



Belgische Zertifizierungsrichtlinie & Zertifizierungserklärung für die eID PKI-Infrastruktur Foreigner CA

OIDs: 2.16.56.1.1.1.2
2.16.56.9.1.1.2
2.16.56.10.1.1.2
2.16.56.12.1.1.2

Company: Certipost
Version: 4.4
Status: Endgültige Version
Veröff. Datum: 16/05/2019

Dokumentkontrolle

Datum	Version	Bearbeitet von	Änderung
13.02.2017	3.0	Bart Eeman	Originalfassung 1.0
15.03.2017	3.1	Bart Eeman	Originalfassung 1.1
24.03.2017	3.2	Don Giot	Aktualisierte Version 1.2
10.04.2017	3.3	Bart Eeman	Zetes Zusatz
13.04.2017	3.4	Bart Eeman	Bemerkungen RRN
04.09.2017	4.0	Don Giot/Cristof Fleurus	eIDAS Aktualisierung & QA
29.05.2018	4.1	Bart Eeman/Don Giot	Aktualisierte Version 4.1 & QA
13.07.2018	4.2	Bart Eeman	Endgültige Version Überarbeitung 2018
08.04.2018	4.4	Bart Eeman/Bono Vanderpoorten/Guillaume Nguyen	Review 2019

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

Dokumentkontrolle.....	1
Haftungsausschluss.....	1
Inhaltsverzeichnis	2
1 Einleitung	11
1.1 Übersicht.....	Fout! Bladwijzer niet gedefinieerd.
1.2 die eid Hierarchie.....	13
1.3 Name und Identifizierung des Dokuments	14
1.4 PKI-Teilnehmer.....	14
1.4.1 Zertifizierungsbehörden	15
1.4.2 Registrierungsbehörden oder RA.....	16
1.4.3 Abonent & Benutzer	16
1.4.4 Vertrauende Parteien	17
1.4.5 Andere Teilnehmer	17
1.4.5.1 Kartenersteller (Card Manufacturer).....	17
1.4.5.2 Lieferant des Root Sign-Zertifikats.....	18
1.4.5.3 Subauftragnehmer	18
1.5 Benutzung der Zertifikate	18
1.6 Policy-Verwaltung	19
1.6.1 Organisation für die Verwaltung des Dokuments	19
1.6.2 Kontaktperson.....	19
1.6.3 Person, die die CPS-Eignung für die Policy bestimmt.....	19
1.7 Definitionen und Akronyme.....	20
1.7.1 Definitionen	20
1.7.2 Akronyme.....	20
2 Haftung in Sachen Veröffentlichung und Archivierung	21
2.1 Archive	21
2.2 Veröffentlichung von Zertifizierungsinformation.....	21
2.3 Zeit oder Häufigkeit der Veröffentlichung.....	21
2.4 Kontrolle des Zugangs zu den Archiven.....	22
3 Identifizierung und Authentifizierung.....	23
3.1 Benennung.....	23

3.1.1	Arten von Namen.....	23
3.1.2	Notwendigkeit aussagefähiger Namen.....	23
3.1.3	Anonymität oder Pseudonymität von Abonnenten	23
3.1.4	Regeln zum Interpretieren verschiedener Namensformen.....	23
3.1.5	Eindeutigkeit von Namen.....	23
3.1.6	Erkennung, Authentifizierung und Rolle von Handelsmarken	23
3.2	Anfängliche Gültigkeitserklärung der Identität	23
3.2.1	Verfahren zum Nachweis des Besitzes eines Privatschlüssels	23
3.2.2	Authentifizierung der Organisationsidentität.....	24
3.2.3	Authentifizierung der individuellen Identität	24
3.2.4	Nicht überprüfte Abonnenteninformation.....	24
3.2.5	Gültigkeitserklärung der Behörde.....	24
3.2.6	Kriterien für Interoperation	24
3.3	Identifizierung und Authentifizierung für Anfragen nach neuen Schlüsseln	24
3.3.1	Identifizierung und Authentifizierung für Routine-Neuverschlüsselung.....	24
3.3.2	Identifizierung und Authentifizierung für Neuverschlüsselung nach Widerrufung.....	24
3.4	Identifizierung und Authentifizierung für Widerrufungsantrag	24
4	Operationelle Erfordernisse Für Die Lebensdauer Eines Zertifikats.....	26
4.1	Zertifikatantrag	26
4.1.1	Wer kann einen Zertifikatantrag stellen?	26
4.1.2	Einschreibeprozess und Verantwortungen	26
4.2	Bearbeitung des Zertifikatantrags	27
4.2.1	Durchführung von Identifikations- und Authentifizierungsfunktionen.....	27
4.2.2	Genehmigung oder Ablehnung von Zertifikatanträgen.....	27
4.2.3	Zeit zum Verarbeiten von Zertifikatanträgen	27
4.3	Ausstellung der Zertifikate.....	27
4.3.1	Handlungen der CA während der Zertifikatausstellung	28
4.3.2	Benachrichtigung des Abonnenten durch die CA über die Zertifikatausstellung	28
4.4	Annahme der Zertifikate.....	28
4.4.1	Handlung, die eine Annahme des Zertifikats darstellt	28
4.4.2	Veröffentlichung des Zertifikats durch die CA.....	28

4.4.3	Benachrichtigung anderer Entitäten über die Zertifikatausstellung durch die CA	28
4.5	Benutzung von Schlüsselpaaren und Zertifikaten	28
4.5.1	Benutzung von Schlüsselpaaren und Zertifikaten durch Benutzer	29
4.5.2	Benutzung von Schlüsselpaaren und Zertifikaten durch vertrauende Parteien.....	29
4.6	Erneuerung von Zertifikaten.....	29
4.6.1	Voraussetzungen für die Erneuerung von Zertifikaten	29
4.6.2	Wer darf eine Erneuerung beantragen?.....	29
4.6.3	Bearbeitung von Anträgen auf Zertifikaterneuerung.....	29
4.6.4	Benachrichtigung von Abonnet über die Ausstellung neuer Zertifikate	29
4.6.5	Handlung, die die Annahme einer Zertifikaterneuerung darstellt	29
4.6.6	Veröffentlichung des Erneuerungszertifikats durch die CA.....	30
4.6.7	Benachrichtigung anderer Entitäten über die Zertifikatausstellung durch die CA	30
4.7	Neuverschlüsselung von Zertifikaten.....	30
4.7.1	Voraussetzungen für die Neuverschlüsselung eines Zertifikats	30
4.7.2	Wer darf die Zertifizierung eines neuen öffentlichen Schlüssels beantragen.	30
4.7.3	Bearbeitung von Anträgen auf Neuverschlüsselung von Zertifikaten.....	30
4.7.4	Benachrichtigung von Abonnet über die Ausstellung neuer Zertifikate	30
4.7.5	Handlung, die die Annahme eines neu verschlüsselten Zertifikats darstellt ..	30
4.7.6	Veröffentlichung des neu verschlüsselten Zertifikats durch die CA.....	30
4.7.7	Benachrichtigung anderer Entitäten über die Zertifikatausstellung durch die CA	30
4.8	Änderung eines Zertifikats.....	30
4.9	Sperrung und Widerrufung von Zertifikaten	30
4.9.1	Umstände für Widerrufung	32
4.9.2	Wer kann eine Widerrufung beantragen?.....	32
4.9.3	Verfahren zur Beantragung von Widerrufung.....	32
4.9.4	Toleranzfrist für Widerrufungsantrag.....	32
4.9.5	Zeit, in der die CA den Widerrufungsantrag bearbeiten muss.....	33
4.9.6	Anforderungen zur Widerrufungsprüfung für vertrauende Parteien	33
4.9.7	CRL-Ausstellungshäufigkeit (falls anwendbar)	33
4.9.8	Längste Wartezeit für CRLs (falls anwendbar).....	33
4.9.9	Verfügbarkeit der Online-Prüfung von Widerrufung/Status.....	33

4.9.10	Anforderungen für Online-Widerrufungsprüfung	33
4.9.11	Andere verfügbare Formen von Widerrufungsankündigung	33
4.9.12	Besondere Anforderungen für Neuverschlüsselungsgefährdung	33
4.9.13	Umstände für Sperrung	33
4.9.14	Wer kann eine Sperrung beantragen?.....	34
4.9.15	Verfahren für Sperrungsanträge.....	34
4.9.16	Begrenzungen des Sperrzeitraums	34
4.10	Dienste für Zertifikatsstatus.....	34
4.10.1	CRLs und Delta CRLs	34
4.10.2	OCSP	34
4.10.3	Betriebsmerkmale.....	34
4.10.4	Dienstverfügbarkeit	34
4.10.5	Optionale Merkmale	35
4.11	Ende des Abonnements	35
4.12	Abgabe und Abholen der Schlüssel	35
5	Kontrollen betreffend Einrichtungen, Management und Betrieb.....	36
5.1	Physische Kontrollen.....	36
5.1.1	Lage und Konstruktion der Standorte.....	36
5.1.2	Physischer Zugang.....	36
5.1.3	Stromversorgung und Klimatisierung	36
5.1.4	Aussetzung an Wasser	36
5.1.5	Brandverhütung und -schutz	37
5.1.6	Aufbewahrung von Medien	37
5.1.7	Abfallentsorgung.....	37
5.1.8	Backup entfernt vom Standort	37
5.2	Verfahrenskontrollen.....	37
5.2.1	Vertrauensrollen	37
5.3	Personalkontrollen.....	38
5.3.1	Anforderungen hinsichtlich Qualifikationen, Erfahrung und Genehmigungen.....	38
5.3.2	Hintergrundprüfverfahren.....	38
5.3.3	Ausbildungsanforderungen	38
5.3.4	Häufigkeit und Anforderungen für Fortbildung.....	38
5.3.5	Häufigkeit und Reihenfolge des turnusmäßigen Tätigkeitswechsels	38

5.3.6	Strafen für unbefugte Handlungen.....	38
5.3.7	Anforderungen an unabhängige Vertragsparteien	38
5.3.8	Dokumentation, ausgehändigt an das Personal.....	39
5.4	Verfahren für Audit-Logging	39
5.4.1	Arten aufgezeichneter Ereignisse	40
5.4.2	Häufigkeit der Kontrollverarbeitung.....	40
5.4.3	Aufbewahrungszeitraum für Kontrollberichte	40
5.4.4	Schutz des Kontrollberichts	40
5.4.5	Backup-Verfahren für Kontrollberichte	40
5.4.6	Kontrollsammlungssystem.....	41
5.4.7	Benachrichtigung an ereignisverursachenden Benutzer.....	41
5.4.8	Verletzlichkeitsbeurteilungen.....	41
5.5	Archivierung der Verzeichnisse.....	41
5.5.1	Arten archivierter Verzeichnisse.....	41
5.5.2	Aufbewahrungszeitraum für Archive.....	41
5.5.3	Schutz des Archivs.....	41
5.5.4	Verfahren für das Backup der Archive.....	42
5.5.5	Anforderungen zum Anbringen von Zeitstempeln auf den Verzeichnissen....	42
5.5.6	Archivsammlungssystem (intern oder extern)	42
5.5.7	Verfahren zur Erhaltung und Überprüfung der Archivierungsinformationen.	42
5.6	Schlüsselübergabe	42
5.7	Risiken und Wiederherstellung nach einer Katastrophe.....	43
5.7.1	Verfahren zur Behandlung von Zwischenfällen und Risiken	43
5.7.2	Beschädigung der EDV-Hilfsmittel, Softwares und/oder Daten.....	43
5.7.3	Verfahren im Fall eines kompromittierten Entitäts-Privatschlüssels.....	43
5.7.4	Fortsetzung der Geschäftsfähigkeit nach einer Katastrophe	44
5.8	CA- oder RA-Beendigung	44
6	Kontrollen der technischen Sicherheit	45
6.1	Generierung und Installierung des Schlüsselpaares.....	45
6.1.1	Schlüsselpaargenerierung.....	45
6.1.2	Lieferung von Privatschlüssel an einen Benutzer	45
6.1.3	Lieferung von öffentlichem Schlüssel an Zertifikataussteller.....	45
6.1.4	Lieferung von öffentlichem CA-Schlüssel an vertrauende Parteien.....	45
6.1.5	Schlüsselgrößen	45

6.1.6	Generierung und Qualitätsprüfung von Parametern öffentlicher Schlüssel...	46
6.1.7	Zwecke für Schlüsselnutzung (gemäß X.509 v3 Schlüsselnutzungsfeld)	46
6.2	Schutz des Privatschlüssels und Kontrollen des kryptographischen Moduls	46
6.2.1	Sicheres kryptographisches Modul.....	46
6.2.2	Generierung des Privatschlüssels	46
6.2.3	Kontrolle des Privatschlüssels durch mehrere Personen	46
6.2.4	Hinterlegung des Privatschlüssels.....	46
6.2.5	Backup des Privatschlüssels.....	46
6.2.6	Archivierung des Privatschlüssels	46
6.2.7	Privatschlüsselübertragung zu oder von einem kryptographischen Modul....	47
6.2.8	Privatschlüsselspeicherung auf kryptographischem Modul.....	47
6.2.9	Verfahren zum Aktivieren von Privatschlüsseln	47
6.2.10	Verfahren zum Vernichten von Privatschlüsseln.....	47
6.2.11	Beurteilung kryptographischer Module.....	47
6.3	Andere Aspekte der Verwaltung des Schlüsselpaares.....	47
6.3.1	Archivierung von öffentlichen Schlüsseln.....	47
6.3.2	Lebensdauer von Zertifikaten und Nutzungsdauer von Schlüsselpaaren	47
6.4	Aktivierungsdaten	48
6.4.1	Generierung und Installierung von Aktivierungsdaten	48
6.4.2	Schutz der Aktivierungsdaten	48
6.4.3	Andere Aspekte von Aktivierungsdaten	48
6.5	Computersicherheitskontrollen.....	48
6.5.1	Spezifische technische Anforderungen an die Computersicherheit	48
6.5.2	Beurteilung der Computersicherheit	49
6.6	Technische Kontrollen der Lebensdauer	49
6.6.1	Systementwicklungskontrollen.....	49
6.6.2	Sicherheitsverwaltungskontrollen	49
6.6.3	Sicherheitskontrollen der Lebensdauer.....	50
6.7	Netzwerksicherheitskontrollen.....	50
6.8	Zeitstempel	50
7	Zertifikat-, CRL- und OCSP-Profile	51
7.1	Profil der Zertifikate	51
7.1.1	.Versionsnummer(n)	51
7.1.2	Erweiterungen des Zertifikats.....	51

7.1.3	Algorithmusobjektidentifikatoren	51
7.1.4	Namensformen	51
7.1.5	Namensbeschränkungen	51
7.1.6	Objektidentifikator der Zertifikat-Policy	51
7.1.7	Verwendung der Erweiterung der Policy-Beschränkung	51
7.1.8	Syntax und Semantik der Policy-Qualifikatoren	51
7.1.9	Verarbeitung der Semantik für die Erweiterung kritischer Zertifizierungspolicies	51
7.1.10	Gültigkeit des Zertifikats	51
7.2	CRL-Profil	52
7.2.1	Versionsnummer(n)	52
7.2.2	CRL und CRL-Eingabeerweiterungen	52
7.3	OCSP-Profil	52
7.3.1	Versionsnummer(n)	52
7.3.2	OCSP-Erweiterungen	52
8	Audit der Übereinstimmung und andere Bewertungen	53
8.1	Häufigkeit oder Umstände der Beurteilung	53
8.2	Identität/Qualifikationen des Prüfers	53
8.3	Beziehung des Prüfers mit der geprüften Entität	53
8.4	Von der Beurteilung abgedeckte Themen	54
8.5	Maßnahmen bei Unzulänglichkeit	54
8.6	Kommunikation der Ergebnisse	54
9	Andere geschäftliche und gesetzliche Fragen	55
9.1	Gebühren	55
9.1.1	Gebühren für Ausstellung oder Erneuerung von Zertifikaten	55
9.1.2	Gebühren für Zugang zu Zertifikaten	55
9.1.3	Gebühren für Widerrufung oder Zugang zu Statusinformation	55
9.1.4	Gebühren für andere Dienste	55
9.1.5	Erstattungspolitik	56
9.2	Finanzielle Verantwortung	56
9.2.1	Versicherungsdeckung	56
9.2.2	Andere Vermögenswerte	56
9.2.3	Versicherungs- oder Garantiedeckung für End-Entitäten	56
9.3	Vertraulichkeit von Geschäftsinformationen	56

9.3.1	Umfang vertraulicher Informationen	56
9.3.2	Informationen außerhalb des Umfangs vertraulicher Informationen	57
9.3.3	Verantwortung für den Schutz vertraulicher Informationen	57
9.4	Schutz der personenbezogenen Informationen	57
9.4.1	Schutzplan	57
9.4.2	Als privat behandelte Information	57
9.4.3	Als nicht privat betrachtete Information	57
9.4.4	Verantwortung für den Schutz privater Information	58
9.4.5	Benachrichtigung und Zustimmung zur Benutzung von privater Information	58
9.4.6	Offenbarung aufgrund gerichtlicher oder administrativer Prozesse	58
9.4.7	Andere Umstände für Offenbarung von Information	58
9.5	Rechte an geistigem Eigentum	59
9.6	Vertretungen und Garantien	59
9.6.1	CA-Vertretungen und -Garantien	59
9.6.1.1	Vertrauen auf eigenes Risiko	61
9.6.1.2	Korrektheit der Informationen	61
9.6.2	RA-Vertretungen und Garantien	61
9.6.3	Vertretungen und Garantien des Benutzers	61
9.6.4	Vertretungen und Garantien von Vertrauenden Parteien	62
9.6.5	Vertretungen und Garantien anderer Teilnehmer	62
9.7	Abweisung von Garantien	63
9.8	Begrenzung der Haftung	63
9.8.1	Haftungen des TSP	63
9.8.2	Qualifizierte Zertifikate	63
9.8.3	Zertifikate, die nicht als qualifizierte Zertifikate betrachtet werden können	64
9.8.4	Haftungsausschluss	64
9.9	Schadenersatz	65
9.10	Laufzeit und Beendigung des CP/CPS	65
9.10.1	Laufzeit	65
9.10.2	Beendigung	65
9.10.3	Auswirkung von Beendigung und Fortbestand	65
9.11	Individuelle Mitteilungen und Kommunikation mit Teilnehmern	66
9.12	Änderungen	66

9.12.1	Verfahren für Änderungen.....	66
9.12.2	Mechanismen und Zeitraum für Benachrichtigungen.....	66
9.12.3	Umstände, die eine Änderung des OID erforderlich machen	66
9.13	Verfahren zur Beilegung von Streitfällen.....	66
9.14	Anwendbares Recht.....	67
9.15	Übereinstimmung mit geltendem Gesetz	67
9.16	Verschiedene Bestimmungen.....	67
9.16.1	Gesamte Vereinbarung.....	67
9.16.2	Übertragung.....	67
9.16.3	Abtrennbarkeit (Salvatorische Klausel)	67
9.16.4	Durchsetzung (Anwaltshonorare und Verzicht auf Rechte).....	67
9.16.5	Höhere Gewalt.....	68
9.17	Andere Bestimmungen	68
Anhangen	69

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 innerhalb 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 unilaterale öffentliche Erklärung der Richtlinien, die die „Foreigner CA“ bei der Bereitstellung von Zertifizierungsdiensten einhält, und es wird umfassend 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 („Grundanforderungen“), 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 innerhalb der CA-Domäne verwendet 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 Förderale 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:

- 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-Erklärungen.
- 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
- Der ISO/IEC 27001 Standard über Informationssicherheit 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 § 1 **Fout! Ongeldige bladwijzerverwijzing.**).

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

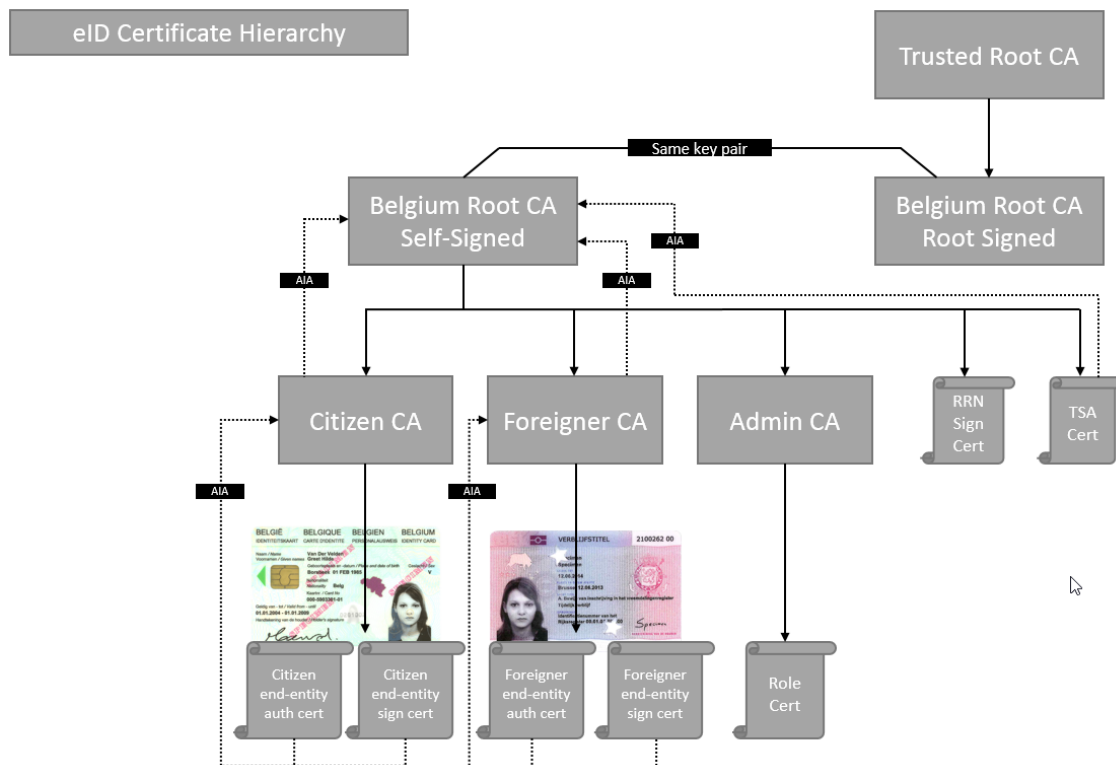


Abbildung: Belgische eID PKI-Hierarchie

1.3 Name und Identifizierung des Dokuments

<p>Name dieses Dokuments</p>	<p><i>Belgian Certificate Policy & Certification Practice Statement für eID PKI Infrastruktur-Foreigner CA</i></p>
<p>Dokumentversion</p>	<p>2.16.56.12.1. – V4.4</p> <p><i>Diese Zertifikatspolicy wird durch ihren Namen und ihre Versionsnummer identifiziert.</i></p> <p><i>Diese Dokument-OID ersetzt folgende OIDs</i></p> <p>2.16.56.1.1</p> <p>2.16.56.9.1</p> <p>2.16.56.10.1</p> <p><i>Diese Foreigner CP/CPS hebt ab dem Datum der Veröffentlichung alle anderen Versionen von Foreigner CP/CPS auf.</i></p>
<p>OID, der auf dieses Dokument verweist</p>	<p><i>Die Identifizierer unter der Kontrolle von Certipost:</i></p> <p>BRCA (1) <i>OID: 2.16.56.1.1.1.7 – Foreigner CA</i> <i>OID: 2.16.56.1.1.1.7.1 – Foreigner Unterzeichnungszertifikat</i> <i>OID: 2.16.56.1.1.1.7.2 – Foreigner Authentifizierungszertifikat</i></p> <p>BRCA 2 <i>OID: 2.16.56.9.1.1.7 – Foreigner CA</i> <i>OID: 2.16.56.9.1.1.7.1 – Foreigner Unterzeichnungszertifikat</i> <i>OID: 2.16.56.9.1.1.7.2 – Foreigner Authentifizierungszertifikat</i></p> <p>BRCA 3 <i>OID: 2.16.56.10.1.1.7 – Foreigner CA</i> <i>OID: 2.16.56.10.1.1.7.1 – Foreigner Unterzeichnungszertifikat</i> <i>OID: 2.16.56.10.1.1.7.2 – Foreigner Authentifizierungszertifikat</i></p> <p>BRCA 4 <i>OID: 2.16.56.12.1.1.7 – Foreigner CA</i> <i>OID: 2.16.56.12.1.1.7.1 – Foreigner Unterzeichnungszertifikat</i> <i>OID: 2.16.56.12.1.1.7.2 – Foreigner Authentifizierungszertifikat</i></p>

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 Registrierungsbehörden 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 Aktivierungs-codes 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 Aktivierungscode 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.rn.fgov.be/nl/identiteitsdocumenten/eid/reglementering/

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

Deutsch: www.ibz.rn.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. Certipost überprüft zweimal im Jahr, ob die Belgische eID-Karte auf der EU-QSCD-Liste steht.

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 Widerrufsanspruch

Die Identifizierung des Ausländers, der eine 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 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 Widerrufsanhträge an die CA über die RA. Die RA ist der einzige Kontaktpunkt, über welchen die CA einen Widerrufsanhtrag empfangen kann.

Die RA sendet den digital unterschriebenen Widerrufsanhtrag 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 Gültigkeitserklärung 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.rn.gov.be/nl/identiteitsdocumenten/eid/reglementering/

Französisch: www.ibz.rn.gov.be/fr/documents-didentite/eid/reglementation/

Deutsch: www.ibz.rn.gov.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 der Herstellung des elektronischen Personalausweises befinden sich die Zertifikate in einem nicht aktivierten Zustand, dh sie wurden auf der Karte ausgestellt, bleiben jedoch gesperrt. Die LRA aktiviert den elektronischen Personalausweis in Anwesenheit des Ausländer, indem die Aussetzung der Zertifikate aufgehoben wird. 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

Laut RFC 3647 Bescheinigung ist Erneuerung definiert als "*The issuance of a new Certificate without changing the Public Key or any other information in the Certificate*". Für Ende-Zertifikate (Authentifizierung und Signaturzertifikat) ist diese Funktion nicht unterstützt.

4.6.1 Voraussetzungen für die Erneuerung von Zertifikaten

Erneuerung von Zertifikaten ist nicht unterstützt.

4.6.2 Wer darf eine Erneuerung beantragen?

Siehe Abschnitt 4.6.1.

4.6.3 Bearbeitung von Anträgen auf Zertifikaterneuerung

Siehe Abschnitt 4.6.1.

4.6.4 Benachrichtigung von Abonnet über die Ausstellung neuer Zertifikate

Siehe Abschnitt 4.6.1.

4.6.5 Handlung, die die Annahme einer Zertifikaterneuerung darstellt

Siehe Abschnitt 4.6.1.

4.6.6 Veröffentlichung des Erneuerungszertifikats durch die CA.

Siehe Abschnitt 4.6.1.

4.6.7 Benachrichtigung anderer Entitäten über die Zertifikatausstellung durch die CA

Siehe Abschnitt 4.6.1.

4.7 Neuverschlüsselung von Zertifikaten

Nach RFC 3647 ist ein Zertifikat neu-Verschlüsselung definiert als "... a subscriber or other participant generating a new key pair and applying for the issuance of a new certificate that certifies the new public key". Im Rahmen der eID bedeutet dies, dass das Thema (der Bürger) für die Ausstellung eines neuen Zertifikats mit den gleichen Daten, aber mit einem anderen öffentlichen Schlüssel und Gültigkeitszeitraum gelten. Sorgfalt, Schlüsselpaar-Erzeugung, Lieferung und Verwaltung sind in Übereinstimmung mit dieser CP/CPS durchgeführt.

4.7.1 Voraussetzungen für die Neuverschlüsselung eines Zertifikats

Neuverschlüsselung von Zertifikaten ist unterstützt.

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

Zertifikat-Re-Key-Anforderungen werden auf die gleiche Weise wie Anforderungen für neue Authentifizierungs- oder Signatur-Zertifikate und in Übereinstimmung mit den Bestimmungen dieses CP / CPS verarbeitet.

4.7.4 Benachrichtigung von Abonnet 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. Die RAs und LRAs sorgen dafür, dass dieser Forderung nachgekommen wird.

Um die Widerrufung eines Zertifikats zu beantragen, muss der Ausländer mit einer LRA, der Polizei oder [DOCSTOP](#) Kontakt aufnehmen. Während die Öffnungszeiten einer LRA begrenzt sind, ist DOCSTOP rund um die Uhr, sieben Tage die Woche zugänglich.

Inaktivierte Personalausweise mit entzogenen Zertifikate werden direkt an Belgische Bürger im Ausland geliefert. Danach können sie beim Konsulat vorbeigehen, um den Chip und die Zertifikate zu aktivieren. Diese Aktivierung ist jedoch nicht zeitlich begrenzt.

Die Polizei, die LRA, DOCSTOP oder der RA beantragen die Widerrufung 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 gesetzlich dazu verpflichtet wird.

Auf Anfrage der RA oder des TSP 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.

Unter gewissen Umständen (z.B. Vermeidung 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 Widerrufe 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 Widerrufsinformation über die Gültigkeitsperiode des Zertifikats durch die CRL verfügbar.

4.9.1 Umstände für Widerrufung

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 Widerrufsfrist anfordern Gnade beträgt der Zeitraum vom Aufforderung zum Thema (d. h. die Bürger) eine Zertifikatsperrung durch Kontaktaufnahme mit der LRA, die Polizei oder DOCSTOP bis die Zertifikatsperrung in den Zertifikatsdiensten Validierung niederschlägt.

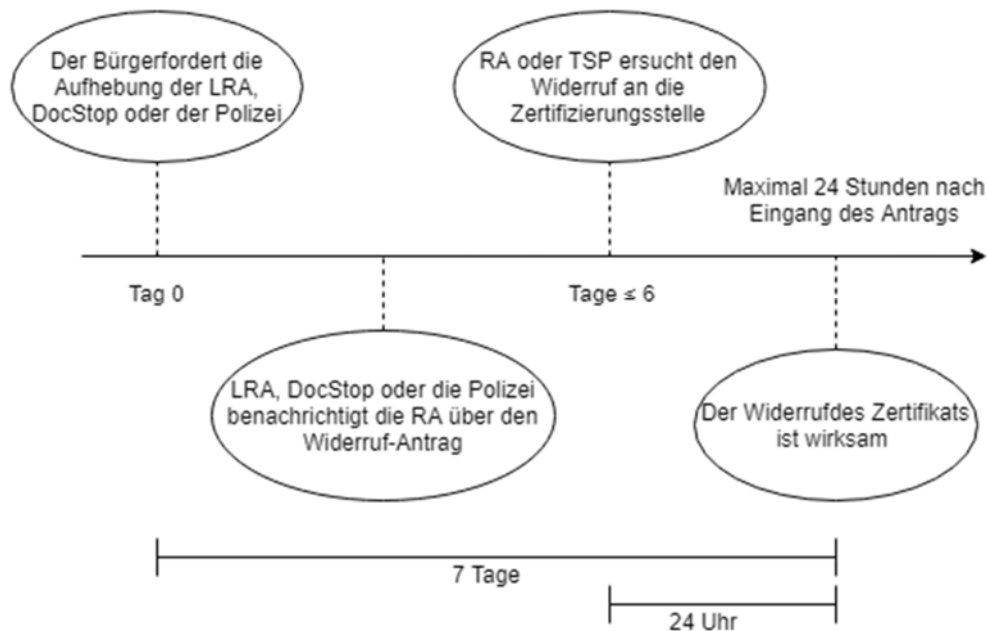


Abbildung 1: Widerruf Zeitplan

Abbildung 1: Widerruf Zeitplan zeigt der Widerruf Zeitplan und zeigt, dass im Rahmen des eID es ein Maximum von 6 Tagen gibt bis die TSP den Widerrufanforderung bekommt und maximal 3 Stunden ab diesem Zeitpunkt bis zum wirksamen Widerrufs erhält.

Die Nachfrist für die Bearbeitung der Widerrufanforderung beträgt 7 Kalendertage. Jedoch wann die Widerrufanforderung beträgt von der Zertifizierungsstelle ist empfangen, wird der aktualisierte Status innerhalb von 3 Stunden in den Zertifikatprüfungsdienst wiedergegeben.

4.9.5 Zeit, in der die CA den Widerrufungsantrag bearbeiten muss

Die CA widerruft 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 Widerrufs oder der Meldung und dem Entschluss, 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 Widerrufsankündigung

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.

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 Zertifikatsstatusdienste 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 Funktionen wie Schlüsselgenerierung, Benutzerauthentifizierung, Zertifikatsausstellung, 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 benutzt 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 eintreten, 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 unbefugte 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 TSP kontrolliert 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 Einbruchversuche 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 25 Jahren nach Ablauf des Zertifikats;
- Auditbericht über die Ausstellung der Zertifikate für einen Zeitraum von mindestens 25 Jahren nach Ausstellung des Zertifikats;
- Auditbericht über die Widerrufung eines Zertifikats von mindestens 25 Jahren nach Widerruf des Zertifikats;
- CRLs und Delta CRLs von mindestens 25 Jahren nach deren Veröffentlichung;
- Der TSP muss das letzte Backup der CA-Archive von mindestens 25 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-Website](#) verfügbar):

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-Entitätzertifikaten im nächsten Jahr. In der Schlüsselzeremonie werden die Foreigner CA-Zertifikate von den BRCAAs 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-Entitätzertifikate 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-Privatschlüssels

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 [6.1.1 SCHLÜSSELPAARGENERIERUNG](#)

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 vertrauenswürdigen 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 berücksichtigt:

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 Antiviruschutzes.
- 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 5 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, abgeändert durch das Gesetz vom 11. Dezember 1998, 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. Und im Rahmen des *verordnung (eu) 2016/679 des europäischen parlaments und des rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung.*

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 Widerrufs Antrag 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 DOCSTOP zu benachrichtigen, um die Widerrufung 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 ausgestellte 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

Anhangen

This page is intentionally left blank.

Anhang A

Definitions & acronyms

CA	Certification Authority
CC	Common Criteria
CM	Kartenersteller (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) Registrierungsstelle

Anhang B

ANFORDERUNGEN AN ZERTIFIZIERUNGSBEHÖRDEN

Die kryptografischen Module, die von Zertifizierungsbehörden angewendet werden, WERDEN bewertet und in Übereinstimmung mit einem der folgenden Standards zertifiziert:

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

Anhang C

ISSUING CAs EID HIERARCHY CERTIFICATE PROFILE EXTRACTED FROM EID-DEL-004

Starting from next page

Table of contents

Table of contents	4
1. Certificate profiles.....	6
1.1. Version	6
1.2. Certificates Serial Number	6
1.3. Signature	7
1.4. Issuer	7
1.5. Validity	8
1.6. Subject	9
1.7. Subject Public Key Info.....	11
1.8. Key usage	11
1.9. Extended Key usage	12
1.10. Authority and Subject Key Identifiers	12
1.11. NetscapeCertType.....	12
1.12. Policy mapping.....	13
1.13. Policy constraint.....	13
1.14. Certificate policies.....	14
1.15. Basic constraint	15
1.16. CRL Distribution Point	15
1.17. Freshest CRL - Delta CRL Distribution Point.....	16
1.18. Authority Information Access	16
1.19. Subject Directory attributes.....	17
1.20. Qualified Certificate Statement	17
2. CRL profiles	19
2.1. CRL Profile	19
2.2. Δ CRL Profile.....	19
2.3. CRL Issuance Frequency.....	20
3. CA configuration settings.....	21
3.1. Auto-revocation	21
3.2. Unique DN check.....	21
3.3. Variable validity	22
3.4. Delta CRL	22

4. Naming conventions	23
4.1. Serial number to reference a CA.....	23
4.2. CRL and delta CRL names.....	24
4.3. CA certificate file names	24

1. Certificate profiles

The different CAs are profiled according to PKIX certificate profile, and made up to three parts according to RFC5280: tbsCertificate, Signature algorithm and Signature value.

Note: All the URI's specified in the certificate profiles are resolved by BOSA¹.

Hereunder the most significant certificate profile fields will be described. Changes that were made to these fields during the course of the eID project are reflected by specifying a release date, which is the date the change was put in operations.

1.1. Version

The version field indicates the X.509 version of the certificate format. In eID project, only certificates complying with version 3 of the X.509 recommendation, allowing for extensions, are used.

Version	
All certificates	Version 3 – Value = "2"

1.2. Certificates Serial Number

The field certificate serial number specifies the unique, numerical identifier of the certificate within all certificates issued by the same Certification Authority (CA).

The RRN² can assign a serial number to the eID hierarchy certificates.

The CA operator checks the uniqueness of the end-user certificate serial numbers before processing the certification requests.

All serial numbers are maximal 16 bytes long, except for the Self-signed Belgium Root CA2 where the serial number is 8 bytes.

Serial Number	
eID hierarchy certificates	Generated by the CA at the time of Key Generation Process

Remark: if no serial number is received in the requests issued by the RRN, the CA provider will generate this number using its own allocation scheme.

¹ BOSA is the acronym for FOD beleid en ondersteuning / Stratégie et appui

² RRN is an acronym for Rijksregister – Registre National

1.3. Signature

The signature field determines the cryptographic algorithm used by a CA to sign a certificate. The algorithm identifier, which is a number registered with an internationally recognised standards organisation, specifies both the public-key algorithm and the hashing algorithm used by the CA to sign certificates. The Object Identifier for SHA1withRSA is 1.2.840.113549.1.1.5. The Object Identifier for SHA256withRSA is 1.2.840.113549.1.1.11.

Signature	
Certificates under BRCA1, BRCA2 and BRCA3	SHA1withRSA
Certificates under BRCA4	SHA256withRSA

1.4. Issuer

The Issuer field identifies the certification authority that has signed and issued the certificate. Issuer is structured as a “Distinguished Name”, that is a hierarchically structured name, composed of attributes, most of which are standardised in the X.500 attributes. The ones used are: country, organisation, serial number, common name, locality. The subject serial number mentioned in the issuer field is the serial number attributed by the RRN to identify the CA.

Issuer		
Certificate	Releases	Field attributes
eID hierarchy <u>Operational CA certificates</u> Citizen CA, Foreigner CA	<2008 >=2008 >=06/2013	C: BE, CN: Belgium Root CA C: BE, CN: Belgium Root CA2 C: BE, CN: Belgium Root CA3 C: BE, CN: Belgium Root CA4
<u>End user certificates</u> Citizen	<2005 >=2005	C: BE, CN: Citizen CA C: BE, CN: Citizen CA, Serial Number: <yyy><ss> ³
Foreigner		C: BE, CN: Foreigner CA, Serial Number: <yyy><ss>
<u>End user certificates</u> Citizen		C: BE, CN: Citizen CA,

³ See paragraph 4.1 Serial number to reference a CA

Foreigner	>=2017	Serial Number: <yyyy><ss> ⁴ O: Certipost N.V. / S.A. L: Brussels C: BE, CN: Foreigner CA, Serial Number: <yyyy><ss> O: Certipost N.V. / S.A. L: Brussels
-----------	--------	---

1.5. Validity

The validity field indicates the time interval during which the certificate can be used and on which the issuing CA maintains certificate status information.

The certificates can be used, unless a certificate is suspended or revoked during its period of validity. Validity should be interpreted as the period when the (non-revoked) certificate can be trusted to perform a certain transaction. All transactions executed after this period based on the certificate should be handled as not trusted.

Validity				
	Release	Not before	Not after	Validity period ⁵
eID hierarchy <u>Operational CA certificates</u> Citizen CA	2003/1		6y 5m	
	2003/2		6y 2m	
Foreigner CA	>2004 - <2014		6y 8m	
	>=2014		11 yr, 8m	
	>=2006		6y 8m	
	>=2015		11y 8m	
	Release	Standard validity period ⁶		
eID hierarchy <u>End user certificates</u> Citizen	2003/1		5 years	
	2003/2		5 years	
	2004		5 years	
	2005		5y 3m	
	2006		5y 3m	
	2007		5y 3m	
	2008		5y 3m	

⁴ See paragraph 4.1 Serial number to reference a CA

⁵ Certificate validity periods defined during key ceremony.

⁶ for end user certificates variable validity periods are applied from April 1st 2006.

Foreigner	>=2014	10y 3m
	>=2006	5y 3m
	>=2015	10y 3m

1.6. Subject

The Subject field identifies the entity holding the private key corresponding to the public key published in the certificate. Subject is structured as a set of attributes, defined in the X.500 attributes.

Subject		
Certificate	Release	Field attributes
eID hierarchy		
<u>Root certificate</u>		
Belgium Root CA Self-signed crt	<2008	C: BE, CN: Belgium Root CA
	>=2008-2013	C: BE, CN: Belgium Root CA2
	>=2013	C: BE, CN: Belgium Root CA3 C: BE, CN: Belgium Root CA4
<u>Operational CA certificates</u>		
Citizen CA		
	<2005	C: BE, CN: Citizen CA
	>=2005	C: BE, CN: Citizen CA, Serial Number: <yyy><ss> ⁷
	>=2017	C: BE, CN: Citizen CA, Serial Number: <yyy><ss> ⁸ O: Certipost N.V. / S.A. L: Brussels
Foreigner CA		
	<2017	C: BE, CN: Foreigner CA, Serial Number: <yyy><ss>
	>=2017	C: BE, CN: Citizen CA, Serial Number: <yyy><ss> ⁹ O: Certipost N.V. / S.A. L: Brussels

⁷ See paragraph 4.1 Serial number to reference a CA

⁸ See paragraph 4.1 Serial number to reference a CA

⁹ See paragraph 4.1 Serial number to reference a CA

<u>End user certificates</u> Citizen, Foreigner RRN signing	>=2005	See Table "End use certificate Subject field (eID Hierarchy)" C:BE, CN:RRN, O:RRN
---	--------	--

End user certificate Subject fields definition (eID hierarchy)			
Field	Length	Description	Example
C (countryName)	2	countryName is a dynamic element corresponding to the two letter country code ISO3166 standard. The country code is provided with the certificate creation request by the RRN. It is not checked by the CA.	C=BE
CN (commonName)	Max 255 Min 1	Concatenation of <ul style="list-style-type: none"> • <given name>: first given name of the card holder • <surname>: surname of the eID card owner • (<purpose>): (Authentication) or (Signature) 	CN=John Smith (Authentication) CN=John Smith (Signature)
surname	Max 255 Min 1	Surname of the eID card owner	S=Smith
givenName	Max 255 Min 1	1 or 2 given names of the eID card owner (This field may not appear in case the owner has no given name)	G=John William
subjectSerialNumber	Max 255 Min 1	This is a unique number provided by the RRN ("Rijksregisternummer" – 11 digits long).	SN=12345678901

The CA operator does not perform a check on the content provided by the RRN, except that the subject distinguished name has to be unique.

1.7. Subject Public Key Info

The Subject Public Key Info field is used to carry the public key being certified and identify the algorithms with which the key has been generated.

Subject Public Key Info	
eID hierarchy	
<u>Root certificate</u> Self-signed Belgium Root CA1 & 2 Self-signed Belgium Root CA3 & 4 <u>Operational CA certificates</u> Citizen CA, Foreigner CA <2014 Citizen CA, Foreigner CA >=2014 <u>End user certificates</u> Citizen, Foreigner <2014 Citizen, Foreigner CA >=2014	RSA 2048 bits key RSA 4096 bits key RSA 2048 bits key RSA 4096 bits key RSA 1024 bits key RSA 2048 bits key

1.8. Key usage

The Key usage field specifies the purpose of the key contained in the certificate.

Key usage									
Key usage	Digital Signature	Non Repudiation	Key Encipherment	Data Encipherment	Key Agreement	Key Certificate Signing	Crl Signing	Encipher Only	Decipher Only
eID hierarchy									
<u>Root certificate</u> Self-signed Belgium Root CA	NA	NA	NA	NA	NA	A	A	NA	NA
<u>Operational CA certificates</u> Citizen CA, Foreigner CA	NA	NA	NA	NA	NA	A	A	NA	NA
<u>End user certificates</u> Citizen, Foreigner Authentication crt Citizen, Foreigner Signature crt	A NA	NA A	NA NA	NA NA	NA NA	NA NA	NA NA	NA NA	NA NA

The digital signature bit is not asserted in the Citizen & Foreigner Signature Certificates for strict application of the standards, and to prevent possible mistakes with applications.

1.9. Extended Key usage

The Extended Key usage field specifies the purpose of the key contained in the certificate.

Extended Key usage							
Extended Key usage	Any Key Usage	Server Authentication	Client Authentication	Code Signing	Email Protection	Time Stamping	OCSP Signing
eID hierarchy							
<u>Root certificate</u>							
Self-signed Belgium Root CA	NA	NA	NA	NA	NA	NA	NA
<u>Operational CA certificates</u>							
Citizen CA, Foreigner CA	NA	NA	A	NA	A	NA	NA
<u>End user certificates</u>							
Citizen, Foreigner Authentication crt	NA	NA	A	NA	NA	NA	NA
Citizen, Foreigner Signature crt	NA	NA	NA	NA	A	NA	NA

The client authentication & email protection bit is asserted in the Citizen & Foreigner CA Certificates to comply with the CA/B Forum's Baseline requirements regarding technical constraints for the eID PKI.

1.10. Authority and Subject Key Identifiers

To facilitate certification path construction, the authority and subject key identifier appears in all conforming CA certificates, that is, all certificates including the basic constraints extension where the value of CA is TRUE. The value of the subject key identifier is the value placed in the key identifier field of the Authority Key Identifier extension of certificates issued by the subject of this certificate.

The Authority Key Identifier extension is present in the Root signing and end user certificates of the eID hierarchy.

The Subject Key Identifier will be present in the Citizen CA and the Foreigner CA certificate(s). It will not be present in end-user certificates.

1.11. NetscapeCertType

This extension was removed as from 05/2017. This extension can be used to limit the applications for a certificate. If the extension exists in a certificate, it will limit the uses of the certificate to those specified. If the extension is not present, the certificate can be used for all applications except Object Signing.

- bit-0 SSL client - this cert is certified for SSL client authentication use
- bit-1 SSL server - this cert is certified for SSL server authentication use

- bit-2 S/MIME - this cert is certified for use by clients
- bit-3 Object Signing - this cert is certified for signing objects such as Java applets and plugins
- bit-4 Reserved - this bit is reserved for future use
- bit-5 SSL CA - this cert is certified for issuing certs for SSL use
- bit-6 S/MIME CA - this cert is certified for issuing certs for S/MIME use
- bit-7 Object Signing CA - this cert is certified for issuing certs for Object Signing

NetscapeCertType Key usage extension								
Netscape Key usage	bit-0 - SSL client	bit-1 - SSL server	bit-2 - S/MIME	bit-3 - Object Signing	bit-4 - Reserved	bit-5 - SSL CA	bit-6 - S/MIME CA	bit-7 - Object Signing CA
eID hierarchy								
<u>Root certificate</u>								
Self-signed Belgium Root CA	NA	NA	NA	NA	NA	A	A	A
<u>Operational CA certificate</u>								
Citizen CA, Foreigner CA	NA	NA	NA	NA	NA	A	A	A
<u>End user certificates</u>								
Citizen, Foreigner Authentication crt	A	NA	A	NA	NA	NA	NA	NA
Citizen, Foreigner Signature crt	NA	NA	A	NA	NA	NA	NA	NA

1.12. Policy mapping

This extension is only useful in case of cross-certification between CAs. It makes indeed little sense to have a policy mapping between a commercial CA and a Governmental CA. Also this extension is not handled by Netscape or by Microsoft products. As such the Policy Mapping has not been implemented.

1.13. Policy constraint

This extension can be used in CA certificates only. It can be used to constrain path validation in two ways: to prohibit policy mapping, or to require that each certificate in a path contain an acceptable policy identifier. If present, this extension should be marked critical [X509].

For the same reasons as mentioned in chapter 1.12, the Policy Constraint has not been implemented.

1.14. Certificate policies

Certificate policies are identified in the eID certificates using a CPS Pointer qualifier containing a pointer to the Certification Practice Statement (CPS) published by the CA.

The same sequence will be used for all eID certificates as it has been decided this qualifier will point to a web page that may reference multiple applicable documents.

With the implementation of the Belgium Root CA2 new OID's are being used to address the different policy in the certificate profiles. The new OID tree that is used is 2.16.56.9.1.*

With the implementation of the Belgium Root CA3 new OID's are being used to address the different policy in the certificate profiles. The new OID tree that is used is 2.16.56.10.1.*

With the implementation of the Belgium Root CA new OID's are being used to address the different policy in the certificate profiles. The new OID tree that is used is 2.16.56.12.1.*

Certificate Policies				
	Policy Identifier	Policy Qualifiers	Policy Qualifier Id	Qualifier
eID hierarchy				
<u>Operational CA certificates</u>				
Citizen CA	2.16.56.1.1.1.2	NA	CPS	https://repository.eid.belgium.be
	2.16.56.9.1.1.2			
	2.16.56.10.1.1.2			
	2.16.56.12.1.1.2			
Foreigner CA	2.16.56.1.1.1.7	NA	CPS	https://repository.eid.belgium.be
	2.16.56.9.1.1.7			
	2.16.56.10.1.1.7			
	2.16.56.12.1.1.7			
<u>End user certificates</u>				
Citizen Authentication certificate	2.16.56.1.1.1.2.2	NA	CPS	https://repository.eid.belgium.be
	2.16.56.9.1.1.2.2			
	2.16.56.10.1.1.2.2			
	2.16.56.12.1.1.2.2			
Citizen Signature certificate	2.16.56.1.1.1.2.1	NA	CPS	https://repository.eid.belgium.be
	2.16.56.9.1.1.2.1			
	2.16.56.10.1.1.2.1			
	2.16.56.12.1.1.2.1			

Foreigner Authentication certificate	2.16.56.1.1.1.7.2 2.16.56.9.1.1.7.2 2.16.56.10.1.1.7.2 2.16.56.12.1.1.7.2	NA	CPS	https://repository.eid.belgium.be
Foreigner Signature certificate	2.16.56.1.1.1.7.1 2.16.56.9.1.1.7.1 2.16.56.10.1.1.7.1 2.16.56.12.1.1.7.1	NA	CPS	http://repository.eid.belgium.be

1.15. Basic constraint

The Basic Constraints extension specifies whether the subject of the certificate may act as a CA or only as an end-user. If the subject may act as a CA, then the certificate is a cross-certificate, and it may also specify the maximum acceptable length of a certificate beyond the cross-certificate. This extension should always be marked as critical; otherwise some implementations will ignore it and allow a non-CA certificate to be used as a CA certificate.

Basic constraint extension		
	CA	Path Length Constraint
eID hierarchy		
<u>Root certificate</u>		
Self-signed Belgium Root CA	TRUE	None
<u>Operational CA certificate</u>		
Citizen CA, Foreigner CA	TRUE	0
<u>End user certificates</u>		
Citizen, Foreigner Authentication	FALSE	-
Citizen, Foreigner Signature	FALSE	-

1.16. CRL Distribution Point

The CRL Distribution Points extension identifies the CRL distribution point or points to which a certificate user should refer to ascertain if the certificate has been revoked. A certificate user can obtain a CRL from an applicable distribution point or it may be able to obtain a current complete CRL from the authority directory entry.

CRL Distribution Point extension (CDP)		
	Releases	Distribution Point
eID hierarchy		
<u>Operational CA certificates</u>		
Citizen CA	<2008	http://crl.eid.belgium.be/belgium.crl
	>=2008	http://crl.eid.belgium.be/belgium2.crl
Foreigner CA	<2014	
	>=2014	http://crl.eid.belgium.be/belgium3.crl http://crl.eid.belgium.be/belgium4.crl
<u>End user certificates</u>		
Citizen certificates	2003/1	http://crl.eid.belgium.be/eidc0001.crl
	2003/2	http://crl.eid.belgium.be/eidc0002.crl
	2004	http://crl.eid.belgium.be/eidc2004-1.crl
	>=2005	<a href="http://crl.eid.belgium.be/eidc<yyyy><ss>^10.crl">http://crl.eid.belgium.be/eidc<yyyy><ss>¹⁰.crl
Foreigner certificates		<a href="http://crl.eid.belgium.be/eidf<yyyy><ss>.crl">http://crl.eid.belgium.be/eidf<yyyy><ss>.crl

1.17. Freshest CRL - Delta CRL Distribution Point

This field is implemented for CRL certificates issued by operational CA certificates.

The freshest CRL extension identifies how delta CRL information is obtained.

The same syntax is used for this extension and the CRL Distribution point extension, and is described in Section 5.15.

1.18. Authority Information Access

The Authority Information Access extension indicates how to access the information and services provided by the issuer of a certificate, such as on-line validation services or LDAP server location.

An HTTP reference to the issuing CA has been added as a calssuers element in order to allow the certificate chain to be reconstructed up to a trusted root.

¹⁰ See paragraph 4.2 CRL and delta CRL names

Authority Information Access extension		
	Access Method	Access Location
eID hierarchy		
<u>Root certificate</u>		
Self-signed Belgium Root CA	None	None
<u>Operational CA certificate</u>		
Citizen CA, Foreigner CA	None	None
>2017	id-ad-ocsp (OCSP)	http://ocsp.eid.belgium.be/2
	id-ad-calssuers (HTTP)	http://certs.eid.belgium.be/belgiumrs4.crt
<u>End user certificates</u>		
Citizen, Foreigner certificates		
<2008	id-ad-ocsp (OCSP)	http://ocsp.eid.belgium.be
>=2008		
<2014		
>=2014		http://ocsp.eid.belgium.be/2
<2008	id-ad-calssuers (HTTP)	http://certs.eid.belgium.be/belgiumrs.crt
>=2008		http://certs.eid.belgium.be/belgiumrs2.crt
<2014		http://certs.eid.belgium.be/belgiumrs3.crt
>=2014		http://certs.eid.belgium.be/belgiumrs4.crt
>2017		<a href="http://certs.eid.belgium.be/<issuingca>">http://certs.eid.belgium.be/<issuingca>

RFC5280 specifies: “The id-ad-calssuers OID is used when the additional information lists CAs that have issued certificates superior to the CA that issued the certificate containing this extension. The referenced CA issuers’ description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user.” It has no practical use to put accessMethod calssuers in the Admin hierarchy and the eID Operational CA certificates. The LDAP access method will not be used in any of the eID certificate profiles described in this document.

1.19. Subject Directory attributes

The Subject Directory Attributes are applicable to Citizen or Foreigner certificates only, and convey any desired Directory attribute values for the subject of the certificate that are complement to the information contained in the subject field. This extension is always non-critical.

No subject directory attributes will be present in the eID certificates

1.20. Qualified Certificate Statement

The Qualified Certificate Statement, identified by the OID { id-etsi-qcs 1 } is present in end-user signature certificates as per ETSI TS 101 862 V1.3.2.

As from 05/2017 the Qualified Certificate Statements, identified by the OIDs { id-etsi-qcs 4 } { id-etsi-qcs 5 } { id-etsi-qcs 6 } are present in end-user signature certificates.

2. CRL profiles

The CRLs and Δ CRLs will be created according to the profiles as described in the chapters 2.1 and 2.2. All CRLs and Δ CRLs are signed by the issuing CA.

2.1. CRL Profile

Version	v2
Signature	Sha256RSA
Issuer	<subject CA>
ThisUpdate	<creation time>
NextUpdate	<creation time> + 7 days
RevokedCertificates	
UserCertificate	<certificate serial number>
RevocationDate	<revocation time>
CrlEntryExtensions	
CRL Reason Code	certificateHold(6) (for suspended certificates) Note: otherwise not included
CrlExtensions	
Authority Key Identifier	non-critical <subject key identifier CA>
Freshest CRL	non-critical <location of delta CRL>
CRL Number	non-critical <The CA operator assigned unique number>
ExpiredCertsOnCRL	non-critical <GeneralizedTime of Bootstrap of the CitizenCA>

'nextUpdate' is the latest time that the CRL can be used by the certificate holder.

2.2. Δ CRL Profile

Version	v2
signature	Sha256RSA
Issuer	<subject CA>
thisUpdate	<creation time>
nextUpdate	<creation time> + 7 days
RevokedCertificates	
userCertificate	<certificate serial number>
revocationDate	<revocation time>
crlEntryExtensions	
CRL Reason Code	certificateHold(6) (for suspended certificates) removeFromCrl(8) (to unsuspend certificates) Note: otherwise not included

crlExtensions	
Authority Key Identifier	non-critical <subject key identifier CA>
CRL Number	non-critical <The CA operator assigned unique number>
Delta CRL Indicator	critical <base CRL Number>
ExpiredCertsOnCRL	non-critical < GeneralizedTime of Bootstrap of the CitizenCA >

'nextUpdate' is the latest time that the delta CRL can be used by the certificate holder.

2.3. CRL Issuance Frequency

Each Citizen / Foreigner CA issues a CRL every three hours. Each Citizen / Foreigner CA also issues a Δ CRL certificate corresponding to the previous CRL every three hours.

3. CA configuration settings

The table below specifies the configuration settings on the CA's these configuration settings are explained hereafter

CA configurations settings							
Setting	Auto-revocation	Unique DN check	Group	Variable validity	Delta CRL creation		
eID hierarchy							
<u>Operational CA certificates</u>							
Citizen CA	A	A	G1 ¹¹	A	A		
Foreigner CA	NA	A	G1	A	A		

3.1. Auto-revocation

Auto-revocation is the configuration setting which automatically revokes a certificate which has been suspended for more than a week after being active. Certificates which are created get the suspend status upon creation; called initial suspend. Certificates with the initial suspend status are not revoked after one week because these certificates were never active before.

3.2. Unique DN check

The Subject Distinguished Name (DN) consists of a set of selected certificate subject fields which is used to uniquely identify the subject of a certificate. The Unique DN check guarantees that only one certificate with a specific DN can be active at a time.

The unique DN check is carried out when a certificate is:

- 1) Un-suspended
- 2) Generated with a 'Valid' status.

The unique DN check applies to all certificates issued under the CA's belonging to the same unique DN group.

¹¹ Citizen CA and Foreigner CA are included in the same unique DN group G1

3.3. Variable validity

Variable validity is the CA configuration setting which provide the possibility to change the default validity period (Start of Validity and End of Validity) of requested certificates.

The variable validity feature is only available through XKMS interface.

3.4. Delta CRL

As the creation of delta CRLs is not a requirement for all CA's it is one of the specific configuration parameters of a CA.

4. Naming conventions

This chapter reflect the latest naming conventions and are not necessarily coherent with the names used in the past. Applying the naming conventions below is mandatory for all future changes to the PKI hierarchy and certificate profiles.

4.1. Serial number to reference a CA

<Serial number>			
Characteristics	Length	Format	Range
Multiple versions of the same CA issued in the same year	7	<yyyy><ss> <ul style="list-style-type: none"> ○ <yyyy> represents the year where the CA will be used ○ <ss> represents the unique serial number to be added for that year Applicable for: <ul style="list-style-type: none"> ○ certificate subject or issuer field serial numbers ○ CRL and dCRL file names ○ CA certificate file names 	2003 .. 9999 01 .. 99
Single version of a CA issued per year	4	<yyyy> <ul style="list-style-type: none"> ○ <yyyy> represents the year where the CA will be used Applicable for: <ul style="list-style-type: none"> ○ certificate subject or issuer field serial numbers ○ CRL and dCRL file names ○ CA certificate file names 	2003 .. 9999

Remark: The CA's created for the year 2008 the following scheme with respect to the serial numbers:

- CA'S created under Belgium Root CA:
 - Citizen 200801 until 200816
 - Foreigner01 until Foreigner04
- CA's created under Belgium Root CA2:
 - Citizen 200817 until 200820
 - Foreigner200805
- >2009 created under BRCA2

4.2. CRL and delta CRL names

<CRL and delta CRL names>			
CA	type	Format	Example
Citizen CA	Base CRL	eidc<serial number>.crl	eidc201721.crl
	Delta CRL	eidcd<serial number>.crl	eidcd201721.crl
Foreigner CA	Base CRL	eidf<serial number>.crl	eidf201721.crl
	Delta CRL	eidfd<serial number>.crl	eidfd201721.crl

4.3. CA certificate file names

<CA certificates file name>		
CA	Format	Example
Citizen CA	citizen<serial number>.crt	citizen201721.crt
Foreigner CA	foreigner<serial number>.crt	foreigner201721.crt