Citizen CA Zertifizierungsrichtlinie

BRCA 3

OID: 2.16.56.10.1.1.2

OID: 2.16.56.10.1.1.2.1 OID: 2.16.56.10.1.1.2.2

BRCA 4

OID: 2.16.56.12.1.1.2

OID: 2.16.56.12.1.1.2.1

OID: 2.16.56.12.1.1.2.2

Inhaltsverzeichnis

1 EINLEITUNG

1.1 Vorbemerkung

Die vorliegende Darlegung der Zertifizierungsrichtlinie (abgekürzt zu „CPS“ für „Certification Practice Statement“) beschreibt die Zertifizierungsverfahren, die auf die digitalen Zertifikate anwendbar sind, die durch den Zertifizierungsdienstleister für die „Citizen CA“ (abgekürzt zu CSP für „Certificate Service Provider“) für die belgischen Bürger ausgegeben werden.

Diese CPS muss ebenfalls als Zertifizierungspolicy (abgekürzt zu „CP“) für die von der „Citizen CA“-Zertifizierungsstelle ausgegebenen Zertifikate betrachtet werden.

Als elektronischer Personalausweis gilt sowohl das elektronische Identitätsdokument für belgische Bürger ab dem 12. Lebensjahr als auch das auf Anfrage erhältliche Identitätsdokument für Kinder (belgische Bürger unter 12 Jahren). Gegebenenfalls werden die Unterschiede zwischen beiden Identitätsdokumenten angegeben durch die jeweilige Bezeichnung: „elektronischer Personalausweis ab 12 Jahre“ und „elektronischer Personalausweis bis 12 Jahre“.

1.1.1 Genehmigte Entitäten, die vom vorliegenden CPS verwaltet werden

Der CSP ist zur Zeit die „CERTIPOST Aktiengesellschaft“, deren Sitz Muntcentrum / Centre Monnaie, in 1000 Brüssel gelegen ist und die zu diesem Zweck von den Belgischen Föderalen Behörden als vertragsschließende Behörde für das eID-Projekt unter den folgenden Bedingungen eingesetzt wurde:

CERTIPOST übernimmt die Rolle eines Zertifizierungsdienstleister („CSP“) im Sinne des Gesetzes vom 9. Juli 2001 (hiernach „das Gesetz über die elektronischen Unterschriften“) und der europäischen Richtlinie 1999/93 .

„Citizen CA“ ist der technische Name der Zertifizierungsstelle, die die Identitäts- und Unterschriftsbescheinigungen für den elektronischen Personalausweis ausstellt.

CERTIPOST übernimmt, im Auftrag und für Rechnung der belgischen Behörden, die Aufgabe von CA und CSP für die Citizen CA und ist in dieser Eigenschaft verantwortlich für die Bürgerzertifikate, die im Rahmen der Citizen CA ausgegeben werden. Die belgischen Behörden sind als CSP verantwortlich für die "Belgium Root CA" und für die CA-Zertifikate, die unter den "Belgium Root CA" ausgestellt werden.

Neben dem CSP sind andere Parteien im Projekt der belgischen elektronischen Personalausweise einbezogen. Diese Parteien sind:

Die Behörden

Die **Registrierungsstelle** („RA“ für Registration Authority), die im Namen und auf Rechnung des CSP bescheinigt, dass ein gewisser öffentlicher Schlüssel einer bestimmten Entität gehört (zum Beispiel einer Person), indem sie ein digital 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 Einwohnerverwaltungsstellen, in den

Gemeinden[1] 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 Authentifizierung der Bürger,

(ii) die Aufnahme der zu zertifizierenden Angaben,

(i) die Genehmigung zur Ausstellung eines Zertifikats für einen bestimmten Bürger,

(ii) die Garantie, dass die Zertifikate der Bürger auf der korrekten Identitätskarte gespeichert werden,

(iii) die Garantie, dass der Bürger genau die Karte erhält, die er erhalten soll und dass die betreffende Karte nur dann aktiviert wird, wenn sie dem richtigen Bürger ordnungsgemäß zugewiesen wurde,

(iv) die **SRA** (Suspension and Revocation Authority - Sperr - und Widerrufungsbehörde): das Rechtssubjekt, das die Zertifikate im Sinne des Gesetzes über digitale Unterschriften sperrt und/oder widerruft.

Der Kartenhersteller (Card Manufacturer):

Hersteller der Karten ("CM"[2]) ist die Gesellschaft Zetes, die zu diesem Zweck von der Belgischen Föderalen Behörde als vertragsschließende Behörde für das eID-Projekt eingestellt und mit der Herstellung, Personalisierung, Initialisierung und Verteilung der belgischen elektronischen Personalausweise beauftragt wurde. Die Zertifikate werden in diese Karten durch den CM, der ebenfalls die Schlüsselpaare generiert, eingetragen. Diese Aufgaben werden insbesondere auf diejenigen beschränkt, der in Posten 1 und 3 des Sonderlastenhefts RRN 006/2001 vermerkt stehen.

1.1.2 Beziehungen zwischen den vom vorliegenden CPS verwalteten Entitäten

Die Beziehung zwischen CERTIPOST als CSP für die „Citizen CA" und den Inhabern der Bescheinigungen, den belgischen Bürgern, wird in großem Maße durch das Gesetz vom 19. Juli 1991 über die Bevölkerungsregister und die Personalausweise, so wie durch das Gesetz vom 25. März 2003 erweitert, hiernach als „*Gesetz über die Personalausweise*" erwähnt, regiert. CERTIPOST informiert die Zertifikatsinhaber über ihre Rechte und Pflichten mit Hilfe eines Prospekts, der von der Gemeindeverwaltung verteilt wird.

CERTIPOST übernimmt die Rolle und Verantwortung des CSP.

In Übereinstimmung mit der Norm ETSI 101 456 zur Unterstützung der Europäischen Richtlinie 1999/93 in Sachen elektronischer Unterschrift gewährleistet CERTIPOST die Verwaltung ihrer CSPAufgaben über ein **PKI Management Board (CEPRAC)**, der über die erforderliche Erfahrung verfügt.

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

[1] Die "Gemeinden" sind die örtlichen Gemeindeverwaltung in Belgien und Belgiens diplomatische Vertretungen im Ausland. Die Rechte und Pflichten der diplomatischen Vertretungen sind im Gesetz vom 26. Juni 2002 "De wet inzake consulaire bevolkingsregister en identiteitskaarten" definiert.

[2] CM: Abkürzung für Card Manufacturer

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

1.1.3 Die belgischen Root CA

Ab 2008 wurde ein zusätzliche Belgium Root Certification Authority (BRCA) in die eID PKI Umgebung eingeführt. Diese Belgium Root Certification Authority2 (BRCA2) wurde notwendig, um nach dem 26. Oktober 2008 weiter Zertifikate ausstellen zu können.

2013 wurden 2 neue BRCA (BRCA3 und BRCA4) eingeführt, um die 10-jährige Gültigkeit der neuen eID-Karten 2014 zu unterstützen. Ab diesem Datum (der Ausstellung unter BRCA3) ist es nicht mehr möglich, Zertifikate im Rahmen der ursprünglichen BRCA auszustellen.

Diese CPS gilt für alle Citizen CA unter beiden BRCA (3 und 4).

Mit Einführung dieser BRCA wird ein neuer Satz OID-Nummern verwendet, um den Unterschied zwischen BRCA(1), BRCA2, BRCA3 und BRCA4 deutlich zu machen.

Verweise auf die BRCA im vorliegenden Dokument gelten für beide BRCA, sofern nicht ausdrücklich etwas anderes angegeben wurde.

Um Missverständnisse in Bezug auf Verweise auf die BRCA zu vermeiden, gilt folgende Konvention:

- Bei Bezug auf die erste BRCA ist von BRCA(1) die Rede, wobei die Ziffer “1” in Klammern steht, da die tatsächliche Bezeichnung dieser BRCA die Zahl “1” nicht enthält.

- Bei Bezugnahme auf die anderen BRCA innerhalb des vorliegenden Dokuments ist von BRCA3 und BRCA4 die Rede.

Technische Einzelheiten bezüglich der BRCA Zertifikate entnehmen Sie bitte Kapitel *7 ZERTIFIKAT UND CRL-PROFILE*

1.2 Tragweite des vorliegenden CPS

Eine Darlegung der Zertifizierungsrichtlinie (CPS) ist eine einseitige Erklärung der Verfahren, die von einer Zertifizierungsdienstleister eingehalten werden, wenn diese die Zertifizierungsdienste liefert. Ein CPS ist eine ausführliche Beschreibung der Art und Weise, mit welcher der CSP seine Dienste zur Verfügung stellt. Dieses CPS sollte nur im Bereich des CSP[3] benutzt werden. Das CPS zielt darauf ab, den Bereich der im Rahmen des CSP-Bereichs an Bürger und vertrauende Parteien[4] geleisteten Zertifizierungsdienste abzugrenzen. Dieses CPS umschreibt ebenfalls die Beziehung zwischen der „Citizen CA“ und anderen Zertifizierungsbehörden in der PKI-Hierarchie der Belgischen Föderalen Behörde wie die Belgium Root Certification Authority (BRCA)[5]. Es

[3] Der Bereich des CSP ist der Kompetenzbereich des CSP in Sachen Leistung con Zertifizierungsdiensten. Mit anderen Worten umfasst der Bereich des CSP die Anwendungen nicht, die die Zertifikate, usw. benutzen.

[4] Siehe 1.7.7: Entitäten, die sich auf eine Bescheinigung verlassen

[5] Die BRCA ist die CA, die die “Citizen CA” zertifiziert hat. Das Vertrauen zur BRCA zieht automatisch ein implizites Vertrauen zur “Citizen CA” mit sich.

beschreibt ebenfalls die Beziehung zwischen dem CSP und den anderen Organisationen, die bei der Ausstellung von Zertifikaten für die belgischen elektronischen Personalausweise (hiernach „Bürgerzertifikate“) mitarbeiten.

Dieses CPS liefert ebenfalls operationelle Richtlinien für alle Bürger und vertrauende 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 dem CSP und allen anderen Entitäten, die eine Rolle im Kontext des belgischen elektronischen Personalausweises spielen wie der Personalisierer der Karte oder der Initialisierer. Die Belgische Föderale Behörde erwirbt diese Dienste mittels des Rahmenvertrags. Schließlich sieht dieses CPS Informationen in Sachen Beglaubigung und Aufsicht für Kontrollbehörden, Beglaubigungsorgane, beglaubigte Buchprüfer, usw. in Bezug auf die Verfahren des CSP vor.

Dieses CPS unterschreibt die folgenden Normen und bringt sie zur Ausführung:

- RFC 2527: Internet X.509 Public Key Infrastructure – Zertifikatspolitik und Zertifizierungsverfahren
- RFC 5280: Internet X.509 Public Key Infrastructure – Zertifikat und CRL-Profil.
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualifiziertes Zertifikatsprofil.
- RFC 6960: X.509 Internet Public Key Infrastructure – Protokoll zur OnlineGültigkeitserklärung von Zertifikaten – OCSP
- ETSI TS 101 456: Politische Forderungen für die Zertifizierungsbehörden, die qualifizierte Zertifikate ausstellen.
- ETSI TS 101 862: Qualifiziertes Zertifikatsprofil.
- ETSI TS 102 042: Politische Forderungen für die Zertifizierungsbehörden, die Zertifikate von öffentlichen Schlüsseln ausstellen (nur normalisierte Stufe).
- Die Norm ISO/IEC 27001 in Sachen Sicherheit und Infrastruktur.

Das CPS bespricht die Policies und die technischen, prozedur-und organisationsbezogenen Verfahren der CA für alle angebotenen Zertifizierungsdienste, und dies während der gesamten Gültigkeitsdauer der von der „Citizen 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 Verzeichnis des CSP verfügbar auf der Adresse: http://repository.eid.belgium.be.

Das vorliegende CPS wurde online im Verzeichnis des CSP unter der Adresse http://repository.eid.belgium.be. zur Verfügung gestellt.

Der CSP nimmt die Kommentare über das vorliegende CPS an. Diese sind an folgende Adresse zu richten: CSP für die „Citizen CA“ p/a CERTIPOST, Muntcentruim / Centre Monnaie, B-1000 Brüssel.

Das vorliegende CPS entspricht den formellen Forderungen der Internet Engineering Task Force (IETF) RFC 2527, Version vom 12. Juli 2001, auf Ebene des Formats und des Inhalts. Indem gewisse Abschnittstitel gemäß der Struktur vom RFC 2527 eingeschlossen sind, kann es sein, dass das Thema auf die Anwendung der Zertifizierungsdienste des CSP für die „Citizen CA“ nicht zutrifft. Solche Abschnitte werden mit der Anmerkung „Abschnitt nicht anwendbar“ gekennzeichnet. Kleine redaktionelle Änderungen der RFC 2527-Vorschriften wurden in das vorliegende CPS inseriert, um die Struktur vom RFC 2527 den Bedürfnissen dieses Anwendungsgebiets besser anzupassen.

Nähere mit dem vorliegenden CPS verbundene Informationen sind beim CSP für die „Citizen CA“ p/a CERTIPOST, Muntcentruim / Centre Monnaie, B-1000 Brüssel erhältlich.

1.3 Die Zertifikate des belgischen elektronischen Personalausweises

Das Gesetz vom 19. Juli 1991 bezüglich des Bevölkerungsregisters, der Personalausweise, der Ausländerkarten und der Aufenthaltsgenehmigungen zur Abänderung des Gesetzes vom 8. August 1983 zur Organisation eines Nationalregisters der natürlichen Personen, so wie durch das Gesetz vom 25. März 2003 geändert, hiernach *„Gesetz über die Personalausweise"* genannt, und die königlichen Beschlüsse zur Ausführung des Gesetzes, führt den belgischen elektronischen Personalausweis ein. Der Elektronische Personalausweis (Electronic Identity Card) basiert auf einer Chipkarte, die Informationen im graphischen Format, die auf der Oberfläche der Karte gedruckt sind, sowie Informationen im elektronischen Format in einem in der Karte inserierten Chip enthält. Das Gesetz regiert den juristischen Rahmen für die Ausstellung und die Benutzung des elektronischen Personalausweises. Das vorliegende CPS bespricht die Aspekte der Zertifizierungsverfahren innerhalb der belgischen Gesetzgebung. Bei der Ausführung ihrer Rolle als CSP für die „Citizen CA" ist CERTIPOST vor allem gehalten, die Verfügungen des Gesetzes einzuhalten.

Auf den elektronischen Personalausweisen befinden sich zwei Arten von Zertifikaten, mit denen die Inhaber der Personalausweise je nach ihrem Alter (i) sich identifizieren können und (ii) eine elektronische Unterschrift benutzen können:

- Ein Identitätszertifikat: Der Inhaber des elektronischen Personalausweises kann dieses Zertifikat benutzen, um sich bei elektronischen Transaktionen zu identifizieren, wenn er bei Beantragung des elektronischen Personalausweises das Alter von 6 Jahren erreicht hat. Das Identitätszertifikat enthält die Identität des Inhabers sowie den öffentlichen Schlüssel, der dem Privatschlüssel entspricht, der zur Identifizierung eines eID-Benutzers auf der Karte gespeichert ist. Dieser Privatschlüssel darf nur benutzt werden, um einen Benutzer des Personalausweises zu identifizieren.
- Ein Qualifiziertes Zertifikat für Elektronische Unterschriften (oder E-Signatures): Dieses Zertifikat enthält die Identität des Inhabers und den öffentlichen Schlüssel, der dem Privatschlüssel entspricht, der nur zur Erstellung einer elektronischen Unterschrift auf der Karte gespeichert ist. Dieses Zertifikat wird gemäß der europäischen Richtlinie 99/93/CE Qualifiziertes Zertifikat genannt. Das qualifizierte Zertifikat für elektronische Unterschriften entspricht den Verfügungen des Gesetzes und der europäischen Richtlinie 1999/93 und kann auf dem Personalausweis aktiviert werden, sobald der Bürger das Alter von 18 Jahren erreicht hat..

Die strengsten Forderungen in Sachen Sicherheit empfehlen, für die elektronische Unterschrift ***nicht*** die Identitätszertifikate sondern ein getrenntes qualifiziertes Zertifikat zu benutzen. Das ist der Grund, weshalb das Identitätszertifikat den Status eines qualifiziertes Zertifikats nicht erhielt, was es allen betreffenden Parteien ermöglicht, das Identitätszertifikat von dem Qualifizierten Zertifikat für Elektronische Unterschrift klar zu unterscheiden.

Der Bürger hat die Wahl ob er die Zertifikate auf seinem elektronischen Personalausweis aktivieren will. Demzufolge kann ein Bürger sich dazu entscheiden, die Benutzung der Schlüssel und der Zertifikate auf seinem Personalausweis zu „aktivieren" oder nicht.

Die Technologie, die für die Zertifizierungsdienste für diese Zertifikate benutzt wird, ist die „PKITechnologie". PKI (**P**ublic **K**ey **I**nfrastructure) ist das Akronym für ein System zur Sicherung von Öffentlichen Schlüsseln (Public Key) kombiniert mit einer Infrastruktur, die dazu konzipiert wurde, für die übermittelten und gespeicherten elektronischen Informationen eine Sicherheitsstufe zu bieten, die hoch genug ist, um das Vertrauen, das Unternehmen, Verbraucher, Regierungen und Gerichte solchen Informationen schenken, zu rechtfertigen.

Die Instanz, die die Zertifikate ausstellt, wird Zertifizierungsstelle (CA, Certification Authority) genannt. Die Instanz die beauftragt ist mit der Identifizierung der Person, die einen Zertifikatsantrag einreicht, wird Registrierungsstelle (RA, Registration Authority) genannt. In diesem Kontext wird die Rolle des Zertifikatsausstellers von CERTIPOST übernommen. Die Rolle der RA wird vom RRN übernommen. Jedoch ist im Kontext des belgischen elektronischen Personalausweises nur die RA dazu befugt, die „Citizen CA" dazu aufzufordern, einem Bürger ein Zertifikat auszustellen.

Die RA nimmt die physische Identifizierung des Antragstellers selbst nicht vor, sondern delegiert diese Verantwortung an die Örtlichen Registrierungsstellen (LRA, Local Registration Authorities). In diesem Kontext werden die Gemeindeverwaltungen als LRA fungieren. Als solche werden die Gemeindeverwaltungen als Schnittstelle zwischen den Antragstellern (d.h. den Bürgern) und der RA dienen.

1.4 Verhältnis zwischen dem vorliegenden CPS und anderen Dokumenten

Wie hiervor beschrieben, stellt das vorliegende CPS eine einseitige Erklärung an die Öffentlichkeit im Allgemeinen dar, die sich auf die Handlungsweisen bezieht, die vom CSP für die „Citizen CA“ befolgt werden, wenn er Zertifizierungsdienste leistet. Es handelt sich um eine ausführliche Beschreibung der Art und Weise, mit der der CSP seine Dienste zur Verfügung stellt.

Entsprechend der ausführlicheren Beschreibung hiernach dient das RRN, im Einvernehmen mit den Gemeindeverwaltungen, als RA auf dem Gebiet des CSP unter Ausschluss aller anderen. Allein das RRN und die Gemeindeverwaltungen können über die Ausstellung eines Zertifikats aufgrund des vorliegenden CPS entscheiden. Allein das RRN, die Gemeindeverwaltungen oder der CSP können über die Aussetzung und den Widerruf eines Zertifikats aufgrund des vorliegenden CPS entscheiden.

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

1.5 Positionierung der „Citizen CA“ in der CA-Hierarchie

Zur vollen Nutzung des belgischen elektronischen Personalausweises gehört es sich, sowohl von der Identität des Bürgers wie von der Identität der technischen Infrastruktur, d.h. der bei den Anwendungen des belgischen Staates erforderlichen Server zu vergewissern. Deshalb müssen verschiedene Zertifikatstypen außer den Bürgerzertifikaten (Citizen Certificates) benutzt werden. Die „Citizen CA“ gehört zu einem breiteren Bereich der Zertifizierungsstellen der Belgischen Föderalen Behörde. Um eine Atmosphäre des Vertrauens zwischen den verschiedenen beteiligten Zertifizierungsstellen zu fördern, hat die Belgische Föderale Behörde eine CA-Hierarchie aufgestellt.

Oben in dieser Hierarchie steht das Stammzertifikat genannt “Belgium Root CA“ (BRCA), dessen Ziel unter anderem es ist, das Vertrauen zwischen den verschiedenen Zertifizierungsstellen innerhalb des Bereichs der Belgischen Föderalen Behörde zu erwirken. Die (selbst unterschriebene) BRCA hat jeden der Privatschlüssel der Zertifizierungsstellen im Bereich der Belgischen Föderalen Behörde, einschließlich der „Citizen CA“, zertifiziert. Durch Gültigerklärung des Zertifikats einer solchen CA kann das Vertrauen zur BRCA ebenfalls auf die CA angewandt werden, die sie zertifiziert hat. In dem Maße, wo die BRCA das Vertrauen genießt, kann dem Zertifikat des Endbenutzers ebenfalls Vertrauen geschenkt werden.

Das Vertrauen zur BRCA innerhalb der Softwareanwendungen wird ebenfalls über ein „Root Sign“-Zertifikat erwirkt, das von einem Drittanbieter (CYBERTRUST – BALTIMORE ; digicert) hergestellt wird, dessen Wurzel in die Anwendungssoftware reichlich integriert wurde.

Die BRCA operiert nach Verfahrensweisen, die in einem dedizierten CPS veröffentlicht wurden, das auf http://repository.eid.belgium.be verfügbar ist.

Bezüglich der Einführung einer zusätzlichen BRCA verweisen wir auf Abschnitt 1.1.3 und Kapitel 7 ZERTIFIKAT UND CRL-PROFILE.

Das Vertrauen zu den Bürgerzertifikaten kann wie folgt überprüft werden:

1. Herstellung eines gesicherten Weges

Das Bürgerzertifikat wird kontrolliert, um zu prüfen, dass sie tatsächlich von der „Citizen CA“ ausgestellt wurde. Dementsprechend wird das Zertifikat der „Citizen CA“ mit dem Ziel

kontrolliert, sich zu vergewissern, dass sie tatsächlich von der BRCA ausgestellt wurde. Wenn das Ergebnis dieser Kontrollen sich als positiv erweist, kann das der BRCA geschenkte Vertrauen über die „Citizen CA“ das Bürgerzertifikat weiter geschenkt werden.

Überprüfung des BRCA-Zertifikats:

Im Allgemeinen wird das BRCA-Zertifikat im Zertifikatsspeicher der Anwendung als Vertrauensbescheinigung erwähnt. Im unwahrscheinlichen Fall, wo der Endbenutzer von der Tatsache benachrichtigt würde, dass das BRCA-Zertifikat nicht mehr gültig wäre, braucht er nur, das BRCA-Zertifikat aus dem Zertifikatespeicher zu löschen, um diesen Bereich von seinen Vertrauensbereichen auszuschließen, um sich zu vergewissern, dass dieser Teil der Überprüfung gescheitert ist.

2. Die Überprüfung des „Citizen CA“-Zertifikats kann vorgenommen werden, indem folgende Maßnahmen getroffen werden:

- 2.1 Kontrolle der Gültigkeit des „Citizen CA“-Zertifikats (z.B. Prüfung des Ablaufdatums)
- 2.2 Kontrolle des Status des „Citizen CA“-Zertifikats (z.B. Prüfung der Sperrung oder des Widerrufs).[6]

3. Die Überprüfung des Bürgerzertifikats kann vorgenommen werden, indem folgende Maßnahmen getroffen werden:

- 3.1 Kontrolle der Gültigkeit des Bürgerzertifikats (z.B. Prüfung der Gültigkeitsperiode).
- 3.2 Kontrolle des Status des Bürgerzertifikats (z.B. Prüfung der Sperrung oder des Widerrufs).

Im Allgemeinen werden die meisten oder alle Operationen durch die Anwendung, für welche die Zertifikate benutzt werden, automatisch ausgeführt, so dass fast kein Zwischenkommen des Endbenutzers nötig ist, wenn überhaupt.

Die Vertrauenshierarchie der Bürgerzertifikate folgt der folgenden Architektur:

1. Eine kleine Hierarchie, für welche alle zur Offline-Gültigerklärung der Bürgerzertifikate erforderlichen Informationen auf die Karte gespeichert werden können.

2. Ein starker Vorzug für automatisches Vertrauen in Zertifikate, die durch die Infrastruktur des belgischen Staates ausgestellt werden. Für die Online-Überprüfung ist kein Zwischenkommen des Endbenutzers notwendig. Diese komplexere Hierarchie wird in Abbildung 1 beschrieben:

[6] Die von der CA geleisteten Dienste zur Statusüberprüfung werden in Kapitel 4.10 (Dienste für Zertifikatsstatus) auf Seite 25 beschrieben.

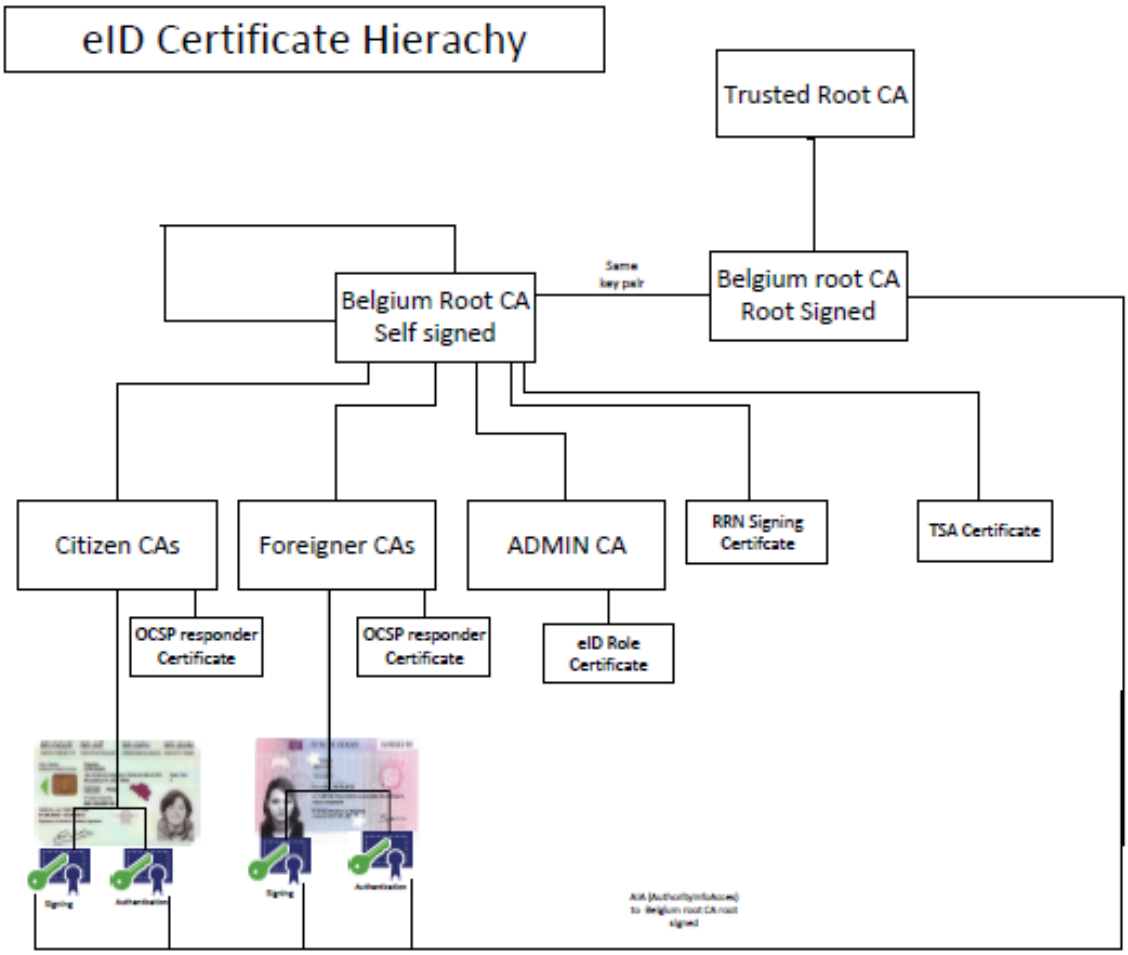

Abbildung 1: PKI-Hierarchie

Um diesen beiden Erfordernissen zu genügen, sieht die eID-Hierarchie die Kombination eines Modells in zwei oder drei Schichten vor.

Im Zweischichtenmodell bilden die „Citizen CA“ und die selbst unterschriebene Belgium Root CA[7] eine
Hierarchie, die im Offline-Modus die Bestätigung der eID Signaturzertifikate und der Authentifizierungszertifikate ermöglicht. In diesem Modell ist der Schlüssel der Belgium Root CA selbst unterschrieben. In diesem Fall kann die Partei, die die Bestätigung vornimmt (z.B. der Zollbeamte, der Polizeioffizier, usw.) die selbst unterschriebene BRCA-Bescheinigung seines eigenen elektronischen Personalausweises benutzen, um das „Citizen CA“-Zertifikat und die Bürgerzertifikate der zu bestätigenden Karte zu bestätigen.

Im Dreischichtenmodell bilden die „Citizen CA“, die Belgium Root CA mit unterschriebener Root und die Cybertrust-Baltimore ; digicert Root CA die Hierarchie. In diesem Modell wird dieses Mal derselbe Privatschlüssel, der für die selbst unterschriebene Belgium Root CA benutzt wird, durch die Cybertrust-Baltimore ; digicert Root CA bestätigt. Diese Arbeitsweise ermöglicht die

[7] Ein selbstunterschriebenes Zertifikat ist eine Zertifikat, die mit dem Privatschlüssel der zertifizierten Entität selbst unterschrieben wird. Da es in der Vertrauenshierarchie keinen höheren Vertrauenspunkt gibt, kann dieses Zertifikat oder jedes Zertifikat, die eine niedrigere Position in der Hierarchie hat, kein Vertrauen geschenkt werden, wenn dieses selbstunterschriebene Zertifikat nicht zuverlässig ist. Es handelt sich aber dabei um einen Fall, der sehr selten vorkommen soll.

automatische Bestätigung bei den meisten allgemein benutzten Anwendungen, wie zum Beispiel Suchmaschinen, weil diese das Cybertrust-Baltimore ; digicert Top Root CA-Zertifikat bereits erkannt haben und sie in ihrer Liste von vertrauten Zertifikaten erscheint. Genauso wie die „Citizen CA“ über die BRCA das Vertrauen erhält, erhält die BRCA das Vertrauen über die CybertrustBaltimore ; digicert Root CA. Dieses dreiteilige Modell schließt die Notwendigkeit aus, das selbst unterschriebene Belgium Root CA-Zertifikat individuell einzuführen.

Weil die selbst unterschriebene Belgium Root CA und die Belgium Root CA mit unterschriebenem Root dasselbe Schlüsselpaar benutzen, sei es mit zwei verschiedenen Zertifikaten, kann das Zertifikat, die mit dem Privatschlüssel dieses Schlüsselpaares unterschrieben wird, mit beiden Belgium Root-Zertifikaten bestätigt werden.

Meistens wird der Entwickler der Anwendung eines der beiden zu benutzenden Modelle vorgesehen haben und der Endbenutzer wird nicht zwischen beiden Modellen wählen müssen.

1.6 Name und Identifizierung des Dokuments

Das vorliegende CPS kann von irgendwelcher Partei über die folgenden OIDs identifiziert werden[8]:

- OID 2.16.56.10.1.1.2 für von BCRA3 unterzeichnete Citizen CA Zertifikate □OID 2.16.56.10.1.1.2.1 für elektronische Bürgersignaturzertifikate.
- OID 2.16.56.10.1.1.2.2 für Bürgeridentitätszertifikate.

- OID 2.16.56.12.1.1.2 für von BRCA4 unterzeichnete Citizen CA Zertifikate □OID 2.16.56.12.1.1.2.1 für elektronische Bürgersignaturzertifikate.
- OID 2.16.56.12.1.1.2.2 für Bürgeridentitätszertifikate.

1.7 PKI-Teilnehmer

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

1.7.1 CSP für die Citizen CA

Eine Zertifizierungsstelle ist eine Anstalt, die digitale Zertifikate ausstellt, die in der Öffentlichkeit, in einem kommerziellen Kontext oder im Rahmen von Transaktionen benutzt werden. Bei der „Citizen CA“ handelt es sich um eine solche Zertifizierungsstelle.

Der CSP ist zur Ausstellung von Bürgerzertifikaten ermächtigt. Diese Genehmigung wird durch die Belgium Root Certification Authority (hiernach „BRCA“ genannt) gewährt.

Der CSP garantiert die Verfügbarkeit aller Dienstleistungen in Verbindung mit den Zertifikaten, einschließlich der Ausstellung, des Widerrufs, der Statusüberprüfung und der Anbringung von Zeitstempeln, sobald sie bei spezifischen Anwendungen verfügbar oder erforderlich werden.

Der CSP wird entsprechend den Bestimmungen von Artikel 20 des Gesetzes über die elektronischen Unterschriften kontrolliert.

Der CSP ist in Belgien ansässig. Er kann unter der im vorliegenden CPS veröffentlichten Adresse kontaktiert werden. Zur Leistung der CA-Dienste, die die Ausstellung, die Sperrung, den Widerruf, die Erneuerung und die Statusüberprüfung von Zertifikaten umfasst, bewirtschaftet

[8] Object IDentifier = Gegenstandsidentifizierer.

der CSP ein gesichertes System und sieht ein Hilfezentrum in Belgien vor, um die Kontinuität der CA-Dienste zu gewährleisten.

Das Verantwortungsgebiet des CSP umfasst die allgemeine Verwaltung der Lebensdauer der Zertifikate, einschließlich:

- der Ausstellung;
- der Sperrung/Aufhebung der Sperrung;
- des Widerrufs;
- der Statusüberprüfung (Dienst für Zertifikatstatus); □des Verzeichnisdienstes.

1.7.2 Lieferant des Root Sign Zertifikats

Der Lieferant des „Root Sign“ Zertifikats garantiert das Vertrauen zur BRCA in weit verbreiteten Anwendungen. Der Lieferant des Root Sign Zertifikats sorgt dafür, dass diese Anwendungen ihr Vertrauen zu seiner Root behalten und benachrichtigt die RA von allen Ereignissen, die das Vertrauen zu seinem eigenen Root beeinflussen. Der Root Sign-Lieferant der BRCA ist CYBERTRUST-BALTIMORE ; digicert (http://cybertrust.omniroot.com/repository/).

1.7.3 Registrierungsstelle und örtliche Registrierungsstellen

Das RRN (Nationalregister) und die Gemeindeverwaltungen sind die RA innerhalb des CSPBereiches für die „Citizen CA“ unter Ausschluss jedweder Anstalt. Das RRN ist konstituiert und handelt entsprechend den Verfügungen und des „Gesetzes über die Personalausweise“ *vgl. 1.3*..

Nur das RRN und die Gemeindeverwaltungen können über die Ausstellung eines Zertifikats im Sinne des vorliegenden CPS entscheiden. Allein das RRN, die Gemeindeverwaltungen oder der CSP können über die Sperrung und den Widerruf eines Zertifikats im Sinne des vorliegenden CPS entscheiden.

Das RRN (Nationalregister) und die Gemeindeverwaltungen sind die RA innerhalb des CSPBereiches für die „Citizen CA“ unter Ausschluss jedweder Anstalt. Die LRAs registrieren und überprüfen die Daten des Bürgers im Namen der RA. Was die Registrierung betrifft, haben die LRAs keinen einzigen unmittelbaren Kontakt mit der „Citizen CA“.

Die RA legt der „Citizen CA“ die nötigen Angaben zur Generierung und zum Widerruf der Zertifikate vor.

Die LRAs (Gemeindeverwaltungen) arbeiten unmittelbar mit den Bürgern, um dem Endbenutzer öffentliche Zertifizierungsdienste anzubieten. Die Aufgaben der LRAs sind hauptsächlich die folgenden:

- Sendung eines Schreibens an den Bürger, das ihn zur Kontaktaufnahme mit dem geeigneten Verwaltungsdienst auffordert, zum Beispiel, wenn der Personalausweis des Bürgers erneuert werden muss;
- Einhaltung aller zum Ausfüllen der Basisdokumente erforderlichen Prozeduren[9]. Danach heißt der Bürger das Basisdokument gut. Die LRA sendet dann die gesicherten Daten des Basisdokuments an den Ausweispersonalisierer, um den Zertifikatsantrag weiter zu bearbeiten. Der Ausweispersonalisierer stellt einen Personalausweis erst nach Genehmigung durch die RA aus. Diese Genehmigung wird vom Ausweispersonalisierer beantragt;
- Das Verfahren anfassen, um die Statusveränderung eines Zertifikats über die RA bei der CA zu beantragen;
- Übergabe der ausgestellten elektronischen Personalausweise an die Bürger.

[9] Das Basisdokument dient dazu, Informationen zu sammeln, die die Ausstellung eines Personalausweises ermöglichen. Der Öffentliche Föderale Dienst Inneres übermittelt den Gemeindeverwaltungen das Modell dieses Dokuments.

Die RA arbeitet indirekt mit den Bürgern und direkt mit der CA zusammen, um dem Endbenutzer öffentliche Zertifizierungsdienste anzubieten. Die Aufgaben der RA sind hauptsächlich folgende:

- Aufstellung eines Hilfsdienstes, wo der Inhaber des elektronischen Personalausweises den Verlust, Diebstahl oder die Zerstörung seines elektronischen Personalausweises melden kann, wenn er dies nicht bei der Gemeindeverwaltung oder bei der Polizei tun kann. Dieser Hilfsdienst wird hiernach „RA Helpdesk“ genannt;
- Registrierung der Bürger für Zertifizierungsdienste;
- Fordert die CA auf, bei Genehmigung eines Antrags ein Zertifikat auszustellen;
- Setzt die Prozedur zum Widerruf eines Zertifikats in Gang und fordert die CA auf, ein Zertifikat zu widerrufen oder sperren.

Die RA legt der „Citizen CA“ die zur Ausstellung der Zertifikate erforderlichen Angaben vor. Für jedes Zertifikat liefert die RA die Identität des Inhabers und die Seriennummer des erforderliches Zertifikat sowie den öffentlichen Schlüssel, der mit dem in besagter Zertifikat zu vermerkenden Bürger verbunden ist.

Alle Kommunikationen zwischen der LRA, der RA und der CA, die eine der Phasen des Lebenszyklus von Bürgerzertifikate betreffen, werden durch Verschlüsselungs- und Unterschriftstechniken gesichert, die auf einem kryptografischen System mit öffentlichem Schlüssel basieren, um Vertraulichkeit und gegenseitige Authentifizierung zu garantieren. Es handelt sich um Informationsaustausche bezüglich des Antrags, der Ausstellung, der Sperrung, der Aufhebung der Sperrung und des Widerrufs von Zertifikaten.

1.7.4 Ausweispersonalisierer

Der Ausweispersonalisierer macht intelligente nicht personalisierte Ausweise zu personalisierten elektronischen Personalausweisen, indem er die Identitätsangaben und das Foto des Bürgers auf den Ausweis druckt. Der Ausweispersonalisierer ist ebenfalls für die gesicherte Übermittlung dieser personalisierten Ausweise an den Ausweisinitialisierer verantwortlich. Zur Zeit wird die Rolle des Ausweispersonalisierers aufgrund einer mit der Belgischen Föderalen Behörde abgeschlossenen Rahmenvereinbarung von der AG ZETES[10] erfüllt.

1.7.5 Ausweisinitialisierer

Der Ausweisinitialisierer leistet folgende Dienste:

- Generierung der für den Ausweis erforderlichen Schlüsselpaare;
- Speicherung der beiden eID-Bürgerzertifikate auf dem Ausweis;
- Generierung der persönlichen Aktivierungscodes des Antragstellers und der Gemeindeverwaltung und des anfänglichen PIN-Codes des Antragstellers;
- Laden der aktiven Stammzertifikate der Behörde auf den Ausweis;
- Lieferung des elektronischen Personalausweises an die Gemeindeverwaltung;
- Lieferung des persönlichen Aktivierungscodes und des PIN-Codes an den Antragsteller;
- Aufnahme der Angaben im Register der Personalausweise.

Zurzeit wird die Rolle des Ausweisinitialisierers aufgrund einer mit der Belgischen Föderalen Behörde abgeschlossenen Rahmenvereinbarung von der AG ZETES erfüllt.

[10] http://www.zetes.com

1.7.6 Benutzer

Die Benutzer der CA-Dienste im „Citizen CA“-Bereich sind Bürger, die Inhaber eines elektronischen Personalausweises mit gemäß dem Gesetz über die Personalausweise aktivierte Zertifikate sind. Weiter im vorliegenden Dokument kann das Wort „Benutzer“ durch das Wort „Bürger“ ersetzt werden.

Diese Bürger:

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

Die Bürger haben das Recht, am Anfang des Antrags auf ihren elektronischen Personalausweis anzugeben, ob sie Bürgerzertifikate möchten. Der elektronische Personalausweis wird den Bürgern geliefert mit geladenen Bürgerzertifikaten. Bei Bürgern, die die Bürgerzertifikate nicht benutzen wollen, werden diese Zertifikate widerrufen.

Für Bürger, die das Alter von 6 Jahren noch nicht erreicht haben, werden bei einem Antrag auf einen elektronischen Personalausweis die Zertifikate zur Identifizierung und elektronischen Unterschrift nicht installiert.

Für Bürger, die zwischen 6 und 18 Jahre alt sind, wird das Zertifikat für elektronische Unterschrift nicht installiert.

1.7.7 Vertrauende Parteien

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

Vertrauende Parteien müssen die Gültigkeit eines digitalen Zertifikats, das sie empfangen haben, stets prüfen, basierend auf die Gültigkeitsperiode des Zertifikats und die Gültigkeitserklärung des Zertifikats durch den CA-Dienst (über OCSP, CRL, Delta CRL oder WebSchnittstelle), bevor Sie Informationen vertrauen, die in ein Zertifikat aufgenommen sind.

1.8 Benutzung der Zertifikate

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

Die von der „Citizen CA“ ausgestellten Identifizierungszertifikate können für spezifische Verrichtungen mit elektronischer Identifizierung gebraucht werden, die Zugang zu den Webseiten verschaffen und andere Online-Inhalte, E-Mails, usw. unterstützen. Diese werden immer von der Belgischen Föderalen Behörde zur Verfügung gestellt. Die gegenwärtigen Vorschriften in Sachen Sicherheit empfehlen, Identitätszertifikate ***nicht*** für elektronische Unterschriften zu gebrauchen. Der CSP für die „Citizen CA“ übernimmt deshalb den vertrauenden Parteien gegenüber in allen Fällen, wo die Identitätszertifikate zur Generierung von elektronischen Unterschriften benutzt wird, keine Haftung.

1.9 Administrative Verwaltung

Die administrative Verwaltung ist CERTIPOST vorbehalten. Kontaktdaten:

☐ Per Post:

Certipost nv / sa

Policy administration - Citizen CA

Centre Monnaie
1000 Brüssel

☐ Per E-Mail:

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

1.10 Begriffe und Akronyme

Am Ende dieses CPS finden Sie eine Liste mit Definitionen und Akronymen.

2 HAFTUNG IN SACHEN VERÖFFENTLICHUNG UND ARCHIVIERUNG

Der CSP veröffentlicht Informationen über die digitale Zertifikate, die er ausstellt. Diese Informationen sind in einem oder mehreren Online-Archiven in der Internet-Domain "eid.belgium.be" zu finden und sind für die Öffentlichkeit zugänglich. Die CA behält sich das Recht vor, Informationen über den Status der Zertifikate in Drittrepertorien zu veröffentlichen.

Der CSP behält ein Online-Repertorium der Dokumente, in denen er gewisse Aktivitäten und Prozeduren sowie den Inhalt gewisser Aspekte seiner Politik, einschließlich seines CPS, die 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.

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 digitaler Zertifikate, so wie im vorliegenden CPS angegeben.

Die CA stellt ein Verzeichnis aller Zertifikate auf, die sie ausgestellt hat, und sorgt für dessen Instandhaltung. Dieses Verzeichnis zeigt auch den Status eines ausgestellten Zertifikats.

Die CA veröffentlicht CRLs[11] in regelmäßigen Abständen auf http://crl.eid.belgium.be. Die CA veröffentlicht regelmäßig Delta CRLs, die die seit der Veröffentlichung der vorherigen CRL oder Delta CRL angebrachten Änderungen enthält. Jede neue veröffentlichte CRL enthält alle Aktualisierungen der vorherigen Delta CRLs.

Die CA stellt einen OCSP[12]-Server zur Verfügung unter http://ocsp.eid.belgium.be/2, um über den Status einer auf Antrag einer vertrauenden Partei ausgestelltes Zertifikat gemäß IETF RFC 6960 zu informieren. Der Status eines Zertifikats kann auch unter der folgenden Adresse überprüft werden: http://status.eid.belgium.be. Der Status eines Zertifikats, die in einer CRL oder einer Delta CRL aufgeführt ist, muss den vom OCSP-Server gelieferten Informationen entsprechen.

Die CA bewahrt die CRL und die Informationen auf dieser URL, bis jedes Zertifikat, die die CRL enthält, verfällt. Gutgeheißene Versionen von Dokumenten, die im Archiv veröffentlicht werden müssen innerhalb von 24 Stunden im Verzeichnis platziert werden.

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

2.1 Kontrolle des Zugangs zu den Archiven

Obwohl der CSP alles einsetzt, damit der Zugang zu den veröffentlichten Angaben kostenlos bleibt, könnte er im Rahmen seines Vertrags mit der Regierung solche Dienste wie die Veröffentlichung von Statusinformationen in Datenbanken von Drittparteien, Privatverzeichnisse, usw. zahlen lassen.

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

[11] Eine CRL oder Zertifikatswiderrufsliste (Certificate Revocation List) ist eine Liste, die von einer CA ausgegeben und digital unterzeichnet wird und die Seriennummern der widerrufenen und gesperrten Zertifikaten umfasst. Die vertrauenden Parteien müssen diese Liste systematisch zu Rate ziehen, bevor sie auf die Informationen vertrauen, die in einem Zertifikat aufgenommen sind.

[12] Das Online-Protokoll für Zertifikatstatus (RFC 6960) ist eine unmittelbare Quelle für Statusinformationen, um den jetzigen status eines digitales Zertifikat zu bestimmen, ohne auf CRLs zuzugreifen.

Im Rahmen des Vertrags mit der Belgischen Föderalen Behörde ist der Zugang zu den vom CSP 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. Insbesondere:

Die Anzahl von OCSP-Anträgen durch eine einzige Person ist auf 10 Anträge pro Tag begrenzt. Die CA kann die Verarbeitung von OCSP-Anträgen für eine Partei nicht beschränken, die aufgrund ihrer Aktivitäten genötigt ist, den OCSP-Status regelmäßig zu überprüfen.

Die Anzahl der Anträge auf Zertifikatstatusüberprüfung per Internet durch einen Benutzer ist auf 10 Anträge pro Tag begrenzt.

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1 Benennung

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

3.2 Anfängliche Gültigkeitserklärung der Identität

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

3.3 Identifizierung und Authentifizierung für Anfragen nach neuen Schlüsseln

Die Identifizierung und Authentisierung des Bürgers der eine Neu-Verschlüsselung anfragt wird ausgeführt entsprechend des Verfahrens das in der RA spezifiziert und in den LRAs implementiert ist.

3.4 Identifizierung und Authentifizierung für Widerrufungs- und Aussetzungsanträge

Die Identifizierung des Bürgers, der einen Widerruf oder eine Sperre seiner Bürgerzertifikate beantragt, erfolgt in Übereinstimmung mit den Prozeduren und Regeln, die auf die Ausstellung von elektronischen Personalausweisen anwendbar sind.

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

- die Gemeindeverwaltung,
- die Polizei,
- das RA-Helpdesk, das hierfür von der RA eingerichtet wird.

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

4 OPERATIONELLE ERFORDERNISSE FÜR DEN LEBENSZYKLUS EINES ZERTIFIKATS

Alle Entitäten im Befugnisbereich des CSP, einschließlich der LRAs, Bürgern, 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 nimmt die Ausstellung, den Widerruf oder die Sperre von Zertifikaten nur auf Anfrage der RA vor, unter Ausschluss jeder anderen Behörde, es sei denn die RA oder der CSP andere ausdrückliche Anweisungen gibt.

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

4.1 Zertifikatsantrag

Der Einschreibeprozess, den der Bürger durchlaufen muss, um die Zertifikate zu beantragen, ist Bestandteil der Prozeduren für die Bearbeitung des elektronischen Personalausweises durch seine Gemeindeverwaltung, d.h. die LRA. Die Prozedur, die die LRA für die Einschreibung der Bürger befolgt, wird von der RA vorgesehen.

4.2 Bearbeitung des Zertifikatsantrags

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

Wenn ein Zertifikat beantragt wird, kann die LRA den Antrag für elektronischen Personalausweis genehmigen oder ablehnen. Dies bringt auch die Genehmigung oder Ablehnung des Zertifikatsantrags 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.

4.3 Ausstellung des Zertifikats

Nach Genehmigung eines Zertifikatsantrags 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 Zertifikatsantrag zuweist, tatsächlich eine einmalige Seriennummer ist, die nicht vorher für ein anderes Bürgerzertifikat 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 das durch die RA zugewiesene Seriennummer für das Zertifikat, enthält.

Nach der Ausstellung eines Zertifikats, kündigt dies die CA in einem Archiv an und stellt das Zertifikat aus. Das Zertifikat wird dann an die RA übermittelt.

Die RA bittet den Ausweisinitialisierer darum, die Bürgerzertifikate auf den elektronischen Personalausweis zu laden. Der Ausweisinitialisierer übermittelt der LRA über einen gesicherten Weg den elektronischen Personalausweis mit den Bürgerzertifikaten.

4.4 Annahme der Zertifikate

Nach Erstellung des elektronischen Personalausweises ist dieser noch nicht aktiviert. Die LRA aktiviert den elektronischen Personalausweis im Beisein des Bürgers durch Aktualisierung des Status in der RA-Identitätsdatenbank. Sowohl der Bürger wie die RA brauchen die Aktivierungsangaben für den Ausweis. Diese Angaben werden vom Ausweisinitialisierer über einen gesicherten Weg geliefert. Der Ausweis kann nur mittels der kombinierten Aktivierungsangaben der LRA und des Bürgers aktiviert werden.

Nur der Bürger (bei Antrag auf einen elektronischen Personalausweis für Bürger ab 12 Jahren) oder die Person/Personen, die die elterliche Gewalt über ein Kind unter 12 Jahren ausübt/ausüben (bei Antrag auf einen elektronischen Personalausweis für Bürger bis 12 Jahren),kann/können entscheiden, die Bürgerzertifikate zu aktivieren oder nicht. Wenn die Bürgerzertifikate nicht aktiviert werden, kann der Zugang zu gewissen Diensten, die die Belgische Föderale Behörde und andere Lieferanten als Drittparteien auf Basis der eIDInfrastruktur in Belgien und im Ausland anbieten, begrenzt werden.

Um die Bürgerzertifikate zu aktivieren, muss ein Antrag auf Aufhebung der Sperrung über die RA bei der CA eingereicht werden. Nach Aktivierung der Zertifikate kann der Bürger die Bürgerzertifikate und deren Inhalt bestätigen. Falls die Bestätigung erfolgreich ist, gilt das Zertifikat als angenommen.

Ein Zertifikat kann zum Beispiel abgelehnt werden, wenn die Angaben bezüglich des Bürgers nicht richtig sind oder der Bürger das rechtmäßige Alter für die Verwendung des Zertifikats nicht erreicht hat.

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

4.5 Schlüsselpaare und Benutzung der Zertifikate

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

4.5.1 Rechte und Pflichten des Bürgers

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

- Er darf keine Zertifikate verfälschen;
- Er darf die Zertifikate ausschließlich zu gesetzlich genehmigten Zwecken unter Einhaltung des CPS benutzen;
- Er muss ein Zertifikat im Rahmen des Angemessenem unter Berücksichtigung der Umstände benutzen;
- Er muss Risiken, Verlust, Enthüllung, Änderung oder irgendwelchen anderen unbefugten Gebrauch seiner Privatschlüssel vermeiden.

4.5.2 Rechte und Pflichte der vertrauenden Partei

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 der Prozedur zur Bestätigung des vollständigen Zertifikatspfad;
- wird auf ein Zertifikat nur dann vertrauen, wenn dies nicht gesperrt oder widerrufen worden ist;
- wird sich im Rahmen des Angemessenen unter Berücksichtigung der Umstände auf ein Zertifikat vertrauen.

4.6 Erneuerung von Zertifikaten

Die Bürgerzertifikate werden erneuert, wenn:

o die elektronische Unterschrift erneuert wird, o der Bürger eine Erneuerung beantragt, nachdem die Zertifikate widerrufen wurden.

4.7 Neuer Schlüssel für Zertifikate

Nach dem Widerruf des Zertifikates kann das Bürgerzertifikat nicht wieder aktiviert werden und muss daher durch ein neues Zertifikat ersetzt werden. Auf Anfrage des Bürgers generiert der LRA ein neues Schlüsselpaar auf dem Elektronischen Personalausweis und ersetzt das widerrufene Zertifikat durch ein neues.

4.8 Änderung eines Zertifikats

Abschnitt nicht anwendbar.

4.9 Widerruf und Sperrung des Zertifikats

Bürgerzertifikate in einem elektronischen Personalausweis bleiben im Sperrungszustand, bis der Bürger sie annimmt oder ablehnt. Ein Bürgerzertifikat muss für zum ersten Mal innerhalb eines Monats nach der Ausstellung aktiviert werden. Die RAs und LRAs sorgen dafür, dass dieser Forderung nachgekommen wird.

Um den Widerruf oder die Sperrung eines Zertifikats zu beantragen, muss der Bürger mit einer LRA, der Polizei oder dem RA-Helpdesk Kontakt aufnehmen. Während die Öffnungszeiten einer LRA begrenzt sind, ist der RA-Helpdesk rund um die Uhr, sieben Tage die Woche zugänglich.

Die Polizei, die LRA oder der RA-Helpdesk beantragen die Sperrung von Bürgerzertifikaten über die RA, nachdem:

- eine Bekanntgabe vom Bürger empfangen worden ist, in der mitgeteilt wird, dass die Vermutung besteht, dass der Privatschlüssel einer oder beider Bürgerzertifikate verloren, gestohlen, geändert oder auf unbefugte Weise enthüllt oder 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;

- eine Bekanntgabe vom Bürger empfangen worden ist, in der mitgeteilt wird, dass der Privatschlüssel einer seiner oder beider seiner Bürgerzertifikate verloren, gestohlen, geändert oder auf unbefugte Weise enthüllt oder kompromittiert worden ist;
- die in einem Bürgerzertifikat 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 CA auf Antrag der RA Bürgerzertifikate sperrt oder widerruft.

Ein gesperrtes Zertifikat wird nach einem Zeitraum von einer Woche, gesperrt wenn sie vom Bürger keine Bekanntgabe der Aufhebung der Sperrung des Zertifikats erhält.

Unter gewissen Umständen (z.B. Vermeiden einer Katastrophe, Risiko für einen CA-Schlüssel, Sicherheitsverletzung, usw.) kann der CSP beantragen, dass Zertifikate gesperrt und/oder widerrufen werden. Der CSP bittet den eID CSP Steering 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 Bürger von dieser Sperrung/diesem Widerruf benachrichtigt werden.

Um den Status der Zertifikate zu kontrollieren, müssen die vertrauenden Parteien OnlineHilfsmittel 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.

4.9.1 Dauer und Ende der Sperrung und des Widerrufs

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

- Der Bürger muss sich dessen sicher sein, dass die Vermutung, dass der Privatschlüssel einer oder beider Bürgerzertifikate verloren, gestohlen, geändert oder auf unbefugte Weise enthüllt oder kompromittiert wäre, unbegründet war;
- Es gibt keinen anderen Grund, die Zuverlässigkeit und die Vertraulichkeit der Privatschlüssel dieser beiden Bürgerzertifikate zu bezweifeln.

Um die Aufhebung der Sperrung seiner Bürgerzertifikate zu beantragen, muss der Bürger mit einer LRA, der Polizei oder der RA-Helpdesk Kontakt aufnehmen.

Die Polizei, die LRA oder der RA-Helpdesk beantragen die Aufhebung der Sperrung von ein paar Bürgerzertifikaten über die RA, nachdem:

- eine Bekanntgabe vom Bürger empfangen worden ist, in der mitgeteilt wird, dass die Vermutung, dass der Privatschlüssel einer oder beider Bürgerzertifikate verloren, gestohlen, geändert oder auf unbefugte Weise enthüllt oder kompromittiert worden wäre, unbegründet war;
- die Vermutung, dass die Informationen einer anderen Person bedroht oder kompromittiert sein wäre, weil die Erfüllung einer Verpflichtung der RA gemäß

dem vorliegenden CPS durch eine Naturkatastrophe, eine EDV-Störung oder einen Kommunikationsfehler oder durch eine andere Ursache, die außerhalb der eigenen Kontrolle der Person liegt, verzögert oder verhindert wurde, unmissverständlich unrichtig zu sein scheint;

- die CA auf Antrag der RA ein paar Bürgerzertifikate sperrt oder widerruft.

Nach einem Zeitraum von einer Woche widerruft die CA ein gesperrtes Zertifikat automatisch, wenn sie in der Zwischenzeit von der RA keine Bekanntgabe der Aufhebung der Sperrung des Zertifikats erhält. Die CA gibt der RA alle vorgenommenen Widerrufe bekannt.

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

4.10 Dienste für Zertifikatsstatus

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

CRL und delta CRL http://crl.eid.belgium.be

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

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

Eine CRL wird alle 24 Stunden zu vereinbarter Zeit veröffentlicht. Eine Delta CRL wird alle 3 Stunden gemäß einem vereinbarten Zeitplan veröffentlicht.

Die CA stellt alle CRLs und Delta CRLs, die in den vorigen 12 Monaten ausgegeben wurden, auf der Webseite zur Verfügung.

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

Die CA stellt dem Belgischen Staat die OCSP-Antworten zur Verfügung. Dieser gebraucht sie über die eigenen Netze der öffentlichen Verwaltung.

Webseite des Statusüberprüfungsdienstes http://status.eid.belgium.be

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 für Statusüberprüfungsdienste zum Gebrauch über und innerhalb der eigenen Netze der öffentlichen Verwaltung dem Belgischen Staat zur Verfügung.

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

4.11 Abgabe und Zurückerhaltung der Schlüssel

Das Abgeben und Abholen der Schlüssel ist nicht zugelassen.

5 VERWALTUNGSKONTROLLEN, OPERATIONELLE UND PHYSISCHE KONTROLLEN

In diesem Kapitel werden die nicht technischen Sicherheitskontrollen beschrieben, die der CSP und andere PKI-Partner für die Generierung von Schlüsseln für die Authentifizierung von Bürgern, die Ausstellung von Zertifikaten für den Widerruf von Zertifikaten, für die Revision und für die Archivierung gebrauchen.

5.1 Physische Sicherheitskontrollen

Der CSP führt physische Kontrollen auf seiner Site aus. Unter die physischen Kontrollen des CSP fallen folgende:

- 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 CSP-Aktivitäten in einem gesicherten EDV-Raum mit physischer Bewachung und Sicherheitsalarmen betreffen, wobei ein Badge und Zugangskontrolllisten gebraucht werden, um sich von einer Zone nach der anderen zu bewegen.
- Redundante Stromversorgung und Klimaregelung.
- Die Räume werden gegen Überflutung geschützt.
- Der CSP trifft Brandschutzmaßnahmen.
- Die Ausrüstungen werden in aller Sicherheit gelagert. Die Backup-Ausrüstungen werden an einem anderen Ort gelagert, der physisch gegen Brand und Überflutung geschützt ist.
- Zur Verhütung jeglicher unerwünschten Verbreitung empfindlicher Daten, werden die Abfälle auf gesicherte Weise vernichtet.
- Der CSP führt das Backup teilweise außerhalb der Site aus.

Die CSP-Rechenzentralen beherbergen die zur Leistung der CA-Dienste nötige Infrastruktur. Der CSP sorgt für geeignete Sicherheitskontrollen an seinen Standorten, mitsamt Zugangskontrolle, Einbruchmeldung 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.

5.2 Prozedurenkontrolle

Der CSP wendet in Sachen Personal und Management Prozeduren 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 CSP einreichen, in der es bestätigt keine gegensätzlichen Interessen beim CSP zu haben, dass es die Vertraulichkeit bewahren und die persönlichen Angaben schützen wird.

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

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

Falls eine Kontrolle gemäß des 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 CSP garantiert, dass alle Handlungen in Verbindung mit dem CSP dem System des CSP und dem CSP-Personalmitglied, das diese Handlung ausgeführt hat, zugewiesen werden können.

Für kritische CSP-Funktionen führt der CSP eine Kontrolle gemäß des 4-Augen-Prinzips.

Der CSP unterscheidet zwischen folgenden Arbeitsgruppen:

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

5.3 Sicherheitskontrollen für das Personal

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

5.3.1 Qualifikationen, Erfahrung, Genehmigungen

Der CSP 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 Hintergrundkontrollen und Genehmigungsprozeduren

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

5.3.3 Ausbildungsbedürfnisse und -prozeduren

Der CSP bietet dem Personal Ausbildungen an, damit dieses seine CA-Funktionen übernehmen kann.

5.3.4 Fortbildungszeitraum und -prozeduren

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

5.3.5 Rotation der Funktionen

Abschnitt nicht anwendbar.

5.3.6 Bestrafung des Personals

Der CSP bestraft das Personal für unbefugte Handlungen, den unbefugten Gebrauch von Befugnis und den unbefugten Gebrauch von Systemen mit dem Ziel, gegebenenfalls das CSPPersonal zur Verantwortung zu ziehen.

5.3.7 Kontrolle der unabhängigen Vertragsparteien

Die unabhängigen Vertragsparteien des CSP und ihr Personal sind Gegenstand derselben Hintergrundkontrollen wie das CSP-Personal. Die Hintergrundkontrollen umfassen:

- Strafrechtliche Verurteilungen wegen Schwerverbrechen;
- Falsche Erklärungen des Bewerbers;
- Richtigkeit der Referenzen;
- Gegebenenfalls, die Genehmigungen;
- Schutz der Vertraulichkeit;
- Vertraulichkeitsbedingungen.

5.3.8 Dokumentation für die anfängliche Ausbildung und die Weiterbildung

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

5.4 Prozeduren für Audit-Logging

Unter die Prozeduren für Audit-Logging fallen unter anderem das Event-Logging und die Systemkontrolle. Diese Prozeduren werden angewandt, um eine sichere Umgebung instand zu halten. Der CSP führt folgende Kontrollen aus:

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

- Ausstellung eines Zertifikats;
- Widerruf eines Zertifikats;
- Sperrung eines Zertifikats;
- Automatischer Widerruf;
- Veröffentlichung einer CRL oder Delta CRL;
- Reaktivierung eines Zertifikats;

Der CSP 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 CSP 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 CSP-Standorts;

- Das Backup und die Herstellung;
- Den Bericht über die Wiederinbetriebnahmetests nach einer Katastrophe;
- Die Kontrollinspektionen;
- Die Erweiterungen und Änderungen der Systeme, Softwares und der Infrastruktur;
- Die Einbrüche und Einbruchsversuche in den gesicherten Zonen.

Andere erforderliche Dokumente für die Kontrollen sind unter anderem:

- Pläne und Beschreibungen der Infrastruktur;
- Pläne und Beschreibungen der Standorte; □ Konfiguration des Materials und der Softwares;
- Zugangskontrolllisten für das Personal.

Der CSP 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 Kontrolleure archiviert. Die Logdateien sind auf geeignete Weise durch einen Zugangskontrollmechanismus zu schützen. Die Logdateien und die Kontrollberichte sind Gegenstand eines Backups.

Kontrollhandlungen werden nicht gemeldet.

5.5 Archivierung der Verzeichnisse

Der CSP bewahrt interne Verzeichnisse der folgenden Elemente auf:

- Alle Bescheinigungen während eines Zeitraums von mindestens 30 Jahren nach Ablauf des Zertifikats;
- Kontrolljournal über die Ausstellung der Zertifikate für einen Zeitraum von mindestens 30 Jahren nach Ausstellung des Zertifikats;
- Kontrolljournal über den Widerruf eines Zertifikats von mindestens 30 Jahren nach Widerruf des Zertifikats;
- CRL und Delta CRL von mindestens 30 Jahren nach deren Veröffentlichung;
- Der CSP muss das letzte Backup der CA-Archive von mindestens 30 Jahren nach Ausstellung des letztes Zertifikats aufbewahren.

Die CA bewahrt die Archive in einem leicht nachzuschlagendem Format auf.

Die CA sorgt für die Integrität der Apparaturen zur physischen Lagerung und gebraucht eigene Kopiersysteme, um den Verlust von Daten vorzukommen.

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

5.5.1 Verzeichnistypen

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

5.5.2 Aufbewahrungszeitraum

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

5.5.3 Archivschutz

Nur der Verzeichnisverwalter (Teammitglied, das mit der Aufbewahrung der Verzeichnisse beauftragt ist) kann Zugang zu den CSP-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 welchen die Archive gelagert sind, wie die regelmäßige Verlegung der Angaben auf ungebrauchte Medien.

Der CSP handelt gemäß der potentiellen Anwendung durch die Belgische Föderale Behörde der Prozedur 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 solchem 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 Bürgerzertifikaten gehören.

5.5.4 Prozeduren für das Backup der Archive

Ein differentielles Backup der Archive der CA wird an Werktagen täglich vorgenommen.

5.5.5 Bedingung zum Anbringen von Zeitstempeln auf den Verzeichnissen

Abschnitt nicht Anwendbar.

5.5.6 Sammlung der Archive

Das System zur Sammlung der CA-Archive ist intern.

5.5.7 Prozeduren zur Erhaltung und Überprüfung der Archivierungsinformationen

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

Die CA bewahrt die Verzeichnisse im elektronischen Format oder auf Papier auf.

5.6 Schlüsselübergabe

Abschnitt nicht anwendbar.

5.7 Risiken und Wiederherstellung nach einer Katastrophe

In einem getrennten internen Dokument spezifiziert die CA die Prozeduren für die Meldung und die
Behandlung von den Zwischenfällen und Risiken. Die CA 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.

Die CA bestimmt die nötigen Maßnahmen, um die vollständige und automatische Wiederherstellung im Falle von Katastrophe, defekten Servern, Softwares und Daten zu gewährleisten.

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

All diese Maßnahmen entsprechen der ISO 1-27001-Norm.

Die CSP 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 InternetKommunikationsprotokolle 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.

5.8 Kündigung der CSP

Sobald die CSP von der Belgischen Föderalen Behörde vernimmt, dass der Vertrag gekündigt werden soll und/oder sobald der Vertrag frühzeitig annulliert wird, wird die CSP den belgischen Staat zu Rate ziehen, um zu bestimmen, welche Schritte erforderlich sind, um (1) eine einwandfreie Übertragung der Dienstleistung an die neue CSP zu gewährleisten und um (2) die Zerstörung, die Entfernung, die Wiederherstellung und/oder die Sicherung der Informationen, personenbezogenen Daten und Dateien, die die CSP im Rahmen ihrer Aufgaben als CSP empfangen hat, zu gewährleisten.

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 CABereiches.

6.1.1 Generierungsprozedur für Privatschlüssel

Die CA benutzt eine zuverlässige Prozedur für die Generierung ihres Root-Privatschlüssels gemäß einer dokumentierten Prozedur. Die CA verteilt die Geheimnisteile ihres (ihrer) Privatschlüssel(s). Der CSP ist dazu befugt, den Inhabern von Geheimnisteilen diese Geheimnisteile gemäß einer dokumentierten Prozedur zu übermitteln.

6.1.1.1 Benutzung des CA-Privatschlüssels

Der Privatschlüssel der „Citizen CA“ wird benutzt, um die ausgestellten Zertifikate, die Zertifikatwiderrufslisten und die OCSP-Zertifikate zu unterzeichnen. Andere Benutzungen sind begrenzt.

6.1.1.2 CA-Privatschlüsseltyp

A. Belgium Root CA 3 (BRCA3)

Für ihren Root-Schlüssel gebraucht die CA, Belgium Root CA 3, den Algorithmus RSA SHA-1 mit einer Schlüssellänge von 4096 Bit.Der erste Privatschlüssel der Belgium Root CA 3 wird für den Zeitraum vom 26. Juni 2013 bis zum 28. Januar 2028 bestätigt.

Für ihren Hauptschlüssel gebraucht die „Citizen CA“ den Algorithmus RSA SHA-1 mit einer Schlüssellänge von 4096 Bit. Die neuen Privatschlüssel der „Citizen CA“ werden für 11 Jahre bestätigt. Ein neuer Schlüssel wird den aktiven ersetzen, bevor der Gültigkeitszeitraum des aktiven Schlüssels unter 10 Jahre fällt.

B. Belgium Root CA 4 (BRCA4)

Für den Belgium Root CA 4 wird der Algorithmus RSA SHA-2 mit einer Schlüssellänge von 4096 Bit verwendet.

Der Privatschlüssel der Belgium Root CA 4 wird für den Zeitraum vom 26. Juni 2013 bis zum 28. Januar 2028 bestätigt.

Für ihren Hauptschlüssel gebraucht die „Citizen CA“ den Algorithmus RSA SHA-2 mit einer Schlüssellänge von 4096 Bit. Die neuen Privatschlüssel der „Citizen CA“ werden für 11 Jahre bestätigt. Ein neuer Schlüssel wird den aktiven ersetzen, bevor der Gültigkeitszeitraum des aktiven Schlüssels unter 10 Jahre fällt.

6.1.2 Generierung des CA-Schlüssels

Die CA generiert und schützt den (die) Privatschlüssel auf gesicherte Weise mit Hilfe eines zuverlässigen Systems und trifft die nötigen Vorkehrungen, um jeden Betrug oder unbefugten Gebrauch ihres (ihrer) Privatschlüssel(s) vorzubeugen. Der Prozess wird von Vertretern der Belgischen Föderalen Behörde überwacht, damit die geeignete und sichere Ausführung der Prozedur zur Generierung des CA-Schlüssels gewährleistet wird. Die CA führt mit diesem CPS Online-Prozeduren aus. Die CA nimmt die auf die Zuverlässigkeit der Systeme anwendbaren öffentlichen, internationalen und europäischen Normen an. Mindestens drei Personen, die eine Vertrauensposition inne haben, nehmen an der Generierung und der Installierung des (der) CAPrivatschlüssel(s) teil.

6.2 Wiedergenerierung und Wiederinstallierung des Schlüsselpaares

Wenn der (die) Geheimschlüssel durch (einen) neue(en) ersetzt wird (werden), muss die CA genau dieselbe Prozedur wie für den ersten befolgen. Die CA muss die früher benutzten Schlüssel sowie die unverfälschbaren Vorrichtungen und alle Backup-Kopien dieser Privatschlüssel unmittelbar außer Betrieb setzen und zerstören, sobald sie verfügbar sind.

6.2.1 Vorrichtungen zur Generierung des CA-Schlüssels

Die Generierung des Privatschlüssels der „Citizen CA“ wird mit Hilfe einer gesicherten kryptografischen Vorrichtung vorgenommen, die den erforderlichen Bedingungen, einschließlich FIPS 140-1 Stufe 3, entspricht.

Die Generierung des CA-Privatschlüssels erfordert die Kontrolle von mehreren befugten Mitgliedern des CA-Teams, die Vertrauenspositionen inne haben, und von mindestens einem Vertreter der CSP. Mehrere Mitglieder der CA-Leitung erteilen die Genehmigung zur Generierung der Schlüssel schriftlich.

6.2.2 Speicherung des CA-Privatschlüssels

Die CA wendet eine gesicherte kryptografische Vorrichtung an, um ihren eigenen Privatschlüssel gemäß den Forderungen FIPS 140-1 Stufe 3 zu speichern.

6.2.2.1 Kontrollen der Speicherung des CA-Schlüssels

Die Speicherung des CA-Privatschlüssels erfordert mehrere Kontrollen durch befugte CSPPersonalmitglieder, die Vertrauenspositionen inne haben. Mehrere Mitglieder der CSP-Leitung erteilen die Genehmigungen für die Speicherung des Schlüssels und das befugte Personal schriftlich.

6.2.2.2 Backup des CA-Schlüssels

Der (die) CA-Privatschlüssel ist (sind) Gegenstand eines Backups, wird (werden) gespeichert und von den befugten CSP-Personalmitgliedern, die Vertrauenspositionen inne haben, abgerufen. Mehrere Mitglieder der CSP-Leitung erteilen die Genehmigungen für die Speicherung des Schlüssels und das befugte Personal schriftlich.

6.2.2.3 Geheimnisteile

Die CA-Geheimnisteile werden von mehreren gefugten Inhabern zur Speicherung und Verbesserung der Zuverlässigkeit der Privatschlüssel aufbewahrt. Die CA bewahrt den (die) Privatschlüssel in mehreren unverfälschbaren Vorrichtungen auf. Mindestens drei CSP-Mitglieder müssen gemeinsam handeln, um den Privatschlüssel der CA zu aktivieren.

Die Privatschlüssel der CA dürfen nicht in die Hände von Dritten gegeben werden. Im Falle einer internen Katastrophe trifft der CSP Zurückerhaltungsmaßnahmen.

6.2.2.4 Annahme der Geheimnisteile

Bevor Inhaber von Geheimnisteilen einen Geheimnisteil annehmen, müssen sie bei der Herstellung, der Wiederherstellung und der Verteilung des Geheimnisteils oder der darauf folgenden Aufbewahrungskette persönlich anwesend sein.

Der Inhaber eines Geheimnisteils empfängt diesen über ein physisches Medium so wie ein von der CA gutgeheißenes kryptographisches Modul. Die CA bewahrt schriftliche Aufnahmen der Verteilung der Geheimnisteile auf.

6.2.3 Verteilung des CA-Privatschlüssels

Die CA dokumentiert die Verteilung ihres eigenen Privatschlüssels. Wenn die Aufbewahrer der Tokens ersetzt werden müssen, wird die CA eine Spur der neuen Tokens-Verteilung bewahren.

6.2.4 Zerstörung des CA-Privatschlüssels

Am Ende ihrer Lebensdauer werden die Privatschlüssel der CA von mindestens drei Mitgliedern des CSP-Teams, die eine Vertrauensposition inne halten, bei Anwesenheit eines Vertreters der

Belgischen Föderalen Behörde zerstört, damit garantiert werden kann, dass die Privatschlüssel nicht mehr abgerufen und wieder gebraucht werden können.

Die Zerstörung der Schlüssel der CA erfolgt durch Zerreißen der Haupt -und BackupSpeicherträger, durch Löschen der Geheimnisteile und durch Ausschaltung und endgültige Entfernung aller Hardwaremodule, auf denen die Schlüssel aufbewahrt werden.

Der Schlüsselzerstörungsprozess wird dokumentiert und alle damit verbundenen Akten werden archiviert.

6.3 Schutz des Privatschlüssels und Kontrollen des kryptographischen Moduls

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

Diese Vorrichtungen entsprechen den Bedingungen vom FIPS 140-1 Stufe 3 oder höher, der unter anderem garantiert, dass jeder Verletzungsversuch bei der Vorrichtung unmittelbar detektiert wird und dass die Privatschlüssel die Vorrichtungen nicht unverschlüsselt lassen können.

Hardware- und Softwaremechanismen, die die Privatschlüssel der CA schützen, werden dokumentiert.

Die HSMs verlassen die gesicherte Umgebung des CA-Standorts nicht. Wenn die HSMs unterhalten oder repariert werden müssen, was am CA-Standort nicht vorgenommen werden kann, dann müssen Sie an den Hersteller in aller Sicherheit gesandt werden. Der (die) CAPrivatschlüssel ist (sind) auf den HSMs nicht vorhanden, wenn sie zur Wartung außerhalb des gesicherten Standorts der CA gesandt werden. Zwischen den Benutzungssitzungen werden die HSMs auf der gesicherten Site der CA behalten.

Der Privatschlüssel der CA steht unter der Kontrolle von 3 aus 5 möglichen Personen.

Der Privatschlüssel der CA darf in die Hände von Dritten nicht gegeben werden.

Am Ende der Generierung der Schlüssel werden die neuen Schlüssel der CA codiert und auf einem CD-ROM gebrannt (Speicherung des Schlüssel-Backups). Die CA registriert jede Stufe dieses Prozesses mit Hilfe eines spezifischen Formulars für Loginformation.

Der CA-Privatschlüssel wird an den Standorten der CA örtlich archiviert.

CA-Bewahrer werden mit der Aktivierung und der Deaktivierung des Privatschlüssels beauftragt. Der Schlüssel ist dann für einen bestimmten Zeitraum aktiviert.

Der Privatschlüssel der CA kann am Ende seiner Lebensdauer zerstört werden.

6.4 Andere Aspekte der Verwaltung des Schlüsselpaares

Die CA archiviert ihre(n) eigenen öffentlichen Schlüssel. Die CA stellt Bürgerzertifikate mit den Gültigkeitszeiträumen aus, so wie auf die Zertifikate vermerkt.

6.4.1 Entartung der EDV-Hilfsmittel, Softwares und/oder Daten

Die CA trifft die nötigen Maßnahmen, um die vollständige und automatische Wiederherstellung des Dienstes im Falle von Katastrophe, Entartung der Server, Softwares und Daten zu gewährleisten. All diese Maßnahmen entsprechen der ISO 17799-Norm.

Die CA bestimmt Wiederherstellungsmittel in genügender Entfernung von den Hauptmitteln, um zu vermeiden, dass beide im Falle einer Katastrophe davon betroffen werden. Die CA sorgt weiter für genug schnelle Kommunikationsmittel zwischen beiden Standorten, um die Integrität der Daten zu garantieren. Die CA stellt eine gesicherte Kommunikationsinfrastruktur von beiden Standorten aus zur RA, zum Internet und den Netzen der öffentlichen Verwaltung auf.

Die CA trifft die nötigen Maßnahmen, um die Infrastruktur und die Prozeduren zur Wiederherstellung des Dienstes im Falle einer Katastrophe mindestens einmal im Jahr ohne Dienstunterbrechung oder –beschädigung zu testen.

6.4.2 Widerruf des öffentlichen Schlüssels der CA

Falls der öffentliche Schlüssel der „Citizen CA“ widerrufen wird, muss die CA unmittelbar:

- alle bei der Zertifizierung einbezogenen Zertifizierungsbehörden davon benachrichtigen.
- die RA davon benachrichtigen.
- die Öffentlichkeit über verschiedene Wege davon benachrichtigen, darunter:
  - eine Nachricht auf der Website der CA. o eine Pressemitteilung in den belgischen Medien.
  - Anzeigen in den bedeutendsten belgischen Tageszeitungen.
- das Zertifikat der CA in den CRLs und den Delta CRLs aufnehmen.
- den Status des Zertifikats im Web-Schnittstellendienst aktualisieren.
- alle Zertifikate widerrufen, die mit das widerrufenes Zertifikat unterzeichnet wurden.
- Nachdem sie die Gründe des Widerrufs bewertet und Maßnahmen getroffen hat, um vorzubeugen, dass sich dies in Zukunft wiederholt, und nachdem sie die Genehmigung der RA erhalten hat, kann die CA: o ein neues Schlüsselpaar und die damit verbundenes Zertifikat generieren. o alle widerrufene Zertifikate wieder ausstellen.

6.4.3 Schwindel mit dem CA-Privatschlüssel

Bei Schwindel mit dem CA-Privatschlüssel muss das entsprechende Zertifikat unmittelbar widerrufen werden. Außerdem trifft die CA alle unter Punkt 6.4.2. beschriebenen Maßnahmen.

6.5 Aktivierungsdaten

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

6.6 EDV-Sicherheitskontrollen

Die CA führt gewisse EDV-Sicherheitskontrollen aus.

6.7 Sicherheitskontrollen des Lebenszyklus

Die CA führt regelmäßig Entwicklungs- und Sicherheitskontrollen aus.

6.8 Netzsicherheitskontrollen

Die CA sorgt für die Sicherheit der Systeme, einschließlich der Firewalls. Einbrüche ins Netz werden überwacht und aufgespürt. Im Besonderen:

Alle Kommunikationen zwischen der CA und dem RA-Betreiber bezüglich irgendwelcher Phase des Lebenszyklus des Zertifikats werden durch eine PKI-Verschlüsselung und Unterschriftstechniken gesichert, um die Vertraulichkeit und die gegenseitige Authentifizierung zu gewährleisten, was unter anderem Zertifikatsanträge, -ausstellung, -sperrung, Aufhebung der Sperrung und Zertifikatswiderruf betrifft.

Die Website der CA liefert verschlüsselte Verbindungen mit Hilfe des Secure Socket LayerProtokolls (SSL) und eines Antivirusschutzes.

Das Netz der CA wird durch eine Firewall und ein Einbruchmeldesystem geschützt.

Der Zugang zu den empfindlichen CA-Quellen, einschließlich der CA-Datenbanken außerhalb des Netzes des CA-Betreibers, ist verboten.

Die Internet-Verbindungen für die Informationsanfrage und –lieferung werden verschlüsselt.

7 ZERTIFIKAT UND CRL-PROFILE

In diesem Kapitel wird auf das Format von Zertifikaten, CRL und OCSP tiefer eingegangen.

7.1 Profil der Zertifikate

7.1.1 Identitätszertifikat

Die Beschreibung der Felder dieses Zertifikats wird in der Tabelle hierunter wiedergegeben. Pseudonyme dürfen in dieses Zertifikat nicht gebraucht werden.

eID citizen Authentication Certificate					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5 1.2.840.113549.1.1.11	X		Certificates issued under BRCA3 SHA-1 with RSA Encryption Certificates issued under BRCA4 SHA-2 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		Provided by the RRN	Dynamic
Signature		X		Under BRCA3 Sha-1WithRSAEncryption Under BRCA4 Sha-2WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 10 years and 3 months	

SubjectPublicKeyInfo		X		RSA 1024	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Citizen CA	Fixed
SerialNumber		X		<yyyy><ss>[13]	
Subject			Required		
countryName	{ id-at-6 }		YES	provided by RRN	Dynamic
commonName	{ id-at-3 }		YES	Concatenation of first given name, surname and certificate purpose between brackets	Dynamic
Surname	{ id-at-4 }		YES	provided by RRN	Dynamic
GivenName	{ id-at-42 }		NO	optionally provided by RRN (0, 1 or 2 given names)	Dynamic
serialNumber	{ id-at-5 }		YES	provided by RRN (11 Digits numeric value)	Dynamic
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		Certificates issued under BRCA3 2.16.56.10.1.1.2.2	Fixed
				Certificates issued under BRCA4 2.16.56.12.1.1.2.2	
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
					Fixed
Qualifier		X		http://repository.eid.belgium.be	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
digitalSignature				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		ttp://crl.eid.belgium.be/eidc<yyyy><ss>[14].crl	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslClient - smime	Fixed
Private Extensions	OID	Include	Critical	Value	
AuthorityInfoAccess	{id-pe 1}	X	FALSE		

[13] <yyyy>: represents the year when the CA will be used, e.g. 2006; <ss>: unique serial number to support applications to find corresponding CA certificate only based on this field.

[14] <yyyy> represents the year when the CA will be used, e.g. 2006; <ss>: unique serial number to support applications to find corresponding CA certificate only based on this field

accessMethod	{ id-ad-2 }	X			
accessLocation		X		Certificates issued under BRCA3 http://certs.eid.belgium.be/belgiumrs3.crt Certificates issued under BRCA4 http://certs.eid.belgium.be/belgiumrs4.crt	
accessMethod	{ id-ad-1 }	X			
accessLocation		X		http://ocsp.eid.belgium.be/2	

7.1.2 Unterschriftszertifikat

Die Beschreibung der Felder dieses Zertifikats wird in der Tabelle hierunter wiedergegeben. Pseudonyme dürfen in diesem Zertifikat nicht verwendet werden.

eID citizen Signature Certificate					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5 1.2.840.113549.1.1.11	X		Certificates issued under BRCA3 SHA-1 with RSA Encryption Certificates issued under BRCA4 SHA-2 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		Provided by the RRN	Dynamic
Signature		X		Certificates under BRCA3 Sha-1WithRSAEncryption Certificates under BRCA4 Sha-2WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 10 years and 3 months**Error! Bookmark not defined.**	
SubjectPublicKeyInfo		X		RSA 2048	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Citizen CA	Fixed
SerialNumber		X		<yyyy><ss>[15]	
Subject			Required		

[15] <yyyy>: represents the year when the CA will be used, e.g. 2006; <ss>: unique serial number to support applications to find corresponding CA certificate only based on this field.

countryName	{ id-at-6 }		YES	provided by RRN	Dynamic
commonName	{ id-at-3 }		YES	Concatenation of first given name, surname and certificate purpose between brackets	Dynamic
Surname	{ id-at-4 }		YES	provided by RRN	Dynamic
GivenName	{ id-at-42 }		NO	optionally provided by RRN (0, 1 or 2 given names)	Dynamic
serialNumber	{ id-at-5 }		YES	provided by RRN (11 Digits numeric value)	Dynamic
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		Certificates issued under the BRCA3 2.16.56.10.1.1.2.1 Certificates issued under the BRCA242.16.56.129.1.1.2.1	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.eid.belgium.be	Fixed
policyQualifierId	{ id-qt-2 }	X		UserNotice	Fixed
		X		Gebruik onderworpen aan aansprakelijkheidsbeperkingen, zie CPS - Usage	
				mitations de responsabilité, voir CPS - unterliegt Haftungsbeschränkungen, Verwendung gemäss CPS	
Qualified Certificate Statement					
qcStatement	{id-etsi-qcs-QcCompliance }	X			
qcStatement	{ id-etsi-qcs-QcSSCD}	X			
KeyUsage	{id-ce 15}	X	TRUE	N/a	
nonRepudiation				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		

distributionPoint					
FullName		X		http://crl.eid.belgium.be/eidc<yyyy><ss>[16].crl	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sMime	Fixed
Private Extensions	OID	Include	Critical	Value	
AuthorityInfoAccess	{id-pe 1}	X	FALSE		
accessMethod	{ id-ad-2 }	X			
accessLocation		X		Certificates issued under the BRCA3 http://certs.eid.belgium.be/belgiumrs3.crt Certificates issued under the BRCA4 http://certs.eid.belgium.be/belgiumrs4.crt	
accessMethod	{ id-ad-1 }	X			
accessLocation		X		http://ocsp.eid.belgium.be/2	

7.1.3 CA-Zertifikat

Dieses Zertifikat wird durch die BRCA ausgestellt, um die CA mit Hilfe einer digitalen Unterschrift zu identifizieren. Die Beschreibung der Felder dieses Zertifikats wird in der Tabelle hierunter wiedergegeben.

Citizen CA					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5 1.2.840.113549.1.1.11	X		Certificates issued under BRCA3 SHA-1 with RSA Encryption Certificates issued under BRCA4 SHA-2 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		16 Bytes Generated by the CA at Key Generation Process Time	
Signature		X		Certificates under BRCA3 Sha-1WithRSAEncryption Certificates under BRCA4 Sha-2WithRSAEncryption	

[16] <yyyy>: represents the year when the CA will be used, e.g. 2006; <ss>: unique serial number to support applications to find corresponding CA certificate only based on this field.

Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 11 years and 8 months	Fixed
SubjectPublicKeyInfo		X		RSA 4096	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Certificate issued under the BRCA3 Belgium Root CA3 Certificates issued under the BRCA4: Belgium Root CA4	Fixed
Subject					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Citizen CA	Fixed
SerialNumber		X		<yyyy><ss>	
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		Certificates issued under the BRCA3: 2.16.56.10.1.1.2 Certificates issued under the BRCA4: 2.16.56.12.1.1.2	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.eid.belgium.be	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
CertificateSigning				Set	Fixed
CrlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
DistributionPoint					
FullName		X		Certificates issued under the BRCA3: http://crl.eid.belgium.be/belgium3.crl Certificates issued under the BRCA4: http://crl.eid.belgium.be/belgium4.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE	N/a	
CA		X		TRUE	Fixed

pathLenConstraint		X		0 (Zero)	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			SslCA – smimeCA – ObjectSigning CA	Fixed

7.2 CRL-Profil

In Übereinstimmung mit IETF PKIX RFC 5280 unterstützt die CA CRLs entsprechend:
den für CRLs unterstützten Versionsnummern,
dem Inhalt von CRLs und den Erweiterungen von CRLs und deren Kritikalität.

Das Profil der Zertifikatswiderrufsliste wird in der Tabelle hierunter wiedergegeben:

Version	v2
Signature	sha1RSA
Issuer	<subject CA>
ThisUpdate	<creation time>
NextUpdate	<creation time+7 days >
RevokedCertificates	
UserCertificate	<certificate serial number>
RevocationDate	<revocation time>
CrlEntryExtensions	
CRL Reason Code	Certificate Hold(6) (for suspended certificates) Note: Otherwise NOT included!
CrlExtensions	
Authority Key Identifier	non-critical <subject key identifier CA>
CRL Number	non-critical <CA assigned unique number>

Das Profil der Delta-Zertifikatswiderrufsliste wird in der Tabelle hierunter wiedergegeben:

Version	v2
signature	sha1RSA
Issuer	<subject CA>
thisUpdate	<creation time>
nextUpdate	<creation time> +7 days
RevokedCertificates	
userCertificate	<certificate serial number>

revocationDate	<revocation time>
crlEntryExtensions	
CRL Reason Code	Certificate Hold(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 <CA assigned unique number>
Delta CRL Indicator	<base CRL Number>

Die CRLs und Delta-CRLs der CA unterstützen die Felder und die Erweiterungen, die in Kapitel 5 von RFC 5280 spezifiziert sind: „Internet X.509 Öffentliche Schlüsselinfrastruktur und CRL-Profil".

7.3 OCSP-Profil

Das OCSP-Profil folgt IETF PKIX RFC6960 OCSP v1. Keine OCSP-Erweiterung wird unterstützt. Die CA unterstützt verschiedene Zertifikatsstatus in einem einzigen OCSP-Antrag, soweit sie von derselben CA unterschrieben werden. Die OCSP-Antwort wird durch eine „Cross-zertifizierte OCSP Wurzel der CA unterzeichnet.

Dieses Zertifikat wird durch die Root-CA der Belgischen Föderalen Behörde ausgestellt, um die OCSP-Garanten zu zertifizieren. Die Beschreibung der Felder dieses Zertifikats wird in der Tabelle hierunter wiedergegeben.

Belgium OCSP Responder					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		Generated by the CA at Key Generation Process Time	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 1 Year	Fixed

SubjectPublicKeyInfo		X		RSA 2048	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		[Issuing CA]	Fixed
SerialNumber		X		Certificates issued before 5th of June 2005: N/a Certificates issued after 5th of June 2005: <yyyy><ss>[17]	
Subject					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }			Belgium OCSP Responder	Fixed
Standard Extensions	OID	Include	Critical	Value	
KeyUsage	{id-ce 15}	X	TRUE	N/a	
DigitalSignature				Set	Fixed
enhancedKeyUsage			FALSE		
ocspSigning	1.3.6.1.5.5.7.3.9	X			
authorityKeyIdentifier	{id-ce 35}	X	FALSE	N/a	
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
ocspNoCheck	{ id-pkix-ocsp 5 } 1.3.6.1.5.5.7.48.1.5		FALSE		
Null		X			

8 AUDIT DER ÜBEREINSTIMMUNG UND ANDERE BEWERTUNGEN

Was das Qualifiziertes Zertifikat für elektronische Unterschriften betrifft, arbeitet der CSP gemäß den Bestimmungen des Gesetzes vom 9. Juli 2001, das den gesetzlichen Rahmen für elektronische Unterschriften in Belgien festlegt. Die CA genügt den Forderungen, die in den ETSI-Policy-Dokumenten festgelegt sind, die sich auf die qualifizierte Zertifikate beziehen, einschließlich:

- der TS 101 456-Policy-Forderungen für die Zertifizierungsbehörden, die qualifizierte Bescheinigungen ausstellen;
- des TS 101 862-Profils von qualifizierter Bescheinigung.

[17] <yyyy>: Das Jahr, in dem die CA erstmals verwendet wird, z.B. 2006; <ss>: Eindeutige Seriennummer, die verwendet wird, um CA-Zertifikate ausschließlich unter Verwendung dieses Feldes zur Unterstützung von Anwendungen zu suchen..

Was die Identitätszertifikate betrifft, genügt der CSP den Forderungen, die in den ETSI-PolicyDokumenten festgelegt sind, die sich auf die Zertifikate mit öffentlichen Schlüsseln beziehen, einschließlich:

- der TS 102 042-Policy-Forderungen für die Zertifizierungsbehörden, die Bescheinigungen mit öffentlichen Schlüsseln ausstellen (standardisiertes Niveau).

Der CSP nimmt die Übereinstimmungsaudits an, um sich dessen zu vergewissern, dass er den Forderungen, Normen, Prozeduren und Dienstniveaus gemäß dem vorliegenden CPS genügt. Der CSP nimmt diese Audits auf die eigenen Praktiken und Prozeduren 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 Behörde, die die Zertifizierungsdienstleister in Belgien beaufsichtigt und unter der Autorität der Belgischen Föderalen Behörde handelt.
- die Belgische Föderale Behörde oder eine von der Belgischen Föderalen Behörde bezeichnete Drittpartei.

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

Zur Ausführung dieser Audits wird ein unabhängiger Kontrolleur ernannt, der weder unmittelbar noch mittelbar auf irgendwelche Weise mit dem CSP oder mit irgendwelcher CA in Beziehung steht, wobei demzufolge keine Interessenkonflikte in Frage kommen.

Beim Audit wird auf die folgenden Elemente Acht gegeben:

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

Falls Abweichungen festgestellt werden, wird der CSP dem Auditoren 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 werden, um die Konformität zu garantieren.

Certipost NV entspricht der aktuellen Version der Baseline-Anforderungen für die Ausgabe und Verwaltung von öffentlich vertrauenswürdigen Zertifikaten ("Baseline Requirements"), die unter http://www.cabforum.org veröffentlicht werden. Im Falle eines Widerspruchs zwischen diesem Dokument und diesen Anforderungen haben diese Anforderungen Vorrang vor diesem Dokument.

9 ANDERE GESCHÄFTLICHE UND GESETZLICHE FRAGEN

9.1 Vergütungen

Der Artikel 6 des Gesetzes vom 19. Juli 1991 angelegt im Punkt §1.3 des Kapitels 1, regelt einerseits die Vergütung für die Einfügung der Zertifikaten auf den Karten (Art. 6, § 5), und andererseits die Rückforderung von Herstellkosten für die Karte durch den Innenminister (Art. 6, § 8).

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

Die CA wird dem Bürger die folgenden Dienste gebührenfrei leisten:

- Ausstellung, Veröffentlichung und Erneuerung der Zertifikate;
- Widerruf der Zertifikate;
- Aussetzung der Zertifikate;
- Veröffentlichung der CRLS und der Delta CRLs.

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

- Überprüfung des OCSP-Status.
- Herunterladen der CRLs und Delta CRLs.
- Überprüfung des Zertifikatsstatus.
- Zertifikatsverzeichnis.

Mit Hilfe von dedizierten Prozeduren stellt die CA jedem einzelnen Benutzer folgende Dienste, die Gegenstand eines Antrags sein können, gebührenfrei zur Verfügung:

Dienst	Gratis
Überprüfung des OCSP-Status	10 Anträge pro Benutzer pro Tag
CRL-Herunterladen	1 Herunterladung pro Benutzer pro Woche
Herunterladen einer Delta-CRL	8 Herunterladungen pro Benutzer pro Tag
Zertifikatsverzeichnis	30 Herunterladungen pro Woche
Darlegung der Zertifizierungsverfahren	2 Herunterladungen pro Benutzer pro Tag

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

9.2 Haftung

Die Haftung vom CSP 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 sind.

9.2.1 Qualifizierte Zertifikate

Was die Ausstellung der qualifizierte Zertifikate in Sachen elektronische Unterschrift (Unterschriftszertifikate) betrifft, regelt Artikel 14 des Gesetzes über die elektronischen Unterschriften die Haftung vom CSP.

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

(a) die Richtigkeit aller in das qualifizierte Zertifikat aufgenommenen Informationen am Datum, wo sie ausgestellt wurde, und das Vorhandensein aller für ein qualifiziertes Zertifikat vorgeschriebenen Angaben in dieses Zertifikat;

(b) die Garantie, dass zum Zeitpunkt der Ausstellung des qualifiziertes Zertifikat der in das qualifizierte Zertifikat identifizierte Unterzeichner den Privatschlüssel besaß, der dem in das Zertifikat angegebenen oder identifizierten öffentlichen Schlüssel entspricht;

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

Der CSP 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 CSP kann beweisen, dass er nicht nachlässig gewesen ist.

9.2.2 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 CSP ausgestelltes Zertifikat verlässt.

Der CSP 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.

9.3 Vertraulichkeit der Informationen

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.

Der CSP hält die Vorschriften über personenbezogene Daten ein, so wie im vorliegenden CPS beschrieben.

Die vertraulichen Informationen umfassen:

- jede persönliche identifizierbare Information über Bürger anders als diejenigen, die in ein Zertifikat aufgenommen sind.
- den genauen Grund des Widerrufs oder der 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.

Die folgenden Elemente gelten nicht als vertrauliche Informationen:

- die Zertifikate und deren Inhalt.
- der Status eines Zertifikats.

Der CSP verbreitet keine vertrauliche Information und ist nicht dazu gehalten ohne authentisierte 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.

Im Rahmen des Rahmenvertrags zwischen dem CSP und der Belgischen Föderalen Behörde darf der CSP Verwaltungskosten berechnen, um solche Informationsverbreitungen vorzunehmen.

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.

9.3.1 Bedingungen bezüglich der Verbreitung

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

- Der Status ein einziges Zertifikat wird auf Anfrage eines Bürgers oder einer vertrauenden Partei geliefert;
- Die Bürger können nicht vertrauliche Informationen zu Rate ziehen, die der CSP über sie besitzt.

Die vertraulichen Informationen werden vom CSP weder den Bürgern noch den vertrauenden Parteien bekannt gegeben werden, 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.

Der CSP verwaltet die Bekanntmachung von Informationen an das CSP-Personal.

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

- Vorlage eines Authentifizierungszertifikat auf Antrag des Bürgers oder der vertrauenden Partei
- Unterzeichnung der Antworten auf OCSP-, CRLs- und Delta CRLs-Anfragen.

Die CA 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 CSP verfügt die RA auch über Informationen über die Bürgerzertifikate, 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 Bürger, über die das RRN verfügt.

9.3.2 Schutz der personenbezogenen Informationen

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

Der CSP bewahrt keine anderen Angaben bezüglich der Zertifikate oder der Bürger 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 CSP behandelten personenbezogenen Daten zu keinen anderen Zwecken benutzt werden.

9.3.3 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 vom CSP herkommen, verbunden sind, einschließlich des vorliegenden CPS.

Der CSP 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 CSP im Rahmen des Projekts des belgischen elektronischen Personalausweises entwickelt werden, sind das exklusive Eigentum vom belgischen Staat.

9.4 Vertretungen und Garantien

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

9.4.1 Pflichten des Bürgers

Außer wenn im CPS anders angegeben, umfassen die Pflichten des Bürgers die folgenden Pflichten:

- sich davon enthalten, ein Zertifikat zu verfälschen.
- Zertifikate nur zu gesetzlichen und zugelassenen Zwecken gemäß dem CPS benutzen.
- einen neuen elektronischen Personalausweis (und also Bürgerzertifikate) im Falle einer Änderung der in das Zertifikat veröffentlichten Information beantragen;
- sich davon enthalten, den öffentlichen Bürgerschlüssel in eines ausgestelltes Bürgerzertifikat für die Ausstellung von anderen Zertifikate zu benutzen;
- unter allen Umständen ein Zertifikat auf angemessene Weise benutzen;
- Kompromittierung, Verlust, Enthüllung, Änderung oder irgendwelchen anderen unzulässigen Gebrauch seiner Privatschlüssel vorbeugen.
- die Polizei, die Gemeindeverwaltung oder das Helpdesk der RA benachrichtigen, um die Aussetzung eines Zertifikats bei der Vermutung eines Zwischenfalls, der das Zertifikat materiell schaden könnte, zu beantragen. Dabei werden Meldungen von

Verlust, Diebstahl, Änderung, unbefugter Verbreitung oder anderen Kompromittierungen des Privatschlüssels einer der Bürgerbescheinigungen oder von beiden gemeint.

- sein Schlüsselpaar nur in Übereinstimmung mit jeder angekündigten Begrenzung gebrauchen.
- sein Privatschlüssel jederzeit gegen den Diebstahl, die Verbreitung an eine andere Partei, die Änderung und die unbefugte Benutzung gemäß dem geltenden CPS schützen.
- das RA-Helpdesk unverzüglich benachrichtigen, wenn die Kontrolle seines Privatschlüssels aufgrund einer Kompromittierung des PIN-Codes verloren worden ist.
- Verpflichtung, jede Benutzung des Privatschlüssels zu stoppen, sobald dieser kompromittiert wird.

9.4.2 Pflichten der vertrauenden Partei

Die Parteien, die auf ein Zertifikat des CSP vertrauen:

- werden über den Gebrauch von digitalen Zertifikate und PKI genügend informiert werden;
- werden informiert werden und die Bedingungen des vorliegenden CPS sowie die verbundenen Bedingungen für die vertrauenden Parteien einhalten;
- werden ein Zertifikat mit Hilfe einer CRL-, Delta CRL-, OCSP- oder Web-basierte Zertifikatsbestätigung gemäß der Prozedur zur Herstellung eines gesicherten Weges des Zertifikats bestätigen;
- werden auf ein Zertifikat nur dann vertrauen, wenn diese 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 wird, dann muss sie das RA-Helpdesk unmittelbar davon benachrichtigen.

9.4.3 Haftung des Bürgers gegenüber den vertrauenden Parteien

Ein Bürger, der im Besitz eines elektronischen Personalausweises mit aktivierten Schlüsseln für die Authentifizierung und Unterschriften ist, haftet den vertrauenden Parteien gegenüber für jede Benutzung dieses Ausweises, einschließlich der Schlüssel und Zertifikate, es sei denn, dass er beweisen kann, dass sein Schlüssel kompromittiert wurde, und dass er alle notwendigen Maßnahmen getroffen hat, um seine Zertifikate rechtzeitig widerrufen zu lassen.

9.4.4 Bedingungen für die Benutzung der Bezugsarchive und der Website

Alle Parteien, einschließlich der Bürger und der vertrauenden Parteien, die Zugang zu den Bezugsarchiven und zur Website der CA haben, sind mit den Bestimmungen des vorliegenden CPS sowie mit allen anderen Benutzungsbedingungen einverstanden. Die Bürger und die vertrauenden Parteien zeigen sich mit den Benutzungsbedingungen und dem vorliegenden CPS einverstanden, indem sie einen Antrag bezüglich des Status eines digitales Zertifikats einreichen oder indem sie irgendwie die gelieferten Informationen oder Dienste in Anspruch nehmen oder

auf diese vertrauen. Die Bezugsarchive der CA können auf verschiedene Weisen benutzt werden:

- um Informationen als Ergebnis einer Suche nach ein digitales Zertifikat zu erhalten;
- um den Status von digitalen Unterschriften zu überprüfen, die mit einem Privatschlüssel gemacht worden sind, der einem öffentlichen Schlüssel entspricht, der in ein Zertifikat enthalten ist;
- um Informationen zu erhalten, die auf der Website der CA veröffentlicht werden;
- für alle anderen Dienste, die die CA über seine Website fördern oder liefern könnte.

9.4.4.1 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.

9.4.4.2 Korrektheit der Informationen

Die CA setzt alles ein, damit den Parteien, denen Zugang zu den Bezugsarchiven gewährt wird, genaue, aktualisierte und richtige Informationen erhalten. Der CSP darf jedoch keine Haftung jenseits der unter Artikel 9.2. des CPS festgesetzten Grenzen übernehmen.

9.4.5 Pflichten des CSP

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

- das vorliegende CPS und dessen Änderungen, so wie unter http://repository.eid.belgium.be veröffentlicht, einhalten;
- 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 Prozeduren zur Verteilung von Geheimen bezüglich seiner eigenen Infrastruktur;
- die RA im Falle einer Kompromittierung seines (seiner) eigenen Privatschlüssel 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 schnell widerrufen, nachdem er einen authentifizierten Widerrufsantrag von der RA empfangen hat;
- ein Zertifikat gemäß dem CPS schnell sperren, nachdem er einen authentifizierten Sperrungsantrag von der RA empfangen hat;
- die Sperrung eines Zertifikats gemäß dem CPS schnell 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. Konkret, allen mit einem Profil qualifiziertes Zertifikat verbundenen gesetzlichen Forderungen entsprechen, die aus dem belgischen Gesetz vom 9. Juli 2001 über die elektronischen Unterschriften hervorgehen, das die europäische Richtlinie 1999/93 in den gemeinschaftlichen Rahmen für die elektronischen Unterschriften einführt.

Wenn der CSP 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 CSP sein Bestes tun, um die finanzielle und zivile Verantwortlichkeit dieses Subunternehmers zu garantieren.

Den Bürgern und vertrauenden Parteien gegenüber haftet der CSP 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;
- die Nicht-Erklärung eines widerrufenes oder gesperrtes Zertifikat durch den OCSPBeantworter;
- die Nicht-Erklärung von Informationen über den Status eines Zertifikats durch eine WebSchnittstelle;
- die unbefugte Verbreitung von vertraulichen Informationen oder von Privatangaben gemäß den Punkten 9.3 und 9.4.
- verantwortlich, so wie unter 9.2 bestimmt.

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

9.4.6 Messung des Dienstniveaus

Die Belgische Föderale Behörde, zusammen mit den eID-Partnern, erlegt Kontrollen auf, die dazu bestimmt sind, die Konformität der mit dem elektronischen Personalausweis (eID) verbundenen Dienste mit den im vorliegenden CPS bestimmten Dienstniveauvereinbarungen zu garantieren.

9.4.7 Pflichten der RA (auf das RRN anwendbar)

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

- bei ihren Kommunikationen 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;
- Zertifikatsanträge gemäß dem vorliegenden CPS erstellen;
- alle durch die CA-Prozeduren und das vorliegende CPS vorgeschriebenen Überprüfungen und Authentifizierungen vornehmen;
- der CA den Antrag des Antragstellers in einer unterschriebenen Nachricht vorlegen;
- alle Anträge auf Widerruf, Sperrung und Aufhebung der Sperrung eines Zertifikats gemäß den CA-Prozeduren und dem vorliegenden CPS erhalten, überprüfen und an die CA übermitteln;
- die Richtigkeit und die Authentizität der Informationen überprüfen, die vom Bürger 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 Bürgers 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 vom RRN.

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

9.4.8 Pflichten des Ausweispersonalisierers und -initialisierers (CM)

Der Ersteller der elektronischen Personalausweise (CM) ist verantwortlich für das Initialisieren, Personalisieren und Verteilen der Personalausweise, die die 2 Bürgerzertifikate enthalten.

Das Initialisieren erfordert folgende Verrichtungen im Chip:

- Generieren von drei Schlüsselpaaren,
- Aufnehmen der Identifizierungsdaten und der Zertifikate,
- Authentifizieren der Daten sowie Initialisieren der verschiedenen Dateien.

Die CM verteilt auf sichere Weise die Basisdokumente, die Aufrufbriefe, die neuen personalisierten und die initialisierten Personalausweise sowie die personalisierten gesicherten Briefe, die für die Bürger bestimmt sind und die PIN- und PUK1-Codes enthalten..

Realisieren eines gesicherten Systems zum Einsammeln und Vernichten der verfallenen oder annullierten Ausweise durch die Gemeinden.

9.5 Abweisung von Garantien

In diesem Abschnitt wird auf die Abweisung von Expressgarantien eingegangen.

9.5.1 Ausschluss von bestimmten Schadensaspekten

Innerhalb der durch das belgische Gesetz festgesetzten Grenzen und die Haftung nach art 9.2 und 9.2.1, haftet der CSP auf keinen Fall (außer im Falle von Betrug oder absichtlichem Verstoß) für:

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

9.6 Dauer und Kündigung

Das vorliegende CPS bleibt anwendbar, bis der CSP das Gegenteil in seinen Bezugsarchiven unter der Site http://repository.eid.belgium.be ausdrücklich mitteilt.

Bekannt gegebene Änderungen werden durch eine Versionsnummer angegeben.

9.7 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

Bemerkungen bezüglich des vorliegenden CPS sind an CERTIPOST zu richten. Kontaktdaten:

☐ Per Post:

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

☐ Per E-Mail:

Betr.: Policy administration - Citizen CA
An: eid.csp@bpost.be

9.8 Erzwingbarkeit

Wenn eine Bestimmung des vorliegenden CPS nicht ausgeführt werden kann, dann wird der Rest des CPS auf solche Weise interpretiert, dass die ursprünglichen Absichten der Parteien verwirklicht werden.

9.9 Änderungen

Änderungen des vorliegenden CPS werden von der zuständigen Richtlinienadministration bei CERTIPOST verwaltet. Alle vorgeschlagenen Änderungen des CPS müssen vom PKI Management Board genehmigt werden. 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.

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 CPSIndex (URL) geändert zu werden, der vom CSP 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.

9.10 Prozeduren 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 SMB_CTP_EID_CSP@bpost.be, Adresse, Postanschrift. Eine Empfangsbestätigung wird innerhalb von 2 Arbeitstagen nach Eintreffen der Beschwerde versandt. Eine Antwort erfolgt innerhalb von 10 Arbeitstagen nach Eintreffen der Beschwerde.

9.11 Anwendbares Recht

Der CSP liefert seine Dienste gemäß den Bestimmungen des belgischen Gesetzes.

9.12 Verschiedene Bestimmungen

Der CSP 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 Bürgerzertifikat 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.

10 LISTE DER BEGRIFFE

Authority Information Access (AIA)	Ein Informationsfeld, das als Erweiterung in das Zertifikat aufgenommen wurde, um automatisch den Weg zur Überprüfung der Vertrauenshierarchien innerhalb der allgemeinsten verwendeten Anwendungen wie z.B. Browsern aufzubauen.
ARCHIV	Um Aufnahmen während eines bestimmten Zeitraums aus Sicherheits-, Speicherungs- oder Überprüfungszwecken aufzubewahren
AUDIT	Prozedur, die zur Bestätigung der Konformität mit formellen Kriterien oder Kontrollen angewandt wird

AUSGEBER EINES GEHEIMNISTEILS	Person, die Geheimnisteile erstellt und verteilt, unter anderem eine CA.
AUSSTELLUNG DER ZERTIFIKATE	Ausstellung von digitalen Zertifikaten X.509 v3, die für die Identifizierung und die digitale Unterzeichnung auf Basis von personenbezogenen Daten und öffentlichen Schlüsseln bestimmt sind, die von der RA geliefert werden und dem CPS genügen.
AUTHENTIFIZIERUNG	Prozedur, die angewandt wird, um die Identität einer Person zu bestätigen oder die Integrität von spezifischen Informationen zu beweisen, indem sie in den richtigen Kontext platziert werden und die Verbindung überprüft wird
BEGLAUBIGUNG	Formelle Erklärung durch eine zustimmende Behörde, nach der eine gegebene Funktion/Entität spezifische formelle Forderungen erfüllt.
BEMERKUNG	Ergebnis einer Bekanntmachung an die Parteien, auf welche sich die CA-Dienste beziehen, in Übereinstimmung mit dem vorliegenden CPS.
DARLEGUNG DER ZERTIFIZIERUNGSVERFAHREN ODER CPS	Darlegung der Verfahren zur Verwaltung von Zertifikaten während aller Phasen des Lebenszyklus der Zertifikate.
DIENSTE FÜR ZERTIFIKATSTATUS	Dienst, der es vertrauenden und anderen Parteien ermöglicht, den Status von Zertifikate zu überprüfen.
DIGITALE UNTERSCHRIFT	Dient für das Kodieren einer Nachricht mit Hilfe eines asymmetrischen Verschlüsselungssystems und einer Analysefunktion, sodass die Person, die im Besitz der ursprünglichen Nachricht und des öffentlichen Schlüssels des Unterzeichners ist, genau bestimmen kann, ob die Transformation mit dem Privatschlüssel ausgeführt wurde, der dem öffentlichen Schlüssel des Unterzeichners entspricht, und ob die ursprüngliche Nachricht seit der Transformation geändert wurde.
DISTINKTIVER NAME	Die gesamten Angaben, die eine Entität der realen Welt, wie eine Person im EDV-Kontext, identifizieren.
EID	Das gesamte System der eID-Karte, unter anderem Organisation, Infrastruktur, Prozeduren, Kontakte und alle nötigen Quellen, die sich auf die eID-Karte beziehen.
EINE ZERTIFIKAT WIDERRUFEN	Dem Gültigkeitszeitraum eines Zertifikates ab einem spezifizierten Zeitpunkt endgültig ein Ende setzen.
EINE ZERTIFIKATSKETTE BESTÄTIGEN	Eine Zertifikatskette bestätigen, um jedes Zertifikat der Zertifikatskette zu bestätigen, damit ein Bürgerzertifikat des Endbenutzers bestätigt wird.
ELEKTRONISCHE UNTERSCHRIFT	Angaben in elektronischer Form, die an anderen elektronischen Angaben festgeheftet oder mit diesen logisch verbunden sind und die Authentifizierungsmethode aktivieren.
ERWEITERUNG DES ZERTIFIKATS	Feld des digitales Zertifikats, das dazu gebraucht wird, zusätzliche Informationen zu übermitteln wie: öffentlicher Schlüssel, zertifizierter Bürger, Ausgeber des Zertifikates und/oder Zertifizierungsprozess.
EUROPÄISCHE RICHTLINIE	Die europäische Richtlinie 1999/93 des europäischen Parlaments und des Rats vom 13. Dezember 1999 „über einen gemeinschaftlichen Rahmen für die elektronischen Unterschriften“.

GEGENSTANDSIDENTIFIZIERER (OID)	Eine Reihe von integren Komponenten kann einem registrierten Gegenstand zugewiesen werden und hat die Eigenschaft, unter allen Gegenstandsidentifizierern innerhalb eines spezifischen Bereichs einmalig zu sein.
GEHEIMNISTEILUNG	Ein Teil eines kryptographischen Geheimnisses, der unter einer Anzahl physischer Kennzeichen, wie Chipkarten, usw. geteilt wird.
GENERIERUNG EINES SCHLÜSSELPAARS	Zuverlässiger Prozess, der dazu bestimmt ist, mathematisch verbundene Privatschlüssel und öffentliche Schlüssel zu erstellen (z.B.: gemäß dem RSA-Algorithmus).
GESPERRTES ZERTIFIKAT	Zeitweilig abgelehntes Zertifikat, das jedoch ein Woche lang aufbewahrt wird, bis das RRN den endgültigen Widerruf oder die Reaktivierung des Zertifikats an die CA bekannt gibt.
GÜLTIGKEITSABLAUF DES ZERTIFIKATS	Ablauf des Gültigkeitszeitraums eines digitales Zertifikats.
HSM	Ein HSM (Hardware Security Module) ist eine HardwareSicherheitsausrüstung, die kryptographische Schlüssel generiert, speichert und schützt.
INFRASTRUKTUR MIT ÖFFENTLICHEN SCHLÜSSELN (PKI)	Architektur, Organisation, Techniken, Verhalten und Prozeduren, die die Installation und den Betrieb eines auf ein Zertifikat basierenden Veschlüsselungssystems mit öffentlichem Schlüssel gemeinsam unterstützen.
INHABER EINES GEHEIMNISTEILS	Person, die einen Geheimnisteil besitzt.
NORMALISIERTES ZERTIFIKAT	Zertifikat, das benutzt wird, um irgendwelchen Gebrauch zu unterstützen außer den qualifizierten elektronischen Unterschriften eines kryptographischen Schlüsselpaars, von dem das entsprechende öffentliche Schlüsselpaar bestätigt ist. Die verschiedenen Gebrauchsarten von zertifizierten Schlüsseln können folgende sein: Verschlüsselung, Authentifizierung, unqualifizierte Unterschriften, usw. Das normalisiertes Zertifikat wird gemäß den Forderungen der technischen Norm TS 102 042 vom ETSI ausgestellt.
ÖFFENTLICHER SCHLÜSSEL	Mathematischer Schlüssel, der der Öffentlichkeit zur Verfügung gestellt und benutzt werden kann, um die mit Hilfe des entsprechenden Privatschlüssels generierten Unterschriften zu überprüfen. Je nach dem Algorithmus können die öffentlichen Schlüssel auch dazu dienen, Nachrichten oder Dateien zu verschlüsseln, die dann mit dem entsprechenden Privatschlüssel dekodiert werden können.
ÖRTLICHE REGISTRIERUNGSSTELLE ODER LRA	Eine LRA ist eine Entität (Instanz), die von einer RA beauftragt wird, um die Anträge auf digitale Zertifikate zu registrieren. Die LRA wird damit beauftragt, andere Entitäten zu registrieren und ihnen einen relativen Unterscheidungswert, wie einen distinktiven Namen oder eine Analysefunktion, die in diesem Bereich einzigartig ist, zuzuweisen
PER REFERENZ AUFNEHMEN	Bedeutet ein Dokument in einem anderen Dokument aufnehmen, indem das aufzunehmende Dokument mit Hilfe von Informationen identifiziert wird, die dem Adressaten Zugang zum gesamten aufgenommenen Dokument bietet, und wobei deutlich gemacht wird, dass es zu einem anderen Dokument gehört. Ein solches aufgenommenes Dokument hat dieselbe Wirkung, als es in der Nachricht vollständig erwähnt würde.

PKI-HIERARCHIE	Die gesamten Zertifizierungsbehörden, deren Funktionen nach dem Prinzip der Befugnisdelegierung gestaltet werden und die miteinander als untergeordnete und übergeordnete CA verbunden sind.
PRIVATSCHLÜSSEL	Mathematischer Schlüssel, der gebraucht wird, um digitale Unterschriften zu erstellen und manchmal (je nach Algorithmus) Nachrichten in Kombination mit dem entsprechenden öffentlichen Schlüssel zu dekodieren.
PROTOKOLL ZUR ONLINEGÜLTIGKEITSÜBERPRÜFUNG VON BESCHEINIGUNGEN (OCSP)	Das Protokoll zur Online-Gültigkeitsüberprüfung von Zertifikaten (RFC 6960) ist eine Quelle von Informationen über den Zustand in Realzeit, die dazu benutzt wird, den gegenwärtigen Status eines digitales Zertifikates zu bestimmen, ohne dass CRLs notwendig sind.
QUALIFIZIERTES ZERTIFIKAT	Ein Zertifikat, das ausschließlich zur Unterstützung von elektronischen Unterschriften gebraucht wird, den Forderungen von Anhang I der europäischen Richtlinie 1999/93 genügt und von Zertifizierungsdiensteanbieter geliefert wird, der Bedingungen von Anhang II der europäischen Richtlinie 1999/93 genügt, mit Verweisung auf das belgische Gesetz vom 09. Juli 2001, die technische Norm ETS TS 101 456, die technischen Normen ETSI TS „Profil von qualifizierte Zertifikate“ und die Norm RFC 3039 „Internet X 509 Öffentliche Schlüsselinfrastruktur und Profil von qualifizierte Zertifikate“.
REFERENZARCHIVE	Datenbank und/oder –Verzeichnis, die die digitale Zertifikate und andere relevante Informationen enthalten, die online zugänglich sind
REGISTRIERUNGSSTELLE ODER RA	Entität, die mit der Identifizierung und der Authentifizierung der Bürger beauftragt ist. Die RA stellt keine Zertifikate aus. Im Bereich der CA ist das RRN die RA
ROOT SIGNING	Vertrauen unter gewissen Bedingungen schenkt. Im Rahmen des belgischen elektronischen Personalausweises ist Cybertrust-Baltimore ; digicert eine Root Sign-Autorität, die es der eID-CA ermöglicht, dieselbe Vertrauensposition für SoftwareAnwendungen als die Bescheinigungen von CybertrustBaltimore ; digicert zu genießen.
SCHLÜSSELPAAR	Ein Privatschlüssel und der entsprechende öffentliche Schlüssel, in einer asymmetrischen Kodierung.
SERIENNUMMER EINES ZERTIFIKATES	Folgenummer, die ein Zertifikat im Bereich der CA auf einmalige Weise identifiziert.
SPERRUNG VON ZERTIFIKATEN	Online-Dienst, der benutzt wird, um ein digitales Zertifikat zeitweilig zu deaktivieren und sie automatisch zu widerrufen, wenn keine Aufhebung der Sperrung innerhalb einer gewissen Frist beantragt wird.
STATUSÜBERPRÜFUNG	Ein Online-Dienst, der zum Beispiel auf das Protokoll zur Online-Überprüfung von Zertifikaten (RFC 6960) basiert und dazu benutzt wird, den jetzigen Status eines digitalen Zertifikats zu bestimmen, ohne dass CRLs notwendig sind. Im Rahmen von eID sind verschiedene Mechanismen verfügbar, um diesen Status zu überprüfen, wie CRLs, Delta CRLs, OCSP und Web-

Schnittstellen.

SUBSKRIBENT	Person, deren Identität und öffentlicher Schlüssel in Bürgerzertifikate bestätigt sind.
UNTERSCHRIFT	Methode, die vom Verfasser eines Dokuments benutzt oder adoptiert wird, um sich zu identifizieren. Diese Methode kann vom Adressaten angenommen werden oder ihre Benutzung ist unter den gegebenen Umständen gebräuchlich.
UNTERZEICHNER	Person, die das Gerät zur Erstellung von Unterschriften bedient, das zur Generierung einer digitalen Unterschrift gebraucht wird.
VERSCHLÜSSELUNG MIT ÖFFENTLICHEN SCHLÜSSELN	Verschlüsselung, die auf einem mathematisch verbundenen kryptographischen Schlüsselpaar beruht.
VERTRAUEN	Die Tatsache, dass man eine digitale Unterschrift annimmt, weil man sie als glaubenswürdig betrachtet, und danach handelt.
VERTRAUENDE PARTEI	Jede Entität, die auf ein Zertifikat vertraut, um zu handeln.
VERTRAUENSPOSITION	Eine Rolle innerhalb der CA mit Zugang zu oder Kontrolle von kryptographischen Handlungen, die einen privilegierten Zugang zur Ausstellung, Benutzung, Sperrung oder Widerrufung von Zertifikaten bieten, einschließlich des Zugangs oder der Kontrolle von Handlungen, die den Zugang zu Bezugsarchiven begrenzen.
VERTRAULICHKEIT	Verteilung von Daten nur an ausgewählte und befugte Parteien.
VERWALTUNG VON ZERTIFIKATEN	Handlungen, die mit der Verwaltung von Zertifikaten wie Lagerung, Verteilung, Veröffentlichung, Widerruf und Sperrung von Zertifikaten verbunden sind.
WIDERRUF VON ZERTIFIKATEN	Online-Dienst, der zur permanenten Deaktivierung ein digitales Zertifikat vor ihrem Ablaufdatum benutzt wird.
X.509	Der ITU-T-Standard (International Telecommunications Union-T) für digitale Zertifikate.
ZERTIFIKAT	Elektronische Erklärung, die die Überprüfungsdaten der Unterschrift mit einer natürlichen oder juristischen Person verbindet und die Identität dieser Person bestätigt.
ZERTIFIKATSHIERARCHIE	Eine auf Niveaus basierende Nachfolge von Zertifikaten von einer (Root) CA und von untergeordneten Entitäten, worunter die Zertifizierungsbehörden und die Bürger.
ZERTIFIKATSKETTE	Hierarchische Liste von Zertifikaten, die ein Endbenutzerzertifikat und das Zertifikat der CA umfasst.
Zertifikatswiderrufsliste (CRL)	Von einer CA ausgestellte und digital unterzeichnete Liste, die widerrufenen oder gesperrten Zertifikate enthält. Diese Liste kann jederzeit von den vertrauenden Parteien abgerufen werden, bevor sie auf die in ein Zertifikat aufgenommenen Informationen vertrauen.
ZERTIFIZIERUNGSDIENSTE	Dienste bezüglich des Lebenszyklus der Bürgerzertifikate. Die Zertifizierungsdienste sind öffentliche Dienste.

Zertifizierungsdienstleister (Certification Service Provider)	Natürliche oder juristische Person, die Zertifikate ausstellt und verwaltet oder andere Dienstleistungen in Zusammenhang mit elektronischen Signaturen erbringt. Im Kontext des vorliegenden CPS ist der Zertifizierungsdienstleister CERTIPOST s.a./n.v., mit eingetragenem Sitz in Muntcentrum ,B-1000 Brüssel, Belgien.
ZERTIFIZIERUNGSSTELLE ODER CA	Behörde, die damit beauftragt ist, einen öffentlichen Schlüssel mit den Informationen über die betreffende Person, die in ein Zertifikat aufgenommen sind, zu verbinden, indem sie diese mit ihrem Privatschlüssel unterzeichnet. Außer bei ausdrücklichem Hinweis beschreibt hier die CA die „Citizen Certification Authority“.
ZUVERLÄSSIGES SYSTEM	Computer-Hardware, Software und Prozeduren, die ein akzeptables Niveau in Sachen Sicherheit, Verfügbarkeit, Zuverlässigkeit und korrektes Funktionieren bieten und eine Sicherheitspolicy bewerkstelligen.

11 LISTE DER AKRONYME

BRCA: Belgium Root CA	Root-CA für Belgien (generell zur Angabe von BRCA(1) und BRCA2 verwendet)
BRCA(1)	Erster Root-CA für Belgien in der eID PKI Umgebung
BRCA2	Zweiter Root-CA für Belgien in der eID PKI Umgebung
CA: Certification Authority	Zertifizierungsstelle
CM: Card Manufacturer	Kartenhersteller
CP : Certificate Policy	Certificate Policy
CPS: Certificate Practise Statement	Zertifizierungsrichtlinie
CRL: Certificate Revocation List	Zertifikatswiderrufsliste
HSM: Hardware Security Module	Hardwaresicherheitsmodul
LRA: Local Registration Authority	Örtliche Zertifizierungsstelle
OID: Object Identifier	Gegenstandsidentifizierer
OCSP: Online Certificate Status Protocol	Protokoll zur Online-Überprüfung des Zertifikatsstatus
PKI: Public Key Infrastructure	Infrastruktur mit öffentlichen Schlüsseln
RA: Registration Authority	Registrierungsstelle
SRA: Suspension and Revocation Authority	Sperrungs-und Widerrufungsstelle
OID: Object Identifier	Gegenstandsidentifizierer
URL: Uniform Resource Locator	Internetadressenverzeichnis
PIN: Personal Identification Number	Persönlicher Identifizierungscode
PUK: Personal Unblocking Key	Persönlicher Entsperrungscode