FedICT – Federal Information & Communication Technologies
Address: Rue Marie Thérèse 1-3 Maria Theresastraat
B-1000 Brussels – Belgium
Web: www.fedict.be Tel: +32 2 212 96 00
Email: info@fedict.be Fax: +32 2 212 96 99

PKI Belgium

Belgium Root CA

Certification Practice Statement

2.16.56.1.1.1

Document Control and References

Copyright Notice

Changes history

Issue	Status	Date	Changes
1.0	Final	04/03/2003	-
1.1	Final	03/02/2006	WebTrust4CA requirements

Distribution List

Organization	Name	Email
public	public	-

Table of Content

Acknowledgments

This Belgium Root Certification Authority CPS endorses the following standards:

- RFC 2527: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework,
- RFC 2459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.
- RFC 3039: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile.
- RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP
- ETSI TS 101 042: Policy requirements for certification authorities issuing public key certificates (Normalised level).
- The ISO 1-7799 standard on security and infrastructure.

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 taken into account. These documents will be available through the BRCA repository at: http:// pki.belgium.be.

This CPS complies with the formal requirements of Internet Engineering Task Force (IETF) RFC 2527, version 12 July 2001 with regard to format and content. While certain section titles are included according to the structure of RFC 2527, 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.

Further information with regard to this CPS and the BRCA can be obtained from the BRCA, attn. Fedict Legal Practices, Rue Marie Thèrèse 1/3, B-1000 Brussels, Belgium.

1.1 Overview

To support the Belgian government's plan to issue 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 is such an operational CA that subsequently issues certificates to end users who are beneficiaries of the electronic identity programme 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 **P**ublic **K**ey cryptography combined with an **I**nfrastructure 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 BRCA and identifies the roles, responsibilities and practices of e.g. CA, 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 with regard to practices, level of services, responsibilities and liability bind all parties involved including the BRCA, subscribers, which are other CAs and relying parties. This CPS prescribes the provisions of the Belgium Root Certification Authority (BRCA). This CPS also endorses certain provisions prevailing within the domain of the Certification Authority known as GlobalSign with regard to the root signing function of the BRCA by the former.

This CPS governs the issuance of the CA certificates during the application period during which the CA may issue certificates. This CPS is made available on-line in the Repository of the issuing CA under http://repository.pki.belgium.be .

This CPS is maintained by Fedict.

This CPS describes the policy requirements to issue, manage and use certificates within the scope of the BRCA domain. The BRCA issues certificates to CAs that carry out electronic certification services within their own domains and in support of multiple types of certificates.

The BRCA accepts comments regarding this CPS addressed to: by email to info@fedict.be or by post to attn. Fedict Legal Practices, Rue Marie Thèrèse 1/3, B-1000 Brussels, Belgium.

1.2 Trust hierarchy

The BRCA belongs to the broader domain of CAs of the Belgian State. To facilitate the building of trust among the various participating CAs, the Belgian State has set up a CA hierarchy.

In this hierarchy, it is the Belgium Root CA (BRCA) that has as purpose amongst others to build trust in the various CAs within the government domain. The BRCA has certified each of the private keys of the operational CAs in the government domain including for instance:

- the Citizen CA: used to sign Certificates for Belgian Citizens older than 12Y (both authentication and signature certificates to be loaded on their eID card)
- the Child CA: used to sign Certificates for Belgian Citizens younger than 12Y (only authentication certificates to be loaded on thei child card)
- the Foreigner CA: used to sign Certificates for Belgian Foreigners older than 12Y (both authentication and signature certificates to be loaded on their resident card)

- the Government CA: used to sign Certificates for Belgian authorities (both web server and code signing certificates)
- the Government AA: used to sign Certificates for Belgian authorities (only identity providers and assertion authorities)
- the RRN Sign: used to sign the identity files loaded on the Belgian citizen, child and foreigner eID cards
- the Administration CA: used to sign specific role certificates granting privileged access to eID cards

By validating the certificate of such a CA, the trust in the BRCA can also be applied to the CA it has certified. To the extent that the BRCA is trusted, an end-user certificate can be trusted as well. Trust in BRCA within software applications is also ascertained through root sign carried out by a third party provider, whose root has widely been embedded in application software.

The Trust hierarchy of an end-user certificate follows certain architecture premises. These have impact on the whole Trust hierarchy, thus as well on the Belgium Root CA. These premises are the following:

1. A small hierarchy for which all the required information to validate the end-user certificates off-line can be stored in the card.
2. A high preference for automated trust in certificates issued by the Belgian State infrastructure without requiring end-user intervention, which allows, however, online verification.

This more complex hierarchy is described in figure 1 below:

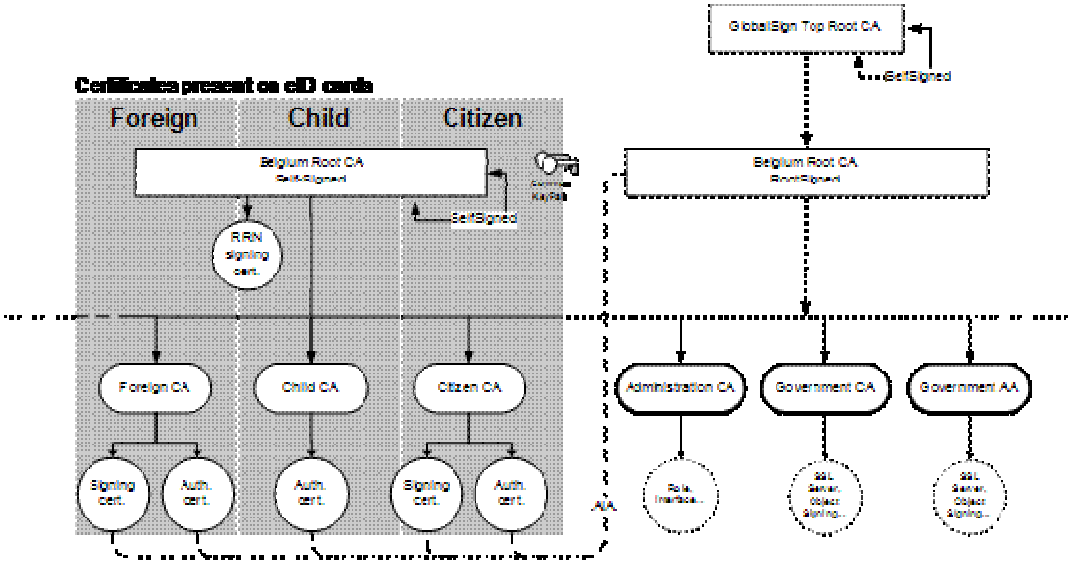

Figure 1: eID hierarchy

To meet both requirements, the eID hierarchy consists of a combination of a two-layered and a three-layered model.

In the two-layered model the eID Citizen CA and the Self-Signed Belgium Root CA[1] form a hierarchy, which in an off-line mode allows validating the eID Citizen signing and authentication certificates. In this model the private key of the Belgium Root CA is self-signed. In that case the party that performs the validation (e.g. Customs Officer, Police Officer, etc.) can use the Self-Signed BRCA certificate from its own eID card, and use it to validate the eID Citizen CA certificate and eID citizen certificates from the card to be validated.

In the three-layered model the eID Citizen CA, the Belgium Root signed Top Root CA and the GlobalSign Root CA form a hierarchy. In this model the same private key as used for the Self-Signed Belgium Root CA is this time certified by the Globalsign Root CA. This approach allows the automated validation within the most widely used applications, e.g. browsers, because these browsers have already embedded the GlobalSign Top Root CA certificate and they list it as a trusted one. Just as the eID Citizen CA inherits trust from the BRCA, the BRCA inherits trust from the GlobalSign Root CA. This three-layered model eliminates the need to individually import the Self Signed Belgium Root CA certificate.

Because both the Self-Signed Belgium Root CA and the Belgium root signed Top Root CA share the same key pair albeit using two different certificates, a certificate signed by the private key of that key pair can be validated with both Belgium Root certificates.

In most case the application builder will have foreseen one of both models to be used, and the end user will not have to choose between the two models.

1.3 Document Name and Identification

The BRCA may also use the following OID's to identify this CPS:

Certificate Type	**OID**
Belgium Root CA certificate	2.16.56.1.1.1
Administration CA certificate	2.16.56.1.1.1.1
Citizen CA certificate	2.16.56.1.1.1.2
Government CA certificate	2.16.56.1.1.1.3
RRN Signing certificate	2.16.56.1.1.1.4
Child CA certificate	2.16.56.1.1.1.5
Government AA certificate	2.16.56.1.1.1.6
Foreigner CA certificate	2.16.56.1.1.1.7

[1] A self-signed certificate is a certificate signed with the private key of the certified entity itself. Since there is no trust point higher above in the Trust hierarchy, no trust can be build on that certificate or any of the certificates that are lower in the hierarchy if that self-signed certificate is not trusted. This, however, is a case that very rarely might occur.

1.4 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.

1.4.1 Certification Authority

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

The BRCA ensures the availability of all services pertaining to the certificates, including the issuing, revocation, re-key, status verification as they may become available or required in specific applications.

Service	**Availability**
CRL publication/download	99.5%
CPS publication/download	99.5%

This is supervised according the requirements of the Belgian accreditation requirements for CAs.

To provide notice or knowledge to relying parties functions associated with the revoked certificates requires appropriate publication in a certificate revocation list. The BRCA operates such a list according to the requirements of the Belgian Government and within the limits set out by of Belgian Law.

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 elsewhere in this CPS. 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 BRCA's domain of responsibility comprises of the overall management of the certificate lifecycle including:

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

The root sign provider

The root sign provider ensures Trust in BRCA in widely used applications. The root sign provider ensures that its root remains trusted by such applications and notifies the RA of any event affecting Trust to its own root.

1.4.2 Registration Authorities and Local 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, FEDICT acts as the RA. When a subscriber requests for the creation of a CA certificate under the Belgium Root CA, it is FEDICT 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.

1.4.3 Subscribers

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.

1.4.4 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.

1.5 Certificate usage

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

1.5.1 Appropriate certificate usage

The certificates issued by BRCA can be used both:

- To sign certificates within a PKI hierarchy. Such certificates can be used to assert the identities.
- To sign attributes. Such signed attributes (assertions) can be used to assert properties.

The purpose of the certificates issued by the BRCA is to authenticate a CA (Certificate Authority) or an AA (Attribute Authority).

1.5.2 Prohibited certificate usage

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

1.6 Policy Administration

The Belgian Government is baring responsibility for the drafting, publishing, OID registration, maintenance, and interpretation of this CPS.

The policy administration of this CPS is distinct and remains independent from other policy authorities managing or approving of policies of other CAs operating within the domain or under the auspices of the Belgian government.

Any policy approved by the BRCA has to ultimately comply with the provisions of this CPS.

1.7 Definitions and 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 on third party repositories.

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.

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

The BRCA sets up and maintains a repository of all certificates it has issued. This repository also indicates the status of a certificate issued.

The BRCA publishes CRL's[2] at http://crl.pki.belgium.be .

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.

Due to their sensitivity the BRCA 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 BRCA owes duty to.

The access to the public repository is free of charge.

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

[2] A CRL or Certificate Revocation List is a list issued and digitally signed by a CA that includes revoked and suspended certificates. Such list is to be consulted by relying parties at all times prior to relying on information featured in a certificate.

3 IDENTIFICATION AND AUTHENTICATION

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.

3.1 Naming

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.

3.2 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.

The BRCA is rootsigned by GlobalSign and it adheres to its Certificate Policy. This CPS is suitable to determine the conditions of interoperation between the GlobalSign Certificate Policy and this CPS.

3.3 Identification and Authentication for Revocation and suspension Requests

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.

4.2 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.

4.3 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 then 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 lead by the Security Officer of the BRCA. During this ceremony the CA key pair will be generated and the public 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.

4.4 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.

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).

4.5 Key Pair and Certificate Usage

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

4.5.1 Subscriber duties

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 duties

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 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.

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 the RA.

4.6.1 Term and Termination of Suspension and Revocation

Revocation is final. Suspension is not applicable.

The BRCA publishes notices of revoked certificates in the Repository.

4.7 Certificate Status Services

The BRCA makes available certificate status checking services including CRLs and appropriate Web interfaces.

CRL

- CRLs are signed and time-marked by the BRCA. A CRL is issued each 6 months, at an agreed time.
- The BRCA makes all CRLs issued in the previous 12 months available on its Website.

OCSP

- The BRCA does not provide for an OCSP service for the certificates it has issued.

4.8 End of Subscription

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

4.9 Certificate re-key

Renewal of CA certificates issued by the BRCA is not applicable.

Re-key of CA certificates issued by the BRCA is treated as a new CA certificate application.

5 MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

This section describes non-technical security controls used by the BRCA Operator to perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.

5.1 Physical Security Controls

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

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

Physical access is restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating CA 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.

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

Premises are protected from any water exposures.

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

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

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

The BRCA implements a partial off-site backup.

The sites of the BRCA host the infrastructure to provide the BRCA services. The BRCA 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 and CRL's.

5.2 Procedural Controls

The BRCA 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 BRCA obtains a signed statement from each member of the staff on not having conflicting interests with the BRCA, 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 BRCA conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to make a reasonable attempt to determine their trustworthiness and competence.

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

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

For critical BRCA functions the BRCA implements dual control.

The BRCA separates among the following discreet work groups:

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

5.3 Personnel Security Controls

The BRCA 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, Clearances

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

- Criminal convictions for serious crimes.
- Misrepresentations by the candidate.
- Appropriateness of references.
- Any clearances as deemed appropriate.

5.3.2 Background Checks and Clearance Procedures

The BRCA 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 and Procedures

The BRCA makes available training for their personnel to perform their CA functions.

5.3.4 Retraining Period and Retraining Procedures

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

5.3.5 Sanctions against Personnel

The BRCA sanctions personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems for the purpose of imposing accountability on the BRCA personnel, as it might be appropriate under the circumstances.

5.3.6 Controls of independent contractors

Independent BRCA subcontractors and their personnel are subject to the same background checks as the BRCA personnel. The background checks include:

- Criminal convictions for serious crimes.

- Misrepresentations by the candidate.
- Appropriateness of references.
- Any clearances as deemed appropriate.
- Privacy protection.
- Confidentiality conditions.

5.3.7 Documentation for initial training and retraining

The BRCA makes available documentation to personnel, during initial training, retraining, or otherwise.

5.4 Audit Logging Procedures

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

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

- Issuance of a certificate.
- Revocation of a certificate.
- Suspension of a certificate.
- Automatic revocation.
- Publishing of a CRL .

The BRCA audits all event-logging records.

Audit trail records contain:

- The identification of the operation.
- The data and time of the operation.
- The identification of the certificate, involved in the operation.
- The identity of the transaction requestor.

In addition, the BRCA 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 BRCA 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 BRCA ensures that designated personnel reviews log files at regular intervals and detects and reports anomalous events.

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

Auditing events are not given log notice.

5.5 Records Archival

The BRCA keeps 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 for a minimum of 30 years after publishing.
- The very last back up of the BRCA archive should be retained for 30 years following the issuance of the last certificate by the BRCA.

The BRCA keeps archives in a retrievable format.

The BRCA 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 Belgian Government, the BRCA and the RA.

5.5.1 Types of records

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

5.5.2 Retention period

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

5.5.3 Protection of archive

Only the records administrator (member of staff assigned with the records retention duty) may access a BRCA 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.

5.5.4 Archive backup procedures

A full backup is taken at each CA Ceremony.

5.5.5 Archive Collection

The BRCA archive collection system is internal.

5.5.6 Procedures to obtain and verify archive information

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

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

5.6 Compromise and Disaster Recovery

In a separate internal document the BRCA specifies applicable incident, compromise reporting and handling procedures. The BRCA specifies the recovery procedures used if computing resources, software, and/or data are corrupted or suspected of being corrupted.

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

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

All such measures are compliant with ISO 1-7799.

The BRCA establishes:

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

Disaster recovery infrastructure and procedures are tested at least yearly.

6 TECHNICAL SECURITY CONTROLS

This section defines the security measures the BRCA takes to protect Belgian Government's 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 CA Private Key Generation Process

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.

6.1.1.1 CA Private Key Usage

The private key of the Belgian Government is used to sign issued CA certificates and the certification revocation lists. Other usages are restricted.

6.1.1.2 CA Private Key Type

For the root key the BRCA makes use of the RSA SHA-1 algorithm with a key length of 2048 bits.

The first eID Belgium Root CA private key is certified for validity from 27 January 2003 till 27 January 2014.

6.1.2 CA Key Generation

The BRCA securely generates and protects the private key(s), using a trustworthy system, and takes necessary precautions to prevent the compromise or unauthorised usage of it. The BRCA implements and documents key generation procedures, in line with this CPS. The BRCA acknowledges public, international and European standards on

trustworthy systems. At least three trusted operatives participate in the generation and installation of BRCA private key(s).

The security measures that are in place for key generation of the Sub-CA's are the same as the measures taken for the BRCA.

6.2 Key Pair re-generation and re-installation

When replacing secret key(s) by new ones, the BRCA must use exactly the same procedure as when initially generating key(s). Subsequently and without delay the BRCA must decommission and destroy (a) key(s) used in the past as well as the active tamper-resistant devices and all backup copies of its private key(s) as they become available.

6.2.1 CA Key Generation Devices

The generation of the private key occurs within a secure cryptographic device meeting appropriate requirements including FIPS 140-1 level 3.

6.2.1.1 CA Key Generation Controls

The generation of the private key requires the control of more than one appropriately authorised member of BRCA staff serving in trustworthy positions, and at least one representative of the Belgian Government. More than one member of the BRCA management makes authorisation of key generation in writing.

6.2.2 CA Private Key Storage

The BRCA uses a secure cryptographic device to store the private key meeting the appropriate FIPS 140-1level 3 requirements.

6.2.2.1 CA Key Storage Controls

The storage of the private key of the BRCA requires multiple controls by appropriately authorised members of staff serving in trustworthy positions. More than one member of the BRCA management makes authorisation of key storage and assigned personnel in writing.

6.2.2.2 CA Key Back Up

The private key(s) is/are backed up, stored and recovered by multiple and appropriately authorised members of BRCA staff serving in trustworthy positions. More than one member of the BRCA management make authorisation of key back up and assigned personnel in writing.

A backup of the generated key material is taken and stored under the same security measures as the primary key material.

6.2.2.3 Secret Sharing

The secret shares are held by multiple authorised holders, to safeguard and improve the trustworthiness of private key(s). The BRCA stores the private key(s) in several tamper-resistant devices. At least three members of staff in trusted positions must act concurrently to activate the private key.

Private keys of the Belgian Government may not be escrowed. The BRCA implements internal disaster recovery measures.

6.2.2.4 Acceptance of Secret Shares

Before secret shareholders accept a secret share they must personally have observed the creation, re-creation, and distribution of the share or its subsequent chain of custody.

A secret shareholder receives the secret share within a physical medium, such as a BRCA approved hardware cryptographic module. The BRCA keeps written records of secret share distribution.

6.2.3 CA Private Key Distribution

The BRCA documents the private key distribution. In case token custodians need to be replaced in their role as token custodians the BRCA will keep track of the renewed token distribution.

6.2.4 CA Private Key Destruction

At the end of their lifetime the private keys are destroyed by at least three trusted BRCA staff members at the presence of a representative of the Belgian Government, in order to ensure that these private keys cannot ever be retrieved and used again.

The BRCA keys are destroyed by shredding their primary and backup storage media, by deleting and shred their shares and by deleting, powering off and removing permanently any hardware modules the keys are stored on.

Key destruction process is documented and any associated records are archived.

6.3 Private Key Protection and Cryptographic Module Engineering Controls

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

These devices meet the requirements of FIPS 140-1 Level 3 or higher, which guarantees, amongst other things, that any device tampering is immediately detected and private keys cannot leave devices unencrypted

Hardware and software mechanisms that protect BRCA private keys are documented.

HSMs do not leave the secure environment of the BRCA premises. In case HSMs require maintenance or repair, which cannot be done within BRCA premises, they are securely shipped to their manufacturer. The BRCA private key(s) are not present on HSMs when those are shipped for maintenance outside the BRCA secure premises. Between usage sessions HSMs are kept within the BRCA secure premises (i.e. security perimeter A, B or C).

The BRCA private key remains under *n* out of *m* multi-person control.

The BRCA private key is not escrowed.

At the end of a key generation ceremony, new BRCA keys are burnt encrypted on a (backup key storage) CD-ROM. The BRCA records each step of the key backup process using a specific form for logging information.

The BRCA private key is locally archived within the BRCA premises.

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

The BRCA private key can be destroyed at the end of its lifetime.

6.4 Other Aspects of Key Pair Management

The BRCA archives the Belgian Government's public key(s). The BRCA issues subscriber certificates with validity periods as indicated on such certificates.

6.4.1 Computing resources, software, and/or data corrupted

The BRCA establishes the necessary measures to ensure full and automatic recovery of the service in case of a disaster, corrupted servers, software or data. Any such measures are compliant with the ISO 1-7799 standard.

The BRCA establishes disaster recovery resources sufficiently distant from the primary resources to avoid that a disaster would corrupt resources at both sites. The BRCA establishes sufficiently fast communications between the two sites to ensure data integrity. The BRCA established communications infrastructure from both sites to the RA, the Internet and networks of the Public Administration.

The BRCA takes the necessary measures to test the disaster recovery infrastructure and procedures at least once a year without interruption or degradation of the service.

6.4.2 CA public key revocation

If a Belgian Government public key is revoked the BRCA will immediately:

- Notify all CAs with whom it is cross-certified.
- Notify the RA.
- Notify the public at large through several channels that include:
  - A message on the BRCA website.
  - A press release to the Belgian media.
  - Advertisements in the major Belgian newspapers.
- Update the BRCA CRL.
- Update the certificate status in the Web interface service.
- Revoke all certificates, signed with the revoked certificate.

After assessing the reasons for revocation and taking measures to avoid the cause of revocation in the future, and after obtaining authorization from the RA, the BRCA may:

- Generate a new key pair and associated certificate.
- Re-issue all certificates that were revoked.

6.4.3 Compromise of the CA private key

If the private key of the Belgian Government is compromised, the corresponding certificate should immediately be revoked. The BRCA will additionally take all measures described under 6.4.2.

6.5 Activation Data

The BRCA securely stores and archives activation data associated with the private key and operations.

6.6 Computer Security Controls

The BRCA implements certain computer security controls.

6.7 Life Cycle Security Controls

The BRCA performs periodic development controls and security management controls.

6.8 Network Security Controls

The BRCA maintains a high-level network of systems security including firewalls. Network intrusions are monitored and detected. In specific:

- The Belgian Government website provides for encrypted connections through the Secure Socket Layer (SSL) protocol and anti-virus protection.
- The BRCA network is protected by a managed firewall and intrusion detection system.
- It is prohibited to access sensitive BRCA resources including BRCA databases from outside of the BRCA's own network.
- There are no online connections with any party that allow atomised requests regarding certificate management (including certification requests and revocation requests).

7 CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

The BRCA publishes the certificate profiles it uses in its CPS. Certificates issued by the BRCA comply with IETF RFC 2459 and IETF RFC 3039.

7.1.1 Belgium Root CA Certificates

All fields of type DirectoryString are of type UTF8String.

RootSigned Belgium Root CA					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		Generated by the CA at Key Generation Process Time	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Not after : Key Generation Process Date + 11 years	Fixed
SubjectPublicKeyInfo		X		RSA 2048	
Issuer					
countryName	{ id-at-6 }	X		BE	Fixed
organisationName	{ id-at-10 }	X		GlobalSign nv-sa	Fixed
organisationUnitName	{ id-at-11 }			Root CA	Fixed
commonName	{ id-at-3 }	X		GlobalSign Root CA	Fixed
Subject					
countryName	{ id-at-6 }	X		BE	Fixed
commonName	{ id-at-3 }			Belgium Root CA	Fixed
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		2.16.56.1.1.1	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.eid.belgium.be	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
CertificateSigning				Set	Fixed
crlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE	N/a	

RootSigned Belgium Root CA					
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://secure.globalsign.net/crl/root.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE	N/a	
CA		X		TRUE	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslCA - smimeCA - objectSigningCA	Fixed

SelfSigned Belgium Root CA					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		16 Bytes provided by FedICT	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Not before: Key Generation Process Date	
NotAfter		X		Not after Key Generation Process Date + 11 years	Fixed
SubjectPublicKeyInfo		X		RSA 2048	
Issuer					
countryName	{ id-at-6 }	X		BE	Fixed
commonName	{ id-at-3 }	X		Belgium Root CA	Fixed
Subject					
countryName	{ id-at-6 }	X		BE	Fixed
commonName	{ id-at-3 }			Belgium Root CA	Fixed
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		2.16.56.1.1.1	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.eid.belgium.be	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
CertificateSigning				Set	Fixed
crlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE	N/a	
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
BasicConstraints	{id-ce 19}	X	TRUE	N/a	
CA		X		TRUE	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslCA - smimeCA - objectSigningCA	Fixed

7.1.2 Citizen CA Certificates

All fields of type DirectoryString are of type UTF8String.

Citizen CA					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		16 Bytes provided by FedICT	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 6 years (6 years 8 months)	Fixed
SubjectPublicKeyInfo		X		RSA 2048	
Issuer					
countryName	{ id-at-6 }	X		BE	Fixed
commonName	{ id-at-3 }	X		Belgium Root CA	Fixed
Subject					
countryName	{ id-at-6 }	X		BE	Fixed
commonName	{ id-at-3 }			Citizen CA	Fixed
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		2.16.56.1.1.1.2	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.eid.belgium.be	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
CertificateSigning				Set	Fixed
crlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.eid.belgium.be/belgium.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslCA – smimeCA – ObjectSigning CA	Fixed

7.1.3 Child CA Certificates

All fields of type DirectoryString are of type UTF8String.

Citizen CA					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		16 Bytes provided by FedICT	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 6 years (6 years 8)	Fixed
SubjectPublicKeyInfo		X		RSA 2048	
Issuer					
countryName	{ id-at-6 }	X		BE	Fixed
commonName	{ id-at-3 }	X		Belgium Root CA	Fixed
Subject					
countryName	{ id-at-6 }	X		BE	Fixed
commonName	{ id-at-3 }			Child CA	Fixed
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		2.16.56.1.1.1.5	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.eid.belgium.be	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
CertificateSigning				Set	Fixed
crlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.eid.belgium.be/belgium.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslCA – smimeCA – ObjectSigning CA	Fixed

7.1.4 Foreigner CA Certificates

All fields of type DirectoryString are of type UTF8String.

Citizen CA					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		16 Bytes provided by FedICT	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 6 years (6 years 8months)	Fixed
SubjectPublicKeyInfo		X		RSA 2048	
Issuer					
countryName	{ id-at-6 }	X		BE	Fixed
commonName	{ id-at-3 }	X		Belgium Root CA	Fixed
Subject					
countryName	{ id-at-6 }	X		BE	Fixed
commonName	{ id-at-3 }			Foreigner CA	Fixed
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		2.16.56.1.1.1.7	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.eid.belgium.be	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
CertificateSigning				Set	Fixed
crlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.eid.belgium.be/belgium.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslCA – smimeCA – ObjectSigning CA	Fixed

7.1.5 Government CA Certificates

All fields of type DirectoryString are of type UTF8String.

Government CA					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		To be provided by FedICT – 16 Bytes	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Genenration Process Date/Time	
NotAfter		X		Key Genenration Process Date/Time + 6 years 8 months	Fixed
SubjectPublicKeyInfo		X		RSA 2048	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Belgium Root CA	Fixed
Subject					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }			Government CA	Fixed
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		2.16.56.1.1.1.3	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.pki.belgium.be	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
CertificateSigning				Set	Fixed
crlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.pki.belgium.be/belgium.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslCA – smimeCA – ObjectSigning CA	Fixed

7.1.6 Government AA Certificates

All fields of type DirectoryString are of type UTF8String.

Citizen CA					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		16 Bytes provided by FedICT	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 6 years (6 years 8 months)	Fixed
SubjectPublicKeyInfo		X		RSA 2048	
Issuer					
countryName	{ id-at-6 }	X		BE	Fixed
commonName	{ id-at-3 }	X		Belgium Root CA	Fixed
Subject					
countryName	{ id-at-6 }	X		BE	Fixed
commonName	{ id-at-3 }			Government AA	Fixed
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		2.16.56.1.1.1.6	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.pki.belgium.be	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
CertificateSigning				Set	Fixed
crlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.pki.belgium.be/belgium.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslCA – smimeCA – ObjectSigning CA	Fixed

7.1.7 Administration CA Certificates

All fields of type DirectoryString are of type UTF8String.

Administration CA					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		To be provided by FedICT – 16 Bytes	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Genenration Process Date/Time	
NotAfter		X		Key Genenration Process Date/Time + 6 years 8 Months	Fixed
SubjectPublicKeyInfo		X		RSA 1024	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Belgium Root CA	Fixed
Subject					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }			Administration CA	Fixed
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		2.16.56.1.1.1.1	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.pki.belgium.be	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
CertificateSigning				Set	Fixed
crlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.pki.belgium.be/belgium.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslCA – smimeCA - ObjectSigning CA	Fixed

7.1.8 RRN Sign Certificates

All fields of type DirectoryString are of type UTF8String.

Citizen CA					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		16 Bytes provided by FedICT	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 6 years (6 years 8 months)	Fixed
SubjectPublicKeyInfo		X		RSA 2048	
Issuer					
countryName	{ id-at-6 }	X		BE	Fixed
commonName	{ id-at-3 }	X		RRN	Fixed
OrganizationName	{ id-at-? }	X		RRN	Fixed
Subject					
countryName	{ id-at-6 }	X		BE	Fixed
commonName	{ id-at-3 }			RRN	Fixed
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		2.16.56.1.1.1.4	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.eid.belgium.be	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
CertificateSigning				Set	Fixed
crlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.eid.belgium.be/belgium.crl	Fixed
BasicConstraints	{id-ce 19}	X	TRUE	N/a	
CA		X		TRUE	Fixed
pathLenConstraint		X		0 (Zero)	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslCA – smimeCA – ObjectSigning CA	Fixed

7.2 CRL Profile

In conformance with IETF PKIX RFC 2459 the BRCA supports CRLs compliant with:

- Version numbers supported for CRLs.
- CRL and CRL entry extensions populated and their criticality.

The profile of the Certificate Revocation List is showing in the table below:

Version	v1
Signature Algorithm	sha1RSA
Issuer	<subject CA>
ThisUpdate	<creation time>
NextUpdate	<creation time+configurable value>
RevokedCertificates	
UserCertificate	<certificate serial number>
RevocationDate	<revocation time>

The CA CRL's support the fields and extensions, specified in chapter 5 of RFC 2459: "Internet X.509 Public Key Infrastructure Certificate and CRL profile".

7.3 OCSP Profile

Section not applicable.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENT

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

- The supervising authority for Certification Service Providers in Belgium acting under the authority of the Belgian government.
- A party that acts as a primary contractor together with the BRCA Operator to deliver the certification services and to which the BRCA Operator owes duty.

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

To carry out the audits there will be an independent auditor appointed who will not be affiliated directly or indirectly in any way with the BRCA or any CA nor having any conflicting interests thereof.

The audit addresses the following aspects:

- Compliance of the BRCA operating procedures and principles with the procedures and service levels defined in the CPS.
- Management of the infrastructure that implements CA services.
- Management of the physical site infrastructure.
- Adherence to the CPS.
- Adherence to relevant Belgian laws.
- Asserting agreed service levels.
- Inspection of audit trails, logs, relevant documents etc.
- Cause of any failure to comply with the conditions above.

If irregularities are detected, the BRCA will submit a report to the RA, 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.

9 OTHER 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 Confidentiality of Information

The BRCA observes personal data privacy rules and confidentiality rules as described in this CPS. Confidential information includes:

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

The following items are not confidential information:

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

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

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

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

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

Disclosure Conditions

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

- The status of a single certificate is provided per inquiry by a subscriber or relying party.
- a CA can consult non-confidential information the BRCA holds about it.

Confidential information will not be disclosed by the BRCA to CAs nor relying parties with the exception of information about:

- Themselves.
- Persons in their custody.

Only the RA is permitted to access confidential information.

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

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

- Presenting an authentication certificate at the request of the citizen or relying party
- Signing responses to OCSP requests, CRLs and delta CRLs.

The BRCA encrypts all communications of confidential information including:

- The communications link between the BRCA and the RA.
- Sessions to deliver certificates and certificate status information.

Next to the information retained by the BRCA, information pertaining to the CA certificates can also be retained by the RA.

9.2 Intellectual Property Rights

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

9.3 Representations and Warranties

The BRCA uses this CPS to convey legal conditions of usage of certificates to subscribers and relying parties.

9.3.1 Subscriber Obligations

Unless otherwise stated in this CPS, subscribers are responsible for:

- Having knowledge and, if necessary, seeking training on using digital certificates and PKI.
- Providing correct and accurate information in their communications with the RA.
- Reading, understanding and agreeing with all terms and conditions in this CPS and associated policies published in the Repository.
- Refraining from tampering with a certificate.
- Using certificates for legal and authorised purposes in accordance with this CPS.
- Notifying the RA of any changes in the information submitted.
- Ceasing to use their own certificate if any featured information becomes invalid.
- Ceasing to use their own certificate when it becomes invalid.
- Using a certificate, as it may be reasonable under the circumstances.
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private key.
- Requesting the revocation of a certificate in case of an occurrence that materially affects the integrity of a certificate.

9.3.2 Relying Party Obligations

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

- Have knowledge of the use of digital certificates and PKI.
- Read and accept of the content of this CPS with regard to obligations pertaining to relying parties.
- Validate a certificate by using a CRL, delta CRL or web based certificate validation in accordance with the certificate path validation procedure.
- Trust a certificate only if it has not been suspended or revoked.
- Rely on a certificate, as it may be reasonable under the circumstances.

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

9.3.3 Subscriber Liability Towards Relying Parties

Without limiting other subscriber obligations stated elsewhere in this CPS, subscribers are liable for any misrepresentations they make in certificates to third parties that, reasonably rely on the representations contained therein and have verified one or more digital signatures with the certificate.

9.3.4 CA Repository and Web site Conditions of Use

Parties (including subscribers and relying parties) accessing the BRCA Repository and web site agree with the provisions of this CPS and any other conditions of usage that the BRCA may make available. Parties demonstrate acceptance of the conditions of usage and this CPS by submitting a query with regard to the status of a digital certificate or by

anyway using or relying upon any such information or services provided. Using BRCA Repositories can happen in the form of:

- Obtaining information as a result of the search for a digital certificate.
- Verifying the status of digital signatures created with a private key corresponding to a public key included in a certificate.
- Obtaining information published on the BRCA web site.
- Any other services that the BRCA might make available through its web site.

9.3.4.1 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. Parties acknowledge that they have received adequate information to decide whether to rely upon any information provided in a certificate.

The BRCA makes every effort to ensure that parties accessing its Repositories receive accurate, updated and correct information.

9.3.5 CA Obligations

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

- Comply with this CPS and its amendments as published under http://repository.pki.belgium.be .
- Provide infrastructure and certification services, including the establishment and operation of the BRCA Repository and web site for the operation of public PKI 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.
- Upon receipt of an authenticated request for revocation from the RA to revoke promptly a certificate in accordance with this CPS.
- Revoke certificates issued to the RA upon receipt of a valid and authenticated request to revoke them.
- Publish certificates in accordance with this CPS.
- Publish CRLs of all 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 BRCA Operator contract with the Belgian Government.
- Notify relying parties of certificate revocation by publishing CRLs on the BRCA repository.

- Make a copy of this CPS and applicable policies available through its web site.
- Operate in compliance with the laws of Belgium.
- If the BRCA 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 make best efforts to ensure the proper financial responsibility and liability of such contractor.

The CA is responsible towards subscriber and relying parties for the following acts or omissions:

- Issue digital certificates not listing data as submitted by the RA.
- If a private signing key of the BRCA is compromised.
- Failure to list a revoked certificate in a CRL or delta CRL.
- 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.

To fulfil its tasks as a BRCA, the Belgian Government uses the services of third party subcontractors. Towards the subscribers and relying parties the Belgian Government assumes full responsibility and accountability for acts or omissions of all third party subcontractors it uses to deliver certification services.

9.3.6 Registration Authority Obligations

The RA operating within the BRCA domain will:

- Provide correct and accurate information in their communications with the BRCA.
- Perform all verification and authenticity actions prescribed by the BRCA procedures and this CPS.
- Receive, verify and relay to the BRCA all requests for revocation of a certificate in accordance with the BRCA procedures and the CPS.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of re-key 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 BRCA.

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

9.4 Disclaimers of Warranties

This section includes disclaimers of express warranties.

9.4.1 Limitation for Other Warranties

Within the limits under Belgian Law the BRCA does not warrant:

- The accuracy of any the information contained in certificates except as it is warranted by the RA that is the party responsible for the ultimate correctness and accuracy of all data transmitted to the BRCA with the intention to be included in a certificate.
- The fitness of any certificate for a particular purpose.

9.4.2 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.

9.5 Term and Termination

This CPS remains in force until notice of the opposite is communicated by the BRCA on its repository under http://repository.pki.belgium.be .

Notified changes are appropriately marked by an indicated version. Changes are applicable 30 days after publication.

9.6 Individual notices and communications with participants

Notices related to this CPS can be addressed to: by email to info@fedict.be or by post to attn. Fedict Legal Practices, Rue Marie Thèrèse 1/3, B-1000 Brussels, Belgium.

9.7 Survival

The obligations and restrictions contained under sections 9 and 5.5 survive the termination of this CPS.

9.8 Severability

If any provision of this CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CPS will be interpreted in such manner as to effect the original intention of the parties.

9.9 Amendments

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, and these changes may require corresponding changes to the CPS OID or CPS pointer qualifier (URL).

9.10 Dispute Resolution Procedures

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

9.11 Governing Law

The BRCA provides its services under the provisions of the Belgian law

9.12 Compliance with Applicable Law

The BRCA complies with applicable laws in Belgium. Export of certain types of software used in certain CA public PKI products and services may require the approval of appropriate government authorities. Parties (including BRCA partners, subscribers and relying parties) agree to conform to applicable export laws and regulations as pertaining in Belgium.

9.13 Miscellaneous Provisions

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

- Terms and conditions in this CPS.

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

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

10 LIST OF DEFINITIONS

ACCREDITATION
A formal declaration by an approving authority that a certain function/entity meets specific formal requirements.
ARCHIVE
To store records for period of time for purposes such as security, backup, or audit.
AUDIT
Procedure used to validate compliance with formal criteria or controls.
AUTHENTICATION
A process used to confirm the identity of a person or to prove the integrity of specific information by placing them within the right context and verifying such relationship.
eID
The complete system of the e-ID card. This includes the organisation, infrastructure, procedures, contacts and all necessary resources, pertaining to the e-ID card.
CERTIFICATE
An electronic statement that maps the signature verification data to a physical or moral person and confirms the identity of this person.
CERTIFICATION AUTHORITY OR **CA**
An entity that is trusted to associate a public key to the information on the subject, contained in the certificate by means of signing it with its private key. Unless explicitly specified, the CA described herein is the eID Citizen Operational Certification Authority.
CERTIFICATE PRACTICE STATEMENT OR **CPS**
A statement of the practices in the management of certificates during all life phases.
CERTIFICATE STATUS SERVICE
A service, enabling relying parties and others to verify the status of certificates.
CERTIFICATION SERVICES
Services related to the eID certificate lifecycle. Certification services are public services.
CONTRACT PERIOD
The duration of the CA contract between the Belgian Government and the CA organization.
CERTIFICATE CHAIN
A hierarchical list certificates containing an end-user certificate and CA certificates.
CERTIFICATE EXPIRATION
The end of the validity period of a digital certificate.
CERTIFICATE EXTENSION
A field in the digital certificate used to convey additional information on issues that include: the public key, the certified citizen, the certificate issuer, and/or the certification process.
CERTIFICATE HIERARCHY
A level based sequence of certificates of one (root) CA and subordinate entities that include, CAs and citizens.
CERTIFICATE MANAGEMENT
Actions associated with certificate management include, storage, dissemination, publication, revocation, and suspension of certificates.
CERTIFICATE REVOCATION LIST (CRL)
A list issued and digitally signed by a CA that includes revoked and suspended certificates. Such list is to me consulted by relying parties at all times prior to relying on information featured in a certificate.
CERTIFICATE SERIAL NUMBER
A sequential number that uniquely identifies a certificate within the domain of a CA.
CERTIFICATE ISSUANCE
Delivery of X.509 v3 digital certificates for authentication and digital signature based on personal data and public keys provided by the RA and compliant with the CPS.
CERTIFICATE SUSPENSION
Online service used to temporarily disable a digital certificate and to automatically revoke it if no request for re-activating it is submitted within a certain time period
CERTIFICATE REVOCATION
Online service used to permanently disable a digital certificate before its expiration date
CONFIDENTIALITY
The condition to disclose data to selected and authorised parties only.
VALIDATE A CERTIFICATE CHAIN
To validate a certificate chain in order to validate each certificate in the certificate chain in order to validate an end-user citizen certificate.
DIGITAL SIGNATURE
To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial message has been altered since the transformation was made.
DISTINGUISHED NAME
A set of data that identifies a real-world entity, such as a person in a computer-based context.

DIRECTORY SERVICE
Online publication of certificates allowing the retrieval of a certificate based on its certificate identifier
ELECTRONIC SIGNATURE
Electronic data, attached or logically linked to other electronic data and enabling authentication method.
EUROPEAN DIRECTIVE
The European Directive 1999/93/CE of the European Parliament and the Council of 13 December 1999 "on a community framework for electronic signature.
EID CARD
Electronic identity card as defined in the Royal Decree of XX Month 2003.
GENERATE A KEY PAIR
A trustworthy process to create mathematically (e.g. according to the RSA algorithm) linked private and public keys.
CAPUBLIC CERTIFICATION SERVICES
A digital certification system made available by the CA as well as the entities that belong to the CA domain as described in this CPS.
INCORPORATE BY REFERENCE
To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.
KEY PAIR
A private key and its corresponding public key in asymmetric encryption.
LOCAL REGISTRATION AUTHORITY OR LRA:
An LRA is an entity (organisation) acting upon delegation by an RA to registerapplications for digital certificates. An LRA is trusted to register other entities and assign them a relative distinguished value such as a distinguished name or, a hash of a certificate that is unambiguous within that domain. The role of local RA is fulfilled by the local administration, also known as *communes*. Local administrations register citizen data and personal information on behalf of RRN and they communicate it thereto.
NOTICE
The result of notification to parties involved in receiving CA services in accordance with this CPS.
NORMALISED CERTIFICATE
A Certificate that is used to support any usage but Qualified Electronic Signatures of a cryptographic key pair whose corresponding public key pair is certified. The certified key usage's can be any or any mix of the following usage's: encryption, authentication, non-Qualified signatures, etc.
A Normalised Certificate is issued according to the requirements of the ETSI technical standard TS 102 042.
OBJECT ODENTIFIER (OID)
A sequence of integer components that can be assigned to a registered object and that has the property of being unique among all object identifiers within a specific domain.
ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)
The Online Certificate Status Protocol (RFC 2560) is a real time status information resource used to determine the current status of a digital certificate without requiring CRLs
PKI HIERARCHY
A set of CAs whose functions are organised according to the principle of delegation of authority and related to each other as subordinate and superior CA.
PRIVATE KEY
A mathematical key to create digital signatures and sometimes (depending upon the algorithm) to decrypt messages in combination with the corresponding public key.
PUBLIC KEY
A mathematical key that can be made publicly available that is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys can also be used to encrypt messages or files which can then be decrypted with the corresponding private key.
PUBLIC KEY CRYPTOGRAPHY
Cryptography that uses a key pair of mathematically related cryptographic keys.
PUBLIC KEY INFRASTRUCTURE (PKI)
The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.
QUALIFIED CERTIFICATE
A Certificate that is used exclusively to support electronic signature and that complies to the requirements of Annex I of the European Directive and is delivered by a Certification Service Provider that satisfies to the Annex II of The European Directive, and by referencing the Belgian 09 July 2001 Law, the technical standard ETS TS 101 456, the technical standard ETSI TS 101 862 "Qualified Certificate profile" and the RFC 3039 "Internet X.509 Public Key Infrastructure Qualified Certificate Profile"
REGISTRATION AUTHORITY OR **RA**
An entity that has the responsibility to identify and authenticate citizens. The RA does not issue certificates. Within the CA domain, RRN is the RA.
RELIANCE
To accept a digital signature and act in a way that shows trust in it.
RELYING PARTY
Any entity that relies on a certificate for carrying out any action.
REPOSITORY
A database and/or directory listing digital certificates and other relevant information accessible on-line.

REVOKE A CERTIFICATE
To permanently end the operational period of a certificate from a specified time forward.
ROOT SIGNING
An action by which a hierarchically higher authority conditionally grants its trust status to an authority at a lower hierarchical level. In eID GlobalSign is a root sign authority that allows the eID CA to benefit from the same Trust status in software applications, as GlobalSign's own certificates do.
SECRET SHARE
A portion of a cryptographic secret that has been divided among a number of physical tokens, such as smart cards etc.
SECRET SHARE HOLDER
An person that holds a secret share.
SECRET SHARE ISSUER
A person that creates and distributes secret shares, including a CA.
SIGNATURE
A method that is used or adopted by a document originator to identify himself or herself, which is either accepted by the recipient or its use is customary under the circumstances.
SIGNATORY
A person who creates a digital signature for a message, or a signature for a document.
STATUS VERIFICATION
Online service based e.g. on the Online Certificate Status Protocol (RFC 2560) used to determine the current status of a digital certificate without requiring CRLs. Within eID several status verification mechanisms are made available, including CRLs, delta CRLs, OCSP and web interfaces.
SUBSCRIBER
The person whose identity and public key are certified in an eID certificates.
SUSPENDED CERTIFICATE
Temporarily discarded certificate, which nevertheless is kept on hold for one week until revocation or reactivation notice is given to the CA by RRN.
TRUSTED POSITION
A role within an CA that includes access to or control over cryptographic operations that may allow for privileged access to the issuance, use, suspension, or revocation of certificates, including operations that restrict access to a repository.
TRUSTWORTHY SYSTEM
Computer hardware, software, and procedures that provide an acceptable level against security risks, provide a reasonable level of availability, reliability, and correct operation and enforce a security policy.
X.509
The standard of the ITU-T (International Telecommunications Union-T) for digital certificates.

11 LIST OF ACRONYMS

BRCA:	Belgium Root CA
CA:	Certification Authority
CPS:	Certificate Practise Statement
CRL:	Certificate Revocation List
LRA:	Local Registration Authority
OID:	Object Identifier
OCSP:	Online Certificate Status Protocol
PKI:	Public Key Infrastructure
RA:	Registration Authority