Citizen CA
Certification Practice statement

OID: 2.16.56.1.1.1.2.2
OID: 2.16.56.1.1.1.2.1

Table of Contents

1 INTRODUCTION 5

1.1 PRELIMINARY WARNING 5

1.1.1 Trusted Entities ruled by this CPS 5

1.1.2 Relationships between entities ruled by this CPS 6

1.2 SCOPE OF THIS CPS 6

1.3 THE CERTIFICATES ON THE BELGIAN ELECTRONIC IDENTITY CARD 7

1.4 RELATIONSHIP OF THIS CPS TO OTHER DOCUMENTS 8

1.5 POSITION OF THE "CITIZEN CA" IN THE CA HIERARCHY 9

1.6 DOCUMENT NAME AND IDENTIFICATION 11

1.7 PKI PARTICIPANTS 11

1.7.1 Citizen Certification Authority 11

1.7.2 Root Sign Provider 12

1.7.3 Registration Authorities and Local Registration Authorities 12

1.7.4 Card Personalisator 13

1.7.5 Card Initialisator 13

1.7.6 Subscribers 13

1.7.7 Relying Parties 14

1.8 CERTIFICATE USAGE 14

1.9 POLICY ADMINISTRATION 14

1.10 DEFINITIONS AND ACRONYMS 14

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 15

2.1 ACCESS CONTROL ON REPOSITORIES 15

3 IDENTIFICATION AND AUTHENTICATION 17

3.1 NAMING 17

3.2 INITIAL IDENTITY VALIDATION 17

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 17

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION AND SUSPENSION REQUESTS 17

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 18

4.1 CERTIFICATE APPLICATION 18

4.2 CERTIFICATE APPLICATION PROCESSING 18

4.3 CERTIFICATE ISSUANCE 18

4.4 CERTIFICATE ACCEPTANCE 19

4.5 KEY PAIR AND CERTIFICATE USAGE 19

4.5.1 Citizen duties 19

4.5.2 Relying party duties 19

4.6 CERTIFICATE RENEWAL 20

4.7 CERTIFICATE RE-KEY 20

4.8 CERTIFICATE MODIFICATION 20

4.9 CERTIFICATE REVOCATION AND SUSPENSION 20

4.9.1 Term and Termination of Suspension and Revocation 21

4.10 CERTIFICATE STATUS SERVICES 21

4.11 KEY ESCROW AND RECOVERY 22

5 MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS 23

5.1 PHYSICAL SECURITY CONTROLS 23
5.2 PROCEDURAL CONTROLS 23
5.3 PERSONNEL SECURITY CONTROLS 24
5.3.1 Qualifications, Experience, Clearances 24
5.3.2 Background Checks and Clearance Procedures 24
5.3.3 Training Requirements and Procedures 24
5.3.4 Retraining Period and Retraining Procedures 24
5.3.5 Job Rotation 24
5.3.6 Sanctions against Personnel 25
5.3.7 Controls of independent contractors 25
5.3.8 Documentation for initial training and retraining 25
5.4 AUDIT LOGGING PROCEDURES 25
5.5 RECORDS ARCHIVAL 26
5.5.1 Types of records 26
5.5.2 Retention period 26
5.5.3 Protection of archive 27
5.5.4 Archive backup procedures 27
5.5.5 Requirements for Time-stamping of Records 27
5.5.6 Archive Collection 27
5.5.7 Procedures to obtain and verify archive information 27
5.6 KEY CHANGEOVER 27
5.7 COMPROMISE AND DISASTER RECOVERY 27
5.8 CSP TERMINATION 28
6 TECHNICAL SECURITY CONTROLS 29
6.1 KEY PAIR GENERATION AND INSTALLATION 29
6.1.1 CA Private Key Generation Process 29
6.1.2 CA Key Generation 29
6.2 KEY PAIR RE-GENERATION AND RE-INSTALLATION 30
6.2.1 CA Key Generation Devices 30
6.2.2 CA Private Key Storage 30
6.2.3 CA Private Key Distribution 31
6.2.4 CA Private Key Destruction 31
6.3 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 31
6.4 OTHER ASPECTS OF KEY PAIR MANAGEMENT 31
6.4.1 Computing resources, software, and/or data corrupted 31
6.4.2 CA public key revocation 32
6.4.3 Compromise of the CA private key 32
6.5 ACTIVATION DATA 32
6.6 COMPUTER SECURITY CONTROLS 32
6.7 LIFE CYCLE SECURITY CONTROLS 32
6.8 NETWORK SECURITY CONTROLS 33
7 CERTIFICATE AND CRL PROFILES 34
7.1 CERTIFICATE PROFILE 34
7.1.1 Certificate for identification 34
7.1.2 Certificate for digital signature 35
7.1.3 "Citizen CA" Certificate 37
7.2 CRL PROFILE 38

7.3 OCSP PROFILE 39
8 COMPLIANCE AUDIT AND OTHER ASSESSMENT 41
9 OTHER BUSINESS AND LEGAL MATTERS 42
9.1 FEES 42
9.2 LIABILITY 42
9.2.1 Qualified certificates 42
9.2.2 Certificates that can not be considered as qualified certificates 43
9.3 CONFIDENTIALITY OF INFORMATION 43
9.3.1 Disclosure Conditions 44
9.3.2 Privacy of Personal Information 44
9.3.3 Intellectual Property Rights 44
9.4 REPRESENTATIONS AND WARRANTIES 45
9.4.1 Citizen Obligations 45
9.4.2 Relying Party Obligations 45
9.4.3 Citizen Liability towards Relying Parties 46
9.4.4 CA Repository and Web site Conditions of Use 46
9.4.5 CSP Obligations 46
9.4.6 Service Level Measurement 47
9.4.7 Registration Authority Obligations (applicable to RRN) 48
9.4.8 Card manufacturer (CM) obligations 48
9.5 DISCLAIMERS OF WARRANTIES 48
9.5.1 Exclusion of Certain Elements of Damages 49
9.6 TERM AND TERMINATION 49
9.7 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 49
9.8 SEVERABILITY 49
9.9 AMENDMENTS 49
9.10 DISPUTE RESOLUTION PROCEDURES 49
9.11 GOVERNING LAW 49
9.12 MISCELLANEOUS PROVISIONS 50
10 LIST OF DEFINITIONS 51
11 LIST OF ACRONYMS 56

1 Introduction

1.1 Preliminary warning

This Certification Practice Statement (further abbreviated to "CPS") describes the certification practices applicable to the digital certificates issued for Belgian Electronic Identity Cards by the CSP for "Citizen Certification Authority" (CSP). This CPS must be also considered as the Certificate Policy (CP) for the certificates issued by the "Citizen CA" certificate authority.

1.1.1 Trusted Entities ruled by this CPS

Currently the CSP for "Citizen CA" is the "Société Anonyme CERTIPOST", having its registered offices at 1000 Brussels Centre Monaie, contracted to do this by the Belgian Authorities in quality of the eID project contracting authority, in the following terms:

CERTIPOST assumes the role of Certification Services Provider ("CSP") in the sense of the Law of 9 July 2001 and of the European Directive 1999/93/EC.

In particular, Certipost is responsible of the "Citizen CA" under a "Framework Agreement" dd. 14 November 2002 (Ref. RRN 006/2001) signed between the NV of public law BELGACOM and the Belgian State and transferred by BELGACOM to CERTIPOST on the 1st July 2004 where Certipost is responsible as Trusted Technical agent of the factory issuing certificates under the responsibility of a CSP, under specific SLA.

According to this Framework Agreement CERTIPOST agrees to deliver, to publish and to maintain the identification and the signature certificates for the Belgian Electronic Identity Cards and to provide the trust services related to these certificates such as the publication of Certificate Revocation Lists ("CRLs"), the provision of OCSP ("Online Certificate Status Protocol") services, archival services and services for certificate consultation. In particular, the tasks are limited to the tasks mentioned in lots 2 en 4 of the Bijzonder Bestek RRN 006/2001 and all agreed change requests, with exclusion of post 10 of Lot 2 and post 9 of Lot 4 such as described in the best and final offer accepted by the authorities.

Certipost assumes both the roles of CA and CSP, knowing that the authorities are the CSP responsible for the Belgium Root CA, and bears thus the overall responsibility for the issuing of the certificates.

Next to the CSP, other parties are involved in the project for the Belgian Electronic Identity Cards. The other parties are:

The authorities:

The Registration Authority ("RA") which, on behalf of the CSP, certifies that a given public key belongs to a given entity (for example, a person) by issuing a digital certificate and signing it with its private key. For the Belgian Electronic Identity Card, the "National Register", which is a public administration belonging to the Federal Government Agency of Internal Affairs accomplishes the role of "RA". The National Register delegates most of the actual registration operations to the local population administrative services in the municipalities, so called Local Registration Authorities ("LRA"). On the basis of this process, the RA requests the CA to issue a certificate.

In particular, RA is responsible for (i) the citizens authentication, (ii) the registration of the to be certified data, (iii) the authorization to issue a certificate for a particular citizen, (iv) taking care that citizen's certificates are stored on the correct citizen eID card and (v) taking care that a citizen receives that precise card he is expected to receive and activate the card in

question only when dully attributed to the correct citizen, (vi) the SRA (Suspension and Revocation Authority): the entity who suspends and/or revokes the certificates in the sense of the 09th July 2001 law.

Card Manufacturer:

The Cards Manufacturer ("CM") is the company Zetes, contracted to do this by the Belgian Authorities in quality of the eID project contracting authority, in charge of the production, personalisation, initialisation and distribution of the Belgian Electronic Identity Cards and "cartes de séjours". The CM, who also generates the key pairs, inserts the certificates in these cards. In particular, the tasks are limited to the tasks mentioned in lots1 and 3 of the RRN/006/2001.

1.1.2 Relationships between entities ruled by this CPS

The relationship between CERTIPOST as the "Citizen CA" and the certificate holders, being the Belgian Citizens, is to a large extent governed by the Law of 19 July 1991 regarding the population registers and the identity cards, amended by the law of 25 March 2003, further referred to as "the Law on Identity Cards". CERTIPOST informs the certificate holders of their rights and obligations through a leaflet that is distributed by the municipality.

The CA, RA and CM have agreed that CERTIPOST will assume the role of CSP and bear all responsibility towards the public.

In conformity with the ETSI 101.456 standard supporting the European Directive (Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures) on electronic signature, Certipost assumes the management of its CSP tasks via a PKI management board encompassing all the required expertise.

By its official participation to the weekly eID project progress meetings, where all the above mentioned parties are dully represented, Certipost gathers all necessary information and asks all relevant questions to these parties in order to perform its 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 President, toward the eID Steering Committee lead by the Authorities, will escalate any issue that could not be solved by this process. This Steering Committee has the possibility to call external experts to get second advise and bears dispute settlement responsibility.

1.2 Scope of this CPS

A certification practice statement (CPS) is a unilateral declaration of the practices that a Certification Authority complies with when it provides certification services. A CPS is a comprehensive description of how the CA makes its services available. This CPS should only be used within the CA domain[1]. The CPS aims at delimiting the domain of providing certification services to the citizens and relying parties[2] within the CA domain. This CPS also outlines the relationship between the Certification Authority (CA) and other Certification Authorities within

[1] The CA domain is the area of competence of the CA to provide certification services. This means the CA domain does for instance not include the applications using the certificates, etc.

[2] See paragraph 1.7.7: entities that rely on a certificate

the Belgian Government PKI hierarchy such as the Belgium Root Certificate Authority (BRCA)[3]. It also describes the relationship between the "Citizen CA" and the other organisations involved in the delivery of the certificates for the Belgian Electronic Identity Cards (hereinafter "Citizen Certificates").

This CPS also provides operational guidelines for all citizens and relying parties, including natural or legal persons in Belgium or abroad. This CPS also provides operational guidelines to other Certification Authorities, such as the BRCA, that belong to the PKI hierarchy of the Belgian State within the legal framework for electronic signatures and electronic identity cards in Belgium. Moreover, this CPS describes the relationships between the "Citizen CA" and all other entities playing a role in the context of the Belgian Electronic Identity Card, such as the Card Personalisator or the Card Initialisator. The Belgian State acquires these services through appropriate agreements concluded with these third party suppliers. Finally, in an accreditation and supervisory perspective this CPS provides guidance to supervising authorities, accreditation bodies, accredited auditors etc. with regard to the practices of the "Citizen CA".

This "Citizen CA CPS" endorses and implements the following standards:

- **RFC 2527: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices**
- **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 101 456: Policy requirements for certification authorities issuing qualified certificates.**
- **ETSI TS 101 862: Qualified certificate profile.**
- **ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates (Normalised level only).**
- **The ISO 1-7799 standard like on security and infrastructure.**

The CPS addresses in detail the technical, procedural and organisational policies and practices of the CA with regard to all certification services it provides and during the complete lifetime of certificates issued by the "Citizen CA". Together with this CPS other documents related to the certification process in the context of the Belgian Electronic Identity Card may have to be taken into account. These documents will be available through the CA repository at: http://repository.eid.belgium.be.

This CPS is made available on-line in the Repository of the "Citizen CA" under http://repository.eid.belgium.be.

The "Citizen CA" accepts comments regarding this CPS addressed to: "Citizen CA" p/a CERTIPOST, Centre Monaie, B-1000 Brussels

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 certification services of the "Citizen CA". Such sections are denoted as "Section not applicable". Minor editorial changes of RFC 2527 prescriptions have been inserted in this CPS to better adapt the structure of RFC 2527 to the needs of this application domain.

Further information with regard to this CPS and the "Citizen CA" can be obtained from the "Citizen CA" p/a CERTIPOST, Centre Monaie, B-1000 Brussels.

1.3 The certificates on the Belgian Electronic Identity Card

The Belgian Law of 19 July 1991 regarding the population registers and the identity cards, amended by the law of 25 March 2003, further referred to as "the Law on Identity Cards", introduces the Belgian Electronic Identity Card. This new type of identity card (Electronic Identity Card) is based on a smart card that contains information in graphical format printed on the surface of the card as well as information in electronic format in a chip embedded in the

[3] The BRCA is the CA that has certified the "Citizen CA". Trust in the BRCA, automatically implies an implicit trust in the "Citizen CA".

card. The Law regulates the framework for the issuance and the use of the Electronic Identity Card. This CPS addresses aspects of certification practices within the limits of the Belgian Law. In the accomplishment of its role as a "Citizen CA", CERTIPOST in the first place has to respect the provisions of the law.

In order to allow citizens that are holders of identity cards to authenticate themselves and to sign electronically, the Electronic Identity Cards contain two types of digital certificates:

- **An Identification Certificate: the holder of the Electronic Identity Card can use this certificate to get authenticated in electronic transactions. The authentication certificate contains the identity of the holder and the public key corresponding to the private key, stored on the card for the purpose of an eID user authentication.**
- **A Qualified Certificate for Electronic Signatures (or E-Signatures): this certificate contains the identity of the holder and the public key corresponding to the private key, stored on the card for the purpose of creating an electronic signature only. This certificate is called Qualified Certificate according to the requirements of the European Directive 99/93/EC. The Electronic Signatures Qualified Certificate is compliant with the provisions of the Belgian Electronic Signatures Law.**

State of the art security requirements recommend not using authentication certificates for electronic signing purposes, but instead using a separate qualified certificate for electronic signing purposes. For this reason the Authentication Certificate has not been given the status of a qualified certificate, hence allowing all parties involved to make a clear distinction between the Identification Certificate and the Electronic Signatures Qualified Certificate.

The activation of the certificates on the Electronic Identity Card is optional to the citizen. A citizen can hence choose to "activate" the use of the keys and the certificates on his/her identity card, or not. By activating the certificates on his/her electronic identity card, the citizen enters into a contractual relationship with CERTIPOST in its role of CSP for "Citizen CA".

The technology used for the certification services for these certificates is "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.

The organisation issuing certificates is called Certification Authority (CA), the organisation in charge of the identification of the person applying for a certificate is called the Registration Authority (RA). In this context the role of the issuer of certificates is assumed by the CERTIPOST. The role of the RA is assumed by the RRN[4]. However, in the context of the Belgian Electronic Identity Card, only the RA can request the "Citizen CA" to issue a certificate to a citizen.

The RA does not perform the face-to-face identification of the applicant itself, but delegates this responsibility to Local Registration Authorities (LRAs). In this context the municipalities will act as LRA's. As such the municipalities will be the interface between the applicants, i.e. the citizens and the RA.

1.4 Relationship of this CPS to other documents

As described above, this CPS is a unilateral declaration to the public in general of the practices that the "Citizen CA" complies with when providing certification services. It is a comprehensive description of how the "Citizen CA" makes its services available.

As will be described in more detail further below, the RRN together with the municipalities acts as the RA within the "Citizen CA" domain to the exclusion of any other. Only the RRN and the municipalities may decide upon the issuance of a certificate under this CPS. The RRN may

[4] RRN is the acronym for "Rijksregister-Registre National". The RRN is an administration within the Federal Government Service for Internal Affairs. It is in charge of the management of e.g. the National Register of natural persons.

however appoint one or more third parties to carry out RA tasks within the "Citizen CA" domain.

Only the RRN, the municipalities or the CSP may decide upon the suspension and revocation of a certificate under this CPS.

The relationship between the Belgian State and the "Citizen CA" is regulated in a Framework Agreement. In case of any contradiction between this CPS and the Framework Agreement, priority should be given to the provisions of the Framework Agreement. This CPS does not create additional rights and obligations for the Belgian State, CERTIPOST, ZETES or any other party involved in the issuance and the management of the Belgian Electronic Identity Card. The CPS is primarily intended to further precise the legal and contractual provisions and to inform all interested parties about the practices of the "Citizen CA".

1.5 Position of the "Citizen CA" in the CA Hierarchy

To use the Belgian Electronic Identity Card to its full extent, it is required to ensure both the citizen's identity and the identity of the technical infrastructure e.g. the servers that are needed in Belgian State applications. It is, therefore, required to use multiple types of certificates beyond the Citizen Certificates. The "Citizen CA" belongs to a broader domain of Certification Authorities of the Belgian State. To facilitate the building of trust between the various participating Certification Authorities, the Belgian State has set up a CA hierarchy.

On the top of this hierarchy, there is a "Belgium Root CA (BRCA)" of which the purpose amongst others is to build trust in the various Certification Authorities within the government domain. The (self- signed) BRCA has certified each of the private keys of the Certification Authorities in the government domain including the "Citizen CA". 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 (GLOBALSIGN), whose root has widely been embedded in application software.

The BRCA operates under practices published in a dedicated CPS available at http://repository.eid.belgium.be.

Trust in the Citizen Certificates can be verified as follows:

1. **Trusted path building**

The Citizen Certificate is checked on whether it has been issued by the "Citizen CA". Pursuant to that, the certificate of the "Citizen CA" is checked on whether it has been indeed issued by the BRCA. When the result of these controls is positive trust from the BRCA can be cascaded via the "Citizen CA" certificate to the Citizen Certificate.

Verification of the BRCA certificate.
Generally the BRCA certificate is indicated in the application's certificate store as a trusted certificate. In the unlikely case that an end user is warned that the BRCA certificate is not valid anymore, it is sufficient that the end user removes the BRCA certificate from the certificate store to exclude that domain from its trusted ones to ascertain that this part of the verification fails.

2. **Verification of the "Citizen CA" certificate** can be ascertained by taking the following steps:

- **2.1 Check of the validity of the "Citizen CA" certificate (e.g. check expiration date)**
- **2.2 Check of the status of the "Citizen CA" certificate (e.g. check the suspension or revocation state).**[5]

[5] The status verification services provided by the CA are described in chapter 4.10 Certificate Status Services on page 21.

3. **Verification of the Citizen Certificate can be ascertained by taking the following steps:**

   - **3.1 Check of the validity of the Citizen Certificate (e.g. check expiration date).**
   - **3.2 Check of the status of the Citizen Certificate (e.g. check the suspension or revocation state).**

Generally most or all of these operations are performed automatically by the application that uses the certificates requiring minimal or no end user interaction.

The Trust hierarchy of Citizen Certificates follows the architecture premises below:

1. A small hierarchy for which all the required information to validate the Citizen 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, for online verification. This more complex hierarchy is described in figure 1 below.

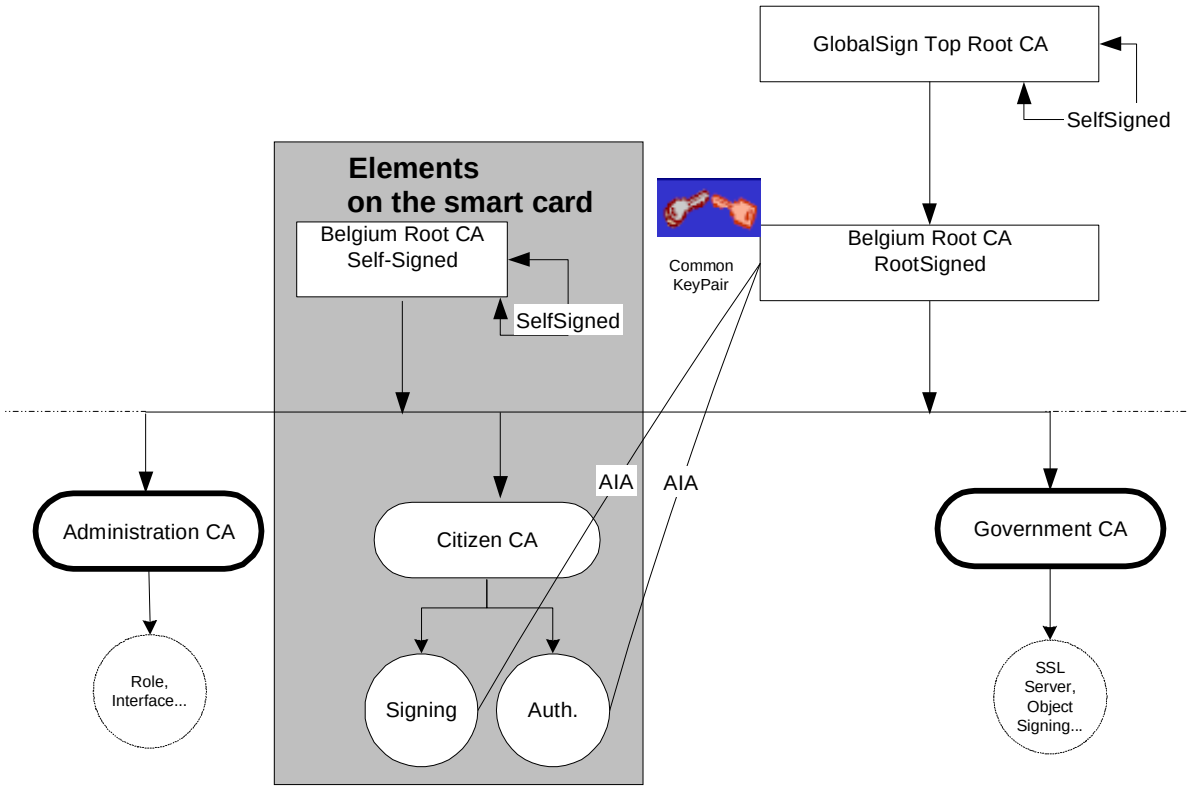

Figure 1: eID hierarchy

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 "Citizen CA" and the Self-Signed Belgium Root CA[6] form a hierarchy, which in an off-line mode allows validating the eID Citizen signing and identification certificates. In this model the 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 Electronic Identity Card, and use it to validate the "Citizen CA" certificate and Citizen Certificates from the card to be validated.

In the three-layered model the "Citizen CA", the Root signed Belgium 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 "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 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.

1.6 Document Name and Identification

This CPS can also be identified by any party through the following OIDs[7]:

- **The OID 2.16.56.1.1.1.2.1 for the electronic signature certificate.**
- **The OID 2.16.56.1.1.1.2.2 for the identification certificate.**

1.7 PKI participants

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

1.7.1 Citizen Certification Authority

A Certification Authority is an organisation that issues digital certificates that are used in the public domain or within a business or transactions context. The "Citizen CA" is a Certification Authority.

The "Citizen CA" operates within a grant of authority for issuing Citizen Certificates. This grant has been provided by the Belgium Root Certification Authority (hereinafter, BRCA).

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

The "Citizen CA", is supervised in application of Article 20 of the Electronic Signatures Law and will be accredited in application of article 17 of the Electronic Signatures Law.

[6] 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.

[7] Object IDentifier

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

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

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

1.7.2 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. The root sign provider of the BRCA is GLOBALSIGN (www.globalsign.com).

1.7.3 Registration Authorities and Local Registration Authorities

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

Only the RRN and the municipalities can decide upon the issuance of a certificate under this CPS. The RRN may appoint a third party to further carry out RA tasks within the "Citizen CA" domain.

Only the RRN, the municipalities or the CSP may decide upon the suspension and revocation of a certificate under this CPS.

Within the domain of the "Citizen CA" the local administrations or municipalities act as sole designated LRAs. The LRAs register and verify citizen data on behalf of the RA. With regard to registration, LRAs have no direct contact with the "Citizen CA".

The RA submits the necessary data for the generation and revocation of the certificates to the "Citizen CA".

The LRAs (the municipalities) directly interact with the citizens to deliver public certification services to the end-user. In specific, the LRAs:

- **Send the citizen the convocation letter to invite the citizen to the proper administration location as required, for example when the citizen's identity card needs replacement;**
- **Follow all procedures required to complete the base document[8]. Subsequently the citizen approves the base document. The LRA then sends the base document data in a secure way to the Card Personalisator so that the certificate request is further processed. The Card Personalisator only issues an identity card following approval of the RA, which is prompted by a request by the Card Personalisator;**
- **Initiate the process to revoke a certificate and request a certificate revocation from the CA via the RA.;**
- **Deliver the issued Electronic Identity Cards to the citizen.**

The RA interacts indirectly with the citizens and directly with the CA to deliver public certification services to the end-user. In specific, the RA:

[8] The base document is used to collect data that is used to issue an identity card. The Minister of Internal Affairs provides the model of this document to the municipalities.

- **Sets up a helpdesk where the holder of the Electronic Identity Card can notify loss, theft or destruction of his Electronic Identity Card when he cannot do this with the municipality or the police. This helpdesk is mentioned hereinafter "the RA Helpdesk";**
- **Register citizens for certification services;**
- **Following approval of an application, request the CA to issue a certificate;**
- **Initiate the process to revoke a certificate and request the CA to revoke or suspend a certificate.**

The RA supplies the "Citizen CA" with the necessary data to enable it to construct the certificates. For each certificate the RA supplies the identity of the holder and the serial number of the requested certificate as well as the public key associated with the citizen to be listed in that certificate.

All communications between the LRA, RA and CA 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.

1.7.4 Card Personalisator

The Card Personalisator customises non-personalised smart cards to personalised Electronic Identity Cards by printing the citizen identity data and photograph on the card. The Card Personalisator is also responsible to send these personalised cards in a secure way to the Card Initialisator. The role of Card Personalisator is currently accomplished by the S.A. ZETES[9] in execution of a Framework Agreement with the Belgian State.

1.7.5 Card Initialisator

The Card Initialisator provides the following services:

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

The role of Card Initialisator is currently accomplished by the S.A. ZETES according to a Framework Agreement with the Belgian State.

1.7.6 Subscribers

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

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

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

The citizens have the right to indicate at the beginning of the Electronic Identity Card application process whether they want to use Citizen Certificates. The Electronic Identity Card is delivered to the citizens with Citizen Certificates loaded. For citizens who do not wish to use the Citizen Certificates, these certificates will be revoked.

1.7.7 Relying Parties

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

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

1.8 Certificate usage

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

The identification certificates issued by the "Citizen CA" can be used for specific electronic authentication transactions that support accessing web sites and other online content, electronic mail etc., as they will be made available by Belgian public authorities. State of the art security requirements recommend not to use identification certificates for electronic signing purposes. The "Citizen CA" therefore declines all liability towards relying parties in all cases where the Identification Certificate is used in the context of applications allowing the use of the Identification Certificate for the generation of electronic signatures.

1.9 Policy Administration

Policy administration is reserved to the "Citizen CA", p/a CERTIPOST, Centre Monaie, B-1000 Brussels

1.10 Definitions and acronyms

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

2 Publication and Repository Responsibilities

The "Citizen CA" publishes information about the digital certificates it issues in (an) online publicly accessible repository(ies) under the Belgian Internet Domain. The CA reserves its right to publish certificate status information on third party repositories.

The "Citizen CA" 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, which will be accessible at http://repository.eid.belgium.be. The CA reserves its right to make available and publish information on its policies by any means it sees fit.

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

The CA publishes CRL's[10] at regular intervals at http://crl.eid.belgium.be. The CA publishes "Delta CRLs" containing any changes since the publication of the previous CRL or Delta CRL, at regular intervals. Any newly published CRL includes all updates of the delta CRL's, published until then.

The CA makes available an OCSP[11] server at *http://ocsp.eid.belgium.be* that provides notice on the status of a certificate, issued by the CA upon request from a relying party, in compliance with IETF RFC 2560. The status of any certificate listed in a CRL or delta CRL, must be consistent with the information, delivered by the OCSP server.

The CA 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 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.

2.1 Access control on repositories

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

The OCSP service, web interface certificate status verification service, the certificate repository and the CRLs and Delta CRLs are publicly available on the CA site on the Internet and are available via the networks of the Belgian Government.

Within the framework of the contract with the Belgian Government, access restrictions to any of these services provided by the "Citizen CA" include:

Through the publicly available interface to the certificate repository, only a single certificate can be delivered per query made by any party except of the RA.

The CA may take reasonable measures to protect against abuse of the OCSP, Web interface status verification and CRL and delta CRL download services. In particular:

The CA may restrict the processing frequency of OCSP requests by a single user to 10 requests per day if the CA can demonstrate that the user is abusing the system. The CA

[10] A CRL or Certificate Revocation List is a list issued and digitally signed by a CA that includes serial number of 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.

[11] 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

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

The CA may restrict the processing frequency of Web interface certificate status verification requests by a single user to 10 requests per day.

3 Identification and Authentication

3.1 Naming

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

3.2 Initial Identity Validation

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

3.3 Identification and Authentication for Re-key Requests

Section not applicable

3.4 Identification and Authentication for Revocation and Suspension Requests

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

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

- **The municipality;**
- **The police;**
- **The helpdesk established by the RA for this purpose.**

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

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

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

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

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

4.1 Certificate Application

The enrolment process for the citizen to request the certificates is an integral part of the Electronic Identity Card process with its municipality, i.e. the LRA. The LRA implements a procedure for citizen enrolment as provided by the RA.

4.2 Certificate Application Processing

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

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

4.3 Certificate Issuance

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

All requests from the RA are granted approval provided that:

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

The CA verifies the identity of the RA on the basis of credentials presented.

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

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

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

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

4.4 Certificate Acceptance

In the presence of the citizen the LRA make the Electronic Identity Card activated in the RA identity database, that citizen identity card until that stage was still in a non activated state. Both the citizen and the RA require the activation data for the card, which has to be supplied by the Card Initialisator in a secure manner. The card can only be activated when using the combined activation data from the RA and the citizen.

It is at the sole discretion of the citizen to choose whether or not to activate his/her Citizen Certificates. Refraining from activating the Citizen Certificates may limit access to certain services provided by the Belgian State as well as other third party providers on the basis of the eID infrastructure in Belgium and abroad.

The certificates activation process requires that an un-suspension request is sent to the CA via the RA. Following activation of the certificates the citizen has to test the Citizen Certificates and validate the Citizen Certificate content. Upon positive validation, the certificate is deemed accepted.

A certificate may be rejected, for inaccurate citizen data, for example.

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

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 Citizen duties

Unless otherwise stated in this CPS, citizen'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 will:

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

4.6 Certificate Renewal

The Citizen Certificates will only be renewed in the case of Electronic Identity Card renewal. As such Citizen Certificate renewal is governed by the same rules as Electronic Identity Card renewal such as described in the applicable laws and royal decrees.

4.7 Certificate Re-key

Section not applicable.

4.8 Certificate Modification

Section not applicable.

4.9 Certificate Revocation and Suspension

Until acceptance or denial by the citizen, Citizen Certificates remain suspended in an Electronic Identity Card. Initial activation of an Citizen Certificate must take place within one month from its issuance. The RA and LRAs act promptly to comply with this requirement.

To request the suspension or revocation of a certificate, a citizen must contact an LRA, the police, or the RA Helpdesk. While an LRA opening hours are limited, the RA helpdesk is available 24 hours per day, 7 days a week.

The police, LRA or RA Helpdesk requests promptly the suspension of a pair of Citizen Certificates via the RA after:

- **Having received notice by the citizen that a suspicion exist that there has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of his Citizen Certificates.**
- **The performance of an obligation of the LRA under this CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, there is a suspicion that another person's information is materially threatened or compromised.**
- **Having received notice by the citizen that there has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of his Citizen Certificates.**
- **There has been a modification of the information contained in a Citizen Certificate.**
- **The performance of an obligation of the RA under this CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, another person's information is materially threatened or compromised.**
- **Upon request from the RA or the CSP the CA suspends or revokes a pair of Citizen Certificates.**
- **The RA revokes a pair of suspended certificates after a period of one week if it does not receive notification from the Citizen to un-suspend the certificate.**
- **Under specific circumstances (e.g. circumvention of a disaster, a CA key comprise, a security breach, ...) , the CSP may request suspension and / or revocation of certificates.**

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

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

The CA grants access to OCSP resources and a web site to which status inquiries can be submitted.

4.9.1 Term and Termination of Suspension and Revocation

Suspension may last for a maximum of seven calendar days in order to establish the conditions that caused the request for suspension. Following negative evidence of such conditions a citizen may request to re-activate (un-suspension of) the Citizen Certificates on the following conditions:

The citizen has ascertained without any doubt that his suspicion that there has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of his Citizen Certificates was incorrect;

No other reasons exist to doubt the reliability and confidentiality of the private keys of both of his Citizen Certificates.

To request the un-suspension of his Citizen Certificates, a citizen must present him self to his/her LRA (his/her municipalities of residence).

The LRA request promptly the un-suspension of a pair of Citizen Certificates via the RA after:

- **Having received notice from the citizen that a suspicion that there has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of his Citizen Certificates was undoubtedly incorrect;**
- **The suspicion has proven undoubtedly incorrect that another person's information would be materially threatened or compromised due to the fact that the performance of an obligation of the RA under this CPS was delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control.**
- **Upon request from the RA, the CA suspends or revokes a pair of Citizen Certificates.**

The CA automatically revokes a suspended certificate after a period of one week if it does not receive in the meantime notification from the RA to un-suspend the certificate. The CA notifies the RA of all revocations made.

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

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. A base CRL of a Delta CRL is updated at least in 14 calendar-day intervals.

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

A CRL is issued each 24 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 Website.

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

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

The OCSP service of the "Citizen CA" is cascaded with the OCSP service of the BRCA.

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

Outside windows maintenance, 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 1.0% of the total number of minutes of that calendar month:

- **OCSP certificate status verification as a result of a request by the RRN, a subscriber or a relying party.**
- **Download of CRL's or ΔCRL's over the Internet or the networks of the government**
- **Web interface certificate status verification service.**

The unavailability of the OCSP service, CRL and ΔCRL 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 ΔCRL's. CRL's and ΔCRL's are archived for a period of at least 30 years after publishing.**

4.11 Key Escrow and Recovery

Key escrow and recovery are not allowed.

5 MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

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

5.1 Physical Security Controls

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

- **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.**
- **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 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.**
- **Power and air conditioning operate with a high degree of redundancy.**
- **Premises are protected from any water exposures.**
- **The CSP 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 CSP implements a partial off-site backup.**

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.

5.2 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.

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

The 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.

For critical CSP functions the CSP implements dual control.

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.**

5.3 Personnel Security 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, Clearances

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;**
- **Any clearances as deemed appropriate.**

5.3.2 Background Checks and Clearance 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 and Procedures

Each CSP party makes available training for their personnel to perform their CSP 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 Job Rotation

Section not applicable.

5.3.6 Sanctions against Personnel

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

5.3.7 Controls of independent contractors

Independent CSP subcontractors and their personnel are subject to the same background checks as the CSP 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.**

5.3.8 Documentation for initial training and retraining

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. The CA implements the following controls:

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

- Issuance of a certificate;
- Revocation of a certificate;
- Suspension of a certificate;
- Automatic revocation;
- 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.

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

Auditing events are not given log notice

5.5 Records Archival

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.

5.5.1 Types of records

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

5.5.2 Retention period

The CSP 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 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 and article 7 of the Law of 12 May 1927. 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 not applicable.

5.5.6 Archive Collection

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

Section not applicable.

5.7 Compromise and Disaster Recovery

In a separate internal document the "Citizen CA" specifies applicable incident, compromise reporting and handling procedures. The CSP specifies the recovery procedures used if 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.

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

All such measures are equivalent to ISO 1-7799.

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 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.

5.8 CSP 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, and to (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

6 TECHNICAL SECURITY CONTROLS

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

6.1 Key Pair Generation and Installation

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

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

6.1.1 CA Private Key Generation Process

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

6.1.1.1 CA Private Key Usage

The private key of the "Citizen CA" is used to sign issued certificates, the certification revocation lists, delta certification revocation list and OCSP certificates. Other usages are restricted.

6.1.1.2 CA Private Key Type

For its root key the CA (Belgium Root CA) makes use of the RSA SHA-1 algorithm with a key length of 2048 bits.

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

For its primary key the "Citizen CA" makes use of the RSA SHA-1 algorithm with a key length of 2048 bits. The first "Citizen CA" private key is certified for validity from 27 January 2003 till 27 June 2009. New "Citizen CA" private keys will be certified for 6 years. A new one will replace the active one before the validity period of the active one becomes less then 5 years.

6.1.2 CA Key Generation

The CA 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. This process is witnessed by government and CSP representatives to ensure confidence of the government in the proper and secure execution of the CA Key Generation procedure. The CA implements and documents key generation procedures, in line with this CPS. The CA acknowledges public, international and European standards on trustworthy systems. At least three trusted operatives participate in the generation and installation of CA private key(s).

6.2 Key Pair re-generation and re-installation

When replacing secret key(s) by new ones, the CA must use exactly the same procedure as when initially generating key(s). Subsequently and without delay the CA 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 of the "Citizen CA" occurs within a secure cryptographic device meeting appropriate requirements including FIPS 140-1 level 3.

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

6.2.2 CA Private Key Storage

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

6.2.2.1 CA Key Storage Controls

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

6.2.2.2 CA Key Back Up

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

6.2.2.3 Secret Sharing

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

Private keys of the CA may not be escrowed. The CA 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 CA approved hardware cryptographic module. The CA keeps written records of secret share distribution.

6.2.3 CA Private Key Distribution

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

6.2.4 CA Private Key Destruction

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

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

The key destruction process is documented and any associated records are archived.

6.3 Private Key Protection and Cryptographic Module Engineering Controls

The CA 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 CA private keys are documented.

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

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

The CA private key is not escrowed.

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

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

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

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

6.4 Other Aspects of Key Pair Management

The CA archives its own public key(s). The CA issues Citizen Certificates with validity periods as indicated on such certificates.

6.4.1 Computing resources, software, and/or data corrupted

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

The CA takes the necessary measures to test the disaster recovery infrastructure and procedures at least once a year.

6.4.2 CA public key revocation

If a "Citizen CA" public key is revoked the CA will immediately:

- Notify all Certification Authorities with whom it is cross-certified.
- Notify the RA.
- Notify the public at large through several channels that include:
- A message on the CA website.
- A press release to the Belgian media.
- Advertisements in the major Belgian newspapers.
- List the certificate of the "Citizen CA" in CRLs and delta CRLs.
- 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 CA 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 CA is compromised, the corresponding certificate should immediately be revoked. The CA will additionally take all measures described under 6.4.2.

6.5 Activation Data

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

6.6 Computer Security Controls

The CA implements certain computer security controls.

6.7 Life Cycle Security Controls

The CA performs periodic development controls and security management controls.

6.8 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, unsuspension and revocation.

The CA website 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.

7 CERTIFICATE AND CRL PROFILES

This section specifies the certificate format, CRL and OCSP formats.

7.1 Certificate Profile

7.1.1 Certificate for identification

The description of the fields for this certificate is contained in the table below. Pseudonyms must not be used in this certificate.

eID citizen Authentication Certificate					
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		Provided by the RRN	Dynamic
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Genenration Process Date/Time	
NotAfter		X		Key Genenration Process Date/Time + 5 years	
SubjectPublicKeyInfo		X		RSA 1024	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Citizen CA	Fixed
Subject			Required		
countryName	{ id-at-6 }		YES	provided by RRN	Dynamic
commonName	{ id-at-3 }		YES	Concatenation of first given name, surname and certificate purpose between brackets	Dynamic
Surname	{ id-at-4 }		YES	provided by RRN	Dynamic
GivenName	{ id-at-42 }		NO	optionally provided by RRN (0, 1 or 2 given names)	Dynamic
serialNumber	{ id-at-5 }		YES	provided by RRN (11 Digits numeric value)	Dynamic
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	

policyIdentifier		X		2.16.56.1.1.1.2.2	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	
digitalSignature				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.eid.belgium.be/eidc0001.crl for the first citizen CA	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslClient - smime	Fixed
Private Extensions	OID	Include	Critical	Value	
AuthorityInfoAccess	{id-pe 1}	X	FALSE		
accessMethod	{ id-ad-2 }	X			
accessLocation		X		http://certs.eid.belgium.be/belgiumrs.crt – Points to RootSigned Governmen top root CA.	
accessMethod	{ id-ad-1 }	X			
accessLocation		X		http://ocsp.eid.belgium.be	

7.1.2 Certificate for digital signature

The description of the fields for this certificate is contained in the table below. Pseudonyms must not be used in this certificate.

eID citizen Signature Certificate					
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		Provided by the RRN	Dynamic
Signature		X		Sha-1WithRSAEncryption	
Validity					

NotBefore		X		Key Genenration Process Date/Time	
NotAfter		X		Key Genenration Process Date/Time + 5 years	
SubjectPublicKeyInfo		X		RSA 1024	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Citizen CA	Fixed
Subject			Required		
countryName	{ id-at-6 }		YES	provided by RRN	Dynamic
commonName	{ id-at-3 }		YES	Concatenation of first given name, surname and certificate purpose between brackets	Dynamic
Surname	{ id-at-4 }		YES	provided by RRN	Dynamic
GivenName	{ id-at-42 }		NO	optionally provided by RRN (0, 1 or 2 given names)	Dynamic
serialNumber	{ id-at-5 }		YES	provided by RRN (11 Digits numeric value)	Dynamic
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		2.16.56.1.1.1.2.1	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://repository.eid.belgium.be	Fixed
Qualified Certificate Statement					
qcStatement	{ id-etsi-qcs 1 }	X			
KeyUsage	{id-ce 15}	X	TRUE	N/a	
nonRepudiation				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://crl.eid.belgium.be/eidc0001.crl for the first citizen CA	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sMime	Fixed
Private Extensions	OID	Include	Critical	Value	
AuthorityInfoAccess	{id-pe 1}	X	FALSE		
accessMethod	{ id-ad-2 }	X			
accessLocation		X		http://certs.eid.belgium.be/belgiumrs.crt – Points to RootSigned Governmen top root CA.	

accessMethod	{ id-ad-1 }	X			
accessLocation		X		http://ocsp.eid.belgium.be	

7.1.3 "Citizen CA" Certificate

This certificate is issued by the BRCA to identify the CA by using a digital certificate. The description of the fields for this certificate is contained in the table below.

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/Time	
NotAfter		X		Key Generation Process Date/Time + 6 years (6 years 5 months for the first certificate) **Key Generation Process Date + 6 years, 8 months (for certificates issued after December 2003)**	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

7.2 CRL Profile

In conformance with IETF PKIX RFC 2459 the CA 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	**v2**
Signature	**sha1RSA**
Issuer	**<subject CA>**
ThisUpdate	**<creation time>**
NextUpdate	**<creation time+7 days >**
RevokedCertificates	
UserCertificate	**<certificate serial number>**
RevocationDate	**<revocation time>**
CrlEntryExtensions	
CRL Reason Code	**Certificate Hold(6) (for suspended certificates)** **Note: Otherwise NOT included!**
CrlExtensions	
Authority Key Identifier	**non-critical <subject key identifier CA>**
CRL Number	**non-critical <CA assigned unique number>**

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

Version	**v2**
signature	**sha1RSA**
Issuer	**<subject CA>**

thisUpdate	**<creation time>**
nextUpdate	**<creation time+7 days >**
RevokedCertificates	
userCertificate	**<certificate serial number>**
revocationDate	**<revocation time>**
crlEntryExtensions	
CRL Reason Code	**Certificate Hold(6) (for suspended certificates)** **removeFromCrl(8) (to unsuspend certificates)** **Note: Otherwise NOT included!**
crlExtensions	
Authority Key Identifier	**non-critical <subject key identifier CA>**
CRL Number	**non-critical <CA assigned unique number>**
Delta CRL Indicator	**<base CRL Number>**

The CA CRL's and delta 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

The OCSP profile follows IETF PKIX RFC2560 OCSP v1. No OCSP extensions are supported. The CA supports multiple certificate status requests in one OCSP request as long as they are signed by the same CA. The OCSP response is signed by a CA cross-certified OCSP root.

This certificate is issued by the Belgian Government's root CA to certify the OCSP responders. The description of the fields for this certificate is contained in the table below.

Belgium OCSP Responder					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		Generated by the CA at Key Generation Process Time	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Genenration Process Date/Time	
NotAfter		X		Key Genenration Process Date/Time + 1 Year Key Generation Process Date + 2 years, 2 months **(for certificates issued after December 2003)**	Fixed
SubjectPublicKeyInfo		X		RSA 2048	

Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		[Issuing CA]	Fixed
Subject					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }			Belgium OCSP Responder	Fixed
Standard Extensions	OID	Include	Critical	Value	
KeyUsage	{id-ce 15}	X	TRUE	N/a	
DigitalSignature				Set	Fixed
enhancedKeyUsage			FALSE		
ocspSigning	1.3.6.1.5.5.7.3.9	X			
authorityKeyIdentifier	{id-ce 35}	X	FALSE	N/a	
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
ocspNoCheck	{ id-pkix-ocsp 5 } 1.3.6.1.5.5.7.48.1.5		FALSE		
Null		X			

8 COMPLIANCE AUDIT AND OTHER ASSESSMENT

With regard to the Qualified Certificate for electronic signature, the CSP operates following the terms of the Law of 9 July 2001 that lays out the legal framework of electronic signatures in Belgium. The CSP meets the requirements set out in ETSI policy documents referring to qualified certificates, including:

- **TS 101 456 Policy requirements for certification authorities issuing qualified certificates;**
- **TS 101 862 Qualified certificate profile.**

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

- **TS 102 042 Policy requirements for certification authorities issuing public key certificates (Normalised level).**

The CSP accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CPS. The CSP 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.**
- **The Belgian government or a third party appointed by the Belgian government.**

The CSP 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 CA or any CA nor having any conflicting interests thereof.

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;**
- **Cause of any failure to comply with the conditions above.**

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.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

The Law on Identity Cards rules the fee due by the citizen for the certificates on his Electronic Identity Card.

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

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

- **Publication of certificates;**
- **Revocation of certificates;**
- **Suspension of certificates;**
- **Publication of CRLs and Delta CRLs.**

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.**

By means of dedicated procedures the CA makes available to each individual user free of charge the following services as they may be requested:

Service	Free of charge
OCSP status verification services	10 requests per user per day
Download of CRL	1 download per user per week
Download of a delta CRL	8 downloads per user per day
Certificate directory service	30 downloads per week
Certification Practice Statement	2 downloads per user per day

The CA implements mechanisms to protect these services from abuse. Accessing in excess of the above stated limits may be subject to a fee invoiced directly to the user by the CA within the framework of the CA contract with the Belgian Government.

9.2 Liability

The liability of the CSP towards the subscriber or a relying party is limited to paying damages amounting to 2500 € per transaction, affected by the events listed in the section 9.2.1.

9.2.1 Qualified certificates

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

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

(a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;

(b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the private key corresponding to the public key given or identified in the certificate;

(c) for assurance that the private key and the public key can be used in a complementary manner;

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

9.2.2 Certificates that can not be considered as qualified certificates

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

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

9.3 Confidentiality of Information

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

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

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

The following items are not confidential information:

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

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

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

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

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

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

9.3.1 Disclosure Conditions

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

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

Confidential information 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.

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

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

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

The CSP encrypts all communications of confidential information including:

- **The communications link between the CA 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 National Register Law rules the access to the Registry of Identity cards and other data on the citizens owned by the RRN.

9.3.2 Privacy of Personal 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 95/46/EC On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data. The CSP also acknowledges Directive 2002/58/EC 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 on 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.

9.3.3 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.

9.4 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.

9.4.1 Citizen Obligations

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

- **Refraining from tampering with a certificate.**
- **Only using certificates for legal and authorised purposes in accordance with the CPS.**
- **Applying for a new Electronic Identity Card (and thus Citizen Certificates) in case of any changes in the information published in the certificate;**
- **Refraining from using the citizen's public key in an issued Citizen Certificate to have other certificates issued;**
- **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;**
- **Notify the police, the municipality or the RA Helpdesk to request the suspension of a certificate in case of the suspicion of an occurrence that materially affects the integrity of a certificate. Such occurrences include indications of loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of the Citizen Certificates;**
- **Notify the police, the municipality or the RA Helpdesk to request the revocation of a certificate in case of an occurrence that materially affects the integrity of a certificate. Such occurrences include loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of the Citizen Certificates, or in case control over private keys has been lost due to compromise of activation data (e.g. PIN code).**
- **Obligation to use the key pair for electronic signature and in accordance with any other limitations notified to the subscriber;**
- **Obligation to exercise reasonable care to avoid unauthorised use of the subscriber's private key;**
- **Following compromise, the obligation to immediately and permanently discontinue the use of the subject's private key.**
- **obligation to use the key pair for electronic signature and in accordance with any other limitations notified to the subscriber;**
- **obligation to exercise reasonable care to avoid unauthorised use of the subscriber's private key;**
- **obligation to only use the private key for signing with the secure user**
- **the obligation to notify without any reasonable delay in case control over the private key has been lost due to compromise of activation data (e.g. PIN code)**
- **following compromise, the obligation to immediately and permanently discontinue the use of the subject's private key.**

9.4.2 Relying Party Obligations

A party relying on a CA certificate will:

- **Be sufficiently informed about the use of digital certificates and PKI;**

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

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

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

9.4.3 Citizen Liability towards Relying Parties

A citizen who holds an Electronic Identity Card with activated keys for authentication and signatures is liable towards relying parties for any use that is made of this card, including the keys and the certificates, unless he can prove that his key has been compromised and that he has taken all the necessary measures for a timely revocation of his certificates.

9.4.4 CA Repository and Web site Conditions of Use

Parties, including citizens and relying parties, accessing the CA Repository and web site agree with the provisions of this CPS and any other conditions of usage. Citizens and relying 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 CA 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 CA web site;**
- **Any other services that the CA might advertise or provide through its web site.**

9.4.4.1 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.

9.4.4.2 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 9.2.

9.4.5 CSP Obligations

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 Directive 99/93/EC on a Community framework for electronic signatures.**

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

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

- **Issue digital certificates not listing data as submitted by the RA;**
- **If a private signing key of the CA is compromised;**
- **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 9.2**

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

9.4.6 Service Level Measurement

Belgian Government together with its eID partners enforce controls to ensure compliance of eID related services with Service Level Agreements defined in this CPS.

9.4.7 Registration Authority Obligations (applicable to RRN)

The RA operating within the CA domain will:

- **Provide correct and accurate information in their communications 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 RRN acts as the sole RA in the CA domain, having the right, nevertheless to sub-delegate registration to LRAs, like the municipalities.

The RA has sole responsibility for the directories it maintains including certificate directories.

The RA is responsible for all audits it makes, the results and recommendations of audits thereof.

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

The RA complies with Belgian laws and regulations pertaining to the functioning of RRN.

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

9.4.8 Card manufacturer (CM) obligations

The card manufacturer (CM) is responsible for the initialisation, for the personalisation and for the distribution of the electronic identity card containing the 2 citizen's certificates.

This initialisation lists the following operation on the smart card:

- **Generation of the 2 key pairs for the identification and signature certificate**
- **Storage of the identification data, of the identification and signature certificates on the smart card**
- **Data authentication, initialisation of the different files stored on the digital identity card**

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

CM will implement a secure process to get back and to destroy from municipalities the non-valid or cancelled identity card

9.5 Disclaimers of Warranties

This section includes disclaimers of express warranties.

9.5.1 Exclusion of Certain Elements of Damages

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

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

9.6 Term and Termination

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

Notified changes are appropriately marked by an indicated version

9.7 Individual notices and communications with participants

Notices related to this CPS can be addressed to the "Citizen CA" p/a CERTIPOST, Centre Monaie, B-1000 Brussels.

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 CA. Major changes that may materially change the acceptability of certificates for specific purposes may require corresponding changes to the CPS OID or CPS pointer qualifier (URL).

9.10 Dispute Resolution Procedures

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

9.11 Governing Law

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

9.12 Miscellaneous Provisions

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

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

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

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.

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 Citizen Certification Authority.

CERTIFICATE POLICY OR CP
A named set of rules that indicate the applicability of a Certificate to a particular community and/or class of application with common security requirements.

CERTIFICATE PRACTICE STATEMENT OR CPS
A statement of the practices in the management of certificates during all life phases.

CERTIFICATE STATUS SERVICE
Service enabling relying parties and others to verify the status of certificates.

CERTIFICATION SERVICES
Services related to the Citizen Certificate lifecycle. Certification services are public services.

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, Certification Authorities 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 identification 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.

CERTIFICATE CHAIN VALIDATION
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.

EID
The complete system of the eID card including the organisation, infrastructure, procedures, contacts and all necessary resources, pertaining to the eID card.

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.

GENERATE A KEY PAIR
A trustworthy process to create mathematically (e.g. according to the RSA algorithm) linked private and public keys.

CA PUBLIC 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 register applications 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.

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 Certification Authorities 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 the context of the Belgian Electronic Identity Card 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 controls the signature creation device used to generate a digital signature.

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 Citizen 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**
CM	**Card Manufacturer**
CPS	**Certificate Practise Statement**
CP	**Certificate Policy**
CRL	**Certificate Revocation List**
HSM	**Hardware Security Module**
LRA	**Local Registration Authority**
OID	**Object Identifier**
OCSP	**Online Certificate Status Protocol**
PKI	**Public Key Infrastructure**
RA	**Registration Authority**
SRA	**Suspension and Revocation Authority**
OID	**Object Identifier**
URL	**Uniform Resource Locator**
PIN	**Personal Identification Number**
PUK	**Personal Unblocking Key**