Belgian Certificate Policy & Practice Statement for eID PKI infrastructure Citizen CA

OIDs: **2.16.56.1.1.1.2**
2.16.56.9.1.1.2
2.16.56.10.1.1.2
2.16.56.12.1.1.2

Company:	*certipost*
Version:	*4.7*
Status:	*FINAL*
Rel. Date:	*03/02/2021*

Document Control

Date	Version	Editor	Change
13/02/2017	3.0	Bart Eeman	Initial version 1.0
15/03/2017	3.1	Bart Eeman	Initial version 1.1
24/03/2017	3.2	Don Giot	Update version 1.2
10/04/2017	3.3	Bart Eeman	Zetes addition
13/04/2017	3.4	Bart Eeman	Remarks RRN
04/09/2017	4.0	Don Giot / Cristof Fleurus	eIDAS Update & QA
29/05/2018	4.1	Bart Eeman / Don Giot	Update version 4.1 & QA
13/07/2018	4.2	Bart Eeman	Final version review 2018
08/04/2019	4.4	Bart Eeman / Bono Vanderpoorten / Guillaume Nguyen	Update 2019
06/09/2019	4.5	Bart Eeman/Jonas Deckers/Guillaume Nguyen	Remarks RRN
15/10/2020	4.6	Bart Eeman	Review 2020
20/01/2021	4.7	Bart Eeman	Review 2021

Table of Contents

1 Introduction

This Certification Practice Statement (further abbreviated as CPS) describes the certification practices applicable to the digital certificates issued for the Belgian Citizen by the Trust Service Provider (further abbreviated as TSP) under the name of "Citizen CA" (further called "the CAs") and installed on the electronic chip cards for citizens (further called "electronic identity cards").

This CPS is a unilateral public declaration of the practices that the "Citizen CA" complies with, when providing certification services and comprehensively describes how the "Citizen CA" makes its services available.

The CPS is primarily intended to further precise the legal and contractual provisions and to inform all interested parties about the practices of the "Citizen CA".

1.1 Overview

Currently the TSP for "Citizen CA" is "CERTIPOST nv/sa" (hereinafter referred to as "certipost"), having its registered offices at 1000 Brussels Centre Monnaie/Muncentrum, contracted to do this by the Belgian Authorities in the capacity of the eID project contracting authority, in the following terms:

certipost assumes the role of Trust Service Provider ("TSP") in the sense of the Law of 21 July 2016, the European regulation No 910/2014 of the European Parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market. certipost assumes, on behalf and for the account of the Belgian authorities, both the roles of CA and TSP for the Citizen CAs and is in that capacity responsible for the Citizen certificates issued under these CAs.

This CPS should only be used within the CA domain. The CPS aims at delimiting the domain of providing certification services to the citizens and relying parties within the CA domain. This CPS also outlines the relationship between the Certification Authority (CA) and other Certification Authorities within the Belgian State PKI hierarchy such as the Belgium Root Certificate Authority (BRCA). It also describes the relationship between the TSP and the other organisations involved in the delivery of the certificates for the Belgian Electronic Identity Cards (hereinafter "Citizen Certificates").

This CPS provides operational guidelines for all citizens and relying parties, including natural or legal persons in Belgium or abroad, and other Certification Authorities, such as the BRCA, that belongs to the PKI hierarchy of the Belgian State within the legal framework for electronic signatures and electronic identity cards in Belgium. Moreover, this CPS describes the relationships between the "Citizen CA" and all other entities playing a role in the context of the Belgian Electronic Identity Card, such as the Card Manufacturer. The Belgian State acquires these services through appropriate agreements concluded with these third party suppliers.

Finally, in an accreditation and supervisory perspective, this CPS provides guidance to supervising authorities, accreditation bodies, auditors etc. with regard to the practices of the TSP.

This “Citizen CA CPS” endorses and implements the following standards:

- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- ETSI EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;
- ETSI EN 319 412-5: Policy and security requirements for Trust Service Providers issuing certificates; Part 5: QCStatements;
- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices;
- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile;
- RFC 6818: Update to the RFC 5280;
- RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile;
- RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP;
- The ISO/IEC 27001 standard on information security and infrastructure.

The CPS addresses in detail the organisational, procedural and technical policies and practices of the CA with regard to all certification services it provides and during the complete lifetime of certificates issued by the “Citizen CA”. Together with this CPS other documents related to the certification process in the context of the Belgian Electronic Identity Card may have to be taken into account. These documents will be available through the CA repository (cfr. § 2 Publication and Repository Responsibilities).

This CPS complies with the formal requirements of Internet Engineering Task Force (IETF) RFC 3647, with regard to format and content. While certain section titles are included according to the structure of RFC 3647, the topic may not necessarily apply in the implementation of the certification services of the “Citizen CA”. Such sections are denoted as “Section not applicable”. Minor editorial changes of RFC 3647 prescriptions have been inserted in this CPS to better adapt the structure of RFC 3647 to the needs of this application domain.

This CPS must also be considered as the Certificate Policy (CP) for the certificates issued by the “Citizen CA” certificate authority.

With respect to the other CAs used by the Belgian State, we refer to following website where a link can be found to each CPS:

- Citizen CA eID Repository Website
- Foreigner CA eID Repository Website
- Belgium Root CA eID Repository Website

Note: Each has its own CP/CPS.

1.2 The eID Hierarchy

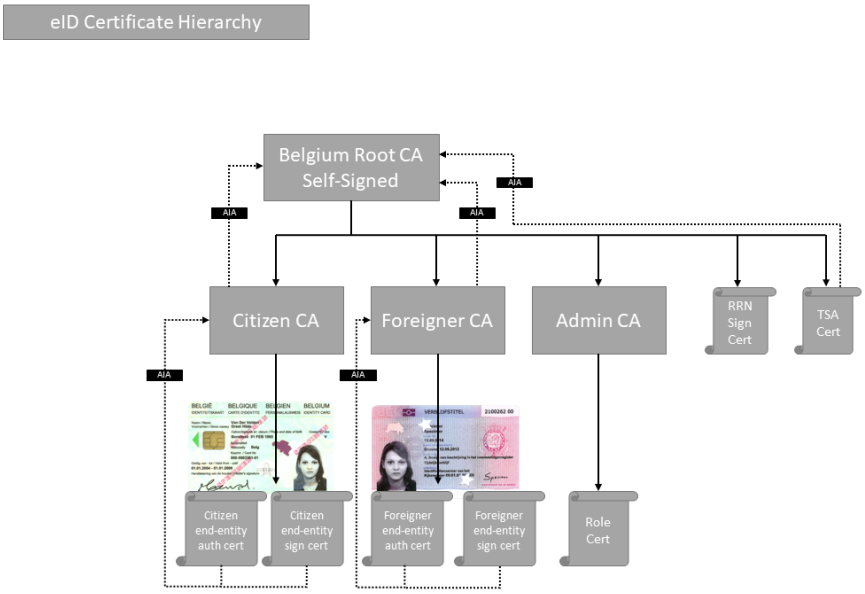

Figure: Belgian eID PKI Hierarchy

1.3 Document Name and Identification

Name of this document	*Belgian Certificate Policy & Practice Statement for eID PKI infrastructure Citizen CA*
Document version	*2.16.56.12.1.* **– v4.6** *This Certificate Policy is identified by its name and version number.*
	This document OID replaces the following OIDs ***2.16.56.1.1*** ***2.16.56.9.1*** ***2.16.56.10.1*** *This Citizen CP/CPS obsoletes all other Citizen CP/CPS versions as of the date of publication.*
OID referring to this document	*The identifiers under control of certipost :* ***BRCA (1)*** *OID: 2.16.56.1.1.1.2 – Citizen CA* *OID: 2.16.56.1.1.1.2.1 – Citizen Signing certificate* *OID: 2.16.56.1.1.1.2.2 – Citizen Authentication certificate*
	BRCA 2 *OID: 2.16.56.9.1.1.2 – Citizen CA* *OID: 2.16.56.9.1.1.2.1 – Citizen Signing certificate* *OID: 2.16.56.9.1.1.2.2 – Citizen Authentication certificate*
	BRCA 3 *OID: 2.16.56.10.1.1.2 – Citizen CA* *OID: 2.16.56.10.1.1.2.1 – Citizen Signing certificate* *OID: 2.16.56.10.1.1.2.2 – Citizen Authentication certificate*
	BRCA 4 *OID: 2.16.56.12.1.1.2 – Citizen CA* *OID: 2.16.56.12.1.1.2.1 – Citizen Signing certificate* *OID: 2.16.56.12.1.1.2.2 – Citizen Authentication certificate*

1.4 PKI Participants

Several parties make up the participants of this PKI hierarchy. The parties mentioned hereunder, including all Certification Authorities (CAs), the Registration Authorities (RA), the Local Registration Authorities (LRAs - the municipalities), citizens and relying parties are collectively called PKI participants.

1.4.1 Certification Authorities

A Certification Authority is an organisation that issues and manages digital certificates corresponding to digital identity.

The certification authority provides the necessary services to check the validity of the issued certificates.

certipost assumes, on behalf of and for the account of the Belgian authorities, both the roles of CA and TSP for the Citizen CAs and is in that capacity responsible for the citizen certificates issued under the Citizen CA. The Belgian authorities are the TSP responsible for the Belgium Root CAs and for the CA certificates issued under the Belgian Root CA.

The “Citizen CA” is a Certification Authority which operates within a grant of authority for issuing Citizen Certificates. This grant has been provided by the BRCA.

The “Citizen CA” ensures the availability of all services pertaining to the certificates, including the issuing, revocation and status verification, as they may become available or required in specific applications.

The “Citizen CA” is established in Belgium. It can be contacted at the address published further in this CPS. To deliver CA services; including the issuance, suspension, revocation, renewal, status verification of certificates; the “Citizen CA” operates in a secure facility and provides for a disaster recovery facility in Belgium.

The domain of responsibility of the “Citizen CA” comprises the overall management of the certificate lifecycle including:

- Issuance;
- Suspension/Unsuspension;
- Revocation;
- Status verification (Certificate Status Service);
- Directory service.

1.4.2 Registration Authorities

The National Register (RRN), together with the municipalities, is the RA within the “Citizen CA” domain to the exclusion of any other. The RRN is established and acts under the provisions of the National Register Law and under the Law on Identity Cards.

The Registration Authority (“RA”) which, on behalf of the TSP, certifies that a given public key belongs to a given entity (i.e. a natural person) by issuing a digital certificate and signing it with its private key. For the Belgian Electronic Identity Card, the “National Register”, which is a public administration belonging to the Federal Public Service of Internal Affairs, accomplishes the role of “RA”. Most of the actual registration operations are performed by the local administrative services in the municipalities, the so called Local Registration Authorities (further called "LRA"). Based on this process, the RA requests the CA to issue a certificate.

In particular, RA and LRA are responsible for:

- The identity validation of citizens;
- The registration of the to be certified data;
- The authorization to issue a certificate for a particular citizen;
- Taking care that citizen’s certificates are stored on the correct identity card;
- Taking care that a citizen receives that precise card he is expected to receive and activate the card in question only when dully attributed to the correct citizen;
- The SRA (Suspension and Revocation Authority): the entity who suspends and/or revokes the certificates according to the referenced ETSI standards.

1.4.3 Subscriber & Subject

certipost, assuming the role of TSP for the Citizen CAs, has a contractual agreement with the Belgian authorities. As such, we can regard the government as the “subscriber” to the CA services in the “Citizen CA” domain.

The subjects of the CA services in the “Citizen CA” domain are citizens who are holder of an Electronic Identity Card with activated certificates according to the Law on Identity Cards. Further in this document, the term subject can be substituted by the term “citizen”. These citizens:

- Are identified in both Citizen Certificates;
- Hold the private keys corresponding to the public keys that are listed in their respective Citizen Certificates.

The citizens have the right to indicate at the beginning of the Electronic Identity Card application process whether they want to have Certificates. The Electronic Identity Card is delivered to the citizens with Citizen Certificates loaded. For citizens who do not wish to have the Citizen Certificates, one or no certificates can be present on the eID card. Refer to document **EID-DEL-004 eID PKI Hierarchy certificate profile (cfr. Appendix C)** for additional information.

The authentication certificate will not be installed for citizens who have not yet reached the age of 6. The electronic signature certificate will not be installed for citizens not having reached the age of 18.

	Authentication certificate	Electronic Signature certificate
0 – 6 year	0	0
6 – 18 year	X	0
+18 year	X	X

The table above describes the certificates and their applicable age categories.

1.4.4 Relying Parties

Relying parties are entities including natural or legal persons who rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a citizen's certificate.

1.4.5 Other Participants

1.4.5.1 Card Manufacturer

The Card Manufacturer for "Citizen CA" is the "Zetes nv/sa", having its registered offices at 1130 Brussels 3 Straatsburgstraat/Rue de Strasbourg, contracted to do this by the Belgian Authorities in the capacity of the eID project contracting authority.

The Card Manufacturer customises non-personalised smart cards to personalised Electronic Identity Cards by printing the citizen identity data and photograph on the card.

The Card Manufacturer also provides the following services:

- Generation of the key pairs required within the card;
- Storage of both eID Citizen certificates on the card;
- Generation of the personal activation codes of the requestor and the municipality, and the initial PIN code of the requestor;
- Loading the active governmental root certificates on the card;
- Provision of the Electronic Identity Card to the municipality;
- Provision of the personal activation code and PIN code to the requestor;
- Recording the data in the Register of Identity Cards.

1.4.5.2 Subcontractor

certipost employs a third party subcontractor to support the TSP with operational tasks and responsibilities. The subcontractor provides the technical support for following services:

- Certificate issuance;
- Certificate revocation / suspension;
- Certificate validation;
    - OCSP;
    - CRL & delta CRL.

A service level agreement exists between the subcontractor, certipost and the government that determines the quality of these provided services in terms of performance and availability. The subcontractor reports on a monthly basis their measured performance indicators to prove compliance with the service level agreement. The subcontractor also provides organisational support during key ceremonies.

1.5 Certificate Usage

Certain limitations apply to the usage of the certificates on the Electronic Identity Card.

Two types of certificates are issued by the “Citizen CA” each with their specific use case:

- Authentication certificate: This certificate is used for electronic authentication transactions that support accessing web sites and other online content;
- Qualified electronic signature certificate: This certificate is used to create qualified electronic signatures.

Every eID provided to a citizen can contain both an authentication certificate and a qualified electronic signature certificate given that state of the art security requirements recommend not using authentication certificates for electronic signature purposes. The “Citizen CA” therefore declines all liability towards relying parties in all cases where the authentication certificate was used for the generation of electronic signatures.

1.6 Policy Administration

1.6.1 Organization Administering the Document

Policy administration is reserved to certipost which can be contacted via:

- Postal service:

  certipost nv / sa
  Policy administration - Citizen CA
  Muntcentrum / Centre Monnaie
  1000 Brussels

- Mail:

  To: eid.cps@bpost.be
  Subject: Policy administration - Citizen CA

1.6.2 Contact Person

The main contact for any questions or suggestions regarding the Citizen CA CP/CPS, is to be found under § 1.6.1 ORGANIZATION ADMINISTERING THE DOCUMENT.

All feedback, positive or negative, is welcome and should be submitted to the above e-mail address to ensure that it is dealt with appropriately and in due time.

1.6.3 Person Determining CPS Suitability for the Policy

In conformity with the ETSI EN 319 411-2 standard supporting the European Regulation (Regulation 910/2014) certipost assumes the management of its TSP tasks via a PKI management board (CEPRAC) incorporating all the required expertise.

By its official participation to the regular eID progress meetings, where all the above mentioned parties are dully represented, certipost gathers all necessary information and asks all relevant questions to these parties in order to perform its TSP responsibility. Issues and questions are analysed within the PKI management board, and if necessary proposition/correction are brought to the progress meeting.

The PKI management board will escalate, towards the eID Steering Committee led by the Belgian Authorities, any issue that could not be solved by this process. This Steering Committee has the possibility to call external experts to get additional advice and bears dispute settlement responsibility.

1.7 Definitions and Acronyms

1.7.1 Definitions

Lists of definitions can be found at the end of this CPS.

1.7.2 Acronyms

Lists of acronyms can be found at the end of this CPS.

2 Publication and Repository Responsibilities

2.1 Repositories

The "Citizen CA" retains an up-to-date online repository of documents where it makes certain disclosures about its practices, procedures and the content of certain of its policies including its CPS, which is accessible at eID Repository Website. The CA reserves its right to make available and publish information on its policies by any means it sees fit.

The Repository is available at the following website eID Repository Website.

2.2 Publication of Certification Information

The CA publishes a repository that lists all Digital Certificates issued and all the Digital Certificates that have been revoked. The location of the repository and Online Certificate Status Protocol (further called "OCSP") responders are given in the individual Certificate Profiles more fully disclosed in **EID-DEL-004 eID PKI Hierarchy certificate profile (cfr. Appendix C).** The CA sets up and maintains a repository of all certificates it has issued. This repository also indicates the status of a certificate issued.

Due to their sensitivity the CA refrains from making publicly available certain subcomponents and elements of such documents including certain security controls, procedures related with the functioning of inter alia registration authorities, internal security polices etc. Such documents and documented practices are, however, conditionally available to audit to designated parties that the TSP owes duty to.

The "Citizen CA" publishes information about the certificates in (an) online publicly accessible repository-(ies) under the "eid.belgium.be" Internet domain. The CA reserves its right to publish certificate status information on third party repositories.

2.3 Time or Frequency of Publication

PKI participants are notified that the CA may publish information they submit directly or indirectly to the CA on publicly accessible directories for purposes associated with the provision of electronic certificate status information. The CA publishes certificate status information in frequent intervals as indicated in this CPS.

Approved versions of documents to be published on the repository are uploaded conform the change management process.

2.4 Access Controls on Repositories

While the “Citizen CA” strives to keep access to its public repository free of charge, it might, within the framework of its contract with the Belgian government, charge for services such as the publication of status information on third party databases, private directories, etc.

The OCSP service, web interface certificate status verification service, the certificate repository and the Certificate Revocation Lists (CRLs and delta CRLs) are publicly available on the CA site on the Internet and are available via the networks of the Belgian State.

Within the framework of the contract with the Belgian State, access restrictions to any of these services provided by the “Citizen CA” includes:

- Through the publicly available interface to the certificate repository, only a single certificate can be delivered per query made by any party except of the RA;
- The CA may take reasonable measures to protect against abuse of the OCSP, Web interface status verification and CRL and delta CRL download services;
- The CA should not restrict the processing of OCSP requests for any party, who, by the nature of its activities, requires frequent OCSP status verification.

3 Identification and Authentication

3.1 Naming

The rules concerning naming and identification of citizens for citizen certificates are the same as the legal rules applied to naming and identification of citizens on identity cards.

3.1.1 Types of Names

End user certificate Subject fields attributes are described in document **EID-DEL-004 eID PKI Hierarchy certificate profile (cfr. Appendix C).**

3.1.2 Need for Names to be Meaningful

See section 3.1.1

3.1.3 Anonymity or Pseudonymity of Subscribers

Section not applicable.

3.1.4 Rules for Interpreting Various Name Forms

See section 3.1.1

3.1.5 Uniqueness of Names

The DN of an end user certificate must be unique.

3.1.6 Recognition, Authentication, and Role of Trademarks

Section not applicable.

3.2 Initial Identity Validation

The identification of the citizen who applies for an Electronic Identity Card is done according to the procedures and regulations applicable to the delivery of Electronic Identity Cards. The RA specifies the procedures to be implemented by the LRAs.

The applicable procedures can be found at:

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

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

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

3.2.1 Method to Prove Possession of Private Key

In accordance with European and Belgian Signature law, private keys are generated on secure signature smart cards. The Card manufacturer is responsible for securing the smart card on which the Qualified Signature Creation Device (QSCD) resides with a Personal Identification Number (PIN). The Certificate Holder, the citizen, is responsible for keeping the PIN for their smart card secret. certipost checks bi-yearly that the Belgian eID card is on the EU QSCD list.

3.2.2 Authentication of Organization Identity

Section not applicable.

3.2.3 Authentication of Individual Identity

See section 3.2

3.2.4 Non-Verified Subscriber Information

Section not applicable.

3.2.5 Validation of Authority

See section 3.2

3.2.6 Criteria for Interoperation

Section not applicable.

3.3 Identification and Authentication for Re-Key Requests

The identification and authentication of the citizen making a re-key request will be done according the procedures specified by the RA and implemented by the LRAs.

The applicable procedures can be found at:

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

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

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

3.3.1 Identification and Authentication for Routine Re-Key

See section 3.3

3.3.2 Identification and Authentication for Re-Key after Revocation

See section 3.3

3.4 Identification for Revocation Request

The identification of the citizen who applies for a revocation of his Citizen Certificate will be done according to the procedures and regulations applicable to the delivery of Electronic Identity Cards.

The identification and authentication of holders wishing the revocation of their Citizen Certificates will be performed by the entity that receives the request. This can be:

- The municipality;
- The police;
- DOCSTOP 00800 2123 2123 or +32 2 518 2123.

Subsequently, this entity refers promptly all revocation requests via the RA to the CA. The RA is the single contact point for the CA to obtain a revocation request.

The RA sends the digital signed Revocation request to the CA, by means of a secured network. The CA confirms the revocation to the RA.

4 Certificate Life-Cycle Operational Requirements

For all entities within the TSP domain including the LRAs, citizens, relying parties and/or other participants there is a continuous obligation to inform directly or indirectly the RA of all changes in the information featured in a certificate during the operational period of such certificate or of any other fact that materially affects the validity of a certificate. The RA will then take appropriate measures to make sure that the situation is rectified (e.g. ask the CA for the revocation of the existing certificates and the generation of new certificates with the correct data).

The CA issues, revokes or suspends certificates only at the request of the RA or the TSP to the exclusion of any other, unless explicitly instructed so by the RA.

To fulfil its tasks the TSP uses the services of third party agents. Towards the citizens and relying parties the TSP assumes full responsibility and accountability for acts or omissions of all third party agents it uses to deliver certification services.

4.1 Certificate Application

4.1.1 Who can submit a Certificate Application

The subscription process initiated by the municipalities (i.e. the LRA) to request certificates for the subjects (the citizens) is an integral part of the applied enrolment process for the Electronic Identity Card. The LRA implements a procedure for citizen enrolment as provided by the RA.

4.1.2 Enrolment Process and Responsibilities

Following approval of the certificate application, the RA sends a certificate issuance request to the CA. The CA does not verify the completeness, integrity and uniqueness of the data, presented by the RA, but relies completely on the RA for the correctness of all data. The CA only verifies that the certificate serial number assigned to the certificate request by the RA is indeed a unique serial number that has not yet been used for any other Citizen Certificate, in which case it notifies the RA.

All requests from the RA are granted approval provided that:

- They are validly formatted;
- Use the proper secure communication channel;
- All appropriate verifications have been performed as defined in the CA contract.

The CA verifies the identity of the RA based on provided credentials.

The CA ensures that the issued certificate contains all data that was presented to it in the request of the RA and especially a serial number assigned to the certificate by the RA.

Following issuance of a certificate, the CA posts an issued certificate on a repository and suspends the certificate. The certificate is thereafter delivered to the RA.

The RA requests the Card Manufacturer to load the issued Citizen Certificates on the Electronic Identity Card. The Card Manufacturer delivers the Electronic Identity Card securely with the Citizen Certificates to the LRA.

4.2 Certificate Application Processing

The LRA acts upon a certificate application to validate an applicant's identity as foreseen in the request of the Electronic Identity Card process. The procedures for the validation of an applicant's identity are addressed in a dedicated document.

Following a certificate application, the LRA either approves or rejects the Electronic Identity Card application, i.e. including the certificate application. If the application is approved, the LRA transmits the registration data to the RA. The RA in its turn either approves or rejects the application.

The applicable procedures can be found at:

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

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

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

4.2.1 Performing Identification and Authentication Functions

Section not applicable.

4.2.2 Approval or Rejection of Certificate Applications

Section not applicable.

4.2.3 Time to Process Certificate Applications

Section not applicable.

4.3 Certificate Issuance

Following approval of the certificate application, the RA sends a certificate issuance request to the CA. The CA does not verify the completeness, integrity and uniqueness of the data, presented by the RA, but relies completely on the RA for the correctness of all data. The CA only verifies that the certificate serial number assigned to the certificate request by the RA is indeed a unique serial number that has not yet been used for any other Citizen Certificate, in which case it notifies the RA.

All requests from the RA are granted approval provided that:

- They are validly formatted;
- Use the proper secure communication channel;
- All appropriate verifications have been performed as defined in the CA contract.

The CA verifies the identity of the RA based on provided credentials.

The CA ensures that the issued certificate contains all data that was presented to it in the request of the RA and especially a serial number assigned to the certificate by the RA.

Following issuance, the CA suspends the certificate and is delivered to the RA.

The RA requests the Card Manufacturer to load the Citizen Certificates on the Electronic Identity Card. The Card Manufacturer delivers securely the Electronic Identity Card with the Citizen Certificates to the LRA.

4.3.1 CA Actions during Certificate Issuance

Section not applicable.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Section not applicable.

4.4 Certificate Acceptance

After production of the Electronic Identity Card, it is in a non-activated state. The LRA activates the Electronic Identity Card in the presence of the citizen. Both the citizen and the RA require the activation data for the card, which has to be supplied by the Card Manufacturer in a secure manner. The card can only be activated when using the combined activation data from the RA and the citizen.

4.4.1 Conduct Constituting Certificate Acceptance

Objections to accepting an issued certificate are notified via the LRA to the RA in order to request the CA to revoke the certificates.

4.4.2 Publication of the Certificate by the CA

Section not applicable.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Section not applicable.

4.5 Key Pair and Certificate Usage

The responsibilities relating to the use of keys and certificates include the ones addressed below.

4.5.1 Subject Private Key and Certificate Usage

Unless otherwise stated in this CPS, citizen's duties include the ones below:

- Refraining from tampering with a certificate;
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private keys;
- Only using certificates for legal and authorised purposes in accordance with this CPS.

4.5.2 Relying Party Public Key and Certificate Usage

A party relying on a certificate will:

- Validate a certificate by using a CRL, delta CRL, OCSP or web based certificate validation in accordance with the certificate path validation procedure;
- Trust a certificate only if it has not been suspended or revoked;

- Rely on a certificate, as may be reasonable under the circumstances;
- To verify the validity of a digital certificate, relying parties must always check the validity period of the certificate and the validity declaration of the certificate by the CA Service (via OCSP, CRL, delta CRL or web interface) prior to relying on information provided in a certificate.

4.6 Certificate Renewal

According to RFC 3647 certificate renewal is defined as "*The issuance of a new Certificate without changing the Public Key or any other information in the Certificate*". For End Entity Certificates (authentication and signing certificate), this capability is not supported.

4.6.1 Circumstance for Certificate Renewal

Certificate renewal is not supported.

4.6.2 Who May Request Renewal

See section 4.6.1

4.6.3 Processing Certificate Renewal Requests

See section 4.6.1

4.6.4 Notification of New Certificate Issuance to Subscriber

See section 4.6.1

4.6.5 Conduct constituting acceptance of a renewal certificate

See section 4.6.1

4.6.6 Publication of the renewal certificate by the CA.

See section 4.6.1

4.6.7 Notification of certificate issuance by the CA to other entities

See section 4.6.1

4.7 Certificate Re-Key

According to RFC 3647 a certificate re-key is defined as "*… a subscriber or other participant generating a new key pair and applying for the issuance of a new certificate that certifies the new public key*". In the context of eID this means that the subject (the citizen) will apply for issuance of a new certificate with the same identifying information but with a different public key and validity period. Due diligence, Key Pair generation, delivery and management are performed in accordance with this CP/CPS.

4.7.1 Circumstance for Certificate Re-Key

Certificate re-keys are supported.

4.7.2 Who May Request Certification of a New Public Key

See Section 4.1.1

4.7.3 Processing Certificate Re-Keying Requests

Certificate re-key requests are processed in the same manner as requests for new authentication or signing certificates and in accordance with the provisions of this CP/CPS.

4.7.4 Notification of New Certificate Issuance to Subscriber

Section not applicable.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Section not applicable.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Section not applicable.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Section not applicable.

4.8 Certificate Modification

Section not applicable.

4.9 Certificate Suspension and Revocation

When a citizen orders a new eID, the card will be delivered to his / her municipality. The citizen certificates will remain in a suspended state. If the citizen does not retrieve the eID promptly, the municipality can send out a reminder. As long as the citizen does not pick the eID card, the certificates will remain in the suspended state.

To request the revocation of a certificate, a citizen must contact an LRA, the police, or DOCSTOP. Note that the LRA opening hours are limited, DOCSTOP is available 24 hours per day, 7 days a week.

Inactivated Identity Cards with suspended certificates are directly delivered to Belgian citizens living abroad. Afterwards, they can pass by the consulate in order to activate the chip and the certificates. However, this activation is not limited in time.

The police, LRA, DOCSTOP or the RA requests promptly the revocation of the Citizen Certificates via the RA after:

- Having received notice that a suspicion exist, that there has been: a loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of his Citizen Certificates;
- The performance of an obligation of the LRA under this CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, there is a suspicion that another person's information is materially threatened or compromised;

- Having received notice by the citizen that there has been: a loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of his Citizen Certificates;
- There has been a modification of the information contained in a Citizen Certificate;
- The performance of an obligation of the RA under this CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, another person's information is materially threatened or compromised;
- A legal obligation imposed on the RA.

Upon request from the RA or the TSP the CA revokes the Citizen Certificates.

In the case that the subject requested the revocation of a certificate through DOCSTOP, the subject is informed of the change of the status of the certificate through a letter sent to their official address.

Under specific circumstances (e.g. circumvention of a disaster, a CA key compromise, a security breach …), the TSP may request suspension and / or revocation of certificates.

The TSP will ask the eID TSP Steering Committee the authorisation to perform such revocations. According to the level of emergency, it is however possible that the eID Steering Committee is warned after completion of the process. The RA takes care that the concerned citizens are warned of such suspension/revocation.

Relying parties must use online resources made available by the CA through its repository to check the status of certificates before relying on them. The CA updates OCSP, the Web interface certification status verification service, CRLs and delta CRLs accordingly. CRLs are updated frequently with minimum intervals of three hours.

The CA grants access to OCSP resources and a website to which status inquiries can be submitted. In addition, for any certificate issued under the Citizen CA, the revocation status information shall be available beyond the validity period of the certificate through the CRL.

4.9.1 Circumstances for Revocation

The CA publishes notices of suspended or revoked certificates in the eID Repository Website.

4.9.2 Who can Request Revocation

See section 4.9.

4.9.3 Procedure for Revocation Request

See section 4.9.

4.9.4 Revocation Request Grace Period

The Revocation Request Grace Period is the period from when the subject (i.e. the citizen) requested a certificate revocation by contacting the LRA, the police or DOCSTOP until the certificate revocation is reflected in the certificate validation services.

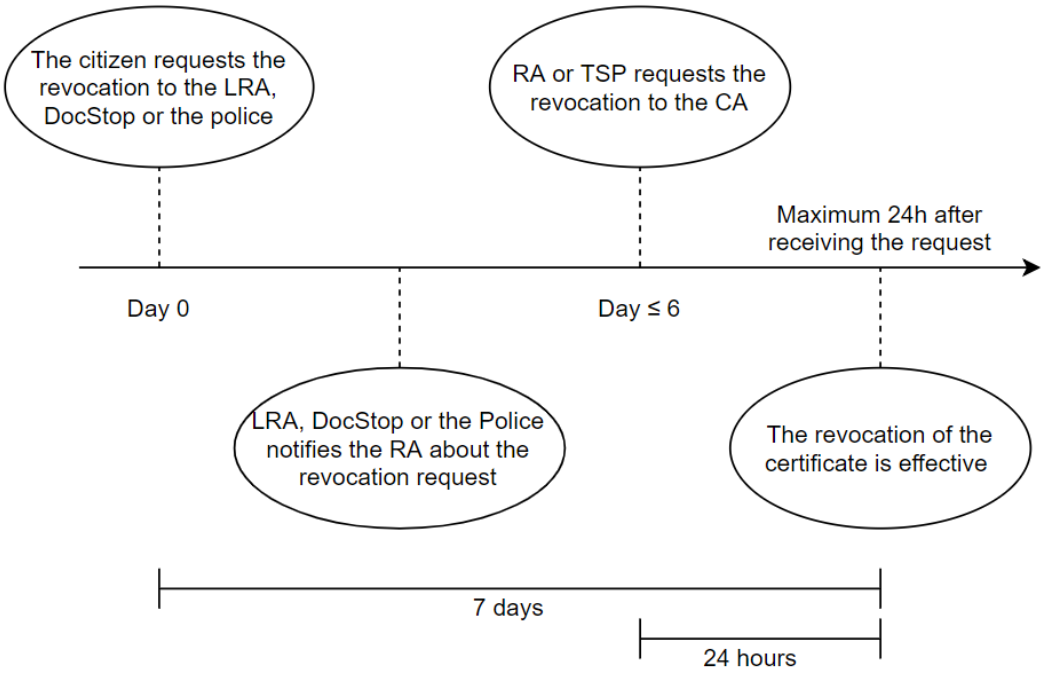

Figure 1: Revocation Timeline

Figure 1: Revocation Timeline depicts the revocation timeline and shows that in the context of eID there is a maximum of 6 days until the CA receives the request of revocation, and a maximum of 24 hours from that moment until effective revocation.

The grace period for processing the revocation request is 7 calendar days. However, when the revocation request is received by the CA, the updated status is reflected within 3 hours in the Validation Services.

4.9.5 Time within which CA Must Process the Revocation Request

The CA will revoke a Citizen Certificate after receiving the revocation request from the RA as quickly as practical after validating the revocation request. The maximum delay between receipt of a revocation request or report and the decision to change its status information being available to all relying parties is at most 24 hours.

Generally following timeframes are used:

- Revocation requests received three or more hours before CRL issuance are processed before the next CRL is published;
- Revocation requests received within three hours of CRL issuance are processed before the following CRL is published;
- Revocation requests are reflected in the OCSP certificate validation service within three hours of receiving the request.

4.9.6 Revocation Checking Requirement for Relying Parties

See **EID-DEL-004 eID PKI Hierarchy certificate profile (cfr. Appendix C)**.

4.9.7 CRL Issuance Frequency (if applicable)

See **EID-DEL-004 eID PKI Hierarchy certificate profile (cfr. Appendix C)**.

4.9.8 Maximum Latency for CRLs (if applicable)

See **EID-DEL-004 eID PKI Hierarchy certificate profile (cfr. Appendix C)**.

4.9.9 On-Line Revocation/Status Checking Availability

See **EID-DEL-004 eID PKI Hierarchy certificate profile (cfr. Appendix C)**.

4.9.10 On-Line Revocation Checking Requirements

See **EID-DEL-004 eID PKI Hierarchy certificate profile (cfr. Appendix C)**.

4.9.11 Other Forms of Revocation Advertisements Available

Section not applicable.

4.9.12 Special Requirements Re-Key Compromise

Section not applicable.

4.9.13 Circumstances for Suspension

See section 4.9.

4.9.14 Who can Request Suspension

See section 4.9.

4.9.15 Procedure for Suspension Request

See section 4.9.

4.9.16 Limits on Suspension Period

See section 4.9

4.10 Certificate Status Services

The CA makes available certificate status checking services including CRLs, delta CRLs, OCSP and appropriate Web interfaces.

4.10.1 CRL and delta CRLs

A delta CRL lists additions since the publishing of the last base CRL.

CRLs and delta CRLs are signed and time-marked by the CA.

A CRL is issued within minimum intervals of three hours at an agreed time. A delta CRL is issued each three hours, according to an agreed time schedule. CRLs and delta CRLs are signed and time marked by the CA. The CRLs and delta CRLs can be found at http://crl.eid.belgium.be.

4.10.2 OCSP

The CA makes OCSP responses available to the Belgian Public Administration to use them through its own Public Administration networks.

A simple web interface for status verification services allows a user to obtain status information on a certificate. The CA makes these web interfaces for status verification services available to the Belgian Public Administration for use through and within its own Public Administration networks.

Web interface for status verification service http://status.eid.belgium.be.

The OCSP responders can be reached at http://ocsp.eid.belgium.be or http://ocsp.eid.belgium.be/2.

4.10.3 Operational Characteristics

*See **EID-DEL-004 eID PKI Hierarchy certificate profile (CFR. APPENDIX C)**.*

4.10.4 Service Availability

Certificate status services are available 24 hours a day, 7 days a week.

Outside maintenance windows, for each calendar month, the total time of unavailability of each of the following CA services, measured in minutes, cumulated over the whole month should not be more than 0.5% of the total number of minutes of that calendar month:

- OCSP certificate status verification as a result of a request by the RRN, a subject or a relying party;
- Download of CRLs or delta CRLs over the Internet or the networks of the government;
- Web interface certificate status verification service.

The unavailability of the OCSP service, CRL and delta CRL download service and the Web interface status verification service includes the unavailability of the local infrastructure of the CA, including local servers, networks and firewalls, but does not include the unavailability of (parts of) the Internet and unavailability of local infrastructure of the service requestor.

The CA internally archives the following items, data and documents pertaining to its service:

- CRLs and delta CRLs:
    - CRLs and delta CRLs are archived for a period of at least 25 years after publishing.

4.10.5 Optional Features

The CA should not restrict the processing of OCSP requests for any party, who, by the nature of its activities, requires frequent OCSP status verification.

4.11 End of Subscription

Section not applicable.

4.12 Key Escrow and Recovery

Key escrow and recovery are not allowed.

5 Facility, Management, and Operational Controls

This section describes non-technical security controls used by the ”Citizen CA” and the other PKI partners, to perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archiving.

5.1 Physical Controls

The TSP implements physical controls on its own premises. The TSP operator’s physical controls include the following:

- The sites of the TSP host the infrastructure to provide the TSP services. The TSP sites implement proper security controls, including access control, intrusion detection and monitoring. Access to the sites is limited to authorised personnel listed on an access control list, which is subject to audit;
- Strict access control is enforced to all areas containing highly sensitive material and infrastructure including material and infrastructure pertaining to signing certificates, CRLs and delta CRLs, OCSP and archives.

5.1.1 Site Location and Construction

The TSP operators secure premises are located in an area appropriate for high-security operations. These premises feature numbered zones and locked rooms, cages, safes, and cabinets.

5.1.2 Physical Access

Physical access is restricted by implementing mechanisms to control access from one area of the facility to another, or access to high-security zones, such as locating TSP operations in a secure computer room physically monitored and supported by security alarms and requiring movement from zone to zone to be accomplished using a token and access control lists.

5.1.3 Power and Air Conditioning

Power and air conditioning operate with a high degree of redundancy.

5.1.4 Water Exposures

Premises are protected from any water exposures.

5.1.5 Fire Prevention and Protection

The TSP implements prevention and protection as well as measures against fire exposures.

5.1.6 Media Storage

Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.

5.1.7 Waste Disposal

To prevent unwanted disclosure of sensitive data waste is disposed of in a secure manner.

5.1.8 Off-Site Backup

The TSP implements a partial off-site backup.

5.2 Procedural Controls

The TSP follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of electronic signature-related technologies.

The TSP obtains a signed statement from each member of the staff on not having conflicting interests with the TSP, maintaining confidentiality and protecting personal data.

All members of the staff operating the key management operations, administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position.

The TSP conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to make a reasonable attempt to determine their trustworthiness and competence.

Where dual control is required at least two trusted staff members need to bring their respective and split knowledge in order to be able to proceed with the ongoing operation.

The TSP ensures that all actions with respect to the TSP can be attributed to the system of the TSP and the member of the TSP staff that has performed the action.

5.2.1 Trusted Roles

The TSP separates among the following discreet work groups:

- TSP operating personnel that manages operations on certificates;
- Administrative personnel to operate the platform supporting the TSP;
- Security personnel to enforce security measures.

5.3 Personnel Controls

The TSP implements certain security controls with regard to the duties and performance of the members of its staff. These security controls are documented in a policy and include the areas below.

5.3.1 Qualifications, Experience, and Clearance Requirements

The TSP performs checks to establish the background, qualifications, and experience needed to perform within the competence context of the specific job. Such background checks include:

- Criminal convictions for serious crimes;

- Misrepresentations by the candidate;
- Appropriateness of references;
- Any clearances as deemed appropriate.

5.3.2 Background Check Procedures

The TSP makes the relevant checks to prospective employees by means of status reports issued by a competent authority, third party statements or signed self-declarations.

5.3.3 Training Requirements

Each TSP party makes available training for their personnel to perform their TSP functions.

5.3.4 Retraining Frequency and Requirements

Periodic training updates might also be carried out to establish continuity and updates in the knowledge of the personnel and procedures.

5.3.5 Job Rotation Frequency and Sequence

Section not applicable.

5.3.6 Sanctions for Unauthorised Actions

The TSP sanctions personnel for unauthorised actions, unauthorised use of authority, and unauthorised use of systems for the purpose of imposing accountability on a participant's personnel, as it might be appropriate under the circumstances.

5.3.7 Independent Contractor Requirements

Independent TSP subcontractors and their personnel are subject to the same background checks as the TSP personnel. SEE 5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS.

5.3.8 Documentation Supplied to Personnel

Each TSP party makes available documentation to personnel, during initial training, retraining, or otherwise.

5.4 Audit Logging Procedures

Audit logging procedures include event logging and systems auditing, implemented for the purpose of maintaining a secure environment. The CA implements the following controls:

The CA event logging system records events that include but are not limited to:

- Issuance of a certificate;
- Revocation of a certificate;
- Suspension of a certificate;
- (Re)activation of a certificate;

- Automatic revocation;
- Publishing of a CRL or delta CRL.

The TSP audits all event-logging records. Audit trail records contain:

- The identification of the operation;
- The date and time of the operation;
- The identification of the certificate involved in the operation;
- The identity of the transaction requestor.

In addition, the TSP maintains internal logs and audit trails of relevant operational events in the infrastructure, including, but not limited to:

- Start and stop of servers;
- Outages and major problems;
- Physical access of personnel and other persons to sensitive parts of the TSP site;
- Back-up and restore;
- Report of disaster recovery tests;
- Audit inspections;
- Upgrades and changes to systems, software and infrastructure;
- Security intrusions and attempts at intrusion.

Other documents that are required for audits include:

- Infrastructure plans and descriptions;
- Physical site plans and descriptions;
- Configuration of hardware and software;
- Personnel access control lists.

The TSP ensures that designated personnel reviews log files at regular intervals and detects and reports anomalous events.

Log files and audit trails are archived for inspection by the authorised personnel of the CA, the RA and designated auditors. The log files should be properly protected by an access control mechanism. Log files and audit trails are backed up.

Auditing events are not given log notice.

5.4.1 Types of Events Recorded

The TSP retains in a trustworthy manner records of digital certificates, audit data, TSP systems information and documentation.

5.4.2 Frequency of Processing Log

The CA reviews the audit logs in search of anomalies or alerts in a regular manner.

5.4.3 Retention Period for Audit Log

The TSP retains in a trustworthy manner records of digital certificates for a term as indicated under article 5.5 if this CPS.

5.4.4 Protection of Audit Log

Only the records administrator (member of staff assigned with the records retention duty) may access a TSP archive. Measures are taken to ensure:

- Protection against modification of archive, such as storing the data on a write once medium;
- Protection against deletion of archive;
- Protection against deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to unused media.

The TSP will act upon a potential application by the Belgian State of the procedure of article 14 of the Law 8 August 1983 *organising a national register of natural persons* and article 7 of the Law of 12 May 1927 *on military requisitions*. In such occurrence, the CA will act upon instructions issued by the person appointed by means of a Royal Decree with regard to data pertaining to Electronic Identity Cards and Citizen Certificates.

5.4.5 Audit Log Backup Procedures

A differential back up of the TSP archives is carried out on a daily basis during working days.

5.4.6 Audit Collection System.

The TSP archive collection system is internal.

5.4.7 Notification to Event-Causing Subject

Section not applicable.

5.4.8 Vulnerability Assessments

Section not applicable.

5.5 Records Archival

The TSP keeps internal records of the following items:

- All certificates for a period of a minimum of 25 years after the expiration of that certificate;
- Audit trails on the issuance of certificates for a period of a minimum of 25 years after issuance of a certificate;
- Audit trail of the revocation of a certificate for a period of a minimum of 25 years after revocation of a certificate;
- CRLs and delta CRLs for a minimum of 25 years after publishing;

- The TSP should retain the very last back up of the CA archive for 25 years following the issuance of the last certificate.

The TSP keeps archives in a retrievable format.

The TSP ensures the integrity of the physical storage media and implements proper copying mechanisms to prevent data loss.

Archives are accessible to authorised personnel of the CA and the RA.

5.5.1 Types of Records Archived

The TSP retains in a trustworthy manner records of digital certificates, audit data, TSP systems information and documentation.

5.5.2 Retention Period for Archive

The TSP retains in a trustworthy manner records of digital certificates for a term as indicated under article 5.5 in this CPS. This requirement is verified by periodic check.

5.5.3 Protection of Archive

Only the records administrator (member of staff assigned with the records retention duty) may access a TSP archive. Measures are taken to ensure:

- Protection against modification of archive, such as storing the data on a write once medium;
- Protection against deletion of archive;
- Protection against deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to unused media.

The TSP will act upon a potential application by the Belgian State of the procedure of article 14 of the Law 8 August 1983 *organising a national register of natural persons* and article 7 of the Law of 12 May 1927 *on military requisitions*. In such occurrence, the CA will act upon instructions issued by the person appointed by means of a Royal Decree with regard to data pertaining to Electronic Identity Cards and Citizen Certificates.

5.5.4 Archive Backup Procedures

A differential back up of the TSP archives is carried out on a daily basis during working days.

5.5.5 Requirements for Time-Stamping of Records

Section not applicable.

5.5.6 Archive Collection System (Internal or External)

The TSP archive collection system is internal.

5.5.7 Procedures to Obtain and Verify Archive Information

Only TSP staff members with a clear hierarchical control and a definite job description may obtain and verify archive information.

The TSP retains records in electronic or in paper-based format.

5.6 Key Changeover

The Citizen CA has a schedule for the key changeover of the subordinated issuing CAs and issuing CA certificates (the Citizen CA certificates are available for download on the eID Repository Website):

At the end of each year an amount of Citizen CA certificates are generated in a key ceremony. This amount is determined by the TSP and government, and is based on the expected demand of End-Entity certificates in the next year. In the key ceremony, the Citizen CA certificates are issued by the BRCAs, which are long-living trust anchors of the eID PKI.

Once the new batch of Citizen CA certificates is put in the production environment, these issuing certificates will be used to issue the End-Entity certificates of the current year, and the previous batch of Citizen CA certificates will no longer be used for issuing new certificates. In other words, a Citizen CA certificate will only be used for one year to issue new certificates. A Citizen CA certificate shall be valid longer than any End-Entity certificate it has issued.

Once a Citizen CA certificate has expired or has been revoked the key material will be destroyed in the next key ceremony.

5.7 Compromise and Disaster Recovery

A business continuity plan has been implemented to ensure business continuity following a natural or other disaster.

All such measures are implemented based on ISO 27001.

The TSP establishes:

- Disaster recovery resources in dual locations sufficiently distant from each other;
- Fast communications between the two sites to ensure data integrity;
- A communication infrastructure from both sites to the RA supporting Internet communication protocols as well as agreed communication protocols used by the Belgian Public Administration;
- Disaster recovery infrastructure and procedures are tested at least yearly.

5.7.1 Incident and Compromise Handling Procedures

In a separate internal document the “Citizen CA” specifies applicable incident, compromise reporting and handling procedures. The TSP specifies the recovery procedures used in case computing resources, software, and/or data are corrupted or suspected of being corrupted.

The TSP establishes the necessary measures to ensure full and automatic recovery of the service in case of a disaster, corrupted servers, software or data.

5.7.2 Computing Resources, Software, and/or Data are Corrupted.

The TSP has specific recovery procedures in place in case computing resources, software, and/or data are corrupted or suspected of being corrupted.

5.7.3 Entity Private Key Compromise Procedures

In case of suspected or known compromise of Citizen CA private key, the TSP Crisis Management procedures are enacted according to the Incident Management process and with approval from certipost senior management and the representatives of the Belgian government. Notification to involved parties is performed through a communication plan and in case of CA Certificate revocation is required, the revoked status is communicated to relying parties through eID Repository Website or through the eID CRL Website.

5.7.4 Business Continuity Capabilities after a Disaster

The TSP has developed the capability to recover its CA operations within four (4) hours following a disaster with support for all the key functions i.e. certificate issuance, certificate revocation, and publication of CRL information.

5.8 CA or RA Termination

From the moment that the TSP receives notice from the Belgian government that its contract will be terminated, and/or from the moment that its contract will be prematurely annulled, the TSP will consult with the Belgian State to determine which steps are required to (1) guarantee the smooth transition of the delivery of services to the new TSP, and to (2) ensure the destruction, deletion, restitution and/or security of the information, personal data and files received by the TSP in the fulfilment of its duty as TSP in accordance to EU regulation 910/2014 laying down some rules in relation to the legal framework for electronic signatures and certification services.

6 Technical Security Controls

This section defines the security measures the CA takes to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares).

6.1 Key Pair Generation and Installation

The CA protects its private key(s) in accordance with this CPS. The CA uses private signing keys only for signing certificates, CRLs, delta CRLs and OCSP responses in accordance with the intended use of each of these keys.

The CA will refrain from using its private keys used within the CA in any way outside the scope of the Citizen CA domain.

6.1.1 Key Pair Generation

The CA and RA use a trustworthy process for the generation of its CA private key according to a documented procedure. The CA distributes the secret shares of its private key(s). The TSP has the authority to transfer such secret shares to authorised secret-shareholders according to a documented procedure.

The key pairs for the subordinated issuing CAs of the Citizen CA (Issuing CA Keys) have been generated in an off line Hardware Security Module (HSM) that meets at least FIPS 140-2 level 3 requirements. Subsequently, the Issuing CA keys have been cloned into an on line HSM meeting at least FIPS 140-2 level 3 requirements.

6.1.2 Private Key Delivery to Subject

The subject's private key is generated by the card manufacturer on and by the QSCD. The private key is not extracted from the QSCD.

6.1.3 Public Key Delivery to Certificate Issuer

The subject's public key is transferred from the card manufacturer after the key pair generation on the QSCD to the RA by means of encrypted message over a secured connection. The RA incorporates the public key in a request and sends it to the CA over a private secure link.

The same method is used to deliver the certificate back to the Card Manufacturer.

6.1.4 CA Public Key Delivery to Relying Parties

The CA public keys are made available from the eID Repository Website.

6.1.5 Key Sizes

For details refer to **EID-DEL-004 eID PKI Hierarchy certificate profile (cfr. Appendix C), Section 1.7 Subject Public Key Info.**

6.1.6 Public Key Parameters Generation and Quality Checking

See section 6.1.1 KEY PAIR GENERATION

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

For details refer to the document EID-DEL-004 eID PKI HIERARCHY CERTIFICATE PROFILE (CFR. APPENDIX C), SECTION 1.8 KEY USAGE.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Secure Cryptographic module

The hardware of the Secure Cryptographic Device is the NXP chip P5CC081, which is EAL5+ certified.

The "Belpic" applet V1.7 which runs on the MultiAppID v2.1 80K CC platform on the chip, is EAL4+ certified.

6.2.2 Private Key Generation

The key pair (private-public key) is generated on the chip.

Only the public key can be exported from the chip. The private key stays secured in the chip.

6.2.3 Private Key Multi-Person Control

Section not applicable. The Secure Cryptographic Device is only to be used by the designated Subject.

6.2.4 Private Key Escrow

Private keys cannot and are never extracted from the Secure Cryptographic Device on which they are generated. Private keys are never put in escrow.

6.2.5 Private Key Backup

Private keys on a Secure Cryptographic Device are generated on-board the device and cannot be backed up.

6.2.6 Private Key Archival

Private keys on a Secure Cryptographic Device are generated on-board the device and cannot be extracted for backup, escrow or archival.

6.2.7 Private Key Transfer into or from a Cryptographic Module

Private keys on a Secure Cryptographic Device cannot be transferred.

6.2.8 Private Key Storage on Cryptographic Module

Private keys on a Secure Cryptographic Device are stored in secure memory. The embedded microchip protects private keys and other security related information against hacks.

6.2.9 Method for Activating Private Keys

Activation data for Secure Cryptographic Device consist of PIN and PUK codes. PIN codes and PUK codes are provided to the Subject in a protective tamper-evident container such as a PIN letter and/or sealed envelope.

6.2.10 Method of Destroying Private Key

The private key can be blocked or even decommissioned (irreversibly blocked) by repeatedly providing an incorrect PIN or PUK code.

6.2.11 Cryptographic Module Rating

Minimum standards for cryptographic modules have been specified in APPENDIX B: REQUIREMENTS FOR CERTIFICATION AUTHORITIES.

6.3 Other Aspects of Key Pair Management

The TSP uses appropriate cryptographic devices to perform CA key management tasks. Those cryptographic devices are known as Hardware Security Modules (HSMs).

Such devices meet formal requirements (FIPS 140-2 level 3 as minimum), which guarantee, amongst other things, that device tampering is immediately detected; and private keys cannot leave devices unencrypted.

Hardware and software mechanisms that protect CA private keys are documented. The document demonstrates that CA key protection mechanisms are of at least equivalent strength to the CA keys they are protecting.

6.3.1 Public Key Archival

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

For details refer to document: **EID-DEL-004 eID PKI HIERARCHY CERTIFICATE PROFILE (CFR. APPENDIX C)**.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation of the Root CA is established by means of key custodians.

The operational CAs are activated by mean of an operational token.

The activation of the subject's key is done:

- First at the reception of the eID (QSCD)-card at the municipality:
  - The card and key can only be activated at the municipality;
  - In cooperation of the civil servant.
- For operational activation the Personal Identification Code of the subject is used.

6.4.2 Activation Data Protection

For the Root CA, the key custodians each have a part of the activation key, these tokens are protected by a passphrase. The protection scheme is M OF N. The tokens are stored in a vault.

The operational CAs are protected by a split operational token which (M of N) tokens are protected by passphrase. The tokens are stored in a vault.

The subject's key is protected by a PIN, the PIN is delivered by means of a postal service in a secured envelope directly to the subject. Activation Data should be memorised, not written down. Activation Data must never be shared. Activation data must not consist solely of information that could be easily guessed, e.g. a Certificate Holder's personal information.

6.4.3 Other Aspects of Activation Data

The CA securely stores and archives activation data associated with its own private key and operations.

6.5 Computer Security Controls

The CA implements appropriate computer security controls including physical and logical access controls, role separation, multi-layered controls, intrusion detection, and multi-factor authentication processes for all personnel who can cause the issuance of a certificate or cause a person to become able to issue a certificate.

6.5.1 Specific Computer Security Technical Requirements

The Citizen CA provides the following functionality through the operating system and a combination of the operating system, the PKI software and physical controls:

- Access control to CA services and PKI roles;
- Enforced separation of duties for PKI roles;
- Identification and authentication of PKI roles and associated identities;
- Use of cryptography for session communication and database security;
- Archival of CA and end entity history and audit data;
- Audit of security related events;
- Recovery mechanisms for keys and the CA system.

Information on this functionality is provided in the respective sections of this CPS.

6.5.2 Computer Security Rating

Section not applicable.

6.6 Life Cycle Technical Controls

All hardware and software procured for operating an Issuing CA within the Citizen CA must be purchased in a manner which will mitigate the risk that any particular component could be tampered with, such as random selection of specific components. Equipment developed for

use within the eID PKI shall be developed in a controlled environment under strict change control procedures.

A continuous chain of accountability, from the location where all hardware and software that has been identified as supporting an Issuing CA within the eID PKI, must be maintained by causing it to be shipped or delivered via controlled methods. Issuing CA equipment shall not have installed any application or component software that is not part of the Issuing CA configuration. All subsequent updates to Issuing CA equipment must be purchased or developed in the same manner as the original equipment and be installed by trusted and trained personnel in a defined manner.

The CA factory has established an approved System Security Policy that incorporates computer security controls that are specific to the eID PKI and address the following:

6.6.1 System Development Controls

Formal procedures are followed for the development and implementation of new systems. An analysis of security requirements is carried out at the design and requirements specification stage. Outsourced software development projects are closely monitored and controlled.

6.6.2 Security Management Controls

The Citizen Certificate Authority follows the Certificate Issuing and Management Components (CIMC) Family of Protections Profiles that defines the requirements for components that issue, revoke and manage Public Key Certificates, such as X.509 Certificates. The CIMC is based on the common Criteria/ISO IS15408 standards.

6.6.3 Life Cycle Security Controls

The CA employs a configuration management methodology for the installation and ongoing maintenance of the Certificate Authority systems. The Certificate Authority software, when first loaded will provide a method for the CA to verify that the software on the system:

- Originates from the software developer;
- Has not been modified prior to installation;
- Is the version intended for use.

The CA Chief Security Officer periodically verifies the integrity of the Certificate Authority software and monitors the configuration of the Certificate Authority systems.

6.7 Network Security Controls

The CA maintains a high-level network of systems security including firewalls. Network intrusions are monitored and detected.

In specific:

- All communications between the CA and the RA operator regarding any phase of the life cycle of Citizen Certificates is secured with PKI based encryption and signing

techniques, to ensure confidentiality and mutual authentication. This includes communications regarding certificate requests, issuance, suspension, un-suspension and revocation;

- The CA web site provides for encrypted connections through the Secure Socket Layer (SSL) protocol and anti-virus protection;
- The CA network is protected by a managed firewall and intrusion detection system;
- It is prohibited to access sensitive CA resources including CA databases from outside of the CA operator's own network;
- Internet sessions for request and delivery of information are encrypted.

6.8 Time-Stamping

Section not applicable.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The certificate profiles and attributes are described in document: **EID-DEL-004 eID PKI HIERARCHY CERTIFICATE PROFILE (CFR. APPENDIX C), SECTION 1 CERTIFICATE PROFILES**.

7.1.1 Version Number(s)

See section 7.1

7.1.2 Certificate Extensions

See section 7.1

7.1.3 Algorithm Object Identifiers

See section 7.1

7.1.4 Name Forms

See section 7.1

7.1.5 Name Constraints

See section 7.1

7.1.6 Certificate Policy Object Identifier

See section 7.1

7.1.7 Usage of Policy Constraints Extension

See section 7.1

7.1.8 Policy Qualifiers Syntax and Semantics

See section 7.1

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Section not applicable.

7.1.10 Certificate Validity

The validity of a Citizen End-Entity certificate has two constraints:

- The validity period shall not be greater than 10 years and 8 months (*see section 7.1*);
- The validity period of the certificate cannot surpass the validity period of the eID card on which the chip is placed wherein the certificate resides.

The RA will always choose the shorter validity period of these two constraints when generating the certificate issuance request.

7.2 CRL Profile

The CRL profiles and attributes are described in document: **EID-DEL-004 eID PKI Hierarchy certificate profile (cfr. Appendix C), Section 2. CRL profiles.**

7.2.1 Version Number(s)

See section 7.2

7.2.2 CRL and CRL Entry Extensions

See section 7.2

7.3 OCSP Profile

The OCSP profiles and attributes are described in document: **EID-DEL-004 eID PKI Hierarchy certificate profile (cfr. Appendix C), Section 2. CRL profiles.**

7.3.1 Version Number(s)

See section 7.3

7.3.2 OCSP Extensions

See section 7.3

8 Compliance Audit and Other Assessments

With regard to the Qualified Certificate for electronic signature, the TSP operates following the terms of EU 910/2014 that stipulates the legal framework of electronic signatures in Belgium.

The TSP meets the requirements set out in ETSI policy documents referring to qualified certificates, including:

- EN 319 411-2: Requirements for trust service providers issuing EU qualified certificates;
- EN 319 412-5 Profiles for Trust Service Provider issuing Certificates; qualified certificate profile. Part 5: Extension for Qualified certificate profile.

The TSP accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CPS. The TSP accepts this auditing of its own practices and procedures it does not publicly disclose under certain conditions such as confidentiality, trade secrets etc. Such audits may be carried out directly or through an agent by:

- The supervising authority for Trust Service Providers in Belgium acting under the authority of the Belgian government;
- The Belgian government or a third party appointed by the Belgian government.

The TSP evaluates the results of such audits before further implementing them.

8.1 Frequency or Circumstances of Assessment

The PKI factory is audited yearly.

8.2 Identity/Qualifications of Assessor

The audit services are to be performed by independent, recognised, credible, and established audit firms or information technology consulting firms; provided they are qualified to perform and are experienced in performing information security audits, specifically having significant experience with PKI and cryptographic technologies.

8.3 Assessor's Relationship to Assessed Entity

The auditor and the Issuing CA under audit must not have any other relationship that would impair the auditor’s independence and objectivity under Generally Accepted Auditing Standards. These relationships include financial, legal, social or other relationships that could result in a conflict of interest.

8.4 Topics Covered by Assessment

The audit addresses the following aspects:

- Compliance of the TSP operating procedures and principles with the procedures and service levels defined in the CPS;

- Management of the infrastructure that implements TSP services;
- Management of the physical site infrastructure;
- Adherence to the CPS;
- Adherence to relevant Belgian Laws;
- Asserting agreed service levels;
- Inspection of audit trails, logs, relevant documents etc.;
- Cause of any failure to comply with the conditions above.

8.5 Actions Taken as a Result of Deficiency

If irregularities are detected, the TSP will submit a report to the auditor, stating the measures that will be taken to rectify the situation and ensure compliance. If the proposed measures are deemed insufficient, a second audit will be carried out to ensure compliance.

8.6 Communication of Results

The audit opinion based on results of the audits will be generally available upon request.

9 Other Business and Legal Matters

Certain legal conditions are applicable to the issuance of the Citizen certificates under this CPS as described in this section.

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Article 6 of the law of 19 July 1991 mentioned under point 1.3 of chapter 1, regulates on the one hand the compensation of the insertion of the certificates on the cards (Art. 6, §5) and on the other hand the collection of the production costs of the cards by the Minister of Interior Affairs (Art. 6, §8).

The CA charges no fee for the publication and retrieval of this CPS.

The CA will provide the citizen free of charge with the following services:

- Publication of CRLs and delta CRLs;
- Access to the repository web pages;
- Status verification web service via repository pages.

The Belgian State may access the following resources free of charge as appropriate:

- OCSP status verification services;
- Download of CRL and delta CRL;
- Certificate status verification service;
- Certificate directory service;
- Publication of certificates;
- Revocation of certificates;
- Suspension of certificates.

The CA implements mechanisms to protect these services from abuse.

9.1.2 Certificate Access Fees

See section 9.1.1

9.1.3 Revocation or Status Information Access Fees

See section 9.1.1

9.1.4 Fees for Other Services

See section 9.1.1

9.1.5 Refund Policy

Section not applicable.

9.2 Financial Responsibility

The TSP is responsible for maintaining its financial books and records in accordance with Belgian GAAP and shall engage the services of an international accounting firm to provide financial services, including periodic audits.

9.2.1 Insurance Coverage

The TSP provides each year the Supervisory body of the Belgian State with proof of the insurance coverages.

9.2.2 Other Assets

The PKI factory and Registration Authorities shall maintain sufficient assets and financial resources to perform their duties within the eID PKI and be reasonably able to bear liability to Certificate Holders and Relying Parties.

9.2.3 Insurance or Warranty Coverage for End-Entities

Section not applicable.

9.3 Confidentiality of Business Information

In the framework of the services performed, the CA and the RA operator (RRN) act as “processor” of personal data in accordance with article 16 of the Law of 8 December 1992, whereas the municipalities act as “processor” for the processing of personal data.

9.3.1 Scope of Confidential Information

The TSP complies with personal data privacy rules and confidentiality rules as described in this CPS. Confidential information includes:

- Any personal identifiable information on citizens, other than that contained in a certificate;
- Exact reason for the revocation or suspension of a certificate;
- Audit trails;
- Logging information for reporting purposes, such as logs of requests by the RA;
- Correspondence regarding CA services;
- CA private key(s).

9.3.2 Information Not Within the Scope of Confidential Information

The following items are not confidential information:

- Certificates and their content;
- Status of a certificate.

9.3.3 Responsibility to Protect Confidential Information

Parties requesting and receiving confidential information are granted permission on the condition that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third parties.

Also these parties are bound to observe personal data privacy rules in accordance with the law.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The TSP does not release nor is it required to release any confidential information without an authenticated and justified request specifying either:

- The party to whom the CA owes a duty to keep information confidential. The CA owes such a duty to the RA and promptly responds to any such requests;
- A court order.

Within the framework of the TSP contract with the Belgian State, the TSP may charge an administrative fee to process such disclosures.

9.4.2 Information Treated as Private

All information, i.e. about the certificate Holders, will not be disclosed by the CA to citizens nor relying parties with the exception of information about:

- Themselves;
- Persons in their custody.

Only the RA is permitted to access confidential information.

9.4.3 Information not Deemed Private

Non-confidential information can be disclosed to any citizen and relying party under the conditions below:

- The status of a single certificate is provided per inquiry by a citizen or relying party;
- Citizens can consult non-confidential information the TSP holds about them;

- The content of Digital Certificates issued is public information and deemed not private.

9.4.4 Responsibility to Protect Private Information

The CA properly manages the disclosure of information to the CA personnel.

The CA authenticates itself to any party requesting the disclosure of information by:

- Signing responses to OCSP requests, CRLs and delta CRLs.

The TSP encrypts all communications of confidential information including:

- The communication link between the CA and the RA;
- Sessions to deliver certificates.

Next to the information retained by the TSP, the RA also retains information pertaining to the Citizen Certificates, more specifically in the Registry of Identity Cards. The Law of 19 June 1991 *defines the access to the Registry of Identity cards and other data on the citizens owned by the National Register.*

9.4.5 Notice and Consent to use Private Information

The TSP operates within the boundaries of the Belgian Law of 8 December 1992 on *Privacy Protection in relation to the Processing of Personal Data* amended by the law of 11 December 1998 *implementing the European Union Directive 1995/46 On the protection of individuals with regard to the processing of personal data and on the free movement of such data.* This is conform to the Law of 13 June 2005 *concerning the processing of personal data and the protection of privacy in the electronic communications sector*. It also acts within the boundaries of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation).

The TSP does not store any other data on certificates or of citizens, other than the data, transferred to it and authorised by the RA. Without consent of the data subject or explicit authorization by law, personal data processed by the TSP will not be used for other purposes.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

See section 9.4.5

9.4.7 Other Information Disclosure Circumstances

certipost is under no obligation to disclose information other than is provided for by a legitimate and lawful judicial order that complies with requirements of this CP/CPS.

9.5 Intellectual Property Rights

The Belgian State owns and reserves all intellectual property rights associated with its own databases, web sites, the CA digital certificates and any other publication whatsoever originating from the CA including this CPS.

The TSP owns and reserves any and all intellectual property rights it holds on its own infrastructure, databases, web site etc.

Any software and documentation developed by the TSP in the framework of the Belgian Electronic Identity Card project, are the exclusive property of the Belgian State.

9.6 Representations and Warranties

All parties within the domain of the TSP, including the CA itself, the CM, the RA, the LRAs and the citizens warrant the integrity of their respective private key(s). If any such party suspects that a private key has been compromised they will immediately notify their LRA (municipality), the police or the RA Helpdesk.

9.6.1 CA Representations and Warranties

To the extent specified in the relevant sections of the CPS, the TSP will:

- Comply with this CPS and its amendments as published under eID Repository Website;
- Provide infrastructure and certification services, including the establishment and operation of the CA Repository and web site for the operation of public certification services;
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure;
- Promptly notify the RA in case of compromise of its own private key(s);
- Issue electronic certificates in accordance with this CPS and fulfil its obligations presented herein;
- Notify the RA if the CA is unable to validate the application according to this CPS;
- Upon receipt of an authenticated request sent by the RA act promptly to issue a certificate in accordance with this CPS;
- Upon receipt of an authenticated request for revocation from the RA to revoke immediately a certificate in accordance with this CPS;
- Upon receipt of an authenticated request for suspension from the RA to suspend immediately a certificate in accordance with this CPS;
- Upon receipt of an authenticated request for un-suspension from the RA to un-suspend immediately a certificate in accordance with this CPS;
- Publish certificates in accordance with this CPS;
- Publish CRLs, delta CRLs and OCSP responses of all suspended and revoked certificates on a regular basis in accordance with this CPS;

- Provide appropriate service levels according to a service level agreement as defined within the framework of the CA contract with the Belgian State;
- Make a copy of this CPS and applicable policies available through its web site;
- Operate in compliance with the laws of Belgium. In particular the TSP meets all legal requirements associated with qualified certificate profile emanating from EU 910/2014 with regard to electronic signatures.

If the TSP becomes aware of or suspects the compromise of a private key including its own, it will immediately notify the RA.

When using third party agents the TSP will make best efforts to ensure the proper financial responsibility and liability of such contractor.

The TSP is responsible towards citizens and relying parties for the following acts or omissions:

- Issue digital certificates not listing data as submitted by the RA;
- If a private signing key of the CA is compromised;
- Failure to list a revoked certificate in a CRL or delta CRL;
- Failure of the OCSP responder to report a certificate as revoked or suspended;
- Failure of a Web interface to report certificate status information;
- Unauthorised disclosure of confidential information or private data according to sections 9.3 and 9.4;
- Liable as defined in 9.8.1.

The TSP acknowledges it has no further obligations under this CPS.

9.6.1.1 Reliance at Own Risk.

It is the sole responsibility of the parties accessing information featured in the Repositories and web site to assess and rely on information featured therein.

9.6.1.2 Accuracy of Information.

The TSP makes every effort to ensure that parties accessing its Repositories receive accurate, updated and correct information. The TSP, however, cannot accept any liability beyond the limits set in this CPS under article 9.8.1.

9.6.2 RA Representations and Warranties

The RA operating within the CA domain will:

- Provide correct and accurate information in their communication with the CA;
- Ensure that the public key submitted to the CA corresponds to the private key used;
- Create certificate requests in accordance with this CPS;

- Perform all verification and authenticity actions prescribed by the CA procedures and this CPS;
- Submit to the CA the applicant's request in a signed message;
- Receive, verify and relay to the CA all requests for revocation, suspension and un-suspension of a certificate in accordance with the CA procedures and the CPS;
- Verify the accuracy and authenticity of the information provided by the foreigner at the time of renewal of a certificate according to this CPS.

If the RA becomes aware of or suspects the compromise of a private key, it will immediately notify the CA.

The RRN acts as the sole RA in the CA domain and has sole responsibility for the directories it maintains including certificate directories. The RA is responsible for all audits it makes, the results and recommendations of audits thereof.

The RA through the LRA is solely responsible for the accuracy of the citizen data as well as any other assigned data it provides the CA with. The RA will not hold the CA liable for any damages suffered as a result of unverified data that has been listed in a certificate.

The RA complies with Belgian Laws and regulations pertaining to the functioning of RRN and is liable for its acts or omissions under Belgian Law.

9.6.3 Subject Representations and Warranties

Unless otherwise stated in this CPS, citizen's obligations include the ones below:

- Refraining from tampering with a certificate;
- Only using certificates for legal and authorised purposes in accordance with the CPS;
- Applying for a new Electronic Identity Card (and thus Citizen Certificates) in case of any changes in the information published in the certificate;
- Refraining from using the citizen's public key in an issued Citizen Certificate to have other certificates issued;
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private keys;
- Notify the police, the municipality or docstop to request the revocation of a certificate in case of the suspicion of an occurrence that materially affects the integrity of a certificate. Such occurrences include indications of loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of the Citizen Certificates;
- Notify the police, the municipality or docstop to request the revocation of a certificate in case of an occurrence that materially affects the integrity of a certificate. Such occurrences include loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of the Citizen Certificates, or in case control over private keys has been lost due to compromise of activation data (e.g. PIN code);

- Obligation to exercise reasonable care to avoid unauthorised use of the subject's private key;
- Following compromise, the obligation to immediately and permanently discontinue the use of the subject's private key;
- The obligation to notify without any reasonable delay in case control over the private key has been lost due to compromise of activation data (e.g. PIN code).

9.6.4 Relying Party Representations and Warranties

A party relying on a CA certificate will:

- Be sufficiently informed about the use of digital certificates and PKI;
- Receive notice and adhere to the conditions this CPS and associated conditions for relying parties;
- Validate a certificate by using a CRL, delta CRL, OCSP or web based certificate validation in accordance with the certificate path validation procedure;
- Trust a certificate within its validity period only if it has not been suspended or revoked;
- Rely on a certificate, as may be reasonable under the circumstances.

It is the sole responsibility of the relying parties accessing information featured in the CA Repositories and web site to assess and rely on information featured therein.

If a relying party becomes aware of or suspects that a private key has been compromised it will immediately notify the RA Helpdesk.

9.6.5 Representations and Warranties of other Participants

Card manufacturer (CM) obligations: the Card Manufacturer (CM) is responsible for the initialisation, the personalisation and the distribution of the electronic identity card containing the 0, 1 or 2 citizen's certificates.

This initialisation lists the following operations on the smart card:

- Generation of the key pairs for the identification and signature certificate;
- Storage of the identification data, of the identification and signature certificates on the smart card;
- Data authentication, initialisation of the different files stored on the digital identity card.

The CM will collect the base documents and distribute convocations, new digital personalized and initialised identity card and the secured envelope containing PIN & PUK codes for citizens in a secure way.

The CM will implement a secure process to retrieve from the municipalities the non-valid or cancelled identity card and destroy them.

9.7 Disclaimers of Warranties

Within the limit set by Belgian Law, in no event (except for fraud or wilful misconduct) will the CA be liable for:

- Any loss of profits;
- Any loss of data;
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures;
- Any other damages.

9.8 Limitations of Liability

9.8.1 The TSP Liabilities

The liability of the TSP towards the subject or a relying party is limited to paying damages amounting to 2500 € per transaction, affected by the events listed in this section here below.

9.8.2 Qualified certificates

As far as the issuance of Qualified Certificates is concerned, Article 14 of the Electronic Signatures Law governs the liability of the TSP.

Following this provision, the TSP is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:

- As regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;
- For assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the private key corresponding to the public key given or identified in the certificate;
- For assurance that the private key and the public key can be used in a complementary manner.

The TSP is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the TSP proves that he has not acted negligently.

9.8.3 Certificates that cannot be considered as qualified certificates

The general rules on liability apply with regard to any damage caused to any entity or legal or natural person who reasonably relies on a certificate issued by the TSP.

The TSP explicitly declines all liability towards relying parties in all cases where the Identification Certificate is used in the context of applications allowing the use of the Identification Certificate for the generation of electronic signatures.

9.8.4 Excluded Liability

The TSP shall bear absolutely no liability for any loss whatsoever involving or arising from any one (or more) of the following circumstances or causes:

- If the Digital Certificate held by the claiming party or otherwise the subject of any claim has been compromised by the unauthorised disclosure or unauthorised use of the Digital Certificate or any password or activation data used to control access thereto;
- If the Digital Certificate held by the claiming party or otherwise the subject of any claim was issued as a result of any misrepresentation, error of fact, or omission of any person, entity, or Organisation;
- If the Digital Certificate held by the claiming party or otherwise the subject of any claim had expired or been revoked prior to the date of the circumstances giving rise to any claim;
- If the Digital Certificate held by the claiming party or otherwise the subject of any claim has been modified or altered in any way or been used otherwise than as permitted by the terms of this Citizen CA CP/CPS and/or the relevant Certificate Holder Agreement or any applicable law or regulation;
- If the private key associated with the Digital Certificate held by the claiming party or otherwise the subject of any claim has been compromised;
- If the Digital Certificate held by the claiming party was issued in a manner that constituted a breach of any applicable law or regulation;
- Computer hardware or software, or mathematical algorithms, are developed that tend to make public key cryptography or asymmetric cryptosystems insecure, provided that certipost uses commercially reasonable practices to protect against breaches in security resulting from such hardware, software, or algorithms;
- Power failure, power interruption, or other disturbances to electrical power, provided certipost uses commercially reasonable methods to protect against such disturbances;
- Failure of one or more computer systems, communications infrastructure, processing, or storage media or mechanisms, or any sub components of the preceding, not under the exclusive control of certipost and/or its subcontractors or service providers;
- One or more of the following events: a natural disaster or Act of God (including without limitation flood, earthquake, or other natural or weather related cause); a labour disturbance; war, insurrection, or overt military hostilities; adverse legislation or governmental action, prohibition, embargo, or boycott; riots or civil disturbances; fire or explosion; catastrophic epidemic; trade embargo; restriction or impediment (including, without limitation, export controls); any lack of telecommunications availability or integrity; legal compulsion including, any judgments of a court of competent jurisdiction to which certipost is, or may be, subject; and any event or occurrence or circumstance or set of circumstances that is beyond the control of certipost.

9.9 Indemnities

See section 9.8

9.10 Term and Termination of the CP/CPS

9.10.1 Term

This CP/CPS becomes effective upon publication in the eID Repository. Amendments to this CP/CPS become effective upon publication in the eID Repository.

9.10.2 Termination

This CPS remains in force until notice of the opposite is communicated by the CA on its repository under eID Repository Website.

9.10.3 Effect of Termination and Survival

The provisions of this Citizen CA CP/CPS shall survive the termination or withdrawal of a Certificate Holder or Relying Party from the eID PKI with respect to all actions based upon the use of or reliance upon a Digital Certificate or other participation within the eID PKI. Any such termination or withdrawal shall not act so as to prejudice or affect any right of action or remedy that may have accrued to any person up to and including the date of withdrawal or termination.

9.11 Individual Notices and Communications with Participants

Notices related to this CPS can be addressed to:

See section 1.5.1

9.12 Amendments

9.12.1 Procedure for Amendment

Changes to this CPS are managed by de policy administration responsible of the TSP**.** All proposed changes to the CPS need to be approved by the PKI management board.

9.12.2 Notification Mechanism and Period

After approval a new version of the CPS is created and published beside the former version on the repository website (eID Repository Website).

9.12.3 Circumstances Under Which OID Must be Changed

Minor changes to this CPS that do not materially affect the assurance level of this CPS are indicated by a decimal number change (e.g. version 1.0 changes to version 1.1), while major changes to this CPS are indicated by an integer number change (e.g. version 1.0 changes to version 2.0).

Minor changes to this CPS do not require a change in the CPS OID or the CPS pointer qualifier (URL) that might be communicated by the CA. Major changes that may materially change the acceptability of certificates for specific purposes may require corresponding changes to the CPS OID or CPS pointer qualifier (URL).

9.13 Dispute Resolution Provisions

All disputes associated with this CPS will be resolved according to Belgian Law.

Complaints related to this CPS and the certificates are addressed to:

See section 1.5.1

A receipt acknowledgement will be sent within 2 working days after arrival of the complaint. An answer will be provided within 10 working days following the arrival of the complaint.

In accordance with Belgian Digital Signature law, any arbitration shall, unless agreed otherwise between the parties take place in Belgium.

9.14 Governing Law

The TSP provides its services under the provisions of the Belgian Law and EU Regulation 910/2014.

9.15 Compliance with Applicable Law

This CP/CPS is subject to applicable law.

9.16 Miscellaneous Provisions

The TSP incorporates by reference the following information in all digital certificates it issues:

- Terms and conditions described in this CPS;
- Any other applicable certificate policy as may be stated on an issued Citizen Certificate;
- The mandatory elements of applicable standards;
- Any non-mandatory but customised elements of applicable standards;
- Content of extensions and enhanced naming not addressed elsewhere;
- Any other information that is indicated to be so in a field of a certificate.

To incorporate information by reference the CA uses computer-based and text-based pointers that include URLs, OIDs etc.

9.16.1 Entire Agreement

Section not applicable.

9.16.2 Assignment

Section not applicable.

9.16.3 Severability

Any provision of this Citizen CA CP/CPS that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Citizen CA CP/CPS or affecting the validity or enforceability of such remaining provisions.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

The failure or delay of the TSP to exercise or enforce any right, power, privilege, or remedy whatsoever, howsoever or otherwise conferred upon it by this Citizen CA CP/CPS ; shall not be deemed to be a waiver of any such right or operate so as to bar the exercise or enforcement thereof at any time or times thereafter, nor shall any single or partial exercise of any such right, power, privilege or remedy preclude any other or further exercise thereof or the exercise of any other right or remedy. No waiver shall be effective unless it is in writing. No right or remedy conferred by any of the provisions of this Citizen CA CP/CPS is intended to be exclusive of any other right or remedy, except as expressly provided in this Citizen CA CP/CPS, and each and every right or remedy shall be cumulative and shall be in addition to every other right or remedy given hereunder or now or hereafter existing in law or in equity or by statute or otherwise.

9.16.5 Force Majeure

The TSP accepts no liability for any breach of warranty, delay or failure in performance that results from events beyond its control such as Acts of God, acts of war, acts of terrorism, epidemics, power or telecommunication services failure, fire, and other natural disasters. See also Section 9.8.2 (Excluded Liability) above.

9.17 Other Provisions

Section not applicable.

Annexes

This page is intentionally left blank.

Appendix A

Definitions & acronyms

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

Appendix B

Requirements for Certification Authorities

The cryptographic modules used by certificate authorities SHALL be evaluated and certified in accordance with one of the following standards:

- FIPS PUB 140-2 level 3 or higher;
- PP-SSCD 4,5,6;
- BSI Cryptographic Modules Security Level “Enhanced”.

Appendix C

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

Starting from next page

Table of contents

1. Certificate profiles

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

Note: All the URI's specified in the certificate profiles are resolved by BOSA[1].

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

1.1. Version

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

Version	
All certificates	Version 3 – Value = "2"

1.2. Certificates Serial Number

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

The RRN[2] can assign a serial number to the eID hierarchy certificates.

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

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

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

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

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

[2] RRN is an acronym for Rijksregister – Registre National.

1.3. Signature

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

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

1.4. Issuer

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

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

[3] See paragraph 4.1 Serial number to reference a CA.

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

1.5. Validity

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

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

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

[4] See paragraph 4.1 Serial number to reference a CA

[5] Certificate validity periods defined during key ceremony

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

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

1.6. Subject

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

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

[7] See paragraph 4.1 Serial number to reference a CA.

[8] See paragraph 4.1 Serial number to reference a CA.

[9] See paragraph 4.1 Serial number to reference a CA.

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

End user certificate Subject fields definition (eID hierarchy)			
Field	**Length**	**Description**	**Example**
C (countryName)	2	countryName is a dynamic element corresponding to the two letter country code ISO3166 standard. The country code is provided with the certificate creation request by the RRN. It is not checked by the CA.	C=BE
CN (commonName)	Max 255 Min 1	Concatenation of • <given name>: first given name of the card holder • <surname>: surname of the eID card owner • (<purpose>): (Authentication) or (Signature)	CN=John Smith (Authentication) CN=John Smith (Signature)
surname	Max 255 Min 1	Surname of the eID card owner	S=Smith
givenName	Max 255 Min 1	1 or 2 given names of the eID card owner (This field may not appear in case the owner has no given name)	G=John William
subjectSerialNumber	Max 255 Min 1	This is a unique number provided by the RRN ("Rijksregisternummer" – 11 digits long).	SN=12345678901

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

1.7. Subject Public Key Info

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

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

1.8. Key usage

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

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

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

1.9. Extended Key usage

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

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

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

1.10. Authority and Subject Key Identifiers

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

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

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

1.11. NetscapeCertType

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

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

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

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

1.12. Policy mapping

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

1.13. Policy constraint

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

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

1.14. Certificate policies

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

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

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

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

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

Certificate Policies				
	Policy Identifier	Policy Qualifiers	Policy Qualifier Id	Qualifier
eID hierarchy				
Operational CA certificates				
Citizen CA	2.16.56.1.1.1.2 2.16.56.9.1.1.2 2.16.56.10.1.1.2 2.16.56.12.1.1.2	NA	CPS	eID Repository Website
Foreigner CA	2.16.56.1.1.1.7 2.16.56.9.1.1.7 2.16.56.10.1.1.7 2.16.56.12.1.1.7	NA	CPS	eID Repository Website
End user certificates				
Citizen Authentication certificate	2.16.56.1.1.1.2.2 2.16.56.9.1.1.2.2 2.16.56.10.1.1.2.2 2.16.56.12.1.1.2.2	NA	CPS	eID Repository Website
Citizen Signature certificate	2.16.56.1.1.1.2.1 2.16.56.9.1.1.2.1 2.16.56.10.1.1.2.1 2.16.56.12.1.1.2.1	NA	CPS	eID Repository Website

Foreigner Authentication certificate	2.16.56.1.1.1.7.2 2.16.56.9.1.1.7.2 2.16.56.10.1.1.7.2 2.16.56.12.1.1.7.2	NA	CPS	eID Repository Website
Foreigner Signature certificate	2.16.56.1.1.1.7.1 2.16.56.9.1.1.7.1 2.16.56.10.1.1.7.1 2.16.56.12.1.1.7.1	NA	CPS	eID Repository Website

1.15. Basic constraint

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

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

1.16. CRL Distribution Point

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

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

1.17. Freshest CRL - delta CRL Distribution Point

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

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

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

1.18. Authority Information Access

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

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

[10] See paragraph 4.2 CRL and delta CRL names.

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

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

1.19. Subject Directory attributes

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

No subject directory attributes will be present in the eID certificates

1.20. Qualified Certificate Statement

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

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

2. CRL profiles

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

2.1. CRL Profile

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

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

2.2. Δ CRL Profile

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

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

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

2.3. CRL Issuance Frequency

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

3. CA configuration settings

The table below specifies the configuration settings on the CAs these configuration settings are explained hereafter:

CA configurations settings								
Setting	Auto-revocation	Unique DN check	Group	Variable validity	delta CRL creation			
eID hierarchy								
Operational CA certificates								
Citizen CA	A	A	G1[11]	A	A			
Foreigner CA	NA	A	G1	A	A			

3.1. Auto-revocation

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

3.2. Unique DN check

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

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

1) Un-suspended;

2) Generated with a 'Valid' status.

The unique DN check applies to all certificates issued under the CAs belonging to the same unique DN group.

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

3.3. Variable validity

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

The variable validity feature is only available through XKMS interface.

3.4. Delta CRL

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

4. Naming conventions

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

4.1. Serial number to reference a CA

<Serial number>			
Characteristics	**Length**	**Format**	**Range**
Multiple versions of the same CA issued in the same year	7	<yyyy><ss> o <yyyy> represents the year where the CA will be used o <ss> represents the unique serial number to be added for that year Applicable for: o certificate subject or issuer field serial numbers o CRL and dCRL file names o CA certificate file names	2003 .. 9999 01 .. 99
Single version of a CA issued per year	4	<yyyy> o <yyyy> represents the year where the CA will be used Applicable for: o certificate subject or issuer field serial numbers o CRL and dCRL file names o CA certificate file names	2003 .. 9999

Remark: The CAs created for the year 2008 the following scheme with respect to the serial numbers:

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

4.2. CRL and delta CRL names

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

4.3. CA certificate file names

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