DG Digitale Transformatie
FOD Beleid en Ondersteuning
DG Transformation digitale
SPF Stratégie et Appui

BELGIAN CERTIFICATE POLICY & PRACTICE STATEMENT FOR EID PKI INFRASTRUCTURE BELGIUM ROOT CA

Siège social / Maatschappelijke zetel
WTCIII • Boulevard Simon Bolivarlaan 30
1000 Bruxelles / Brussel

Numéro d'entreprise / Zakelijke nummer
671.516.647

T +32 (0)2 740 74 74
www.bosa.be

I. DOCUMENT CONTROL

Date	Version	Editor	Change
31/05/2016	1.30 (2.0)	Tim Bracke	Update to RFC 3647
	1.32		intermediate
	1.35		intermediate
	1.40		Pre-release
	1.41	FOD BOSA	Reviewed by FOD BOSA+ changes
20/12/2016	2.00		Final Draft – To be reviewed by FOD BOSA
11/01/2016	2.01	FOD BOSA	Final version
07/06/2017	3.00	Tim Bracke	Change from FOD BOSA to FOD BOSA
01/08/2017	3.01	Tim Bracke	Minor corrections
08/05/2019	3.02	Sam Van den Eynde	Integration of BRCA specifications in document
11/06/2019	3.03	Sam Van den Eynde	Review with legal Work document
06/05/2020	3.04	Sam Van den Eynde	Review WebTrust Minor administrative corrections For release
21/01/2021	3.05	Sam Van den Eynde	Remove Root Signed BRCA stipulations Minor administrative corrections For release

1 INTRODUCTION

This Certification Practice Statement (hereinafter, CPS) of the Belgium Root Certification Authority (hereinafter, the BRCA) applies to all public services of the Belgium Root Certification Authority. Together with this CPS other documents may have to be considered.

This CPS complies with the formal requirements of Internet Engineering Task Force (IETF) RFC 3647, with respect 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 PKI services of the BRCA.

The CPS addresses in detail the technical, procedural and organisational policies and practices of the BRCA with regard to all services available and during the complete lifetime of certificates, issued by the BRCA.

1.1 OVERVIEW

To support the Belgian government issuing electronic identity cards, (eID cards) a Belgium Root Certification Authority (BRCA) is the top authority in Belgium with regard to digital certification services offered to citizens, civil servants and public authorities.

The BRCA issues top level certificates to operational CAs of the Belgian Government that issue end-user certificates or end-user certified properties (assertions). The eID Citizen CA & Foreigner CA are such an operational CAs that subsequently issues certificates to end users who are beneficiaries of the electronic identity SERVICES of the Belgian government, these operational CAs issue certificates to their respective subscribers. Although the number of operational CAs that will be governed by the BRCA will be limited, the final number is not predefined.

The technology used for the certification services for these certificates is the PKI technology. PKI (Public Key Infrastructure) is an acronym for a system of Public Key cryptography combined with an Infrastructure that is designed to provide a level of security for communicated and stored electronic information sufficient to justify trust in such information by business, consumers, governments and the courts.

A certification practice statement (CPS) is a statement of the practices that a Certification Authority employs in issuing certificates. A CPS is a comprehensive treatment of how the CA makes its services available. This CPS is intended to be used within the domain of the BRCA in its function of issuer of top-level certificates to the CAs of the Belgian government. This CPS also outlines the relationship between the BRCA and other CAs within the Belgian Government PKI hierarchy.

This CPS applies to the BRCAs and identifies the roles, responsibilities and practices of e.g. CAs, RAs. This CPS also applies to all subscribers and relying parties including CAs that belong to the PKI hierarchy of the Belgian government as are referenced herein. Finally, this CPS applies to other entities that retain and organisational link with the BRCA like for example for the supply of services, supervision, accreditation etc.

The provisions of this CPS regarding practices, level of services, responsibilities and liability bind all parties involved including the BRCA, operational CAs, subscribers and relying parties. This CPS prescribes the provisions of the Belgium Root Certification Authority (BRCA).

Starting from 2008 an additional Belgium Root Certification Authority (BRCA) has been introduced in the eID PKI environment. This Belgium Root Certification Authority2 (BRCA2) was necessary to continue to issues certificates after 26th of October 2008.

In 2013 we introduced 2 new BRCAs (BRCA3 &BRCA4) to support the 10-year validity for the new eID cards in 2014. As of this date (the issuing under BRCA3) it is impossible to issue certificates under the initial BRCA.

With the introduction of these BRCAs a new set of OID numbers is used to clearly identity the difference between the BRCA(1), BRCA2, BRCA3 and BRCA4.

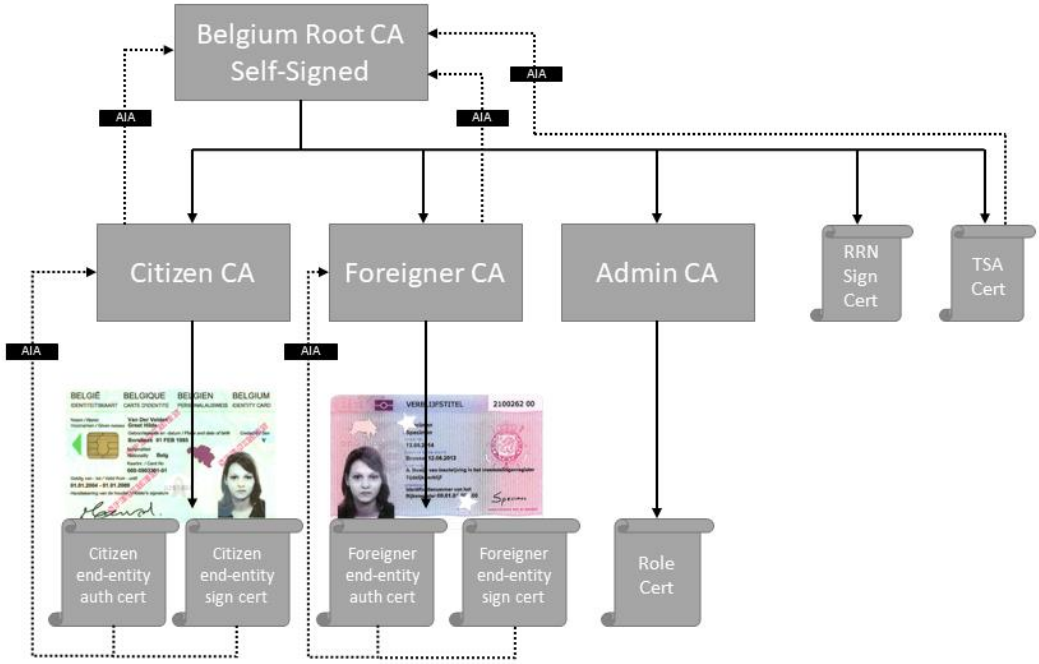
All references to the BRCA in this document are applicable to both BRCAs unless clearly stated.

To overcome any misunderstanding regarding which BRCA is referred to, the following convention is used:

When referring to the first BRCA it will be described as BRCA(1), the number “1” is set between brackets as the real name of this BRCA does not contain the number “1”.

When referring in this document to the other BRCAs it will be describe as BRCA3 or BRCA4.

eID Certificate Hierarchy



1.2 DOCUMENT NAME AND IDENTIFICATION

Name of this document	***Belgian Certificate Policy & Practice Statement for eID PKI infrastructure Belgium Root CA***
Document version	2.16.56.12.1 **– v3.0.5** ***This Certificate Policy is identified by its name and version number.***
	This document OID replaces the following OID's ***2.16.56.1.1*** ***2.16.56.9.1*** ***This BRCA CP/CPS obsoletes all other BRCA CP/CPS versions as of the date of publication.***
OID referring to this document	The identifiers under control of FOD BOSA: **BRCA (1)** OID: 2.16.56.1.1.1 – BRCA Self Signed
	BRCA 2 OID: 2.16.56.9.1.1.2 – BRCA 2 Self Signed
	BRCA 3 OID: 2.16.56.10.1.1.2 – BRCA 3 Self Signed
	BRCA 4 OID: 2.16.56.12.1.1.2 – BRCA 4 Self Signed

OID related to this CPS

The following identifiers are related to the BRCA but not under necessary under the control of FOD BOSA:
BRCA (1) 2.16.56.1.1.1.1 Administration CA 2.16.56.1.1.1.2 Citizen CA 2.16.56.1.1.1.3 Government CA 2.16.56.1.1.1.4 RRN Signing Certificate 2.16.56.1.1.1.5 Child CA 2.16.56.1.1.1.6 Government AA CA 2.16.56.1.1.1.7 Foreigner CA
BRCA 2 2.16.56.9.1.1.1 Administration CA 2.16.56.9.1.1.2 Citizen CA 2.16.56.9.1.1.3 Government CA 2.16.56.9.1.1.4 RRN Signing Certificate 2.16.56.9.1.1.5 Child CA 2.16.56.9.1.1.6 Government AA CA 2.16.56.9.1.1.7 Foreigner CA
BRCA 3 2.16.56.10.1.1.1 Administration CA 2.16.56.10.1.1.2 Citizen CA 2.16.56.10.1.1.3 Government CA 2.16.56.10.1.1.4 RRN Signing Certificate 2.16.56.10.1.1.5 Child CA 2.16.56.10.1.1.6 Government AA CA 2.16.56.10.1.1.7 Foreigner CA
BRCA 4 2.16.56.12.1.1.1 Administration CA 2.16.56.12.1.1.2 Citizen CA 2.16.56.12.1.1.3 Government CA 2.16.56.12.1.1.4 RRN Signing Certificate 2.16.56.12.1.1.5 Child CA 2.16.56.12.1.1.6 Government AA CA 2.16.56.12.1.1.7 Foreigner CA

1.3 PKI PARTICIPANTS

Several parties make up the participants of this PKI hierarchy. The parties mentioned hereunder including all CAs, subscribers and relying parties are collectively called PKI participants.

1.3.1 Certification Authorities

1.3.1.1 Root Certification Authority Root

The Belgium PKI contains the following Root Certificates:

SHA1 Roots	SHA256 Roots
BRCA(1)	
BRCA2	
BRCA3	
	BRCA4

This CP/CPS relates to all generations of the Belgium eID PKI Root CAs (BRCAs).

A Certification Authority is an organisation that issues digital certificates that are used in the public domain or within a business context. The Belgium Root Certificate Authority is a Certification Authority.

In the Belgium Root CA domain, Certipost acts as the BRCA on behalf of the Belgian Government. The actual certification operations including issuance, certificates status, and repository services are delegated to Certipost. Certipost has delegated some of the operations to other third party subcontractors. The BRCA operates within the grant of authority to issue CA certificates, provided by the Belgian Government.

The Belgian Government is responsible to define the policy prevailing in issuing a certain type or class of digital certificates within its own domain.

Pursuant to the broad purpose of digital certificates, the Belgian Government seeks cross recognition with commercial CAs that feature widely embedded top roots, also known as Trust anchors. The BRCA provides root signing to other accredited CAs in the domain of the Belgian Government, amongst others the eID Citizen CA.

The BRCA is established in Belgium. It can be contacted at the address published in this CPS, see 1.5.1 Organization Administering the Document. here. To deliver CA services including the issuance, revocation, re-key, status verification of certificates, the BRCA operates a secure facility and provides for a disaster recovery facility in Belgium.

In specific the BRCAs domain of responsibility comprises of the overall management of the certificate lifecycle including:

- Issuance
- Revocation
- Re-key
- Status verification (Certificate Status Service)
- Directory service

1.3.2 Registration Authorities

In the BRCA domain a single RA is operated with the task to request the issuance, suspension and revocation of a certificate under this CPS. In the Belgium Root CA domain, Belgian Government acts as the RA. When a subscriber requests for the creation of a CA certificate under the Belgium Root CA, it is FOD BOSA that will validate the request and decide whether or not to request the creation of the CA certificate to the BRCA.

In the Belgium Root Domain, there are no Local Registration Authorities.

1.3.3 Subscribers (End Entities)

The subscriber of the BRCA services is an organization that will operate a CA within the Belgium governmental domain. This CA is:

- identified in the CA certificate.
- controls the private key corresponding to the public key that is listed in the CA certificate.

1.3.4 Relying Parties

Within the BRCA domain relying parties are entities including natural or legal persons that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a CA certificate.

To verify the validity of a digital certificate they receive, relying parties must always verify with a CA Validation Service (e.g. CRL, delta CRL, web interface) prior to relying on information featured in a certificate.

1.3.5 Other Participants

Section is not applicable.

1.4 CERTIFICATE USAGE

Certain limitations apply to the usage of certificates issued by the BRCA that include the ones stated hereunder.

1.4.1 Appropriate Certificate Uses

The certificates issued by BRCA can be used both:

- To sign CA certificates within a PKI hierarchy. Such certificates are used to assert the identity of a CA.

1.4.2 Prohibited Certificate Uses

Certain limitations apply to the usage of certificates issued by the BRCA as stated in this CPS.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

Policy administration is reserved to FOD BOSA which can be contacted via:

- *Postal service:*
  FOD BOSA
  FOD BOSA Legal Practices - BRCA
  Boulevard Simon Bolivar 30/9
  1000 Brussels
- *Mail:*
  Subject: FOD BOSA Legal Practices - BRCA
  To: eid@bosa.fgov.be

1.5.2 Contact Person

The main contact for any questions or suggestions regarding the BRCA CP/CPS, is to be found under § 1.5.1 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.

1.5.3 Person Determining CPS Suitability for the Policy

In conformity with the ETSI 319 411-2 standard supporting 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 and repealing Directive 1999/93/EC*) on electronic signature, FOD BOSA assumes the management of its CSP 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, Belgian Government gathers all necessary information and asks all relevant questions to these parties in order to perform its CSP 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 second advice and bears dispute settlement responsibility.

1.5.4 CPS approval procedures

Belgium Root Certificate Authority CPS is prepared and reviewed by the FOD BOSA CEPRAC team.

At the time of review the CEPRAC-team will determine if the change is minor or major. This determination is based on an assessment of the change in the amount of risk from the changes.

o All modifications are enforced once the CEPRAC and if appropriate legal review is completed.

o Minor modifications versions will be incremented in tenths (i.e. replace v1.0 with v1.1).

o Major modifications versions will be incremented in whole number increments (i.e. replace v1.0 with v2.0).

o Major modifications to this CPS must be approved by the CEPRAC and legal affairs, upon a recommendation.

o At the time of review the CEPRAC will also determine if the changes require prior notification to users of the CPS.

If notification is required, the CEPRAC will determine how much notice is to be given (this will usually be approximately 45 calendar days). The eID Service Manager will be responsible for making sure that this CPS is reviewed by the CEPRAC Authority (Steering Committee) at least annually, the clock starts at the time of the most recently approved change.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

A list of definitions can be found at the end of this CPS.

1.6.2 Acronyms

A list of definitions can be found at the end of this CPS.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

The BRCA publishes information about the digital certificates it issues in (an) online publicly accessible repository (ies) under the Belgian Internet Domain. The BRCA reserves its rights to publish certificate status information in third partyrepositories.

2.1 REPOSITORIES

The Repository is available at the following website https://repository.pki.belgium.be.

The BRCA retains an online repository of documents where it makes certain disclosures about its practices, procedures and the content of certain of its policies including its CPS. The BRCA reserves its right to make available and publish information on its policies by any means it sees fit.

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 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 CA owes duty to.

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 digital certificate status information in frequent intervals as indicated in this CPS.

The BRCA maintains the CRL distribution point and the information on this URL until the expiration date of all certificates, containing the CRL distribution point.

Approved versions of documents to be published on the Repository are uploaded within 24 hours.

2.4 ACCESS CONTROLS ON REPOSITORIES

The web interface certificate status verification service, the certificate repository and the CRLs are publicly available on the BRCA site on the Internet.

The access to the public repository is free of charge.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

The RA maintains documented practices and procedures to authenticate the identity and/or other attributes of a certificate applicant. Prior to requesting the issuance of a certificate the RA verifies the identity of the organization that wants to establish a CA under the Belgium Root CA.

The RA authenticates the requests of parties wishing the revocation of certificates under this policy.

To identify the CA, the BRCA follows certain naming and identification rules that include types of names assigned to the subject, such as X.500 distinguished names RFC-822 names and X.400 names.

3.1.1 Types of Names

The (BR)CA certificate Subject fields attributes are described in 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 is not applicable.

3.2 INITIAL IDENTITY VALIDATION

For the identification and authentication procedures of the initial subscriber registration the RA ensures that:

The applicant proves its organisational status identity by providing the RA with appropriate documents issued by a Public Authority and signed by an authorized official.

The RA authenticates the identity of the applicant based on the documentation or credentials produced. The RA may consult additional information to verify the identity of the applicant.

3.2.1 Method to Prove Possession of Private Key

In accordance with European regulation and Belgian Signature law, private keys of the BRCA & SubCA's are generated on the Secure Signature Creation Device (SSCD), under control of the Belgian Government.

3.2.2 Authentication of Organization Identity

Section is not applicable

3.2.3 Authentication of Individual Identity

See section 3.2

3.2.4 Non-Verified Subscriber Information

Section is not applicable.

3.2.5 Validation of Authority

See section 3.2

3.2.6 Criteria for Interoperation

Section is not applicable.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

Identification and Authentication for routine Re-Key is based on the same requirements as issuance of new Certificates.

3.3.2 Identification and Authentication for Re-Key after Revocation

A request to revoke Keys and Digital Certificates may be submitted by persons authorised to do so under relevant contractual documentation.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

For the identification and authentication procedures of revocation requests the RA requires a formal request addressed to the RA and issued by the Public Authority who initially subscribed.

No suspensions will be performed on any of the CA certificates issued by the BRCA.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Any of the CAs for which a certificate has been issued by the BRCA has a continuous obligation to inform 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 BRCA for the revocation of the existing certificates and the generation of new certificates with the correct data).

The BRCA issues and revokes certificates only at the request of the RA to the exclusion of any other, unless explicitly instructed so by the RA, with the exception of a proven key compromise. In case of a proven CA key compromise, the BRCA will immediately revoke the CA certificate, even without request from the RA.

4.1 CERTIFICATE APPLICATION

The BRCA acts upon request of the RA that has the authority and is designated to make a request to issue such a CA certificate.

4.1.1 Who can Submit a Certificate Application.

The CSP of Belgian Citizen & Foreigner CA can submit requests for Issuing CA Certificates, National Registry can submit requests for role certificates used for administration purposes.

4.1.2 Enrolment Process and Responsibilities

The enrolment request of Belgian Citizen & Foreigner CA's or role certificates is accompanied with detailed specifications in APPENDIX C (specific information regarding Citizen & Foreigner CA can be found on https://repository.eid.belgium.be) together with other internal documents.

4.2 CERTIFICATE APPLICATION PROCESSING

The RA acts upon a certificate application to validate the identity of the requesting organization.

Subsequently, the RA either approves or rejects the certificate application. Such approval or rejection does not necessarily have to be justified to the requesting organization or any other party.

In case the RA accepts the certificate application, the RA will determine together with the requesting organization upon all CA details, including the identification of the organization that will act as CA, all required CA procedures and documentation (including CPS, CP's, etc.), description of the CA purpose, the required CA certificate profile and the values of each and any attribute that should be present in the CA certificate (together further referred to as "CA Definition"). This CA Definition is an integral part of the certificate request. Without it, the BRCA is not able to process the CA certificate request

4.2.1 Performing Identification and Authentication Functions

Section is not applicable.

4.2.2 Approval or Rejection of Certificate Applications

Section is not applicable.

4.2.3 Time to Process Certificate Applications

Section is not applicable.

4.3 CERTIFICATE ISSUANCE

Following approval of the certificate application, the RA informs the BRCA of the request. The BRCA specifically verifies the completeness, integrity and uniqueness of the data, presented by the RA and notifies the RA of any problem thereof. The BRCA will indicate technical feasibility of the proposed CA Definition. In case the CA Definition is not acceptable, the BRCA, the RA and the requesting organization will agree upon a modified CA Definition.

Upon final agreement of a CA Definition, the RA, the requesting organization and the BRCA will agree upon a date and a back-up date when mandated people from each organization can make themselves available at the BRCA premises to perform a CA Ceremony.

At least 3 weeks before that date each of the organizations that will be represented at the CA Ceremony should send a letter to the BRCA containing at least:

- *A formal approval from the organization to perform the CA Ceremony*
- *Name and function of the mandated people that will represent the organization at the CA Ceremony*
- *The statement that these people will be available at the foreseen date and back- up date for the CA Ceremony*
- *A signature by a mandated person belonging to the organization other than any of the people mentioned as representatives for the organization during the CA Ceremony.*

At least the following organisations need to be officially represented at the CA Ceremony and thus have to send the above-mentioned letter in time:

- *The Belgian Government*
- *The BRCA*
- *The RA*
- *The requesting organization*

The Belgian Government, the BRCA, the RA and the Requesting Organization can request for the presence of others to be required (e.g. neutral auditor).

At the predefined date, all representatives will gather at the secured premises of the BRCA and will take place to the CA Ceremony that will be led by the Security Officer of the BRCA. During this ceremony, the CA key pair will be generated and the public key will be certified by the BRCA, according to the CA Definition.

Following issuance of a certificate, the BRCA posts an issued certificate on the Repository.

4.3.1 CA Actions during Certificate Issuance

Section is not applicable.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Section is not applicable.

4.4 CERTIFICATE ACCEPTANCE

During the CA Ceremony, all representatives of the organizations present will validate that the generated certificate is fully compliant to the CA Definition, and that the procedures described in the CA Definition have been followed.

4.4.1 Conduct Constituting Certificate Acceptance

Only when each of these people agrees to this and thus accept the certificate, the CA Public Key and the CA certificate will be liberated by the BRCA, and only on that condition the CA private key can be handed over to the organization that will operate the new CA, or the private key can be put in operation by the BRCA (if the BRCA will also operate this new CA).

4.4.2 Publication of the Certificate by the CA

All CA Certificates (Root, Citizen, Foreigner and Government) issued within the BRCA are made available in public repositories.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Section is 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 Subscriber Private Key and Certificate Usage

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

- *Refraining from tampering with a certificate.*
- *Only using certificates for legal and authorised purposes in accordance with the CPS.*
- *Using a certificate, as it may be reasonable under the circumstances.*
- *Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private keys.*

4.5.2 Relying Party Public Key and Certificate Usage

A party relying on a certificate issued by the BRCA will:

- *Validate the certificate by using a CRL or web based certificate validation in accordance with the certificate path validation procedure.*
- *Trust the certificate only if it has not been revoked.*
- *Rely on the certificate, as may be reasonable under the circumstances.*

4.6 CERTIFICATE RENEWAL

Certificate Renewal means the issuance of a new Certificate without changing the Public Key or any other information in the Certificate.

The Belgium Root PKI does not support Certificate Renewal.

4.6.1 Circumstance for Certificate Renewal

Section is not applicable.

4.6.2 Who May Request Renewal

Section is not applicable.

4.6.3 Processing Certificate Renewal Requests

Section is not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Section is not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Section is not applicable.

4.6.6 Publication of the renewal certificate by the CA

Section is not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Section is not applicable.

4.7 CERTIFICATE RE-KEY

Certificate Re-Key is when all the identifying information from a CA Certificate is duplicated in a new Digital Certificate, but there is a different public key and a different 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

CA Certificates may be Re-Keyed upon request.

4.7.2 Who May Request Certification of a New Public Key

Certificate Holders, owners may request Digital Certificate Re-Keys.

4.7.3 Processing Certificate Re-Keying Requests

CA Certificate Re-Key requests are processed in the same manner as requests for new CA Certificates and in accordance with the provisions of this CP/CPS.

4.7.4 Notification of New Certificate Issuance to Subscriber

Section is not applicable.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Section is not applicable.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Section is not applicable.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Section is not applicable.

4.8 CERTIFICATE MODIFICATION

Section is not applicable.

4.8.1 Circumstance for Certificate Modification

Section is not applicable.

4.8.2 Who May Request Certificate Modification

Section is not applicable.

4.8.3 Processing Certificate Modification Requests

Section is not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Section is not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Section is not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Section is not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Section is not applicable.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

Suspension of CA certificates issued by the BRCA is not applicable. Upon request from the RA, the BRCA revokes a CA certificate.

The RA requests promptly the revocation of a certificate after:

- *Having received notice by the subscriber that there has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key of the certificate's subject.*
- *There has been a modification of the information contained in the certificate of the certificate's subject*.

4.9.1 Circumstances for Revocation

CA Certificates shall be revoked when any of the information on a CA Certificate changes or becomes obsolete or when the Private Key associated with the Digital Certificate is compromised or suspected to be compromised. A CA Certificate will be revoked in the following instances upon notification of

- *Belgium Root or SubCA key compromise;*
- *Certificate Holder profile creation error;*
- *Key Compromise including unauthorised access or suspected unauthorised access to Private Keys, lost or suspected lost keys, stolen or suspected stolen keys, destroyed or suspected destroyed keys or superseded by replacement keys and a new Certificate;*
- *The Certificate Holder has failed to meet his, her or its obligations under this or affiliated CP/CPS or any other agreement, regulation, or law that may be in force with respect to that Digital Certificate;*
- *The Certificate was not issued in accordance with the terms and conditions of this CP/CPS or the Certificate Holder provided inaccurate, false or misleading information;*
- *The Private Key corresponding to the Certificate has been used to sign, publish or distribute spyware, Trojans, viruses, rootkits, browser hijackers, or other content, for phishing, or conduct that is harmful, malicious, hostile or to download malicious content onto a user's system without their consent;*
- *The Certificate Holder is a denied party or prohibited person on a government-issued blacklist, or is operating from a prohibited destination;*

4.9.2 Who can Request Revocation

The certificate holder, owner.

4.9.3 Procedure for Revocation Request

Upon having had proof of compromise of the private key of the certificate's subject, the BRCA will immediately revoke the relevant certificate. The BRCA will then notify the RA.

4.9.4 Revocation Request Grace Period

- For certificates under the Citizen CA, the grace period for processing the revocation request is 7 days.
- For certificates under the Foreigner CA, the certificates are immediately revoked.
- For certificates under the BRCAs, the certificates are immediately revoked.

4.9.5 Time Within which CA Must Process the Revocation Request

The CA processes the revocation request immediately.

4.9.6 Revocation Checking Requirement for Relying Parties

See *APPENDIX C*.

4.9.7 CRL Issuance Frequency (if applicable)

See *APPENDIX C*.

4.9.8 Maximum Latency for CRLs (if applicable)

See *APPENDIX C*.

4.9.9 On-Line Revocation/Status Checking Availability

See *4.10* Certificate Status Services and *APPENDIX C*.

4.9.10 On-Line Revocation Checking Requirements

See *APPENDIX C*.

4.9.11 Other Forms of Revocation Advertisements Available

Section is not applicable.

4.9.12 Special Requirements Re-Key Compromise

Section is not applicable.

4.9.13 Circumstances for Suspension

Section is not applicable.

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 4.9.1.

4.10 CERTIFICATE STATUS SERVICES

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

CRL and delta CRLs

http://crl.eid.belgium.be

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 each 3 hours, at an agreed time. A Delta CRL is issued each 3 hours, according to an agreed time schedule.

The CA makes all CRLs and Delta CRLs issued in the previous 12 months available on its Web site.

OCSP

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

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

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

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.

4.10.1 Operational Characteristics

See *APPENDIX C*.

4.10.2 Service Availability

Certificate status service are available 24 hours a day, 7 days a week, 365 days of the year.

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.*
- *Download of CRL's or delta CRL's 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:

- *CRL's and delta CRL's. CRL's and delta CRL's are archived for a period of at least 30 years after publishing.*

4.10.3 Optional Features

The CA status service does not require any additional features.

4.11 END OF SUBSCRIPTION

Subscriber subscription ends when a certificate is revoked, expired or the service is terminated.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

Key escrow and recovery are not allowed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Section is not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This section describes non-technical security controls (that is, physical, procedural, and personnel controls) used by the issuing CA to securely perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, auditing, and archiving.

5.1 PHYSICAL CONTROLS

The CSP implements physical controls on its own premises. The CSP operator's physical controls include the following:

The sites of the CSP host the infrastructure to provide the CSP services. The CSP sites implement proper security controls, including access control, intrusion detection and monitoring. Access to the sites is limited to authorized 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, CRL's and delta CRL's, OCSP and archives.

5.1.1 Site Location and Construction

The CSP 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 CSP 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 CSP 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 CSP implements a partial off-site backup.

5.2 PROCEDURAL CONTROLS

The CSP 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 CSP obtains a signed statement from each member of the staff on not having conflicting interests with the CSP, 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 CSP 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.

5.2.1 Trusted Roles

The CSP separates among the following discreet work groups:

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

5.2.2 Number of Persons Required per Task

The CSP 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.

5.2.3 Identification and Authentication for Each Role

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

5.2.4 Roles Requiring Separation of Duties

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.

For critical CSP functions the CSP implements dual control.

5.3 PERSONNEL CONTROLS

The CSP 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 CSP 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;*

5.3.2 Background Check Procedures

The CSP 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 CSP party makes available training for their personnel to perform their CSP 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 is not applicable.

5.3.6 Sanctions for Unauthorized Actions

The CSP sanctions personnel for unauthorized actions, unauthorized use of authority, and unauthorized 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 CSP subcontractors and their personnel are subject to the same background checks as the CSP personnel. SEE 5.3.1

5.3.8 Documentation Supplied to Personnel

Each CSP 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.

5.4.1 Types of Events Recorded

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;
- Publishing of a CRL or delta CRL.

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

5.4.2 Frequency of Processing Log

Section is not applicable.

5.4.3 Retention Period for Audit Log

The CSP 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 CSP 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 CSP will act upon a potential application by the Belgian Government 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 CSP archives is carried out on a daily basis during working days.

5.4.6 Audit Collection System.

The CSP archive collection system is internal

5.4.7 Notification to Event-Causing Subject

Auditing events are not specifically noted in the log being audited.

5.4.8 Vulnerability Assessments

Both baseline and ongoing threat and risk vulnerability assessments are conducted on all parts of the Belgium Root PKI environment, including the equipment, physical location, records, data, software, personnel, administrative processes, communications, and each Issuing CA. Vulnerability assessment procedures intend to identify Belgium Root PKI threats and vulnerabilities, and determine a risk value based upon existing safeguards and control practices. Management can then make informed choices on determining how to best provide a secure environment with risk reduced to an acceptable level at an acceptable cost to management, clients, and shareholders.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

The CSP keeps internal records of the following items:

- *All certificates for a period of a minimum of 30 years after the expiration of that certificate;*
- *Audit trails on the issuance of certificates for a period of a minimum of 30 years after issuance of a certificate;*
- *Audit trail of the revocation of a certificate for a period of a minimum of 30 years after revocation of a certificate;*
- *CRLs and Delta CRLs for a minimum of 30 years after publishing;*

- *The CSP should retain the very last back up of the CA archive for 30 years following the issuance of the last certificate.*

The CSP keeps archives in a retrievable format.

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

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

5.5.2 Retention Period for Archive

The CSP retains in a trustworthy manner records of digital certificates for a term as indicated under article 5.5.1 in this CPS.

5.5.3 Protection of Archive

Only the records administrator (member of staff assigned with the records retention duty) may access a CSP 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 CSP will act upon a potential application by the Belgian Government 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 CSP archives is carried out on a daily basis during working days.

5.5.5 Requirements for Time-Stamping of Records

Section is not applicable.

5.5.6 Archive Collection System (Internal or External)

The CSP archive collection system is internal.

5.5.7 Procedures to Obtain and Verify Archive Information

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

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

5.6 KEY CHANGEOVER

The Citizen CA will change over all keys of subordinated issuing CAs on a regular basis. All certificates of such subordinated issuing CAs are available for download on the Repository website. These CA certificates are directly signed by the long-living trust anchors (Root CA) of the eID PKI.

The Issuer CA shall periodically change its Private Keys in a manner set forth in the CPS that prevents downtime in the Issuer CA's operation. After key changeover, the Issuer CA shall sign certificates using only the new key. The Issuer CA shall still protect its old Private Keys and shall make the old certificate available to verify signatures until all the certificates signed with the Private Key have expired.

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 equivalent to ISO 27001.

The CSP 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 CSP specifies the recovery procedures used in case computing resources, software, and/or data are corrupted or suspected of being corrupted.

The CSP 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 CSP 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 CSP 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 CSP 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 CSP 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 CSP 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 CSP
2) ensure the destruction, deletion, restitution and/or security of the information, personal data and files received by the CSP in the fulfilment of its duty as CSP in accordance to 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 and repealing Directive 1999/93/EC*)

6 TECHNICAL SECURITY CONTROLS

This section defines the security measures the CA 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 BRCA protects the private key(s) in accordance with this CPS. The BRCA uses private signing keys only for signing CA certificates and CRLs in accordance with the intended use of each of these keys.

6.1.1 Key Pair Generation

The BRCA uses a trustworthy process for the generation of the root private key according to a documented procedure. The BRCA distributes the secret shares of the private key(s). The BRCA acts upon authorisation by the Belgian Government who is the owner of the BRCA private keys, to perform cryptographic operations using the BRCA private key(s). The transfer of such secret shares to authorised secret-shareholders is done according to a documented procedure.

6.1.2 Private Key Delivery to Subscriber

Section is not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

The Belgium Root CAs public key is generated and delivered during the designated key ceremony. The SubCA's signed by the BRCA are also delivered during the designated key ceremony.

6.1.4 CA Public Key Delivery to Relying Parties

The CA public key are made available from the eID Repository website.

6.1.5 Key Sizes

For details refer to APPENDIX C.

6.1.6 Public Key Parameters Generation and Quality Checking

See section 6.1.1

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

For details refer to APPENDIX C.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The CA uses a secure cryptographic device to store its own private key meeting the appropriate FIPS 140-2 level 3 requirements.

6.2.2 Private Key (n out of m) Multi-Person Control

The private key is protected by multi-person control and “n out of m” procedures.

6.2.3 Private Key Escrow

Key escrow is not allowed.

6.2.4 Private Key Backup

The Citizen CA’s private keys are backed up, stored and recovered by multiple and appropriately authorized members of staff serving in trustworthy positions. This action entails dual control.

6.2.5 Private Key Archival

Section is not applicable.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Section is not applicable.

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

CA custodians are assigned with the task to activate the private key. The key is then active for a defined time period.

6.2.9 Method of Deactivating Private Key

CA custodians are witness of the deactivation of the private key. The key is then inactive until the CA custodians activate the private key.

6.2.10 Method of Destroying Private Key

Citizen CA’s private keys are destroyed by at least two trusted operatives present at the end of their lifetime in order to guarantee that they cannot ever be retrieved and used again.

Key destruction process is documented and associated records are archived

6.2.11 Cryptographic Module Rating

Minimum standards for cryptographic modules have been specified in paragraph:

APPENDIX B: REQUIREMENTS FOR CERTIFICATION AUTHORITIES.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

The CSP 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

The Issuer CA shall archive a copy of each Public Key.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

For details refer to 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 subscribers' key is done:

- First at the reception of the eID (SSCD)-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 subscriber is used

6.4.2 Activation Data Protection

Root CA, the key custodian's 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 CA's are protected by a split operational token that (M of N) tokens are protected by passphrase. Tokens are stored in a vault

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 is not applicable.

6.6 LIFE CYCLE TECHNICAL CONTROLS

This section addresses system development controls and security management 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 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 is not applicable.

7 CERTIFICATE, CRL, AND OCSP PROFILES

This section is used to specify the certificate format and, if CRLs and/or OCSP are used, the CRL and/or OCSP format. This includes information on profiles, versions, and extensions used.

7.1 CERTIFICATE PROFILE

The certificate profiles and attributes are described in APPENDIX C.

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 is not applicable.

7.2 CRL PROFILE

The CRL profiles and attributes are described in APPENDIX C.

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 APPENDIX C.

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 BRCA operates following the terms of REGULATION *(EU) 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 and repealing Directive 1999/93/EC.*

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

- *EN 319 411-2 Policy requirements for certification authorities issuing qualified certificates;*
- *EN 319 412-5 Profiles for Trust Service Provider issuing Certificates; Qualified certificate profile. Part 5: Extension for Qualified certificate profile*.

Regarding the Identification certificate, the CA meets the requirements set out in ETSI policy documents referring to public key certificates, including:

- *EN 319 411-3 Policy requirements for certification authorities issuing public key certificates (Normalised level).*

The BRCA accepts compliance audits or provides for compliance audits to ensure it meets requirements, standards, procedures, and service levels according to this CPS, contractual, legal and ETSI requirements.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The BRCA 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 CSP operating procedures and principles with the procedures and service levels defined in the CPS;*
- *Management of the infrastructure that implements CSP 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.;*

8.5 CAUSE OF ANY FAILURE TO COMPLY WITH THE CONDITIONS ABOVE.ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If irregularities are detected, the CSP 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

This section covers general business and legal matters.

Certain Legal conditions apply to the issuance of certificates issued by the BRCA 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 BRCA 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 Government 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.

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 is not applicable.

9.2 FINANCIAL RESPONSIBILITY

Section is not applicable.

9.2.1 Insurance Coverage

Section is not applicable.

9.2.2 Other Assets

Section is not applicable.

9.2.3 Insurance or Warranty Coverage for End-Entities

Section is not applicable.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

Any information held by Issuing CAs related to a Certificate Holder's application and the issuance of Digital Certificates is considered confidential and will not be released without the prior consent of the relevant Holder, unless required otherwise by law or to fulfil the requirements of this BRCA CP/CPS.

9.3.2 Information Not Within the Scope of Confidential Information

Information appearing in CA Certificates or stored in the Repository is not considered confidential, unless statutes or special agreements so dictate.

9.3.3 Responsibility to Protect Confidential Information

The BRCA, Issuing CAs, Registration Authorities, Certificate Holders, Relying Parties and all others are responsible for protecting Confidential Business Information in their possession, custody or control.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

The BRCA, Issuing CAs, Registration Authorities, Certificate Holders, Relying Parties and all others using or accessing any personal data in connection with matters dealt with this CP/CPS shall comply with 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 (GDPR, General Data Protection Regulation and the Belgian law of 08/12/1992 *wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* .

The CSP does not release nor is it required to release any personal data without an authenticated and justified request specifying either:

- The party to whom the the personal data applies ;
- A court order.

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. Information not Deemed Private

Non-personal 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 all information the CSP holds about them.

9.4.3 Information Not Deemed Private

See 9.4.2

9.4.4 Responsibility to Protect Private Information

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

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

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

The CSP encrypts all communications of confidential information including:

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

Next to the information retained by the CSP, the RA also retains information pertaining to the Citizen Certificates, more specifically in the Registry of Identity Cards. *The Law of 19 July 1991 regarding (Citizen register, identity cards, foreigner cards en resident documents)*

9.4.5 Notice and Consent to use Private Information

The CSP 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 and with 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)* This is conform the Law of 13 June 2005 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

The CSP 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 CSP will not be used for other purposes.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Information may be disclosed in the course of any judicial or administrative proceeding. When legally authorized we will try to obtain individual authorization before disclosing personal information.

9.4.7 Other Information Disclosure Circumstances

Section is not applicable.

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 CSP 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 CSP 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 CSP, 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 CSP will:

- Comply with this CPS and its amendments as published under http://repository.eid.belgium.be ;
- 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 promptly a certificate in accordance with this CPS;
- Upon receipt of an authenticated request for suspension from the RA to suspend promptly a certificate in accordance with this CPS;
- Upon receipt of an authenticated request for un-suspension from the RA to un-suspend promptly 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 Government;
- 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 CSP meets all legal requirements associated with qualified certificate profile emanating from Law of Belgium of 9 July 2001 with regard to electronic signatures implementing 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 and repealing Directive 1999/93/EC*).

If the CSP 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 CSP will make best efforts to ensure the proper financial responsibility and liability of such contractor.

The CSP is responsible 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;
- The failure to revoke a suspended certificate after a period of one week;
- Failure to list a revoked or suspended 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

The CSP 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 CSP makes every effort to ensure that parties accessing its Repositories receive accurate, updated and correct information. The CSP, however, cannot accept any liability beyond the limits set in this CPS under article 9.8

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 citizen 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 RA is solely responsible for the accuracy of the 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.

The RA is liable for its acts or omissions under Belgian Law.

9.6.3 Subscriber Representations and Warranties

Section is not applicable.

9.6.4 Relying Party Representations and Warranties

Section is not applicable.

9.6.5 Representations and Warranties of Other Participants

Section is not applicable.

9.7 DISCLAIMERS OF WARRANTIES

This section includes disclaimers of express warranties.

9.7.1 Limitation for Other Warranties

Section is not applicable.

9.7.2 Exclusion of Certain Elements of Damages

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

- Any loss of profits.
- Any liability incurred in any case if the error in such verified information is the result of fraud or wilful misconduct of the applicant or if it is the result of negligence or with intent to deceive the BRCA, or any person receiving or relying on the certificate.
- Any liability incurred as a result of the applicant breaking any laws applicable in Belgium including those related to intellectual property protection, viruses, accessing computer systems etc.

9.8 LIMITATIONS OF LIABILITY

Section is not applicable.

9.9 INDEMNITIES

Indemnity provisions and obligations are contained within relevant contractual documentation.

9.10 TERM AND TERMINATION

9.10.1 Term

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

9.10.2 Termination

This CP/CPS shall remain in force until it is amended or replaced by a new version.

9.10.3 Effect of Termination and Survival

The provisions of this CP/CPS shall survive the termination or withdrawal of a Certificate Holder or Relying Party from the BRCA PKI with respect to all actions based upon the use of or reliance upon a Digital Certificate or other participation within the BRCA 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 CSP**.** 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 (http://repository.eid.belgium.be).

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 version number that contains a decimal number e.g. version 1.1 for a version with minor changes as opposed to e.g. version 2.0 that addresses major issues.

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 BRCA. 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.

Any arbitration shall, unless agreed otherwise between the parties take place in Belgium.

9.14 GOVERNING LAW

The CSP provides its services under the provisions of the Belgian law.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CP/CPS is subject to applicable law.

9.16 MISCELLANEOUS PROVISIONS

The CSP incorporates by reference the following information in all CA certificates it issues:

- Terms and conditions described in this CPS;
- Any other applicable certificate policy as may be stated;
- 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 is not applicable

9.16.2 Assignment

Section is not applicable

9.16.3 Severability

Any provision of this BRCA 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 BRCA 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 CSP to exercise or enforce any right, power, privilege, or remedy whatsoever, howsoever or otherwise conferred upon it by this BRCA 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 BRCA CP/CPS is intended to be exclusive of any other right or remedy, except as expressly provided in this BRCA 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 CSP 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.

9.17 OTHER PROVISIONS

Section is not applicable.

This page is intentionally left blank

APPENDIX A

Definitions & acronyms

BRCA	Belgium Root Certificate Authority
CA	Certification Authority
CC	Common Criteria
CM	Card Manufacturer
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
ETSI	European Telecommunications Standards Institute
PKI	Public Key Infrastructure
SSCD	Secure Signature Creation Device
OCSP	Online Certificate Status Protocol
OID	Object Identifier
RA	Registration Authority

APPENDIX B

Requirements for Certification Authorities

The crypto 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

• EN 14169 PP-SSCD 4,5,6

• BSI Cryptographic Modules Security Level “Enhanced”7

APPENDIX C

Certificate Profile & Specifications

C.1 BRCA 2

C.1.1 BRCA 2 Self-Signed

Self-Signed Belgium Root CA 2								
Base Certificate	**OID**	**Include**	**Critical**	**Fixed / Dynamic**	**Value**	**Old Value**	**Reason**	**Comment**
Certificate								
SignatureAlgorithm								
Algorithm		X		Fixed	1.2.840.113549.1.1.5 (SHA1 with RSA Encryption)			
SignatureValue		X			Issuing CA Signature			
TBSCertificate								
Version		X			2			
SerialNumber		X			Generated by the CA at Key Generation Process Time			
Signature		X			1.2.840.113549.1.1.5 (SHA1 with RSA Encryption)			
Validity								
NotBefore		X			Key Generation Process Date			
NotAfter		X		Fixed	woensdag 15 december 2021 10:00:00			
SubjectPublicKeyInfo		X			RSA 2048			
Issuer								
countryName	{ id-at-6 }	X		Fixed	BE			
commonName	{ id-at-3 }	X		Fixed	Belgium Root CA3			
Subject								
countryName	{ id-at-6 }	X		Fixed	BE			
commonName	{ id-at-3 }			Fixed	Belgium Root CA3			
Standard Extensions	OID	Include	Critical		Value			
CertificatePolicies	{id-ce 32}	X	FALSE					
policyIdentifier		X		Fixed	2.16.56.9.1.1			OID was corrected to 2
policyQualifiers					NA[1]			[1] NA: Not Applicable
policyQualifierId	{ id-qt-1 }	X		Fixed	CPS			
Qualifier		X		Fixed	http://repository.eid.belgium.be			
KeyUsage	{id-ce 15}	X	TRUE					
CertificateSigning				Fixed	Set			
crlSigning				Fixed	Set			
authorityKeyIdentifier	{id-ce 35}	X	FALSE					
KeyIdentifier		X			SHA-1 Hash			
subjectKeyIdentifier	{id-ce 14}	X	FALSE					
KeyIdentifier		X			SHA-1 Hash			
BasicConstraints	{id-ce 19}	X	TRUE					
CA		X		Fixed	TRUE			
NetscapeCertType		X	FALSE					
	2.16.840.1.113730.1.1			Fixed	sslCA - smimeCA - objectSigningCA			

C.1.2 BRCA 2 CRL

CRL Certificate Belgium Root CA 2								
Base Certificate	**OID**	**Include**	**Critical**	**Fixed / Dynamic**	**Value**	**Old Value**	**Reason**	**Comment**
Certificate								
SignatureAlgorithm								
Algorithm		X		Fixed	1.2.840.113549.1.1.11 (SHA256 with RSA Encryption)	1.2.840.113549.1.1.5 (SHA1 with RSA Encryption)	• CAB Ballot 118 - Baseline Requirements - Effective 1 January 2017 SHA-1 MUST NOT be used to issue any kind of certificates.	
SignatureValue		X		Dynamic	Issuing CA Signature			
TBSCertificate								
Version		X		Fixed	1	0	• RFC 5280 compliance	A CRL profile that uses CRL extensions MUST BE version 2 (value 1). The CRL extensions are required
Signature		X		Fixed	1.2.840.113549.1.1.11 (SHA256 with RSA Encryption)	1.2.840.113549.1.1.5 (SHA1 with RSA Encryption)	• CAB Ballot 118 - Baseline Requirements - Effective 1 January 2017 SHA-1 MUST NOT be used to issue any kind of certificates.	
thisUpdate		X		Dynamic	Key Generation Process Date			
nextUpdate		X		Dynamic	CRL Generation Process Date + 8 months			
Issuer								
countryName	{ id-at-6 }	X		Fixed	BE			
commonName	{ id-at-3 }	X		Fixed	Belgium Root CA2			
revokedCertificates								
Sequence								
userCertificate		X		Dynamic	16 Byte serialnumber of the CA			
revocationDate		X		Dynamic	Revocation Date			
CRL Entry Extensions								
cRLReasons	{ id-ce 21 }	X						
reasonCode		X		Dynamic	Reason code for the revocation			
CRL Extensions	OID	Include	Critical		Value			
authorityKeyIdentifier	{ id-ce 35 }	X	FALSE					
KeyIdentifier		X			SHA-1 Hash		• RFC 5280 compliance	
CRLNumber	{ id-ce 20 }	X	FALSE					
CRLNumber		X		Dynamic	Increment previous CRL number by 1		• RFC 5280 compliance • eIDAS Audit - Issue 4	Starting CRL Number is 1

C.2 BRCA 3

C.2.1 BRCA 3 Self-Signed

Self-Signed Belgium Root CA 3								
Base Certificate	**OID**	**Include**	**Critical**	**Fixed / Dynamic**	**Value**	**Old Value**	**Reason**	**Comment**
Certificate								
SignatureAlgorithm								
Algorithm		X		Fixed	1.2.840.113549.1.1.5 (SHA1 with RSA Encryption)			
SignatureValue		X			Issuing CA Signature			
TBSCertificate								
Version		X			2			
SerialNumber		X			Generated by the CA at Key Generation Process Time			
Signature		X			1.2.840.113549.1.1.5 (SHA1 with RSA Encryption)			
Validity								
NotBefore		X			Key Generation Process Date			
NotAfter		X		Fixed	vrijdag 28 januari 2028 14:00:00			
SubjectPublicKeyInfo		X			RSA 4096			
Issuer								
countryName	{ id-at-6 }	X		Fixed	BE			
commonName	{ id-at-3 }	X		Fixed	Belgium Root CA3			
Subject								
countryName	{ id-at-6 }	X		Fixed	BE			
commonName	{ id-at-3 }			Fixed	Belgium Root CA3			
Standard Extensions	OID	Include	Critical		Value			
CertificatePolicies	{id-ce 32}	X	FALSE					
policyIdentifier		X		Fixed	2.16.56.10.1.1			OID was corrected to 2
policyQualifiers					NA[1]			[1] NA: Not Applicable
policyQualifierId	{ id-qt-1 }	X		Fixed	CPS			
Qualifier		X		Fixed	http://repository.eid.belgium.be			
KeyUsage	{id-ce 15}	X	TRUE					
CertificateSigning				Fixed	Set			
crlSigning				Fixed	Set			
authorityKeyIdentifier	{id-ce 35}	X	FALSE					
KeyIdentifier		X			SHA-1 Hash			
subjectKeyIdentifier	{id-ce 14}	X	FALSE					
KeyIdentifier		X			SHA-1 Hash			
BasicConstraints	{id-ce 19}	X	TRUE					
CA		X		Fixed	TRUE			
NetscapeCertType		X	FALSE					
	2.16.840.1.113730.1.1			Fixed	sslCA - smimeCA - objectSigningCA			

C.2.2 BRCA 3 CRL

CRL Certificate Belgium Root CA 3								
Base Certificate	**OID**	**Include**	**Critical**	**Fixed / Dynamic**	**Value**	**Old Value**	**Reason**	**Comment**
Certificate								
SignatureAlgorithm								
Algorithm		X		Fixed	1.2.840.113549.1.1.11 (SHA256 with RSA Encryption)	1.2.840.113549.1.1.5 (SHA1 with RSA Encryption)	• CAB Ballot 118 - Baseline Requirements - Effective 1 January 2017 SHA-1 MUST NOT be used to issue any kind of certificates.	
SignatureValue		X		Dynamic	Issuing CA Signature			
TBSCertificate								
Version		X		Fixed	1	0	• RFC 5280 compliance	A CRL profile that uses CRL extensions MUST BE version 2 (value 1). The CRL extensions are required
Signature		X		Fixed	1.2.840.113549.1.1.11 (SHA256 with RSA Encryption)	1.2.840.113549.1.1.5 (SHA1 with RSA Encryption)	• CAB Ballot 118 - Baseline Requirements - Effective 1 January 2017 SHA-1 MUST NOT be used to issue any kind of certificates.	
thisUpdate		X		Dynamic	Key Generation Process Date			
nextUpdate		X		Dynamic	CRL Generation Process Date + 8 months			
Issuer								
countryName	{ id-at-6 }	X		Fixed	BE			
commonName	{ id-at-3 }	X		Fixed	Belgium Root CA3			
revokedCertificates								
Sequence								
userCertificate		X		Dynamic	16 Byte serialnumber of the CA			
revocationDate		X		Dynamic	Revocation Date			
CRL Entry Extensions								
cRLReasons	{ id-ce 21 }	X						
reasonCode		X		Dynamic	Reason code for the revocation			
CRL Extensions	OID	Include	Critical		Value			
authorityKeyIdentifier	{ id-ce 35 }	X	FALSE					
KeyIdentifier		X			SHA-1 Hash		• RFC 5280 compliance	
CRLNumber	{ id-ce 20 }	X	FALSE					
CRLNumber		X		Dynamic	Increment previous CRL number by 1		• RFC 5280 compliance • eIDAS Audit - Issue 4	Starting CRL Number is 1

C.3 BRCA 4

C.3.1 BRCA 4 Self-Signed

Self-Signed Belgium Root CA 4								
Base Certificate	**OID**	**Include**	**Critical**	**Fixed / Dynamic**	**Value**	**Old Value**	**Reason**	**Comment**
Certificate								
SignatureAlgorithm								
Algorithm		X		Fixed	1.2.840.113549.1.1.11 (SHA256 with RSA Encryption)			
SignatureValue		X			Issuing CA Signature			
TBSCertificate								
Version		X			2			
SerialNumber		X			Generated by the CA at Key Generation Process Time			
Signature		X			Sha256WithRSAEncryption			
Validity								
NotBefore		X			Key Generation Process Date			
NotAfter		X		Fixed	vrijdag 22 oktober 2032 14:00:00			
SubjectPublicKeyInfo		X			RSA 4096			
Issuer								
countryName	{ id-at-6 }	X		Fixed	BE			
commonName	{ id-at-3 }	X		Fixed	Belgium Root CA4			
Subject								
countryName	{ id-at-6 }	X		Fixed	BE			
commonName	{ id-at-3 }			Fixed	Belgium Root CA4			
Standard Extensions	OID	Include	Critical		Value			
CertificatePolicies	{id-ce 32}	X	FALSE					
policyIdentifier		X		Fixed	2.16.56.12.1.1			
policyQualifiers					NA[1]			[1] NA: Not Applicable
policyQualifierId	{ id-qt-1 }	X		Fixed	CPS			
Qualifier		X		Fixed	http://repository.eid.belgium.be			
KeyUsage	{id-ce 15}	X	TRUE					
CertificateSigning				Fixed	Set			
crlSigning				Fixed	Set			
authorityKeyIdentifier	{id-ce 35}	X	FALSE					
KeyIdentifier		X			SHA-1 Hash			
subjectKeyIdentifier	{id-ce 14}	X	FALSE					
KeyIdentifier		X			SHA-1 Hash			
BasicConstraints	{id-ce 19}	X	TRUE					
CA		X		Fixed	TRUE			
NetscapeCertType		X	FALSE					
	2.16.840.1.113730.1.1			Fixed	sslCA - smimeCA - objectSigningCA			

C.3.2 BRCA 4 CRL

CRL Certificate Belgium Root CA 4								
Base Certificate	**OID**	**Include**	**Critical**	**Fixed / Dynamic**	**Value**	**Old Value**	**Reason**	**Comment**
Certificate								
SignatureAlgorithm								
Algorithm		X		Fixed	1.2.840.113549.1.1.11 (SHA256 with RSA Encryption)	1.2.840.113549.1.1.5 (SHA1 with RSA Encryption)	• CAB Ballot 118 - Baseline Requirements - Effective 1 January 2017 SHA-1 MUST NOT be used to issue any kind of certificates.	
SignatureValue		X		Dynamic	Issuing CA Signature			
TBSCertificate								
Version		X		Fixed	1	0	• RFC 5280 compliance	A CRL profile that uses CRL extensions MUST BE version 2 (value 1). The CRL extensions are required
Signature		X		Fixed	1.2.840.113549.1.1.11 (SHA256 with RSA Encryption)	1.2.840.113549.1.1.5 (SHA1 with RSA Encryption)	• CAB Ballot 118 - Baseline Requirements - Effective 1 January 2017 SHA-1 MUST NOT be used to issue any kind of certificates.	
thisUpdate		X		Dynamic	Key Generation Process Date			
nextUpdate		X		Dynamic	CRL Generation Process Date + 8 months			
Issuer								
countryName	{ id-at-6 }	X		Fixed	BE			
commonName	{ id-at-3 }	X		Fixed	Belgium Root CA4			
revokedCertificates								
Sequence								
userCertificate		X		Dynamic	16 Byte serialnumber of the CA			
revocationDate		X		Dynamic	Revocation Date			
CRL Entry Extensions								
cRLReasons	{ id-ce 21 }	X						
reasonCode		X		Dynamic	Reason code for the revocation			
CRL Extensions	OID	Include	Critical		Value			
authorityKeyIdentifier	{ id-ce 35 }	X	FALSE					
KeyIdentifier		X			SHA-1 Hash		• RFC 5280 compliance	
CRLNumber	{ id-ce 20 }	X	FALSE					
CRLNumber		X		Dynamic	Increment previous CRL number by 1		• RFC 5280 compliance • eIDAS Audit - Issue 4	Starting CRL Number is 1