

**FEDICT**  
Federale Overheidsdienst Binnenlandse Zaken  
Service Public Fédéral Intérieur

**eID Hierarchy and Certificate Profiles**

23 May 2003

Ref: EID-DEL-004 – V 2.0

# Table of Contents

1.	EXECUTIVE SUMMARY.....	4
2.	GENERAL INFORMATION .....	5
2.1.	DOCUMENT CHANGE CONTROL .....	5
2.2.	INTRODUCTION .....	5
2.3.	HOW THIS DOCUMENT IS ORGANIZED .....	5
3.	REFERENCES .....	6
4.	STRUCTURE AND ORGANISATION.....	7
4.1.	STRUCTURE .....	7
4.2.	ORGANISATION .....	8
5.	SIGNATURE ALGORITHM .....	8
5.1.	KEY PAIRS.....	8
5.2.	HASHING ALGORITHM.....	8
6.	CERTIFICATE PROFILES.....	8
6.1.	VERSION .....	8
6.2.	CERTIFICATES SERIAL NUMBER.....	9
6.3.	SIGNATURE .....	9
6.4.	ISSUER .....	10
6.5.	VALIDITY .....	10
6.6.	SUBJECT.....	11
6.7.	SUBJECT PUBLIC KEY INFO.....	12
6.8.	KEY USAGE EXTENSION .....	12
6.9.	AUTHORITY AND SUBJECT KEY IDENTIFIERS .....	13
6.10.	NETSCAPECERTTYPE .....	13
6.11.	POLICY MAPPING.....	14
6.12.	POLICY CONSTRAINT .....	14
6.13.	CERTIFICATE POLICIES.....	14
6.14.	BASIC CONSTRAINT .....	15
6.15.	CRL DISTRIBUTION POINT.....	15
6.16.	FRESHEST CRL - DELTA CRL DISTRIBUTION POINT .....	15
6.17.	AUTHORITY INFORMATION ACCESS.....	16
6.18.	SUBJECT DIRECTORY ATTRIBUTES .....	16
7.	QUALIFIED CERTIFICATE STATEMENT .....	17
8.	OCSP CERTIFICATE.....	17
9.	CRL PROFILES.....	17
9.1.	CRL PROFILE.....	17
9.2.	Δ CRL PROFILE.....	18

10. LDAP SCHEME ..... 19

11. RECAPITULATIVE TABLES ..... 20

## 1. Executive Summary

A dedicated PKI infrastructure will be implemented in order to provide the necessary keys and certificates lifecycle management for the eID project.

The eID hierarchy has three levels. The first level is the Belgium Root CA; the second level contains the eID operation CAs (including the citizen CA), while the third level concerns the end entities (citizens).

This document is a part of the specification reports and aims to describe the profiles of certificates that will be used within this project. Two kinds of certificates will be used: CA certificates and citizen certificates. All certificates are formatted according to version 3 of the X509 recommendation. The CRL profile as well as the OCSP profile are following also the international standards.

## 2. General information

### 2.1. Document change control

Last revised version: V 2.0

Last revision date: 23/05/2003

Final author: Stefan Wijnen

### 2.2. Introduction

This document is a part of the functional specification report, and aims to describe the trust products of eID project. The trust products are made of Certificates, CRLs, LDAP and OCSP.

This document is part of a set of documents technically describing the whole eID CA services environment. This set of documents consists of:

- § EID-DEL-004: eID Hierarchy and Certificate Profiles
- § EID-DEL-006: Component Overview
- § EID-DEL-008: Technical Analysis Customer Interface
- § EID-DEL-010: Functional Analysis Customer Services

All these documents together are reflecting the status of the implemented system at the time the documents are created or updated (snapshot of the system).

As the eID project is still in a pilot phase, the current document will continue to evolve without prior notice.

### 2.3. How this document is organized

This document is structured as follows:

Chapter 4 gives an overview of the trust hierarchy used.

Chapter 5 specifies the used cryptographic algorithms.

Chapter 6 describes in detail the profile of the different certificates involved in the eID project.

Chapter 7 will define the Qualified Certificate Statement used to fulfil the ETSI requirements.

Chapter 8 gives a description of the OCSP certificate used.

Chapter 9 defines the used CRL and Delta CRL profile.

Chapter 10 represents the used LDAP scheme in the eID context.

Chapter 11 is a detailed summary of all the certificate profiles used in the eID project.

### 3. References

The following documents should be considered as reference for this document:

- § 'EIK Lot 2 & 4 – Aanvraag voor BAFO' including the 'Raamovereenkomst ref. Nr. RRN 006/2001'
- § 'Verslag Onderhandelingsessie FEDICT-Ubizen op 8 Augustus 2002 14.00' deposited by Ubizen with FEDICT conform point 3 Beschrijving Technische Oplossing in 'EIK Lot 2 & 4 – Aanvraag voor BAFO'
- § 'Bijzonder Bestek' RRN/006/2001: main document.
- § 'Responses to Questions Réponses\_29920515'.
- § 'Requirements for Certification Practices Statement for eID': as per 'Bijzonder Bestek' B.2.1 Lot 2 and Lot 4 – delivery of the trust services associated with the delivery, publication and maintenance of authentication- and signature certificates together with the associated trust services.
- § Government and Administration CAs certificate profiles

Some constraints are taken into account imposed by a number of change request specifications or compatibility related issues towards the industry standards and initial specifications, including:

- § Internet X.509 Certificate and CRL Profile specification, also known as RFC 2459.
- § Internet X 509 Qualified certificates, also known as RFC 3039.
- § X.509 Internet Public Key Infrastructure Online Certificate Status Protocol, also known as RFC 2560.

Besides this technical document describing the eID Hierarchy and the certificates/CRL profiles, the reader should be aware that other documents exists describing certain topics of the eID project:

- § EID-DEL-006: Component Overview
- § EID-DEL-008: Technical Analysis Customer Interface
- § EID-DEL-010: Functional Analysis Customer Services
- § R&S-DEL-005: Role and Server Certificate Profiles

## 4. Structure and organisation

### 4.1. Structure

The eID hierarchy is a hybrid hierarchy that consists of a combination of 2 and 3 layer models. The hierarchy that will be present on the smartcard consists of 2 levels, A Self-Signed Belgium Root CA and an operational Citizen CA certificate. The extensions present in the end user certificate profile will allow another hierarchy to be reconstructed up to a trusted root that is present in common browsers (3-Level hierarchy).

Figure 1 details this structure.

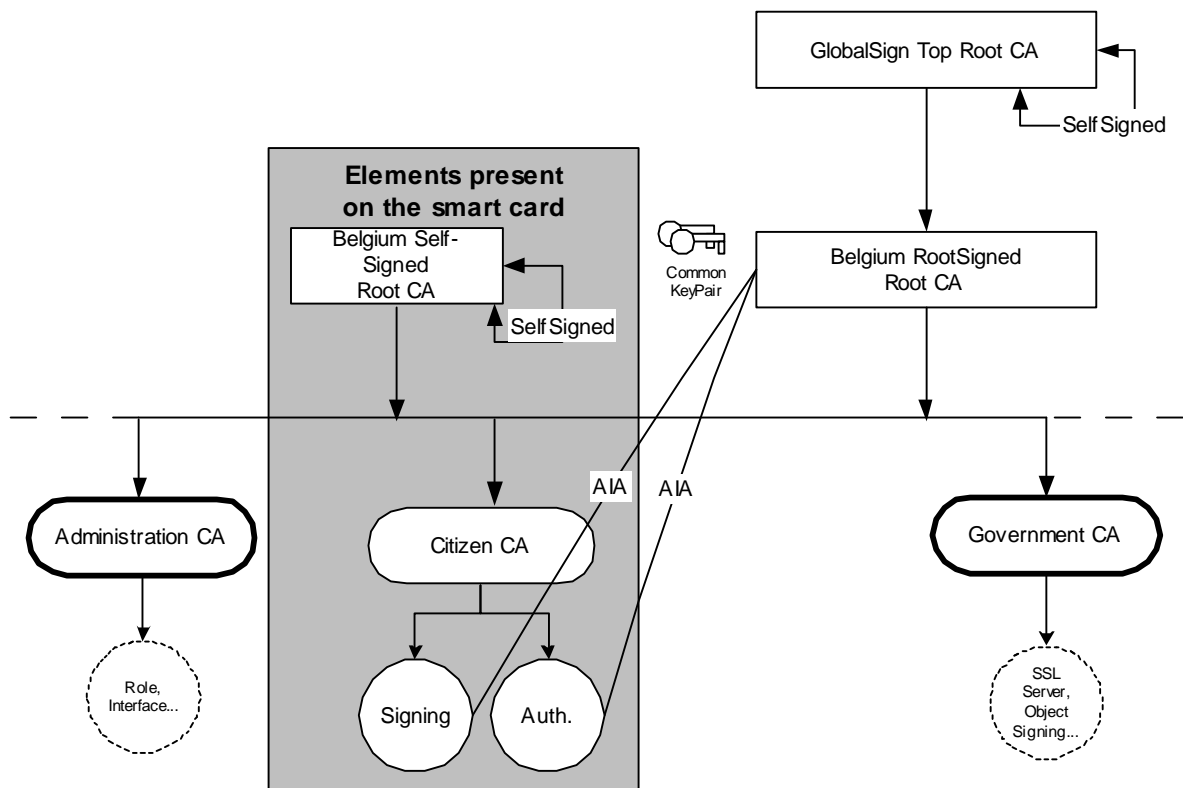


Figure 1: eID Architecture

## 4.2. Organisation

The Belgium Root CA is the entity designated by Government as primary CA to manage the other eID CAs.

The Belgium Root CA is root signed by the GlobalSign Top Root under the terms of a RootSigning™ contract. The CA operator will manage the Belgium Root CA and eID CA key pairs and associated certificate in compliance with the Key Management Policy. Belgium Root CA, Citizen CA and citizen certificates are ruled by the different "eID" CPS-documents (<http://repository.eid.belgium.be>).

## 5. Signature algorithm

### 5.1. Key pairs

The key pairs in this hierarchy will be generated using the RSA cryptographic algorithm. The length of the Belgium Root CA and Citizen CA certificates key pairs are 2048 bits. The citizen certificates key pairs size are 1024 bit. The lifetime of keys is specified as the period of validity of certificates associated to the keys.

### 5.2. Hashing algorithm

The hashing algorithm used is SHA-1 (Secure Hash Algorithm)

## 6. Certificate profiles

The different CAs are profiled according to PKIX certificate profile, and made up of three parts according to RFC 2459: tbsCertificate, Signature algorithm and Signature value.

Note: All the URI's specified in the certificate profiles are resolved by FedICT.

### 6.1. Version

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

Version		
Belgium Root CA certificate	Citizen CA certificate	Citizen certificates

Version 3 – Value = "2"	Version 3 – Value = "2"	Version 3 – Value = "2"
-------------------------	-------------------------	-------------------------

## 6.2. Certificates Serial Number

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

The RRN<sup>1</sup> will assign a serial number to the Self-Signed Belgium Root CA and the Citizen CA. The citizen certificates serial number will be assigned by the RRN. The CA operator will have to check the uniqueness of end-user certificate serial numbers before processing the certification requests.

The CA operator will create the serial number for the RootSigned Belgium Root CA certificate. All serial numbers are maximal 16 bytes long.

Serial Number			
Belgium Root CA RootSigned certificate	Belgium Root Self-Signed CA certificate	Citizen CA certificate	Citizen certificates
Generated by the CA at the time of Key Generation Process	Provided by the RRN	Provided by the RRN	Assigned by RRN in the XKMS / X-BULK requests.

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

## 6.3. Signature

The signature field determines the cryptographic algorithm used by a CA to sign a certificate. The algorithm identifier, which is a number registered with an internationally recognised standards organisation, specifies both the public-key algorithm and the hashing algorithm used by the CA to sign certificates. The Object Identifier for RSAwithSHA1 is 1.2.840.113549.1.1.5.

Signature		
Belgium Root CA certificate	Citizen CA certificate	Citizen certificates
RSAwithSHA1	RSAwithSHA1	RSAwithSHA1

<sup>1</sup> RRN is an acronym for Rijksregister – Registre National

## 6.4. Issuer

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

Issuer			
Belgium Root CA RootSigned certificate	Belgium Root CA SelfSigned certificate	Citizen CA certificate	Citizen certificates
CN = GlobalSign Root CA OU = Root CA O = GlobalSign nv-sa C = BE	CN: Belgium Root CA C: BE	CN: Belgium Root CA C: BE	CN: Citizen CA C: BE

## 6.5. Validity

The validity field indicates the time interval during which the citizen can use the certificate and over which the issuing CA maintains certificate status information.

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

Validity		
Belgium Root CA certificate	Citizen CA certificate	Citizen certificates
NotBefore: 26/01/2003 23:00:00 (UTC Time) NotAfter: 26/01/2014 23:00:00 (UTC Time)	NotBefore: 27/01/2003 00:00:00 (UTC Time). NotAfter: 26/06/2009 23:00:00 (UTC Time)	NotBefore: Certificate issuance date and time in UTCTime. NotAfter: issuing UTCTime + 5 years.

The FIRST eID operational certificate generated has a validity extended to 6 years and 5 months in order to avoid unnecessary additional Key Ceremonies.

## 6.6. Subject

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

Subject		
Belgium Root CA certificate	Citizen CA certificate	Citizen certificates
countryName: BE commonName: Belgium Root CA	countryName: BE commonName: Citizen CA	countryName (Dynamic) commonName (Dynamic) surname (Dynamic) givenName (Dynamic) subjectSerialNumber (Dynamic)

The common name of each Citizen certificate must be formatted as follows:

Field	Length	Description	Example
C ( <i>countryName</i> )	2	countryName is the country of issuance of the certificate. It has thus always "BE" as value. However as it is a dynamic element not checked by the CA, the country code within the request may be changed by the RRN.	C=BE
CN ( <i>commonName</i> )	Max 255 Min 1	Concatenation of <ul style="list-style-type: none"> <li>- &lt;given name&gt;: first given name of the citizen</li> <li>- &lt;surname&gt;: surname of the citizen</li> <li>- (&lt;purpose&gt;): (Authentication) or (Signature)</li> </ul>	CN=John Smith (Authentication)
surname	Max 255 Min 1	Surname of the citizen	S=Smith

givenName	Max 255  Min 1	1 or 2 given names of the citizen (This field may not appear in case the citizen has no given name)	G=John William
subjectSerialNumber	Max 255  Min 1	This is a unique number for each citizen provided by the RRN (so called "Rijksregisternummer" – 11 digits long).	SN=12345678901

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

## 6.7. Subject Public Key Info

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

Subject Public Key Info		
Belgium Root CA certificate	Citizen CA certificate	Citizen certificates
RSA 2048 bits public key	RSA 2048 bits public key	RSA 1024 bits public key

## 6.8. Key usage extension

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

Key usage extension				
Key usage components	Belgium Root CA certificate	Citizen CA certificate	Citizen certificates	
			Authentication	Signature
digitalSignature	not asserted	not asserted	asserted	not asserted
nonRepudiation	not asserted	not asserted	not asserted	asserted
keyEncipherment	not asserted	not asserted	not asserted	not asserted
dataEncipherment	not asserted	not asserted	not asserted	not asserted
keyAgreement	not asserted	not asserted	not asserted	not asserted
keyCertificateSigning	asserted	asserted	not asserted	not asserted

crSigning	asserted	asserted	not asserted	not asserted
encipherOnly	not asserted	not asserted	not asserted	not asserted
decipherOnly	not asserted	not asserted	not asserted	not asserted

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

## 6.9. Authority and Subject Key Identifiers

The Authority Key Identifier extension will be present in the end user certificates, the eID operational CA certificate(s) and the Belgium Root CA certificates (Self-Signed and RootSigned).

The Subject Key Identifier will be present in the Citizen CA certificate(s) and the Belgium Root CA certificates (Self-Signed and RootSigned). It will not be present in end-user certificates.

## 6.10. NetscapeCertType

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

NetscapeCertType Key usage extension				
Netscape Key usage	Belgium Root CA certificate	Citizen CA certificate	Citizen certificates	
			Authentication	Signature
bit-0 - SSL client	not asserted	not asserted	asserted	not asserted
bit-1 - SSL server	not asserted	not asserted	not asserted	not asserted
bit-2 - S/MIME	not asserted	not asserted	asserted	asserted
bit-3 - Object Signing	not asserted	not asserted	not asserted	not asserted
bit-4 - Reserved	not asserted	not asserted	not asserted	not asserted
bit-5 - SSL CA	asserted	asserted	not asserted	not asserted
bit-6 - S/MIME CA	asserted	asserted	not asserted	not asserted
bit-7 - Object Signing CA	asserted	asserted	not asserted	not asserted

## 6.11. Policy mapping

This extension is only useful in case of cross-certification between CAs. It makes indeed little sense to have a policy mapping between a commercial CA and a governmental CA. Also this extension is not handled by Netscape nor by Microsoft products. As such the Policy Mapping has not been implemented.

## 6.12. Policy constraint

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

For the same reasons as mentioned in chapter 6.11, the Policy Constraint has not been implemented.

## 6.13. Certificate policies

Certificate policies will be present in the eID certificates as a CPS Pointer qualifier containing a pointer to the Certification Practice Statement (CPS) published by the CA.

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

CertificatePolicies				
	Belgium Root CA certificate	Citizen CA certificate	Citizen certificates	
			Authentication	signature
policyIdentifier	2.16.56.1.1.1	2.16.56.1.1.1.2	2.16.56.1.1.1.2.2	2.16.56.1.1.1.2.1.
policyQualifiers	N/a			
policyQualifierId	CPS			
Qualifier	<a href="http://repository.eid.belgium.be">http://repository.eid.belgium.be</a>			

## 6.14. Basic constraint

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

Basic constraint extension				
Basic constraint components	Belgium Root CA certificate	Citizen CA certificate	Citizen certificates	
			Authentication	signature
CA	true	True	~	~
PathLengthConstraint	none	0	~	~

## 6.15. CRL Distribution Point

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

CRL Distribution Point extension			
CRL Distribution Point Component	Belgium Root CA certificate	Citizen CA certificate	Citizen certificates
distributionPoint	<a href="http://secure.globalsign.net/crl/root.crl">http://secure.globalsign.net/crl/root.crl</a> CDP present in RootSigned certificate only.	<a href="http://crl.eid.belgium.be/belgium.crl">http://crl.eid.belgium.be/belgium.crl</a>	<a href="http://crl.eid.belgium.be/eidcxxxx.crl">http://crl.eid.belgium.be/eidcxxxx.crl</a>

Note: the 'xxxx' in the distribution point of the citizen certificates should be replaced with a number pointing to the CRL of the issuing operational Citizen CA (e.g. <http://crl.eid.belgium.be/eidc0001.crl>).

## 6.16. Freshest CRL - Delta CRL Distribution Point

As the applications do not yet support 'Delta CRL Distribution Point' it was decided not to implement this now.

## 6.17. Authority Information Access

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

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

As a shared OCSP responder will be used, OCSP validation of CA certificates is not supported.

Authority Information Access extension			
Authority Information Access component	Belgium Root CA certificate	Citizen CA certificate	Citizen certificates
accessMethod	~	~	<i>id-ad-ocsp (OCSP)</i>
accessLocation	~	~	<a href="http://ocsp.eid.belgium.be">http://ocsp.eid.belgium.be</a>
accessMethod	~	~	<i>id-ad-caIssuers (HTTP)</i>
accessLocation	~	~	<a href="http://certs.eid.belgium.be/belgiumrs.crt">http://certs.eid.belgium.be/belgiumrs.crt</a>

RFC3280 specifies: "The id-ad-caIssuers OID is used when the additional information lists CAs that have issued certificates superior to the CA that issued the certificate containing this extension. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user." It doesn't thus make sense to put accessMethod caIssuers in the government and eID CA certificates.

The LDAP access method will not be used in any of the eID certificate profiles described in this document.

## 6.18. Subject Directory attributes

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

No subject directory attributes will be present in the eID certificates

## 7. Qualified Certificate Statement

The Qualified Certificate Statement, identified by the OID { id-etsi-qcs 1 } will be present in end-user signature certificates as per ETSI TS 101 862 V1.2.1.

The certificates contain an OID to the QCStatement, in this case the ETSI registered QCStatement.

## 8. OCSP Certificate

A shared OCSP key pair will be generated under the shared security environment of GlobalSign. A branded OCSP certificate will be created within the scope of the eID project. Due to constraints linked to the use of the shared infrastructure, the OCSP certificate profile has to be identical in terms of extensions and attributes to the standard GlobalSign OCSP responder certificate profile. The only possible changes are the C and CN SDN extensions.

Each operational CA will sign the key-pair of the OCSP server, so that there are as many OCSP certificates as there are operational CAs. All these OCSP certificates are using the same key-pair.

The OCSP certificate profile extension ocsfNoCheck is used to define that there is no need for validation of the full CA chain using OCSP.

## 9. CRL profiles

The CRLs and  $\Delta$  CRLs will be created according to the profiles as described in the chapters 9.1 and 9.2. All CRLs and  $\Delta$  CRLs are signed by the issuing CA.

### 9.1. CRL Profile

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	certificateHold(6) (for suspended certificates) Note: otherwise not included
CrlExtensions	
Authority Key Identifier	non-critical <subject key identifier CA>
CRL Number	non-critical <The CA operator assigned unique number>

'nextUpdate' is the latest time that the delta CRL can be used by a citizen.

## 9.2. **Δ** CRL Profile

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	certificateHold(6) (for suspended certificates) removeFromCrl(8) (to unsuspend certificates) Note: otherwise not included
crlExtensions	
Authority Key Identifier	non-critical <subject key identifier CA>
CRL Number	non-critical <The CA operator assigned unique number>
Delta CRL Indicator	critical <base CRL Number>

'nextUpdate' is the latest time that the delta CRL can be used by a citizen.

## 10. LDAP Scheme

The scheme used for the eID certificates is kept as easy as possible.

The LDAP node under which the eID certificates are published is defined as follows: dc=eid dc=belgium dc=be. All certificates will be published under this node under a flat file structure, where every entry will have an unique 10 digits UID randomly assigned by the CA<sup>2</sup>.

Besides the certificate itself, all certificate subject distinguished name (SDN) information is published in the LDAP. All Subject Distinguished Name information present in the certificates as per the end-user certificate profiles is searchable.

Besides the certificates, the LDAP will also contain CRL and  $\Delta$ CRLs as they are also signed by the CA's.

---

<sup>2</sup> More information about the LDAP services can be found in EID-DEL-006 Component Overview

## 11. Recapitulative Tables

RootSigned Belgium Root CA (Generated under Government Security Environment)					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		Generated by the CA at Key Generation Process Time	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Not after : Key Generation Process Date + 11 years	Fixed
SubjectPublicKeyInfo		X		RSA 2048	
Issuer					
countryName	{ id-at-6 }	X		BE	Fixed
organisationName	{ id-at-10 }	X		GlobalSign nv-sa	Fixed
organisationUnitName	{ id-at-11 }			Root CA	Fixed
commonName	{ id-at-3 }	X		GlobalSign Root CA	Fixed
Subject					
countryName	{ id-at-6 }	X		BE	Fixed
commonName	{ id-at-3 }			Belgium Root CA	Fixed
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		2.16.56.1.1.1	Fixed
policyQualifiers				N/a	

RootSigned Belgium Root CA (Generated under Government Security Environment)					
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		<a href="http://repository.eid.belgium.be">http://repository.eid.belgium.be</a>	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
CertificateSigning				Set	Fixed
crlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE	N/a	
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		<a href="http://secure.globalsign.net/crl/root.crl">http://secure.globalsign.net/crl/root.crl</a>	Fixed
BasicConstraints	{id-ce 19}	X	TRUE	N/a	
CA		X		TRUE	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslCA - smimeCA - objectSigningCA	Fixed

An empty CRL will be generated during the Key ceremony for the Rootsigned Belgium Root CA

SelfSigned Belgium Root CA (Generated under Government Security Environment)					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		16 Bytes provided by FedICT	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Not before: Key Generation Process Date	
NotAfter		X		Not after Key Generation Process Date + 11 years	Fixed
SubjectPublicKeyInfo		X		RSA 2048	
Issuer					
countryName	{ id-at-6 }	X		BE	Fixed
commonName	{ id-at-3 }	X		Belgium Root CA	Fixed
Subject					
countryName	{ id-at-6 }	X		BE	Fixed
commonName	{ id-at-3 }			Belgium Root CA	Fixed
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		2.16.56.1.1.1	Fixed
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		<a href="http://repository.eid.belgium.be">http://repository.eid.belgium.be</a>	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
CertificateSigning				Set	Fixed

SelfSigned Belgium Root CA (Generated under Government Security Environment)					
crlSigning				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE	N/a	
KeyIdentifier		X		SHA-1 Hash	
subjectKeyIdentifier	{id-ce 14}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
BasicConstraints	{id-ce 19}	X	TRUE	N/a	
CA		X		TRUE	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslCA - smimeCA - objectSigningCA	Fixed

Citizen CA (Generated under GlobalSign Security Environment)					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		16 Bytes provided by FedICT	
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Key Generation Process Date + 6 years (6 years 5 months for the first certificate) (	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
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		<a href="http://repository.eid.belgium.be">http://repository.eid.belgium.be</a>	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
CertificateSigning				Set	Fixed

Citizen CA (Generated under GlobalSign Security Environment)					
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		<a href="http://crl.eid.belgium.be/belgium.crl">http://crl.eid.belgium.be/belgium.crl</a>	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

An empty CRL will be generated during the Key ceremony for the Citizen CA

eID End User 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 Generation Process Date/Time	
NotAfter		X		Key Generation 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
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed

eID End User Authentication Certificate					
Qualifier		X		<a href="http://repository.eid.belgium.be">http://repository.eid.belgium.be</a>	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		<a href="http://crl.eid.belgium.be/eidc0001.crl">http://crl.eid.belgium.be/eidc0001.crl</a> 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		<a href="http://certs.eid.belgium.be/belgiumrs.crt">http://certs.eid.belgium.be/belgiumrs.crt</a> – Points to RootSigned Belgium Root CA.	
accessMethod	{ id-ad-1 }	X			
accessLocation		X		<a href="http://ocsp.eid.belgium.be">http://ocsp.eid.belgium.be</a>	

eID End User 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 Generation Process Date/Time	
NotAfter		X		Key Generation 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
policyQualifiers				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed

eID End User Signature Certificate					
Qualifier		X		<a href="http://repository.eid.belgium.be">http://repository.eid.belgium.be</a>	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		<a href="http://crl.eid.belgium.be/eidc0001.crl">http://crl.eid.belgium.be/eidc0001.crl</a> 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		<a href="http://certs.eid.belgium.be/belgiumrs.crt">http://certs.eid.belgium.be/belgiumrs.crt</a> – Points to RootSigned Belgium oot CA.	
accessMethod	{ id-ad-1 }	X			
accessLocation		X		<a href="http://ocsp.eid.belgium.be">http://ocsp.eid.belgium.be</a>	

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