingereichten Angaben nicht, sondern vertraut voll und ganz auf die RA für die Genauigkeit aller Angaben. Die CA prüft nur, ob die Seriennummer des Zertifikats, die die RA dem Zertifikatantrag zuweist, tatsächlich eine einmalige Seriennummer ist, die nicht vorher für ein anderes Ausländerzertifikat gebraucht wurde. Ist dies der Fall, so informiert die CA die RA darüber.

Alle Anträge der RA werden angenommen, unter der Bedingung dass:

- deren Format gültig ist,
- sie über den geeigneten gesicherten Kommunikationskanal eingereicht werden,
- alle Überprüfungen gemäß den Bestimmungen des CA-Vertrags ordentlich vorgenommen wurden.

Die CA überprüft die Identität der RA auf Basis der vorgelegten Beweisstücke.

Die CA vergewissert sich, dass das ausgestellte Zertifikat alle Angaben, die ihr im Antrag der RA vorgelegt wurden, insbesondere die durch die RA zugewiesene Seriennummer für das Zertifikat, enthält.

Nach der Ausstellung eines Zertifikats postet die CA ein ausgestelltes Zertifikat in einem Archiv und sperrt das Zertifikat. Das Zertifikat wird dann an die RA übermittelt.

Die RA bittet den Kartenersteller darum, die Ausländerzertifikate auf den elektronischen Personalausweis zu laden. Der Kartenersteller übermittelt der LRA über einen gesicherten Weg den elektronischen Personalausweis mit den Ausländerzertifikaten.

4.2 Bearbeitung des Zertifikatantrags

Wenn ein Zertifikat beantragt wird, muss die LRA die Identität des Antragstellers gemäß dem Verfahren für den Antrag auf elektronischen Personalausweis bestätigen. Die Verfahren, die auf die Gültigkeitserkärung der Identität des Antragstellers anwendbar sind, werden in einem spezifischen Dokument beschrieben.

Wenn ein Zertifikat beantragt wird, kann die LRA den Antrag für elektronischen Personalausweis genehmigen oder ablehnen. Dies bringt auch die Genehmigung oder Ablehnung des Zertifikatantrags mit sich. Wenn der Antrag angenommen wird, sendet die LRA die Registrierungsangaben an die RA. Die RA nimmt dann den Antrag an oder lehnt ihn ab.

Die anwendbaren Verfahren finden Sie auf:

Niederländisch: www.ibz.rrn.fgov.be/nl/identiteitsdocumenten/eid/reglementering/

Französisch: www.ibz.rrn.fgov.be/fr/documents-didentite/eid/reglementation/

Deutsch: www.ibz.rrn.fgov.be/de/identitaetsdokumente/eid/vorschriften/

4.2.1 Durchführung von Identifikations- und Authentifizierungsfunktionen

Abschnitt nicht anwendbar.

4.2.2 Genehmigung oder Ablehnung von Zertifikatanträgen

Abschnitt nicht anwendbar.

4.2.3 Zeit zum Verarbeiten von Zertifikatanträgen

Abschnitt nicht anwendbar.

4.3 Ausstellung der Zertifikate

Nach Genehmigung eines Zertifikatantrags beantragt die RA die Ausstellung eines Zertifikats bei der CA. Die CA überprüft die Vollständigkeit, die Integrität und die Einmaligkeit der von der RA eingereichten Angaben nicht, sondern vertraut voll und ganz auf die RA für die Genauigkeit aller Angaben. Die CA prüft nur, ob die Seriennummer des Zertifikats, die die RA dem Zertifikatantrag zuweist, tatsächlich eine einmalige Seriennummer ist, die nicht vorher für ein anderes Ausländerzertifikat gebraucht wurde. Ist dies der Fall, so informiert die CA die RA darüber.

Alle Anträge der RA werden angenommen, unter der Bedingung dass:

- deren Format gültig ist,
- sie über den geeigneten gesicherten Kommunikationskanal eingereicht werden,
- alle Überprüfungen gemäß den Bestimmungen des CA-Vertrags ordentlich vorgenommen wurden.

Die CA überprüft die Identität der RA auf Basis der vorgelegten Beweisstücke.

Die CA vergewissert sich, dass das ausgestellte Zertifikat alle Angaben, die ihr im Antrag der RA vorgelegt wurden, insbesondere die durch die RA zugewiesene Seriennummer für das Zertifikat, enthält.

Nach der Ausstellung sperrt die CA das Zertifikat und übermittelt es an die RA.

Die RA bittet den Kartenersteller darum, die Ausländerzertifikate auf den elektronischen Personalausweis zu laden. Der Kartenersteller übermittelt der LRA über einen gesicherten Weg den elektronischen Personalausweis mit den Ausländerzertifikaten.

4.3.1 Handlungen der CA während der Zertifikatausstellung

Abschnitt nicht anwendbar.

4.3.2 Benachrichtigung des Abonnenten durch die CA über die Zertifikatausstellung

Abschnitt nicht anwendbar.

4.4 Annahme der Zertifikate

Nach Erstellung des elektronischen Personalausweises ist dieser noch nicht aktiviert. Die LRA aktiviert den elektronischen Personalausweis in Anwesenheit des Ausländers. Der Ausländer wie auch die RA brauchen die Aktivierungsangaben für den Ausweis. Diese Angaben werden vom Kartenersteller über einen gesicherten Weg geliefert. Der Ausweis kann nur mittels der kombinierten Aktivierungsangaben der LRA und des Ausländers aktiviert werden.

4.4.1 Handlung, die eine Annahme des Zertifikats darstellt

Die RA muss über die LRA über die Beschwerden gegen die Annahme eines ausgestellten Zertifikats informiert werden, damit die CA darum gebeten werden kann, die Zertifikate zu widerrufen.

4.4.2 Veröffentlichung des Zertifikats durch die CA

Abschnitt nicht anwendbar.

4.4.3 Benachrichtigung anderer Entitäten über die Zertifikatausstellung durch die CA

Abschnitt nicht anwendbar.

4.5 Benutzung von Schlüsselpaaren und Zertifikaten

Die mit der Benutzung von Schlüsseln und Zertifikate verbundenen Haftungen werden hierunter beschrieben.

4.5.1 Benutzung von Schlüsselpaaren und Zertifikaten durch Benutzer

Außer bei anders lautendem Hinweis im vorliegenden CPS gelten für den Ausländer folgende Rechte und Pflichten:

- Er darf ein Zertifikat nicht verfälschen.
- Er muss Risiken, Verlust, Enthüllung, Änderung oder jeglichen anderen unbefugten Gebrauch seiner Privatschlüssel vermeiden.
- Er darf Zertifikate nur zu gesetzlichen und zugelassenen Zwecken gemäß dem CPS benutzen.

4.5.2 Benutzung von Schlüsselpaaren und Zertifikaten durch vertrauende Parteien

Ein Partei, die sich auf eine CA-Zertifikat stützt:

- wird ein Zertifikat validieren mit Hilfe einer CRL, einer Delta CRL, eines OCSP oder über die Webseite für Zertifikatskontrolle gemäß dem Verfahren zur Bestätigung des vollständigen Zertifikatspfad;
- wird auf ein Zertifikat nur dann vertrauen, wenn dieses nicht gesperrt oder widerrufen worden ist;
- werden auf ein Zertifikat auf angemessene Weise je nach den Umständen vertrauen.
- Vertrauende Parteien müssen die Gültigkeit eines digitalen Zertifikats stets anhand der Gültigkeitsperiode des Zertifikats und der Gültigkeitserklärung des Zertifikats durch den CA-Dienst (über OCSP, CRL, Delta CRL oder Web-Schnittstelle) prüfen, bevor sie Informationen vertrauen, die in ein Zertifikat aufgenommen sind.

4.6 Erneuerung von Zertifikaten

4.6.1 Voraussetzungen für die Erneuerung von Zertifikaten

Die Ausländerzertifikate werden erneuert, wenn:

- der elektronische Personalausweis erneuert wird,
- einer Neuverschlüsselung nach Widerrufung.

4.6.2 Wer darf eine Erneuerung beantragen?

Siehe Abschnitt 4.1.

4.6.3 Bearbeitung von Anträgen auf Zertifikaterneuerung

Siehe Abschnitt 4.2.

4.6.4 Benachrichtigung von Abonnent über die Ausstellung neuer Zertifikate

Abschnitt nicht anwendbar.

4.6.5 Handlung, die die Annahme einer Zertifikaterneuerung darstellt

Siehe Abschnitt 4.4.1.

4.6.6 Veröffentlichung des Erneuerungszertifikats durch die CA.

Abschnitt nicht anwendbar.

4.6.7 Benachrichtigung anderer Entitäten über die Zertifikatausstellung durch die CA

Abschnitt nicht anwendbar.

4.7 Neuverschlüsselung von Zertifikaten

4.7.1 Voraussetzungen für die Neuverschlüsselung eines Zertifikats

Nach einer Widerrufung können Ausländerzertifikate nicht wieder aktiviert werden und müssen daher durch ein neue Zertifikate ersetzt werden.

4.7.2 Wer darf die Zertifizierung eines neuen öffentlichen Schlüssels beantragen

Siehe Abschnitt 4.1.

4.7.3 Bearbeitung von Anträgen auf Neuverschlüsselung von Zertifikaten

Auf Anfrage des Ausländers generiert die LRA ein neues Schlüsselpaar auf dem elektronischen Personalausweis und ersetzt das widerrufene Zertifikat durch ein neues

4.7.4 Benachrichtigung von Abonnent über die Ausstellung neuer Zertifikate

Abschnitt nicht anwendbar.

4.7.5 Handlung, die die Annahme eines neu verschlüsselten Zertifikats darstellt

Abschnitt nicht anwendbar.

4.7.6 Veröffentlichung des neu verschlüsselten Zertifikats durch die CA

Abschnitt nicht anwendbar.

4.7.7 Benachrichtigung anderer Entitäten über die Zertifikatausstellung durch die CA

Abschnitt nicht anwendbar.

4.8 Änderung eines Zertifikats

Abschnitt nicht anwendbar.

4.9 Sperrung und Widerrufung von Zertifikaten

Bis zur Annahme durch den Ausländer bleiben Ausländerzertifikate im elektronischen Personalausweis gesperrt. Ein Ausländerzertifikat muss zum ersten Mal innerhalb eines Monats nach der Ausstellung aktiviert werden. Die RAs und LRAs sorgen dafür, dass dieser Forderung nachgekommen wird. Mehr Informationen finden Sie über folgenden Link:

https://www.docstop.be/DocStop/docstop_en.jsp

Niederländisch: http://www.ibz.rrn.fgov.be/nl/identiteitsdocumenten/eid/faq/

Französisch: http://www.ibz.rrn.fgov.be/fr/documents-didentite/eid/faq/

Deutsch: http://www.ibz.rrn.fgov.be/de/identitaetsdokumente/eid/faq/

Um die Sperrung oder Widerrufung eines Zertifikats zu beantragen, muss der Ausländer mit einer LRA, der Polizei oder DOCSTOPKontakt aufnehmen. Während die Öffnungszeiten einer LRA begrenzt sind, ist DOCSTOP rund um die Uhr, sieben Tage die Woche zugänglich.

Die Polizei, die LRA, DOCSTOP oder der RA beantragen die Sperrung von Ausländerzertifikaten über die RA, nachdem:

- sie benachrichtigt wurden, dass vermutlich der Privatschlüssel von einem oder beiden der Ausländerzertifikate verloren, gestohlen, geändert, unbefugt offenbart oder anderweitig kompromittiert worden ist;
- die Ausführung einer Verpflichtung der RA im Sinne des vorliegenden CPS aufgrund einer Naturkatastrophe, einer EDV-Störung, einer Unterbrechung der Telekommunikationen oder aufgrund irgendeines Falles, der außerhalb des eigenen Willens der Person liegt, verzögert oder verhindert wird, wobei vermutet wird, dass die Informationen einer Drittperson materiell bedroht oder kompromittiert werden;
- sie von dem Ausländer benachrichtigt wurden, dass der Privatschlüssel von einem oder beiden seiner Ausländerzertifikate verloren, gestohlen, geändert oder auf unbefugte Weise enthüllt oder kompromittiert worden ist;
- die in einem Ausländerzertifikat enthaltenen Informationen geändert worden sind;
- die Ausführung einer Verpflichtung der RA im Sinne des vorliegenden CPS aufgrund einer Naturkatastrophe, einer EDV-Störung, einer Unterbrechung der Telekommunikationen oder aufgrund irgendeines Falls, der außerhalb des eigenen Willens der Person liegt, verzögert oder verhindert wird, wobei die Informationen einer Drittperson materiell bedroht oder kompromittiert werden;
- die RA gesetzlih dazu verpflichtet wird.

Auf Anfrage der RA oder des TSP sperrt oder widerruft die CA die Ausländerzertifikate.

Falls der Benutzer die Sperrung oder Widerrufung eines Zertifikats durch DOCSTOP beantragt hat, wird der Benutzer von der Statusänderung des Zertifikats per Brief an seine offizielle Adresse informiert.

Wenn von dem Ausländer keine Benachrichtigung empfangen wird, die Sperrung des Zertifikats aufzuheben, wird das Zertifikat nach einer Woche widerrufen.

Unter gewissen Umständen (z.B. Vermeiden einer Katastrophe, Risiko für einen CA-Schlüssel, Sicherheitsverletzung, usw.) kann der TSP beantragen, dass Zertifikate gesperrt und/oder widerrufen werden.

Der TSP bittet den eID TSP Lenkungsausschuss um die Genehmigung, diese Widerrufungen vorzunehmen. Je nach Dringlichkeitsgrad kann es jedoch vorkommen, dass der eID CSP Steering erst nach Vollendung des Prozesses benachrichtigt wird. Die RA sorgt dafür, dass die betreffenden Ausländer von dieser Sperrung/Widerrufung benachrichtigt werden

Um den Status der Zertifikate zu kontrollieren, müssen die vertrauenden Parteien Online-Hilfsmittel benutzen, die die CA über das Archiv zur Verfügung stellt, bevor sie auf diese Zertifikate vertrauen. Die CA aktualisiert demnach das OCSP, den Dienst zur Überprüfung des Status der Zertifizierung per Webseite, die CRLs und die Delta CRLs. Die CRLs werden öfter aktualisiert, mindestens alle drei Stunden.

Die CA gibt Zugang zu den OCSP-Hilfsmitteln und zu einer Webseite, auf welcher die Informationsanträge über den Status von Zertifikaten eingereicht werden können. Für alle unter der Foreigner CA ausgestellten Zertifikate ist die Widerrufstatusinformation über die Gültigkeitsperiode des Zertifikats durch die CRL verfügbar.

4.9.1 Umstände für Widerrufung

Eine Sperrung kann höchstens sieben Kalendertage dauern, um die Umstände zu bestimmen, die den Sperrungsantrag begründet haben. Wenn diese Umstände nicht bewiesen werden können, kann ein Ausländer die Reaktivierung (Aufhebung nach Sperrung) der Ausländerzertifikate unter folgenden Bedingungen beantragen:

- Der Ausländer muss sich dessen sicher sein, dass die Vermutung, dass der Privatschlüssel von einem oder beiden der Ausländerzertifikate verloren, gestohlen, geändert oder auf unbefugte Weise enthüllt oder kompromittiert wurde, unbegründet war;
- Es gibt keinen anderen Grund, die Zuverlässigkeit und die Vertraulichkeit der Privatschlüssel dieser beiden Ausländerzertifikate zu bezweifeln.

Um die Aufhebung der Sperrung seiner Ausländerzertifikate zu beantragen, muss der Ausländer selbst bei der LRA (der Gemeindeverwaltung an seinem/ihrem Wohnort) vorstellig werden oder Docstop anrufen, um den gelieferten Sicherheitscode zu bestätigen.

Die LRA beantragt umgehend die Aufhebung der Sperrung eines Paares von Ausländerzertifikaten über die RA, nachdem:

- Sie von dem Ausländer benachrichtigt wurden, dass der Privatschlüssel von einem oder beiden seiner Ausländerzertifikate verloren, gestohlen, geändert oder auf unbefugte Weise enthüllt oder kompromittiert worden ist;
- die Vermutung, dass Informationen einer anderen Person bedroht oder kompromittiert wären, weil die Erfüllung einer Verpflichtung der RA gemäß dem vorliegenden CPS durch eine Naturkatastrophe, eine EDV-Störung oder einen Kommunikationsfehler oder durch eine andere Ursache, die außerhalb der eigenen Kontrolle der Person liegt, verzögert oder verhindert wurde, unmissverständlich unrichtig zu sein scheint;
- Auf Antrag von der RA sperrt oder widerruft die CA ein Paar Ausländerzertifikate.

Nach einem Zeitraum von 7 Wochentagen widerruft die CA ein gesperrtes Zertifikat automatisch, wenn sie in der Zwischenzeit von der RA keine Benachrichtigung von der RA erhält, die Sperrung des Zertifikats aufzuheben.

Die CA veröffentlicht Bekanntgaben von gesperrten oder widerrufenen Zertifikaten im Archiv.

4.9.2 Wer kann eine Widerrufung beantragen?

Siehe Abschnitt 4.9.

4.9.3 Verfahren zur Beantragung von Widerrufung

Siehe Abschnitt 4.9.

4.9.4 Toleranzfrist für Widerrufungsantrag

Die Toleranzfrist für einen Widerrufungsantrag ist der Zeitraum, ab dem der Benutzer (der Ausländer) die Widerrufung eines Zertifikats durch Kontaktaufnahme mit der LRA, der

Polizei oder DOCSTOP beantragt hat, bis die Widerrufung des Zertifikats in den Zertifikatgenehmigungsdiensten wiedergegeben wird.

Die Toleranzfrist für den Widerrufungsantrag beträgt 7 Kalendertage.

4.9.5 Zeit, in der die CA den Widerrufungsantrag bearbeiten muss

Die CA widerruft/sperrt ein Ausländerzertifikat, nachdem sie den Widerrufungsantrag von der RA empfangen hat, so schnell wie möglich nach der Prüfung des Widerrufungsantrags. Die längste Verzögerung zwischen dem Empfang eines Widerrufungs- oder Sperrungsantrags oder der Meldung und dem Entschuss, dass die Statusinformation allen vertrauenden Parteien verfügbar ist, beträgt höchstens 24 Stunden.

Generell werden folgende Zeitfenster verwendet:

- Widerrufungsanträge, die drei oder mehr Stunden vor der CRL-Ausstellung empfangen werden, werden bearbeitet, bevor die nächste CRL veröffentlicht wird, und
- Widerrufungsanträge, die innerhalb von drei Stunden von der CRL-Ausstellung empfangen werden, werden bearbeitet, bevor die nächste CRL veröffentlicht wird.
- Widerrufungsanträge werden im OCSP Zertifikatprüfungsdienst innerhalb von drei Stunden nach Empfang des Antrags wiedergegeben.

4.9.6 Anforderungen zur Widerrufungsprüfung für vertrauende Parteien

Siehe **EID-DEL-004 eID PKI Hierarchy certificate profile**.

4.9.7 CRL-Ausstellungshäufigkeit (falls anwendbar)

Siehe **EID-DEL-004 eID PKI Hierarchy certificate profile**.

4.9.8 Längste Wartezeit für CRLs (falls anwendbar)

Siehe **EID-DEL-004 eID PKI Hierarchy certificate profile**.

4.9.9 Verfügbarkeit der Online-Prüfung von Widerrufung/Status

Siehe **EID-DEL-004 eID PKI Hierarchy certificate profile**.

4.9.10 Anforderungen für Online-Widerrufungsprüfung

Siehe **EID-DEL-004 eID PKI Hierarchy certificate profile**.

4.9.11 Andere verfügbare Formen von Widerrufungsankündigung

Abschnitt nicht anwendbar.

4.9.12 Besondere Anforderungen für Neuverschlüsselungsgefährdung

Abschnitt nicht anwendbar.

4.9.13 Umstände für Sperrung

Siehe Abschnitt 4.9.

4.9.14 Wer kann eine Sperrung beantragen?

Siehe Abschnitt 4.9.

4.9.15 Verfahren für Sperrungsanträge

Siehe Abschnitt 4.9.

4.9.16 Begrenzungen des Sperrzeitraums

Siehe Abschnitt 4.9.1.

4.10 Dienste für Zertifikatsstatus

Die CA stellt Dienste zur Kontrolle des Zertifikatsstatus zur Verfügung, einschließlich CRLs, Delta CRLs, OCSP und geeignete Webseiten.

4.10.1 CRLs und Delta CRLs

In einer Delta CRL werden alle Hinzufügungen aufgenommen, die seit der Veröffentlichung der letzten Basis-CRL erfolgt sind.

Die CRLs und die Delta CRLs werden von der CA unterzeichnet und datiert.

Eine CRL wird in Intervallen von mindestens drei Stunden zu einer vereinbarten Zeit ausgestellt. Eine Delta CRL wird alle drei Stunden gemäß einem vereinbarten Zeitplan ausgestellt. Die CRLs und die Delta CRLs werden von der CA unterzeichnet und datiert. Die CRLs und die Delta CRLs sind zu finden auf:

http://crl.eid.belgium.be

4.10.2 OCSP

Die CA stellt den belgischen öffentlichen Verwaltungsbehörden die OCSP-Antworten zur Verfügung. Dieser benutzt sie über seine eigenen öffentlichen Verwaltungsnetze.

Eine einfache Webseite gibt Zugang zu den Statusüberprüfungsdiensten und ermöglicht es einem Benutzer, Informationen über den Status eines Zertifikats zu erhalten. Die CA stellt diese Webseite den belgischen öffentlichen Behörden für Statusüberprüfungsdienste zur Verfügung, um sie durch ihre un innerhalb ihrer eigenen öffentlichen Verwaltungsnetze zu nutzen.

Webseite für Statusüberprüfungsdienste http://status.eid.belgium.be

Die OCSP-Beantworter sind erreichbar auf:

http://ocsp.eid.belgium.be oder http://ocsp.eid.belgium.be/2

4.10.3 Betriebsmerkmale

*Siehe **EID-DEL-004 eID PKI Hierarchy certificate profile**.*

4.10.4 Dienstverfügbarkeit

Die Zertifikatstatusdienste sind rund um die Uhr an allen 7 Wochentagen verfügbar.

Außerhalb der Wartungsfenster darf pro Kalendermonat die gesamte Zeit, während der die folgenden CA-Dienste unverfügbar sind, in Minuten ausgedrückt, über den gesamten Monat nicht mehr als 0,5 % der Gesamtanzahl Minuten von diesem Kalendermonat betragen:

- OCSP-Überprüfung des Zertifikatsstatus aufgrund eines vom RRN, von einem Benutzer oder von einer vertrauenden Partei eingereichten Antrags;
- Herunterladen von CRLs oder von Delta CRLs über das Internet oder die öffentlichen Netze;
- Dienst zur Überprüfung des Zertifikatsstatus per Webseite..

Während der OCSP-Dienst, der CRL- und Delta CRL-Downloaddienst und der Dienst zur Statusüberprüfung per Webseite unverfügbar sind, wird auch die örtliche Infrastruktur der CA, einschließlich der örtlichen Server, Netze und Firewalls, unverfügbar sein. Das Internet, oder Teile davon, und die örtliche Infrastruktur des Dienstanfragers bleiben dagegen verfügbar.

Die CA stellt ein internes Archiv für die folgenden Elemente, Angaben und Dokumente auf, die den angebotenen Diensten gehören:

- CRL und Delta CRLs. CRLs und Delta CRLs werden während eines Zeitraums von mindestens 30 Jahren nach deren Veröffentlichung archiviert.

4.10.5 Optionale Merkmale

Die CA kann die Verarbeitung von OCSP-Anträgen für eine Partei, die aufgrund ihrer Aktivitäten genötigt ist, den OCSP-Status regelmäßig zu überprüfen, nicht beschränken.

4.11 Ende des Abonnements

Abschnitt nicht anwendbar.

4.12 Abgabe und Abholen der Schlüssel

Das Abgeben und Abholen der Schlüssel ist nicht zugelassen.

5 Kontrollen betreffend Einrichtungen, Management und Betrieb

In diesem Kapitel werden die nicht technischen Sicherheitskontrollen beschrieben, die von der „Foreigner CA“ und anderen PKI-Partner angewendet werden, um Funkeionen wie Schlüsselgenerierung, Benutzerauthentifizierung, Zertifikatausstellung, Zertifikatwiderrufung, Audit und Archivierung durchzuführen.

5.1 Physische Kontrollen

Der TSP führt physische Kontrollen an seinen eigenen Standorten aus. Unter die physischen Kontrollen des TSP fallen folgende:

Die TSP-Standorte beherbergen die zur Leistung der CA-Dienste nötige Infrastruktur. Der TSP sorgt für geeignete Sicherheitskontrollen an seinen Standorten, mitsamt Zugangskontrolle, Einbruchsmeldung und Bewachung. Der Zugang zu den Standorten wird auf das befugte Personal begrenzt. Die Liste, auf der dieses Personal aufgenommen ist, ist zur Kontrolle verfügbar.

Für alle Gebiete, die hochempfindliches Material und hochempfindliche Infrastruktur enthalten, gilt eine strenge Zugangskontrolle. Hierzu gehören das Material und die Infrastruktur, die für die Unterzeichnung von Zertifikaten, CRLs und Delta CRLs, OCSP und Archive nötig sind.

5.1.1 Lage und Konstruktion der Standorte

Die gesicherten Räumlichkeiten der TSP-Betreiber befinden sich in einem Bereich, der für Hochsicherheitsbetrieb geeignet ist. Diese Räumlichkeiten beherbergen nummerierte Zonen und abgeschlossene Räume, Käfige, Safes und Schränke.

5.1.2 Physischer Zugang

Der physische Zugang wird durch den Gebrauch von Kontrollsystemen begrenzt, die den Zugang von einer Zone des Gebäudes zur anderen oder den Zugang zu hoch gesicherten Zonen sowie die Lokalisierung der TSP-Aktivitäten in einem gesicherten EDV-Raum mit physischer Bewachung und Sicherheitsalarmen betreffen, wobei ein Badge und Zugangskontrolllisten benutze werden, um sich von einer Zone nach der anderen zu bewegen.

5.1.3 Stromversorgung und Klimatisierung

Redundante Stromversorgung und Klimaregelung.

5.1.4 Aussetzung an Wasser

Die Räume sind gegen jede Aussetzung an Wasser geschützt.

5.1.5 Brandverhütung und -schutz

Der TSP ergreift Verhütungs- und Schutzmaßnahmen sowie Brandschutzmaßnahmen.

5.1.6 Aufbewahrung von Medien

Medien werden in aller Sicherheit gelagert. Die Backup-Medien werden an einem anderen Ort aufbewahrt, der physisch gegen Brand- und Wasserschäden geschützt ist.

5.1.7 Abfallentsorgung

Zur Verhütung jeglicher unerwünschten Verbreitung empfindlicher Daten, werden die Abfälle auf gesicherte Weise entsorgt.

5.1.8 Backup entfernt vom Standort

Der TSP sorgt für ein teilweises Backup entfernt vom Standort,

5.2 Verfahrenskontrollen

Der TSP wendet in Sachen Personal und Management Praktiken an, die eine angemessene Garantie bieten, was Zuverlässigkeit und Fähigkeit der Teammitglieder sowie zufrieden stellende Ausführung ihrer Aufgaben im Bereich der Technologien der elektronischen Unterzeichnung betrifft.

Jedes Personalmitglied muss eine unterzeichnete Erklärung beim TSP einreichen, in der es bestätigt, keine gegensätzlichen Interessen beim TSP zu haben, dass es die Vertraulichkeit bewahren und die persönlichen Angaben schützen wird.

Die Funktion aller Personalmitglieder, die für die Verwaltung der Schlüssel einstehen, Verwalter, Sicherheitspersonal und Systemkontrolleure, oder für jede andere Aktivität, die solche Handlungen materiell beeinflusst, wird als vertraulich betrachtet.

Der TSP führt eine anfängliche Untersuchung für alle Personalmitglieder aus, die sich für eine Vertraulichkeitsfunktion bewerben, um ihre Zuverlässigkeit und Fähigkeit in angemessenem Maße zu bestimmen.

Falls eine Kontrolle nach dem 4-Augen-Prinzips nötig ist, müssen die jeweiligen getrennten Kenntnisse von mindestens zwei Personen mit Vertrauensposition für die Fortsetzung der laufenden Handlungen in Anspruch genommen werden.

Der TSP garantiert, dass alle Handlungen in Verbindung mit dem TSP dem System des TSP und dem TSP-Personalmitglied, das diese Handlung ausgeführt hat, zugewiesen werden können.

5.2.1 Vertrauensrollen

Der TSP unterscheidet zwischen folgenden Arbeitsgruppen:

- Ausführendes TSP-Personal, das Verrichtungen auf Zertifikate verwaltet.
- Verwaltungspersonal, das die TSP-Stützplattform organisiert.
- Sicherheitspersonal, das die Sicherheitsmaßnahmen trifft.

5.3 Personalkontrollen

Der TSP führt gewisse Sicherheitskontrollen für die Aufgaben und Leistungen der Mitarbeiter seines Teams aus. Diese Sicherheitskontrollen werden in einer Policy dokumentiert und umfassen folgende Elemente.

5.3.1 Anforderungen hinsichtlich Qualifikationen, Erfahrung und Genehmigungen

Der TSP führt Kontrollen aus, um Hintergrund, Qualifikationen und Erfahrung zu bestimmen, die notwendig sind, um im Kompetenzbereich der spezifischen Funktion zu genügen. Solche Hintergrundkontrollen umfassen:

- strafrechtliche Verurteilungen wegen Schwerverbrechen;
- falsche Erklärungen des Bewerbers;
- Richtigkeit der Referenzen;
- gegebenenfalls, die Genehmigungen.

5.3.2 Hintergrundprüfverfahren

Der TSP führt mit Hilfe der von einer befugten Behörde gelieferten Statusberichte, der Erklärungen von Drittparteien oder der unterzeichneten persönlichen Erklärungen die nötigen Kontrollen für die potentiellen Angestellten aus.

5.3.3 Ausbildungsanforderungen

Jeder TSP bietet seinen Mitarbeitern Ausbildungen an, damit diese ihre TSP-Funktionen ausführen können.

5.3.4 Häufigkeit und Anforderungen für Fortbildung

Das Personal kann regelmäßig fortgebildet werden, um für Kontinuität zu sorgen und die Kenntnisse des Personals und die Verfahren zu aktualisieren.

5.3.5 Häufigkeit und Reihenfolge des turnusmäßigen Tätigkeitswechsels

Abschnitt nicht anwendbar.

5.3.6 Strafen für unbefügte Handlungen

Der TSP bestraft das Personal für unbefugte Handlungen, den Missbrauch von Befugnissen und den unbefugten Gebrauch von Systemen mit dem Ziel, gegebenenfalls das Personal eines Beteiligten zur Verantwortung zu ziehen.

5.3.7 Anforderungen an unabhängige Vertragsparteien

Die unabhängigen Vertragsparteien des TSP und ihr Personal sind Gegenstand derselben Hintergrundkontrollen wie das TSP-Personal. SIEHE 5.3.1 ANFORDERUNGEN HINSICHTLICH QUALIFIKATIONEN, ERFAHRUNG UND GENEHMIGUNGEN

5.3.8 Dokumentation, ausgehändigt an das Personal

Jeder TSP stellt dem Personal die nötige Dokumentation während der anfänglichen Ausbildung, der Weiterbildung oder in anderen Fällen zur Verfügung.

5.4 Verfahren für Audit-Logging

Unter die Verfahren für Audit-Logging fallen unter anderem das Event-Logging und die Systemkontrolle. Diese Verfahren werden angewandt, um eine sichere Umgebung aufrecht zu erhalten. Die CA führt folgende Kontrollen aus:

Das Event-Logging-System der CA registriert unter anderem die folgenden Handlungen:

- Ausstellung eines Zertifikats;
- Widerrufung eines Zertifikats;
- Sperrung eines Zertifikats;
- (Re)aktivierung eines Zertifikats;
- Automatische Widerrufung;
- Veröffentlichung einer CRL oder Delta CRL;

Der TSPkontrolliert alle Aufnahmen des Event-Loggings. Die Aufnahmen des Kontrollberichts umfassen:

- Identifizierung der Verrichtung;
- Datum und Uhrzeit der Verrichtung;
- Identifizierung des Zertifikats die von der Verrichtung betroffen ist;
- Identität des Anfragers der Verrichtung.

Außerdem bewahrt der TSP die internen Logbücher und die Kontrollberichte der relevanten operationellen Handlungen in der Infrastruktur auf. Es handelt sich unter anderem um:

- das Starten und Stilllegen der Server;
- die Störungen und Hauptprobleme;
- den physischen Zugang des Personals und von anderen Personen zu den empfindlichen Teilen des TSP-Standorts;
- das Backup und die Herstellung;
- den Bericht über die Wiederinbetriebnahmetests nach einer Katastrophe;
- die Kontrollinspektionen;
- die Erweiterungen und Änderungen der Systeme, Softwares und der Infrastruktur;
- die Einbrüche und Einbruchsversuche in den gesicherten Zonen.

Andere erforderliche Dokumente für die Kontrollen sind unter anderem:

- Pläne und Beschreibungen der Infrastruktur;
- Pläne und Beschreibungen der Standorte;

- Konfiguration von Hardware und Software;
- Zugangskontrolllisten für das Personal.

Der TSP sorgt dafür, dass das hierfür angestellte Personal die Logdateien in regelmäßigen Abständen überprüft und die anormalen Ereignisse meldet.

Die Logdateien und Kontrollberichte werden zur Inspektion durch das befugte CA-Personal, die RAs und die angestellten Prüfer archiviert. Die Logdateien sind auf geeignete Weise durch einen Zugangskontrollmechanismus zu schützen. Die Logdateien und die Kontrollberichte sind Gegenstand eines Backups.

Auditereignisse werden nicht gemeldet.

5.4.1 Arten aufgezeichneter Ereignisse

Der TSP bewahrt auf zuverlässige Weise die Verzeichnisse der digitalen Zertifikate, Auditdaten, Informationen über und Dokumentation der TSP-Systeme auf.

5.4.2 Häufigkeit der Kontrollverarbeitung

Die CA prüft die Kontrollberichte in regelmäßigen Abständen auf Anomalien oder Warnungen.

5.4.3 Aufbewahrungszeitraum für Kontrollberichte

Der TSP bewahrt auf zuverlässige Weise die Verzeichnisse der digitalen Zertifikate während des unter Artikel 5.5 des vorliegenden CPS erwähnten Zeitraums auf.

5.4.4 Schutz des Kontrollberichts

Nur der Verzeichnisverwalter (Teammitglied, das mit der Aufbewahrung der Verzeichnisse beauftragt ist) kann Zugang zu den TSP-Archiven erhalten. Es müssen Maßnahmen getroffen werden, um folgendes zu gewährleisten:

- Schutz gegen die Änderung der Archive, wie die Speicherung von Angaben auf einem einmalig beschreibbaren Medium;
- Schutz gegen das Löschen von Archiven;
- Schutz gegen die Beschädigung der Medien, auf denen die Archive gelagert sind, wie die regelmäßige Verlegung der Angaben auf ungebrauchte Medien.

Der TSP handelt gemäß der potentiellen Anwendung durch die Belgische Föderale Behörde des Verfahrens von Artikel 14 des Gesetzes vom 8. August 1983 *zur Organisation eines Nationalregisters der natürlichen Personen* und von Artikel 7 des Gesetzes vom 12. Mai 1927 *über die militärischen Requisitionen*. In diesem Fall handelt die CA gemäß den Anweisungen, die von der vom königlichen Erlass bezeichneten Person erteilt werden, was die Angaben betrifft, die zu den elektronischen Personalausweisen und den Ausländerzertifikaten gehören

5.4.5 Backup-Verfahren für Kontrollberichte

Ein differentielles Backup der Archive des TSP wird an Werktagen täglich vorgenommen.

5.4.6 Kontrollsammlungssystem

Das System zur Sammlung der TSP-Archive ist intern.

5.4.7 Benachrichtigung an ereignisverursachenden Benutzer

Nicht anwendbar.

5.4.8 Verletzlichkeitsbeurteilungen

Nicht anwendbar.

5.5 Archivierung der Verzeichnisse

Der TSP bewahrt interne Verzeichnisse der folgenden Elemente auf:

- Alle Bescheinigungen während eines Zeitraums von mindestens 30 Jahren nach Ablauf des Zertifikats;
- Auditbericht über die Ausstellung der Zertifikate für einen Zeitraum von mindestens 30 Jahren nach Ausstellung des Zertifikats;
- Auditbericht über die Widerrufung eines Zertifikats von mindestens 30 Jahren nach Widerruf des Zertifikats;
- CRLs und Delta CRLs von mindestens 30 Jahren nach deren Veröffentlichung;
- Der TSP muss das letzte Backup der CA-Archive von mindestens 30 Jahren nach Ausstellung des letzten Zertifikats aufbewahren.

Der TSP bewahrt die Archive in einem leicht nachzuschlagenden Format auf.

Der TSP sorgt für die Integrität der physischen Speichermedien und implementiert eigene Kopiermechanismen, um den Verlust von Daten zu verhindern.

Die Archive sind dem befugten Personal der CA und der RA zugänglich..

5.5.1 Arten archivierter Verzeichnisse

Der TSP bewahrt auf zuverlässige Weise die Verzeichnisse der digitalen Zertifikate, Auditdaten, Informationen über und Dokumentation der TSP-Systeme auf.

5.5.2 Aufbewahrungszeitraum für Archive

Der TSP bewahrt auf zuverlässige Weise die Verzeichnisse der digitalen Zertifikate während des unter Artikel 5.5 des vorliegenden CPS erwähnten Zeitraums auf. Diese Anforderung wird durch regelmäßige Kontrollen überprüft.

5.5.3 Schutz des Archivs

Nur der Verzeichnisverwalter (Teammitglied, das mit der Aufbewahrung der Verzeichnisse beauftragt ist) kann Zugang zu den TSP-Archiven erhalten. Es müssen Maßnahmen getroffen werden, um folgendes zu gewährleisten:

- Schutz gegen die Änderung der Archive, wie die Speicherung von Angaben auf einem einmalig beschreibbaren Medium;
- Schutz gegen das Löschen von Archiven;
- Schutz gegen die Beschädigung der Medien, auf denen die Archive gelagert sind, wie die regelmäßige Verlegung der Angaben auf ungebrauchte Medien.

Der TSP handelt gemäß der potentiellen Anwendung durch die Belgische Föderale Behörde des Verfahrens von Artikel 14 des Gesetzes vom 8. August 1983 *zur Organisation eines Nationalregisters der natürlichen Personen* und von Artikel 7 des Gesetzes vom 12. Mai 1927 *über die militärischen Requisitionen*. In diesem Fall handelt die CA gemäß den Anweisungen, die von der vom königlichen Erlass bezeichneten Person erteilt werden, was die Angaben betrifft, die zu den elektronischen Personalausweisen und den Ausländerzertifikaten gehören.

5.5.4 Verfahren für das Backup der Archive

Ein differentielles Backup der Archive des TSP wird an Werktagen täglich vorgenommen.

5.5.5 Anforderungen zum Anbringen von Zeitstempeln auf den Verzeichnissen

Abschnitt nicht anwendbar.

5.5.6 Archivsammlungssystem (intern oder extern)

Das System zur Sammlung der TSP-Archive ist intern.

5.5.7 Verfahren zur Erhaltung und Überprüfung der Archivierungsinformationen

Nur TSP-Personalmitglieder mit einer deutlichen hierarchischen Kontrolle und einer wohl umrissenen Funktionsbeschreibung können Archivierungsinformationen erhalten und überprüfen

Der TSP bewahrt die Verzeichnisse im elektronischen Format oder auf Papier auf

5.6 Schlüsselübergabe

Die Foreigner CA hat einen Plan für die Schlüsselübergabe der untergeordneten ausstellenden CAs und ausstellenden CA-Zertifikate (die Foreigner CA-Zertifikate sind zum Herunterladen auf der Archiv-Websiteverfügbar):

Am Ende von jedem Jahr wird im Rahmen einer Schlüsselzeremonie eine Anzahl von Foreigner CA-Zertifikaten generiert. Diese Anzahl wird vom TSP und dem Staat bestimmt und beruht auf der erwarteten Nachfrage von End-Entitätszertifikaten im nächsten Jahr. In

der Schlüsselzeremonie werden die Foreigner CA-Zertifikate von den BRCAs ausgestellt, die langfristige Vertrauensanker der eID PKI sind.

Nachdem die neue Charge von Foreigner CA-Zertifikaten in die Produktionsumgebung gebracht wurde, werden diese Ausstellungszertifikate verwendet, um die End-Entitätszertifikate des laufenden Jahres auszustellen, und der vorhergehende Posten an Foreigner CA-Zertifikaten wird nicht mehr zum Ausstellen neuer Zertifikate verwendet. Mit anderen Worten, ein Foreigner CA-Zertifikat wird nur während eines Jahres zum Ausstellen neuer Zertifikate verwendet. Ein Foreigner CA-Zertifikat wird länger gültig sein als jedes End-Entitätszertifikat, das es ausgestellt hat.

Nachdem ein Foreigner CA-Zertifikat verfallen ist oder widerrufen wurde, wird das Schlüsselmaterial in der nächsten Schlüsselzeremonie vernichtet.

5.7 Risiken und Wiederherstellung nach einer Katastrophe

Es wurde ein Plan für die Kontinuität der Unternehmung ausgearbeitet, um die Fortsetzung der Aktivitäten nach einer Naturkatastrophe oder einer anderen Notfallsituation zu gewährleisten.

Alle diese Maßnahmen werden auf Basis der ISO 27001-Norm getroffen.

Der TSP sorgt für:

- Hilfsmittel zur Wiederherstellung im Falle einer Katastrophe, an zwei verschiedenen Orten, die von einander genügend entfernt sind;
- Schnelle Kommunikation zwischen beiden Standorten, um die Integrität der Daten zu gewährleisten;
- Eine Kommunikationsinfrastruktur von beiden Standorten aus zur RA, die die Internet-Kommunikationsprotokolle sowie die von der belgischen öffentlichen Verwaltung gebrauchten Protokolle unterstützt;
- Infrastruktur und Prozeduren zur Wiederherstellung nach einer Katastrophe, die mindestens einmal im Jahr getestet werden.

5.7.1 Verfahren zur Behandlung von Zwischenfällen und Risiken

In einem getrennten internen Dokument spezifiziert die CA die Verfahren für die Meldung und die Behandlung von den Zwischenfällen und Risiken. Der TSP spezifiziert die Wiederherstellungsprozeduren, die angewandt werden, wenn die EDV-Hilfsmittel, die Softwares und/oder die Daten defekt sind oder wenn vermutet wird, dass sie defekt sind.

Der TSP trifft die nötigen Maßnahmen, um die vollständige und automatische Wiederherstellung des Dienstes im Falle von Katastrophe, Beschädigung der Server, Softwares und Daten zu gewährleisten.

5.7.2 Beschädigung der EDV-Hilfsmittel, Softwares und/oder Daten.

Der TSP hat bestimmte Wiederherstellungsverfahren implementiert, falls die EDV-Hilfsmittel, die Softwares und/oder die Daten defekt sind oder wenn vermutet wird, dass sie defekt sind,

5.7.3 Verfahren im Fall eines kompromittierten Entitäts-Privatschlüsels

Falls vermutet wird oder bekannt ist, dass ein CA-Privatschlüssel kompromittiert ist, werden die TSP-Krisenmanagementverfahren gemäß dem Zwischenfallmanagementprozess und mit Genehmigung der Geschäftsleitung von Certipost und den Vertretern der belgischen Regierung aktiviert. Die Benachrichtigung betroffener Parteien erfolgt über einen Kommunikationsplan, und falls eine CA-Zertifikatwiderrufung erforderlich ist wird der Widerrufungsstatus den vertrauenden Parteien über die eID Repository Website oder die eID CRL Website.

5.7.4 Fortsetzung der Geschäftsfähigkeit nach einer Katastrophe

Der TSP hat die Fähigkeit entwickelt, seine CA-Operationen innerhalb von vier (4) Stunden nach einer Katastrophe wiederherzustellen, mit Unterstützung für alle Schlüsselfunktionen, also Zertifikatausstellung, Zertifikatwiderrufung und Veröffentlichung von CRL-Information.

5.8 CA- oder RA-Beendigung

Sobald der TSP von der Belgischen Föderalen Behörde vernimmt, dass der Vertrag gekündigt werden soll und/oder sobald der Vertrag frühzeitig annulliert wird, wird der TSP den belgischen Staat zu Rate ziehen, um zu bestimmen, welche Schritte erforderlich sind, um (1) eine einwandfreie Übertragung der Dienstleistung an den neuen TSP zu gewährleisten und um (2) die Zerstörung, die Entfernung, die Wiederherstellung und/oder die Sicherung der Informationen, personenbezogenen Daten und Dateien, die der TSP im Rahmen der Erfüllung seiner Aufgaben als TSP empfangen hat, zu gewährleisten, in Übereinstimmung mit der EU-Verordnung 910/2014, *die einige Regeln betreffend den gesetzlichen Rahmen für elektronische Unterschriften und Zertifizierungsdienste festlegt.*

6 Kontrollen der technischen Sicherheit

In diesem Kapitel werden die Sicherheitsmaßnahmen bestimmt, die die CA treffen muss, um ihre kryptografischen Schlüssel und die Aktivierungsdaten zu schützen (z.B. PIN, Passwörter oder manuell unterhaltene Schlüssel).

6.1 Generierung und Installierung des Schlüsselpaares

Die CA schützt ihre(n) Privatschlüssel gemäß dem vorliegenden CPS. Die CA benutzt Privatunterschriftsschlüssel nur zur Unterzeichnung der Zertifikate, der CRLs, der Delta CRLs und der OCSP-Antworten in Übereinstimmung mit der Privatbenutzung für jeden dieser Schlüssel.

Die CA unterlässt jede Benutzung dieser CA-Privatschlüssel außerhalb der Reichweite des CA-Bereiches.

6.1.1 Schlüsselpaargenerierung

Die CA und RA benutzen ein zuverlässiges Verfahren für die Generierung ihres CA-Privatschlüssels gemäß einem dokumentierten Verfahren. Die CA verteilt die Geheimnisteile ihres (ihrer) Privatschlüssel(s). Der TSP ist dazu befugt, den Inhabern von Geheimnisteilen diese Geheimnisteile gemäß einem dokumentierten Verfahren zu übermitteln.

Die Schlüsselpaare der untergeordneten ausstellenden CAs der Foreigner CA (Schlüssel der ausstellenden CA) wurden in einem Offline-HSM generiert, das mindestens die Anforderung von FIPS 140-2 Stufe 3 erfüllt. Folglich wurden die Schlüssel der ausstellenden CA in einem Online-HSM geklont, das mindestens die Anforderungen von FIPS 140-2 Stufe 3 erfüllt.

6.1.2 Lieferung von Privatschlüssel an einen Benutzer

Der Privatschlüssel eines Benutzers wird vom Kartenersteller auf dem und durch das QSCD generiert. Der Privatschlüssel wird von dem QSCD nicht entnommen.

6.1.3 Lieferung von öffentlichem Schlüssel an Zertifikataussteller

Der öffentliche Schlüssel des Benutzers wird vom Kartenersteller nach der Schlüsselpaargenerierung auf dem QSCD mittels einer verschlüsselten Nachricht über eine gesicherte Verbindung an die RA übertragen. Die RA bindet den öffentlichen Schlüssel in einen Antrag ein und sendet ihn über eine gesicherte Privatverbindung an die CA.

Nach demselben Verfahren wird das Zertifikat zurück an den Kartenersteller geliefert.

6.1.4 Lieferung von öffentlichem CA-Schlüssel an vertrauende Parteien

Die öffentlichen CA-Schlüssel werden über die Website eID Repository zur Verfügung gestellt.

6.1.5 Schlüsselgrößen

Einzelheiten finden Sie in dem Dokument:

EID-DEL-004 eID PKI Hierarchy certificate profile, Abschnitt 5.7 Subject Public Key Info

6.1.6 Generierung und Qualitätsprüfung von Parametern öffentlicher Schlüssel

Siehe Abschnitt 6.1.1Schlüsselpaargenerierung

6.1.7 Zwecke für Schlüsselnutzung (gemäß X.509 v3 Schlüsselnutzungsfeld)

Einzelheiten finden Sie in dem Dokument EID-DEL-004 eID PKI Hierarchy certificate profile, Abschnitt 5.8 Key usage extension.

6.2 Schutz des Privatschlüssels und Kontrollen des kryptographischen Moduls

6.2.1 Sicheres kryptographisches Modul

Die Hardware der gesicherten Verschlüsselungsvorrichtung ist der NXP-Chip P5CC081, der EAL5+-zertifiziert ist.

Das „Belpic"-Applet, V1.7, das auf der Plattform MultiAppID v2.1 80K CC auf dem Chip läuft, ist EAL4+-zertifiziert.

6.2.2 Generierung des Privatschlüssels

Das Schlüsselpaar (privater-öffentlicher Schlüssel) wird auf dem Chip generiert.

Nur der öffentliche Schlüssel kann von dem Chip exportiert werden. Der Privatschlüssel bleibt gesichert im Chip.

6.2.3 Kontrolle des Privatschlüssels durch mehrere Personen

Nicht anwendbar. Die gesicherte Verschlüsselungsvorrichtung darf nur von dem angewiesenen Benutzer verwendet werden.

6.2.4 Hinterlegung des Privatschlüssels

Privatschlüssel können und werden nie von der gesicherten Verschlüsselungsvorrichtung, auf der sie generiert werden, entnommen. Privatschlüssel werden nie bei einem Dritten hinterlegt.

6.2.5 Backup des Privatschlüssels

Privatschlüssel auf einer gesicherten Verschlüsselungsvorrichtung werden auf der Vorrichtung generiert und es ist nicht möglich, eine Sicherungskopie zu erstellen.

6.2.6 Archivierung des Privatschlüssels

Privatschlüssel auf einer gesicherten Verschlüsselungsvorrichtung werden auf der Vorrichtung generiert und können nicht zu Backup-, Hinterlegungs- oder Archivierungszwecken entnommen werden.

6.2.7 Privatschlüsselübertragung zu oder von einem kryptographischen Modul

Privatschlüssel auf einer gesicherten Verschlüsselungsvorrichtung können nicht übertragen werden.

6.2.8 Privatschlüsselspeicherung auf kryptographischem Modul

Privatschlüssel auf einer gesicherten Verschlüsselungsvorrichtung werden in einem sicheren Speicher gespeichert. Der eingebettete Mikrochip schützt Privatschlüssel und andere sicherheitsrelevante Informationen gegen Hacks.

6.2.9 Verfahren zum Aktivieren von Privatschlüsseln

Die Aktivierungsdaten für ein gesichertes Verschlüsselungsgerät bestehen aus PIN- und PUK-Codes. PIN-Codes und PUK-Codes werden dem Ausländer in einem schützenden, manipulationssicheren Behälter wie etwa einem PIN-Brief und/oder einem versiegelten Umschlag übermittelt.

6.2.10 Verfahren zum Vernichten von Privatschlüsseln

Der Privatschlüssel kann gesperrt oder sogar aufgegeben (unwiderruflich gesperrt) werden, indem man wiederholt einen falschen PIN- oder PUK-Code eingibt.

6.2.11 Beurteilung kryptographischer Module

Mindeststandards für kryptographische Module sind aufgeführt unter:

ANHANG B: ANFORDERUNGEN FÜR ZERTIFIZIERUNGSBEHÖRDEN

6.3 Andere Aspekte der Verwaltung des Schlüsselpaares

Der TSP benutzt geeignete kryptographische Vorrichtungen für die Ausführung der Schlüsselverwaltungsaufgaben der CA. Diese kryptographischen Vorrichtungen werden Hardware Security Modules (HSMs) genannt.

Solche Vorrichtungen entsprechen den formellen Bedingungen (FIPS 140-2 Stufe 3 als Minimum), die unter anderem garantieren, dass jeder Verletzungsversuch bei der Vorrichtung unmittelbar detektiert wird und dass die Privatschlüssel die Vorrichtungen nicht unverschlüsselt verlassen können.

Hardware- und Softwaremechanismen, die die Privatschlüssel der CA schützen, werden dokumentiert. Das Dokument demonstriert, dass CA-Schlüsselschutzmechanismen mindestens gleich stark sind wie die CA-Schlüssel, die von ihnen geschützt werden.

6.3.1 Archivierung von öffentlichen Schlüsseln

6.3.2 Lebensdauer von Zertifikaten und Nutzungsdauer von Schlüsselpaaren

Einzelheiten finden Sie in diesem Dokument:

Einzelheiten finden Sie in diesem Dokument: EID-DEL-004 eID PKI HIERARCHY CERTIFICATE PROFILE.

6.4 Aktivierungsdaten

6.4.1 Generierung und Installierung von Aktivierungsdaten

Die Aktivierung der Root-CA erfolgt mittels sogenannter Schlüsselwächter.

Die operationellen CAs werden mittels eines operationellen Tokens aktiviert.

Die Aktivierung des Schlüssels des Benutzers erfolgt:

- Zuerst bei Empfang der eID (QSCD)-Karte bei der Gemeindeverwaltung.
    - Karte und Schlüssel können nur bei der Gemeindeverwaltung aktiviert werden.
    - In Zusammenarbeit mit dem Gemeindebeamten.
- Für die operationelle Aktivierung wird die PIN des Benutzers verwendet

6.4.2 Schutz der Aktivierungsdaten

Für die Root-CA hat jeder Schlüsselwächter einen Teil des Aktivierungsschlüssels. Diese Token werden durch einen Kennsatz geschützt. Das Schutzschema ist M ODER N. Die Token werden in einem Tresor aufbewahrt.

Die operationellen CAs werden von einem geteilten Token geschützt. Diese (M oder N) Token werden durch einen Kennsatz geschützt. Token werden in einem Tresor aufbewahrt.

Der Schlüssel des Benutzers wird durch eine PIN geschützt. Die PIN wird dem Benutzer direkt per Post in einem gesicherten Umschlag zugestellt. Aktivierungsdaten sollte man sich merken, nicht aufschreiben. Aktivierungsdaten dürfen nie anderen mitgeteilt werden. Aktivierungsdaten dürfen nicht nur aus Information bestehen, die leicht zu erraten ist, wie etwa persönliche Informationen eines Zertifikatinhabers.

6.4.3 Andere Aspekte von Aktivierungsdaten

Die CA speichert und archiviert alle mit seinem eigenen Privatschlüssel und seinen Verrichtungen verbundenen Aktivierungsdaten in aller Sicherheit.

6.5 Computersicherheitskontrollen

Die CA implementiert angemessene Computersicherheitskontrollen, einschließlich physische und logische Zugangskontrollen, Rollentrennung, mehrschichtige Kontrollen, Eindringungsdetektion und Authentifizierungsprozesse mit mehreren Faktoren für das gesamte Personal, das die Ausstellung eines Zertifikats veranlassen kann oder bewirken kann, dass eine Person ein Zertifikataussteller werden kann.

6.5.1 Spezifische technische Anforderungen an die Computersicherheit

Die Foreigner CA stellt folgende Funktionalität durch das Betriebssystem und eine Kombination aus Betriebssystem, PKI und physischen Kontrollen bereit:

- Zugangskontrolle zu CA-Diensten und PKI-Rollen;

- erzwungene Trennung von Pflichten für PKI-Rollen;
- Identifizierung und Authentifizierung von PKI-Rollen und zugehörigen Identitäten;
- Verwendung von Kryptografie für Sitzungskommunikation und Datenbanksicherheit;
- Archivierung von CA und End-Entitätshistorie und Kontrolldaten;
- Prüfung von sicherheitsrelevanten Ereignissen;
- Wiederherstellungsmechanismen für Schlüssel und das CA-System.

Information zu dieser Funktionalität liefern die entsprechenden Abschnitte des vorliegenden CPS.

6.5.2 Beurteilung der Computersicherheit

Nicht anwendbar.

6.6 Technische Kontrollen der Lebensdauer

Die gesamte für den Betrieb einer ausstellenden CA innerhalb der Foreigner CA angeschaffte Hard- und Software muss so gekauft werden, wie etwa durch zufällige Auswahl bestimmter Komponenten, dass das Risiko einer unbefugten Manipulation irgendeiner der Komponenten verringert wird. Ausrüstung, entwickelt zur Verwendung innerhalb der eID PKI, wird in einer kontrollierten Umgebung unter strengen Änderungskontrollverfahren entwickelt.

Eine ununterbrochene Verantwortlichkeitskette, angefangen von dem Standort, wo die gesamte Hard- und Software, die zur Unterstützung einer ausstellenden CA innerhalb der eID PKI identifiziert wurde, muss aufrecht erhalten werden, und Versand und Lieferung müssen gemäß kontrollierten Verfahren erfolgen. Auf der Ausrüstung der ausstellenden CA dürfen keine Anwendungen oder Softwarekomponenten installiert sein, die nicht zu der Konfiguration der ausstellenden CA gehören. Alle nachfolgenden Aktualisierungen der Ausrüstung der ausstellenden CA müssen in derselben Weise wie die Originalausrüstung gekauft oder entwickelt werden und vorschriftsmäßig von vertrauenswürdigem und geschultem Personal installiert werden.

Die CA-Fertigungsstätte hat eine genehmigte Systemsicherheitspolitik eingerichtet, die Computersicherheitskontrollen spezifisch für die eID PKI beinhaltet und die folgende Aspekte berücksichtigten:

6.6.1 Systementwicklungskontrollen

Für die Entwicklung und Implementierung neuer Systeme werden formelle Verfahren befolgt. Eine Analyse der Sicherheitsvoraussetzungen erfolgt in der Phase des Entwurfs und der Spezifikation der Anforderungen. Ausgelagerte Softwareentwicklungsprojekte werden streng überwacht und kontrolliert.

6.6.2 Sicherheitsverwaltungskontrollen

Die Foreigner CA hält sich an die Definition der Certificate Issuing and Management Components (CIMC) der Familie der Schutzprofile, die alle Anforderungen für Komponenten definiert, die Zertifikate für öffentliche Schlüssel ausstellen, widerrufen und verwalten, wie etwa X.509-Zertifikate. CIMC beruht auf den allgemeinen Kriterien/ISO IS15408-Normen.

6.6.3 Sicherheitskontrollen der Lebensdauer

Die CA wendet für die Installation und die laufende Pflege des CA-Systems eine Methodologie zur Konfigurationsverwaltung an. Wenn die CA-Software erstmals geladen wird, liefert sie der CA ein Verfahren zur Überprüfung der Software auf dem System:

- Stammt vom Entwickler der Software.
- Wurde vor der Installation noch nie geändert.
- Ist die zur Verwendung bestimmte Version.

Der Hauptverantwortliche für Sicherheit der CA überprüft regelmäßig die Integrität der CA-Software und überwacht die Konfiguration der CA-Systeme.

6.7 Netzwerksicherheitskontrollen

Die CA sorgt für ein hohes Sicherheitsniveau des Systemnetzwerks, einschließlich Firewalls. Einbrüche ins Netz werden überwacht und aufgespürt.

Im Besonderen:

- Alle Kommunikationen zwischen dem CA- und RA-Betreiber, die eine der Phasen des Lebenszyklus von Ausländerzertifikaten betreffen, werden durch eine PKI-Verschlüsselung und Unterschriftstechniken gesichert, um Vertraulichkeit und gegenseitige Authentifizierung zu garantieren. Dazu gehören Kommunikationen betreffend Anträge, Ausstellungen, Sperrung, Aufhebung der Sperrung und Widerrufung von Zertifikaten.
- Die Website der CA liefert verschlüsselte Verbindungen mit Hilfe des Secure Socket Layer-Protokolls (SSL) und eines Antivirusschutzes.
- Das Netz der CA wird durch eine Firewall und ein Einbruchmeldesystem geschützt.
- Der Zugang zu den empfindlichen CA-Quellen, einschließlich der CA-Datenbanken außerhalb des Netzes des CA-Betreibers, ist verboten.
- Die Internet-Verbindungen für die Informationsanfrage und -lieferung werden verschlüsselt.

6.8 Zeitstempel

Nicht anwendbar.

7 Zertifikat-, CRL- und OCSP-Profile

7.1 Profil der Zertifikate

In diesem Dokument werden die Profile und Attribute der Zertifikate beschrieben: **EID-DEL-004 eID PKI Hierarchy certificate profile, Abschnitt 5. Certificate profile und Anhang 1 eID certificate profile**.

7.1.1 .Versionsnummer(n)

Siehe Abschnitt 7.1.

7.1.2 Erweiterungen des Zertifikats

Siehe Abschnitt 7.1.

7.1.3 Algorithmusobjektidentifikatoren

Siehe Abschnitt 7.1.

7.1.4 Namensformen

Siehe Abschnitt 7.1.

7.1.5 Namensbeschränkungen

Siehe Abschnitt 7.1.

7.1.6 Objektidentifikator der Zertifikat-Policy

Siehe Abschnitt 7.1.

7.1.7 Verwendung der Erweiterung der Policy-Beschränkung

Siehe Abschnitt 7.1.

7.1.8 Syntax und Semantik der Policy-Qualifikatoren

Siehe Abschnitt 7.1.

7.1.9 Verarbeitung der Semantik für die Erweiterung kritischer Zertifizierungspolicies

Abschnitt nicht anwendbar.

7.1.10 Gültigkeit des Zertifikats

Die Gültigkeit des Zertifikats einer Foreigner-End-Entität weist zwei Beschränkungen auf:

- Der Gültigkeitszeitraum darf 10 Jahre und 8 Monate nicht überschreiten (*siehe Abschnitt 7.1*).

- Der Gültigkeitszeitraum des Zertifikats darf den Gültigkeitszeitraum der eID-Karte, auf welcher der Chip angebracht ist, in dem sich das Zertifikat befindet, nicht überschreiten.

Die RA wird beim Generieren des Antrags auf Zertifikatausstellung immer den kürzeren Gültigkeitszeitraum dieser zwei Beschränkungen wählen.

7.2 CRL-Profil

Die CRL-Profile und -Dokumente werden in diesem Dokument beschrieben: **EID-DEL-004 eID PKI Hierarchy certificate profile, Abschnitt 7. CRL profile und Anhang 1 eID certificate profile**.

7.2.1 Versionsnummer(n)

Siehe Abschnitt 7.2.

7.2.2 CRL und CRL-Eingabeerweiterungen

Siehe Abschnitt 7.2.

7.3 OCSP-Profil

Die OCSP-Profile und -Attribute werden in diesem Dokument beschrieben: **EID-DEL-004 eID PKI Hierarchy certificate profile, Abschnitt 7. OCSP Profile und Anhang 1 eID certificate profile**.

7.3.1 Versionsnummer(n)

Siehe Abschnitt 7.3.

7.3.2 OCSP-Erweiterungen

Siehe Abschnitt 7.3.

8 Audit der Übereinstimmung und andere Bewertungen

Was das Qualifizierte Zertifikat für elektronische Unterschriften betrifft, arbeitet der TSP gemäß den Bestimmungen der EU-Verordnung 910/2014, die den gesetzlichen Rahmen für elektronische Unterschriften in Belgien festlegt.

Der TSP erfüllt die Forderungen, die in den ETSI-Policy-Dokumenten festgelegt sind, die sich auf die qualifizierte Zertifikate beziehen, einschließlich:

- EN 319 411-2: Anforderungen an TSP, die EU-qualifizierte Zertifikate ausstellen:
- EN 319 412-5 Profile für TSP, die Zertifikate ausstellen; Qualifiziertes Zertifikatprofil. Teil 5: Erweiterung für Qualifiziertes Zertifikatprofil.

Der TSP nimmt die Übereinstimmungsaudits an, um sich dessen zu vergewissern, dass er den Anforderungen, Normen, Verfahren und Dienstniveaus gemäß dem vorliegenden CPS genügt. Der TSP nimmt diese Audits seiner eigenen Praktiken und Verfahren an, soweit dies nicht gegen bestimmte Bedingungen wie die Vertraulichkeit der Information, geschäftliche Geheimnisse, usw. verstößt. Solche Audits können unmittelbar vorgenommen werden oder durch:

- die Aufsichtsbehörde für TSP in Belgien, die unter der Autorität der Belgischen Föderalen Behörde handelt;
- die Belgische Föderale Behörde oder eine von der Belgischen Föderalen Behörde bezeichnete Drittpartei.

Der TSP bewertet die Ergebnisse dieser Audits, bevor er sie weiter ausführt.

8.1 Häufigkeit oder Umstände der Beurteilung

Die PKI-Fertigungsstätte wird jährlich geprüft.

8.2 Identität/Qualifikationen des Prüfers

Die Auditdienste müssen von unabhängigen, anerkannten, beglaubigten und etablierten Auditfirmen oder von Beratungsfirmen für Informationstechnologie durchgeführt werden; vorausgesetzt sie sind qualifiziert für die und haben Erfahrung mit der Durchführung von Sicherheitsaudits, insbesondere erhebliche Erfahrung mit PKI und Verschlüsselungstechnologien.

8.3 Beziehung des Prüfers mit der geprüften Entität

Der Prüfer und die geprüfte ausstellende CA dürfen keine andere Beziehung haben, die einen Einfluss auf die Unabhängigkeit und Objektivität unter GAAS haben könnte. Dazu gehören finanzielle, rechtliche, soziale oder andere Beziehungen, die zu einem Interessenskonflikt führen könnten.

8.4 Von der Beurteilung abgedeckte Themen

Beim Audit wird auf die folgenden Elemente Acht gegeben:

- Übereinstimmung der Prinzipien und Verfahren des TSP mit den im CPS bestimmten Verfahren und Dienstniveaus;
- Verwaltung der Infrastrukturen, die die TSP-Dienste ausführen;
- Verwaltung der physischen Infrastrukturen vor Ort;
- Beitritt zum CPS;
- Einhaltung der einschlägigen belgischen Gesetze;
- Einhaltung der vereinbarten Dienstniveaus;
- Inspektion der Auditberichte, der Verzeichnisse, der sachbezogenen Dokumente, usw.;
- Gründe, weshalb die vorerwähnten Bedingungen nicht eingehalten werden.

8.5 Maßnahmen bei Unzulänglichkeit

Falls Unregelmäßigkeiten festgestellt werden, wird der TSP dem Prüfer einen Bericht aushändigen, in welchem die zu treffenden Maßnahmen, um die Situation zu berichtigen und die Konformität zu gewährleisten, aufgenommen sind. Wenn die vorgeschlagenen Maßnahmen als ungenügend betrachtet werden, wird ein zweiter Audit vorgenommen, um die Konformität zu garantieren.

8.6 Kommunikation der Ergebnisse

Die Auditerkenntnisse auf der Basis der Ergebnisse der Audits werden allgemein auf Anfrage verfügbar gemacht.

9 Andere geschäftliche und gesetzliche Fragen

Bestimmte gesetzliche Bedingungen gelten für die Ausstellung der Ausländerzertifikaten unter diesem CPS, wie in diesem Abschnitt beschrieben.

9.1 Gebühren

9.1.1 Gebühren für Ausstellung oder Erneuerung von Zertifikaten

Artikel 6 des Gesetzes vom 19. Juli 1991, erwähnt unter Punkt 1.3 von Kapitel 1, regelt einerseits die Vergütung für das Einbringen der Zertifikate auf die Ausweise (Art. 6, §5) und andererseits das Einziehen der Produktionskosten der Ausweise durch den Innenminister (Art. 6, §8).

Die CA berechnet keine Vergütung für die Veröffentlichung und das Abholen des vorliegenden CPS.

- Die CA wird dem Ausländer die folgenden Dienste gebührenfrei leisten: Veröffentlichung der CRLs und der Delta CRLs;
- Zugang zu den Archiv-Webseiten;
- Webdienst für Statusprüfung über Archivseiten.

Die Belgische Föderale Behörde kann nach Bedarf gebührenfreien Zugang zu den folgenden Mitteln erhalten:

- Überprüfung des OCSP-Status.
- Herunterladen der CRLs und Delta CRLs.
- Überprüfung des Zertifikatsstatus.
- Zertifikatsverzeichnis.
- Veröffentlichung der Zertifikate;
- Widerrufung der Zertifikate;
- Sperrung der Zertifikate.

Die CA führt Mechanismen ein, um vorzubeugen, dass diese Dienste missbraucht werden.

9.1.2 Gebühren für Zugang zu Zertifikaten

Siehe Abschnitt 9.1.1.

9.1.3 Gebühren für Widerrufung oder Zugang zu Statusinformation

Siehe Abschnitt 9.1.1.

9.1.4 Gebühren für andere Dienste

Siehe Abschnitt 9.1.1.

9.1.5 Erstattungspolitik

Abschnitt nicht anwendbar.

9.2 Finanzielle Verantwortung

Der TSP ist für die Führung seiner Finanzbücher und Aufzeichnungen verantwortlich, in Übereinstimmung mit den belgischen Rechnungslegungsvorschriften (GAAP, Generally Accepted Accounting Principles) und wird eine internationale Wirtschaftsprüfungsgesellschaft anstellen, um Finanzdienste zu leisten, unter anderem regelmäßige Rechnungsprüfungen.

9.2.1 Versicherungsdeckung

Der TSP liefert dem Aufsichtsgremium des belgischen Staates jedes Jahr einen Nachweis der Versicherungsdeckung.

9.2.2 Andere Vermögenswerte

Die PKI-Fertigungsstätte und die Registrierungsbehörden unterhalten genügend Vermögenswerte und Finanzressourcen, um ihre Pflichten im Rahmen der eID PKI zu erfüllen und in der Lage zu sein, die Haftung gegenüber Zertifikatinhabern und Vertrauenden Parteien zu übernehmen.

9.2.3 Versicherungs- oder Garantiedeckung für End-Entitäten

Abschnitt nicht anwendbar.

9.3 Vertraulichkeit von Geschäftsinformationen

Im Rahmen der gelieferten Dienste treten die CA und der RA-Betreiber (RRN) für die Verarbeitung der Personenangaben gemäß Artikel 16 des Gesetzes vom 8. Dezember 1992 auf, während die Gemeindeverwaltungen für die Behandlung der Personenangaben auftreten.

9.3.1 Umfang vertraulicher Informationen

Der TSP hält die Vorschriften über personenbezogene Daten ein, so wie im vorliegenden CPS beschrieben. Die vertraulichen Informationen umfassen:

- alle persönlichen identifizierbaren Informationen über Ausländer anders als diejenigen, die in ein Zertifikat aufgenommen sind;
- den genauen Grund für die Widerrufung oder Sperrung eines Zertifikats;
- die Auditberichte;

- zum Aufstellen von Berichten eingetragene Informationen, wie die Aufnahmen von Anträgen durch die RA;
- den Briefwechsel bezüglich der CA-Dienste;
- den (die) CA-Privatschlüssel.

9.3.2 Informationen außerhalb des Umfangs vertraulicher Informationen

Die folgenden Elemente gelten nicht als vertrauliche Informationen:

- Zertifikate und deren Inhalt.
- Status eines Zertifikats.

9.3.3 Verantwortung für den Schutz vertraulicher Informationen

Parteien, die vertrauliche Informationen beantragen und erhalten, haben die Genehmigung, diese Informationen zu benutzen, unter der Bedingung, dass diese zu dem angegebenen Zweck benutzt werden und nicht Gegenstand einer Kompromittierung sind und dass sie nicht an Dritte übermittelt oder bekannt gegeben werden.

Diese Parteien sind ebenfalls gehalten, die Vorschriften in Sachen Schutz der personenbezogenen Daten in Übereinstimmung mit dem Gesetz einzuhalten.

9.4 Schutz der personenbezogenen Informationen

9.4.1 Schutzplan

Der TSP verbreitet keine vertrauliche Information und ist nicht dazu gehalten ohne authentifizierte und begründete Anfrage, in welcher folgendes spezifiziert wird:

- die Partei, gegenüber derer die CA sich verpflichtet hat, die Information vertraulich zu halten. Die CA ist in dieser Hinsicht gegenüber der RA verpflichtet und antwortet unmittelbar auf jeden solchen Antrag;
- ein Befehl des Gerichts.

Innerhalb des Rahmenvertrags zwischen dem TSP und der Belgischen Föderalen Behörde darf der TSP-Verwaltungskosten berechnen, um solche Informationsverbreitungen vorzunehmen.

9.4.2 Als privat behandelte Information

Informationen, z. B über die Zertifikatinhaber, werden von der CA weder den Ausländern noch den vertrauenden Parteien bekannt gegeben, mit Ausnahme der Informationen:

- über sie selbst;
- über Personen, für die sie das Sorgerecht haben.

Nur die RA darf Zugang zu den vertraulichen Informationen erhalten.

9.4.3 Als nicht privat betrachtete Information

Nicht vertrauliche Informationen dürfen jedem Ausländer und jeder vertrauenden Partei unter den folgenden Bedingungen bekannt gegeben werden:

- Der Status ein einziges Zertifikat wird auf Anfrage eines Ausländers oder einer vertrauenden Partei geliefert;
- Die Ausländer können nicht vertrauliche Informationen zu Rate ziehen, die der TSP über sie besitzt.
- Der Inhalt ausgestellter digitaler Zertifikate ist öffentliche Information und gilt nicht als privat.

9.4.4 Verantwortung für den Schutz privater Information

Die CA verwaltet die Bekanntmachung von Informationen an das CA-Personal.

Die CA authentifiziert sich gegenüber jeder Partei, die die Verbreitung von Informationen beantragt, durch:

- Unterzeichnung der Antworten auf OCSP-, CRLs- und Delta CRLs-Anfragen.

Der TSP verschlüsselt alle Mitteilungen von vertraulichen Informationen, einschließlich:

- der Mitteilungen zwischen der CA und der RA;
- die Internet-Verbindungen, bei denen Zertifikate ausgehändigt werden.

Außer den Informationen im Besitz des TSP verfügt die RA auch über Informationen über die Ausländerzertifikate, und zwar im Register der Personalausweise. Das Gesetz vom 19. Juni 1991 *regelt den Zugang zum Register der Personalausweise und zu anderen Angaben über die Ausländer, über die das Nationalregister verfügt.*

9.4.5 Benachrichtigung und Zustimmung zur Benutzung von privater Information

Der TSP handelt im Rahmen des belgischen Gesetzes vom 8. Dezember 1992 *über den Schutz der Privatsphäre in Bezug auf die Verarbeitung der personenbezogenen Daten, so wie durch das Gesetz vom 11. Dezember 1998 geändert, das die europäische Richtlinie 1995/46 über den Schutz der natürlichen Personen in Bezug auf die Verarbeitung der personenbezogenen Daten und den freien Verkehr dieser Daten einführt.* Dies ist in Übereinstimmung mit dem Gesetz vom 13. Juni 2005 *über die Verarbeitung der personenbezogenen Daten und den Schutz der Privatsphäre im Sektor der elektronischen Kommunikation.*

Der TSP bewahrt keine anderen Angaben bezüglich der Zertifikate oder der Ausländer auf als diejenigen, die ihm von der RA übermittelt und genehmigt wurden. Ohne das Einverständnis der betreffenden Person oder die ausdrückliche Genehmigung durch das Gesetz werden die vom TSP behandelten personenbezogenen Daten zu keinen anderen Zwecken benutzt.

9.4.6 Offenbarung aufgrund gerichtlicher oder administrativer Prozesse

Siehe Abschnitt 9.4.5*.*

9.4.7 Andere Umstände für Offenbarung von Information

Certipost ist nicht zur Offenbarung von Informationen verpflichtet, außer denen, die durch einen legitimen und gesetzlichen Gerichtsbefehl gemäß den Anforderungen des vorliegenden CP/CPS vorgesehen sind.

9.5 Rechte an geistigem Eigentum

Der belgische Staat besitzt und behält sich alle Rechte an geistigem Eigentum vor, die mit seinen eigenen Datenbanken, seinen Websites, den digitalen CA-Zertifikate und irgendwelcher anderen Veröffentlichung, die von der CA herkommen, verbunden sind, einschließlich des vorliegenden CPS.

Der TSP besitzt und behält sich alle Rechte an geistigem Eigentum vor, die er auf seinen eigenen Infrastrukturen, Datenbanken, Website, usw. besitzt.

Die Softwares und die Dokumentation, die vom TSP im Rahmen des Projekts des belgischen elektronischen Personalausweises entwickelt werden, sind das exklusive Eigentum des belgischen Staates.

9.6 Vertretungen und Garantien

Alle Parteien im Bereich des TSP, einschließlich der CA selbst, der RA, der LRAs und der Ausländer, garantieren die Integrität ihres (ihrer) jeweiligen Privatschlüssel(s). Sollte eine der besagten Parteien vermuten, dass ein Privatschlüssel kompromittiert wurde, so wird sie ihre LRA (Gemeinde), die Polizei oder das RA-Helpdesk unmittelbar davon benachrichtigen.

9.6.1 CA-Vertretungen und -Garantien

Innerhalb der Grenzen von dem, was in den sachbezogenen Teilen des CPS spezifiziert ist, muss der TSP:

- Dem vorliegenden CPS und dessen Änderungen, wie veröffentlicht unter http://repository.eid.belgium.be entsprechen;
- Infrastruktur- und Zertifizierungsdienste liefern, unter anderem die Aufstellung und den Betrieb der Bezugsarchive und der Website der CA für den Betrieb von öffentlichen Zertifizierungsdiensten;
- Vertrauensmechanismen liefern, unter anderem einen Mechanismus zur Schlüsselgenerierung, einen Schlüsselschutz sowie Verfahren zur Verteilung von Geheimnissen bezüglich seiner eigenen Infrastruktur;
- die RA im Falle einer Kompromittierung seines (seiner) eigenen Privatschlüssel(s) benachrichtigen;
- elektronische Zertifikate gemäß dem CPS ausstellen und seinen Verpflichtungen, so wie im vorliegenden CPS angegeben, entsprechen;

- die RA davon benachrichtigen, wenn die CA nicht imstande ist, die Anwendung gemäß dem vorliegenden CPS zu bestätigen;
- schnell handeln, um ein Zertifikat gemäß dem vorliegenden CPS auszustellen, nachdem er einen authentifizierten Antrag von der RA empfangen hat;
- ein Zertifikat gemäß dem CPS sofort widerrufen, nachdem er einen authentifizierten Widerrufungsantrag von der RA empfangen hat;
- ein Zertifikat gemäß dem CPS sofort sperren, nachdem er einen authentifizierten Sperrungsantrag von der RA empfangen hat;
- die Sperrung eines Zertifikats gemäß dem CPS sofort aufheben, nachdem er einen authentifizierten Antrag auf Aufhebung der Sperrung von der RA empfangen hat;
- Zertifikate gemäß dem vorliegenden CPS veröffentlichen;
- die CRL-, Delta CRL-und OCSP-Antworten aller gesperrte und widerrufenen Zertifikate auf regelmäßiger Basis und gemäß dem vorliegenden CPS veröffentlichen;
- geeignete Dienstniveaus liefern in Übereinstimmung mit dem, was im Rahmen der Vereinbarung zwischen der CA und der Belgischen Föderalen Behörde bestimmt wurde;
- eine Kopie des vorliegenden CPS und der über seine Website verfügbaren geltenden Policies machen;
- gemäß den belgischen Gesetzen handeln. Insbesondere erfüllt der TSP alle gesetzlichen Anforderungen verbunden mit qualifiziertem Zertifikatprofilen, ausgehend von der EU-Verordnung 910/2014 über elektronische Unterschriften.

Wenn der TSP die Kompromittierung eines Privatschlüssels, sein eigener eingeschlossen, erfährt oder vermutet, so wird er die RA unverzüglich davon benachrichtigen.

Wenn die Dienste eines Dritten in Anspruch genommen werden, wird der TSP sein Bestes tun, um die finanzielle und zivile Verantwortlichkeit dieses Subunternehmers zu garantieren.

Den Ausländern und den vertrauenden Parteien gegenüber haftet der TSP für folgende Handlungen oder Versäumnisse:

- die Ausstellung von digitalen Zertifikate, die die von der RA vorgelegten Angaben nicht enthalten;
- die Kompromittierung eines Privatunterschriftsschlüssels der CA;
- das Versäumnis, eines gesperrtes Zertifikat nach einem Zeitraum von einer Woche zu widerrufen;
- das Versäumnis, eines widerrufenes oder gesperrtes Zertifikat in einer CRL oder Delta CRL aufzunehmen;
- das Versäumnis des OCSP-Beantworters, ein Zertifikat als widerrufen oder gesperrt zu melden;
- das Versäumnis einer Web-Schnittstelle, Zertifikatstatusinformation zu melden;

- Die unbefugte Verbreitung von vertraulichen Informationen oder von Privatangaben gemäß den Punkten 9.3 und 9.4.
- Verantwortlich, so wie unter 9.8.1 bestimmt.

Der TSP erklärt, keine weiteren Pflichten im Rahmen des vorliegenden CPS zu haben.

9.6.1.1 Vertrauen auf eigenes Risiko.

Nur die vertrauenden Parteien, die Zugang zu den Informationen erhalten, die in den Bezugsarchiven und auf der Website zur Verfügung gestellt werden, haften für die Bewertung dieser Informationen und für das Vertrauen, das sie diesen schenken.

9.6.1.2 Korrektheit der Informationen.

Der TSP setzt alles ein, damit die Parteien, denen Zugang zu den Bezugsarchiven gewährt wird, genaue, aktualisierte und richtige Informationen erhalten. Der TSP darf jedoch keine andere Haftung jenseits der Grenzen übernehmen, wie festgelegt in diesem CPS unter Artikel 9.8.1

9.6.2 RA-Vertretungen und Garantien

Die RA, die im Bereich der CA aktiv ist, muss:

- bei ihrer Kommunikation mit der CA richtige und genaue Informationen liefern;
- dafür sorgen, dass der öffentliche Schlüssel, der an die CA geliefert wird, mit dem benutzten Privatschlüssel übereinstimmt;
- Zertifikatanträge gemäß dem vorliegenden CPS erstellen;
- alle durch die CA-Verfahren und das vorliegende CPS vorgeschriebenen Überprüfungen und Authentifizierungen vornehmen;
- der CA den Antrag des Antragstellers in einer unterschriebenen Nachricht vorlegen;
- alle Anträge auf Widerrufung, Sperrung und Aufhebung der Sperrung eines Zertifikats gemäß den CA-Verfahren und dem vorliegenden CPS erhalten, überprüfen und an die CA übermitteln;
- die Richtigkeit und die Authentizität der Informationen überprüfen, die vom Ausländer zur Zeit der Erneuerung eines Zertifikats gemäß dem vorliegenden CPS geliefert werden.

Wenn die RA die Kompromittierung eines Privatschlüssels erfährt oder vermutet, dann wird sie die CA unmittelbar davon benachrichtigen.

Das RRN tritt als einzige RA im Bereich der CA auf.

Die RA allein haftet für die Verzeichnisse, die sie aktualisiert, einschließlich der Zertifikatsverzeichnisse.

Die RA haftet für alle Audits, die sie vornimmt, sowie für die Ergebnisse und Empfehlungen von solchen Audits.

Die RA allein haftet über die LRA für die Richtigkeit der Angaben des Ausländers sowie für jede andere Angabe, die sie der CA mitteilt. Die RA macht die CA nicht für Schäden haftbar, die aufgrund von nicht kontrollierten Angaben, die in ein Zertifikat aufgenommen worden sind, zugefügt werden.

Die RA fügt sich den belgischen Gesetzen und Vorschriften über den Betrieb des RRN.

Die RA haftet für ihre Handlungen oder Versäumnisse gemäß dem belgischen Gesetz.

9.6.3 Vertretungen und Garantien des Benutzers

Außer wenn im CPS anders angegeben, gehört es unter anderem zu den Pflichten des Ausländers:

- sich davon enthalten, ein Zertifikat zu verfälschen;
- Zertifikate nur zu gesetzlichen und zugelassenen Zwecken gemäß dem CPS zu benutzen;
- einen neuen elektronischen Personalausweis (und also Ausländerzertifikate) im Falle einer Änderung der in dem Zertifikat veröffentlichten Information zu beantragen;
- sich davon zu enthalten, den öffentlichen Ausländerschlüssel in einem ausgestellten Ausländerzertifikat für die Ausstellung von anderen Zertifikaten zu benutzen;
- Kompromittierung, Verlust, Enthüllung, Änderung oder irgendwelchen anderen unzulässigen Gebrauch seiner Privatschlüssel vorzubeugen;
- die Polizei, die Gemeindeverwaltung oder das Helpdesk der RA zu benachrichtigen, um die Sperrung eines Zertifikats bei der Vermutung eines Zwischenfalls, der dem Zertifikat materiell schaden könnte, zu beantragen. Dabei werden Meldungen von Verlust, Diebstahl, Änderung, unbefugter Verbreitung oder anderen Kompromittierungen des Privatschlüssels eines der Ausländerzertifikate oder von beiden gemeint.
- die Polizei, die Gemeindeverwaltung oder das Helpdesk der RA zu benachrichtigen, um die Widerrufung eines Zertifikats bei der Vermutung eines Zwischenfalls, der dem Zertifikat materiell schaden könnte, zu beantragen. Derartige Vorfälle umfassen Verlust, Diebstahl, Änderung, unerlaubte Offenbarung oder eine andere Kompromittierung des Privatschlüssels von einem oder beiden der Ausländerzertifikate oder falls die Kontrolle über Privatschlüssel durch Kompromittierung von Aktivierungsdaten (z. B. PIN-Code) verloren gegangen ist.
- angemessene Sorgfalt auszuüben, um unerlaubte Benutzung des Privatschlüssels des Benutzers zu vermeiden;
- nach einer Kompromittierung, die Verpflichtung, jede Benutzung des Privatschlüssels sofort und dauerhaft einzustellen;
- das RA-Helpdesk unverzüglich benachrichtigen, wenn die Kontrolle seines Privatschlüssels aufgrund einer Kompromittierung des PIN-Codes verloren worden ist.

9.6.4 Vertretungen und Garantien von Vertrauenden Parteien

Parteien, die auf ein CA-Zertifikat vertrauen:

- werden über den Gebrauch von digitalen Zertifikate und PKI genügend informiert werden;
- werden benachrichtigt und halten sich an die Bedingungen des vorliegenden CPS sowie die verbundenen Bedingungen für die vertrauenden Parteien;
- werden ein Zertifikat mit Hilfe einer CRL-, Delta CRL-, OCSP- oder Web-basierte Zertifikatsbestätigung gemäß dem Verfahren zur Herstellung eines gesicherten Weges des Zertifikats bestätigen;
- werden auf ein Zertifikat nur dann vertrauen, wenn dieses nicht gesperrt oder widerrufen worden ist;
- werden auf ein Zertifikat auf angemessene Weise je nach den Umständen vertrauen.

Nur die vertrauenden Parteien, die Zugang zu den Informationen erhalten, die in den Quellen und auf der Website der CA zur Verfügung gestellt werden, haften für die Bewertung dieser Informationen und für das Vertrauen, das sie diesen schenken.

Wenn eine vertrauende Partei feststellt oder vermutet, dass ein Privatschlüssel kompromittiert wurde, dann muss sie das RA-Helpdesk unmittelbar davon benachrichtigen.

9.6.5 Vertretungen und Garantien anderer Teilnehmer

Verpflichtungen des Kartenerstellers: Der Ersteller der elektronischen Personalausweise (CM) ist verantwortlich für das Initialisieren, Personalisieren und Verteilen der Personalausweise, die die 0, 1 oder 2 Ausländerzertifikate enthalten.

Das Initialisieren erfordert folgende Verrichtungen im Chip:

- Generieren der Schlüsselpaaren für das Identifizierungs- und Unterschriftszertifikat;
- Speichern der Identifizierungs- und Unterschriftszertifikate auf der Smart Card;
- Authentifizieren der Daten sowie Initialisieren der verschiedenen auf dem digitalen Personalausweis gespeicherten Dateien.

Die CM sammelt auf sichere Weise die Basisdokumente und verteilt die Aufrufbriefe, die neuen personalisierten und die initialisierten Personalausweise sowie die personalisierten gesicherten Briefe, die für die Ausländer bestimmt sind und die PIN- und PUK-Codes enthalten.

Die CM implementiert ein sicheres Verfahren, um von den Gemeindeverwaltungen die ungültigen oder annullierten Personalausweise zurückzuholen und sie zu vernichten.

9.7 Abweisung von Garantien

Innerhalb der durch das belgische Gesetz festgesetzten Grenzen haftet die CA auf keinen Fall (außer im Falle von Betrug oder absichtlichem Verstoß) für:

- Verdienstverlust;
- Datenverlust;
- Indirekte Schäden, Folgeschäden oder Schadensersatzansprüche zur Abschreckung, die die Folge von oder in Verbindung mit der Benutzung, der Lieferung, der Lizenz und der Ausstellung oder Nicht-Ausstellung von Zertifikaten oder digitalen Unterschriften stehen;
- andere Schäden.

9.8 Begrenzung der Haftung

9.8.1 Haftungen des TSP

Die Haftung des TSP dem Abonnenten oder einer vertrauenden Partei gegenüber wird auf die Zahlung einer Schadensvergütung von höchstens 2500 € pro Transaktion begrenzt, die von den in Abschnitt 9.2.1 aufgeführten Ereignissen betroffen ist.

9.8.2 Qualifizierte Zertifikate

Was die Ausstellung der qualifizierte Zertifikate betrifft, regelt Artikel 14 des Gesetzes über die elektronischen Unterschriften die Haftung des TSP.

Gemäß dieser Bestimmung haftet der TSP für den Schaden, den er jeder Institution oder natürlichen bzw. juristischen Person zufügt, die vernünftigerweise auf die Zertifikate für folgendes vertraut:

a. die Richtigkeit aller in dem qualifizierten Zertifikat enthaltenen Informationen am Datum, an dem 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 qualifiziertes Zertifikats der in dem qualifizierten Zertifikat identifizierte Unterzeichner den Privatschlüssel besaß, der dem in dem Zertifikat angegebenen oder identifizierten öffentlichen Schlüssel entspricht;

c. die Garantie, dass der Privatschlüssel und der öffentliche Schlüssel komplementär gebraucht werden können.

Der TSP haftet für jeden Schaden, den er jeder Institution oder natürlichen bzw. juristischen Person zufügt, die sich vernünftigerweise auf das Zertifikat verlässt, falls der Widerruf des Zertifikates nicht registriert wurde, es sei denn der TSP kann beweisen, dass er nicht nachlässig gewesen ist.

9.8.3 Zertifikate, die nicht als qualifizierte Zertifikate betrachtet werden können

Die allgemeinen Haftungsregeln sind auf jeden Schaden anwendbar, der einer Institution oder natürlichen bzw. juristischen Person zugefügt wird, die sich vernünftigerweise auf eine vom TSP ausgestelltes Zertifikat verlässt.

Der TSP lehnt jede Haftung den vertrauenden Parteien gegenüber in allen Fällen ab, wo das Identitätszertifikat im Kontext von Anwendungen gebraucht wird, die die Benutzung des Identitätszertifikats zur Generierung von elektronischen Unterschriften ermöglichen.

9.8.4 Haftungsausschluss

Der TSP übernimmt keinerlei Haftung für irgendeinen Verlust, der auf eine(n) (oder mehrere) der folgenden Umstände oder Ursachen zurückzuführen ist:

- Das digitale Zertifikat im Besitz der fordernden Partei oder andernfalls der Gegenstand einer Forderung wurde durch unerlaubte Offenbarung oder unerlaubte Nutzung des digitalen Zertifikats oder eines Passworts oder von Aktivierungsdaten zur Kontrolle des Zugriffs darauf kompromittiert.
- Das digitale Zertifikat im Besitz der fordernden Partei oder andernfalls der Gegenstand einer Forderung wurde aufgrund einer Falschangabe, eines sachlichen Fehlers oder einer Auslassung durch eine Person, Entität oder Organisation ausgestellt.
- Das digitale Zertifikat im Besitz der fordernden Partei oder der Gegenstand einer Forderung war abgelaufen oder wurde widerrufen vor dem Datum der Umstände, die Anlass zu einer Forderung gaben.
- Das digitale Zertifikat im Besitz der fordernden Partei oder andernfalls der Gegenstand einer Forderung wurde in irgendeiner Weise angepasst oder geändert oder anders benutzt als gemäß den Bedingungen von Foreigner CA CP/CPS und/oder der relevanten Zertifikatinhabervereinbarung oder einem geltenden Gesetz oder einer geltenden Verordnung erlaubt.
- Der mit dem digitalen Zertifikat verbundene Privatschlüssel im Besitz der fordernden Partei oder andernfalls der Gegenstand einer Forderung wurde kompromittiert.
- Das digitale Zertifikat im Besitz der fordernden Partei wurde in einer Weise ausgestellt, die eine Verletzung eines geltenden Gesetzes oder einer geltenden Verordnung darstellt.
- Computerhard- oder -software oder mathematische Algorithmen werden entwickelt, die dazu neigen, die Verschlüsselung mit öffentlichen Schlüsseln oder asymmetrische Verschlüsselungssysteme unsicher zu machen, es sei denn, Certipost verwendet kommerziell angemessene Praktiken zum Schutz gegen Sicherheitsverletzungen aufgrund solcher Hardware, Software oder Algorithmen.
- Stromausfall, Stromunterbrechung oder andere Störungen der Stromversorgung, es sei denn, Certipost verwendet kommerziell angemessene Methoden zum Schutz gegen derartige Störungen.
- Ausfall von einem oder mehreren der Computersysteme, Kommunikationsinfrastruktur, Verarbeitungs- oder Speichermedien oder -

mechanismen oder von Teilkomponenten der Vorhergehenden, die nicht unter der ausschließlichen Kontrolle von Certipost und/oder ihrer Subauftragsnehmer oder Dienstanbieter sind.

- Eines oder mehrere der folgenden Ereignisse: eine Naturkatastrophe oder höhere Gewalt (einschließlich aber nicht beschränkt auf Überschwemmung, Erdbeben oder andere natürliche oder wetterbedingte Ursachen); Arbeitsunruhen; Krieg, Aufruhr oder offene militärische Feindlichkeiten; feindliche Gesetzgebung oder Regierungshandlung, Prohibition, Embargo oder Boykott; Aufstand oder Bürgeraufruhr; Feuer oder Explosion; katastrophale Epidemie; Handelsembargo; Beschränkung oder Behinderung (einschließlich aber nicht beschränkt auf Exportkontrollen); jeglicher Mangel an Verfügbarkeit oder Integrität von Telekommunikation; gesetzlicher Zwang, einschließlich alle Urteile eines zuständigen Gerichts, dem Certipost unterliegt oder eventuell unterliegt; und jedes Ereignis oder jeder Vorfall oder Umstand oder jede Reihe von Umständen, die sich der Kontrolle von Certipost entziehen.

9.9 Schadenersatz

Siehe Abschnitt 9.8.

9.10 Laufzeit und Beendigung des CP/CPS

9.10.1 Laufzeit

Der vorliegende CP/CPS tritt mit der Veröffentlichung im eID-Archiv in Kraft. Änderungen an dem vorliegenden CP/CPS treten mit der Veröffentlichung im eID-Archiv in Kraft.

9.10.2 Beendigung

Das vorliegende CPS bleibt in Kraft, bis die CA das Gegenteil in ihrem Archiv auf http://repository.eid.belgium.be ausdrücklich mitteilt.

9.10.3 Auswirkung von Beendigung und Fortbestand

Die Bestimmungen von Foreigner CA CP/CPS überdauern die Beendigung oder Widerrufung durch einen Zertifikatinhaber oder einer Vertrauenden Partei von der eID PKI in Bezug auf alle Handlungen, die auf der Verwendung eines digitalen Zertifikats oder dem Vertrauen auf dieses oder einer anderen Beteiligung in der eID PKI beruhen. Jede derartige Beendigung oder Widerrufung beeinträchtigt oder berührt kein Handlungsrecht oder Rechtsmittel, das eine Person bis zu und einschließlich dem Datum der Widerrufung oder Beendigung erworben hat.

9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

Benachrichtigungen betreffend das vorliegenden CPS sind zu richten an:

Siehe Abschnitt 1.5.1.

9.12 Änderungen

9.12.1 Verfahren für Änderungen

Änderungen des vorliegenden CPS werden vom Policy-Verantwortlichen des TSP verwaltet. Alle vorgeschlagenen Änderungen des CPS müssen vom PKI Management Board genehmigt werden.

9.12.2 Mechanismen und Zeitraum für Benachrichtigungen

Nach erfolgter Genehmigung wird eine neue Version des CPS erstellt und neben der früheren Version auf der Archiv-Website (http://repository.eid.belgium.be) veröffentlicht.

9.12.3 Umstände, die eine Änderung des OID erforderlich machen

Weniger wichtige Anpassungen des vorliegenden CPS, die keinen materiellen Einfluss auf das Sicherheitsniveau des vorliegenden CPS haben, werden durch eine Änderung der Dezimalstelle angegeben (z.B. Version 1.0 ändert sich zu 1.1), während wichtigere Änderungen des vorliegenden CPS durch einen Wechsel der ganzen Zahl angegeben werden (z.B. Version 1.0 ändert sich zu 2.0).

Weniger wichtige Anpassungen des vorliegenden CPS brauchen nicht im CPS OID oder im CPS-Index (URL) geändert zu werden, der von der CA mitgeteilt werden könnte. Für wichtigere Anpassungen, die die Annehmbarkeit von Zertifikaten für spezifische Zwecke materiell ändern können, müssen der CPS OID oder CPS-Index (URL) möglicherweise angepasst werden.

9.13 Verfahren zur Beilegung von Streitfällen

Alle mit dem vorliegenden CPS verbundenen Streitfälle werden gemäß dem belgischen Gesetz beigelegt.

Beschwerden in Zusammenhang mit dem vorliegenden CPS und den Zertifikaten sind zu richten an:

Siehe Abschnitt 1.5.1.

Eine Empfangsbestätigung wird innerhalb von 2 Arbeitstagen nach Eintreffen der Beschwerde versandt. Eine Antwort erfolgt innerhalb von 10 Arbeitstagen nach Eintreffen der Beschwerde.

In Übereinstimmung mit dem belgischen Gesetz über digitale Unterschriften findet, sofern nicht anderweitig vereinbart, jede Schlichtung zwischen den Parteien in Belgien statt.

9.14 Anwendbares Recht

Der TSP leistet seine Dienste gemäß den Bestimmungen des belgischen Gesetzes und der EU-Verordnung 910/2014.

9.15 Übereinstimmung mit geltendem Gesetz

Dieser CP/dieses CPS unterliegt dem geltenden Gesetz.

9.16 Verschiedene Bestimmungen

Der TSP nimmt die folgenden Informationen in alle digitale Zertifikate, die er ausstellt, per Referenz auf:

- die im vorliegenden CPS beschriebenen Bedingungen;
- jede andere anwendbare Zertifikatspolicy, so wie sie in einem ausgestellten Ausländerzertifikat erwähnt werden kann;
- die Pflichtelemente der anwendbaren Normen;
- die nicht obligatorischen, aber personalisierten Elemente der anwendbaren Normen;
- den Inhalt von Erweiterungen und die nirgendwo anders erwähnte verbesserte Benennung;
- jede andere Information, die zu einem Feld eines Zertifikats gehört.

Um Informationen per Referenz aufzunehmen, benutzt die CA computer- und textbasierende Indexe, worunter URLs und OIDs.

9.16.1 Gesamte Vereinbarung

Abschnitt nicht anwendbar

9.16.2 Übertragung

Abschnitt nicht anwendbar

9.16.3 Abtrennbarkeit (Salvatorische Klausel)

Sollte eine Bestimmung der vorliegenden Foreigner CA, CP/CPS ungültig oder nicht durchsetzbar sein, dann wird sie in ihrem Umfang unwirksam sein, ohne die übrigen Bestimmungen der vorliegenden Foreigner CA, CP/CPS ungültig zu machen oder die Gültigkeit oder Durchsetzbarkeit dieser übrigen Bestimmungen zu beeinträchtigen.

9.16.4 Durchsetzung (Anwaltshonorare und Verzicht auf Rechte)

Jede Nichtausübung oder Verzögerung seitens des TSP, ein Recht, eine Befugnis ein Privileg oder ein Rechtsmittel, das ihm in irgendeiner Weise oder anderweitig durch diese Foreigner CA, CP/CPS übertragen wurde, gilt nicht als ein Verzicht auf ein derartiges Rechts oder ein Verbot seiner Ausübung oder Durchsetzung zu irgendeiner Zeit danach, noch wird irgendeine einzelne oder teilweise Ausübung dieses Rechts, dieser Befugnis, dieses Privilegs oder dieses Rechtsmittels irgendeine andere oder weitere Ausübung davon oder die Ausübung eines anderen Rechts oder Rechtsmittels ausschließen. Ein Verzicht wird erst wirksam, wenn er schriftlich festgehalten ist. Kein Recht oder Rechtsmittel, das durch eine der Bestimmungen dieser Foreigner CA, CP/CPS übertragen wird, bezweckt, dass es jedes

andere Recht oder Rechtsmittel ausschließt, es sei denn, es ist ausdrücklich in dieser Foreigner CA, CP/CPS so bestimmt, und jedes Recht oder Rechtsmittel wird kumulativ sein und zusätzlich zu jedem anderen Recht oder Rechtsmittel sein, das hierunter gewährt wird oder jetzt oder danach laut Gesetz oder Billigkeit oder Satzung oder anderweitig existiert.

9.16.5 Höhere Gewalt

Der TSP übernimmt keine Haftung für irgendeine Verletzung der Gewährleistung, Verzögerung oder Nichterfüllung der Leistung, die auf Ereignisse zurückzuführen ist, die sich seinem Einfluss entzieht, wie etwa höhere Gewalt, Kriegshandlungen, Terrorismus, Epidemien, Ausfall von Energieversorgung oder Telekommunikationsdiensten, Feuer und andere Naturkatastrophen. Siehe auch Abschnitt 9.8.2 (Haftungsausschluss) oben.

9.17 Andere Bestimmungen

Abschnitt nicht anwendbar.

Anhang A

Definitionen und Akronyme

CA	Certification Authority
CC	Common Criteria
CM	Card Manufacturer
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
EAL	Evaluation Assurance Level
eIDAS	EU Regulation 910/2014 aka eIdentification and Signature Regulation
OID	Object IDentifier
(L)RA	Lokale Registrierungsbehörde

Anhang B

ANFORDERUNGEN AN ZERTIFIZIERUNGSBEHÖRDEN

Die von Zertifizierungsbehörden verwendeten Kryptomodule WERDEN in Übereinstimmung mit einer der folgenden Normen beurteilt und zertifiziert:

- FIPS PUB 140-2 Stufe 3 oder höher
- PP-SSCD 4,5,6
- BSI Cryptographic Modules Security Level “Enhanced”7

Anhang C

Dokumentenliste

BEZEICHNUNG	REFERENZ
EID-DEL-004 EID PKI HIERARCHY CERTIFICATE PROFILE	Link