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

Certipost

eID PKI hierarchy and certificate profiles

Version	8
Release date	31/05/2017
Document ID	EID-DEL-004 eID PKI hierarchy and certificate profile V8

Table of Contents

1. Document control

1.1. Document change control

Last revised version: V8

Last revision date: 31/05/2017

Final author: Bart Eeman – Certipost

1.2. References

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

- 'I'EIK Lot 2 & 4 – Aanvraag voor BAFO' including the 'Raamovereenkomst ref. Nr. RRN 006/2001'
- 'Verslag Onderhandelingssessie 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
- EID-DEL-366 RFC036 Annex A Foreigner CA hierarchy specifications v1 1 and EID-DEL-366 RFC036 Annex B Foreigner CA services specifications v1 3, regarding the foreigner PKI hierarchy and certificate profiles specifications
- Voor TSA: 20070510 Wijziging_raamovereenkomst_eID_Bijlage2_Time_stamping_Notarisatie

The reader should be aware that beside this document other documents exist which describe specific areas of the eID CA services environment (see §2.1).

1.3. Compliance

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 RFC5280.
- Internet X 509 Qualified certificates, also known as RFC3739.
- X.509 Internet Public Key Infrastructure Online Certificate Status Protocol, also known as RFC 6960.

All certificate attributes, extensions, and the validation mechanism are RFC5280 compliant.

The reference for qualified certificates is RFC3739.

2. Executive Summary

2.1. What is the purpose of this document

This document is part of the functional specification reports and aims to describe the installed PKI hierarchy including the different certificate profiles. All certificates are formatted according to version 3 of the X509 recommendation. The CRL profile as well as the OCSP profile is following the international standards.

This document specifies the Certificates, CRLs, LDAP and OCSP trust products and is part of a set of documents that technically describe the whole eID CA services environment.

This set of documents consists out of:

- EID-DEL-004: eID PKI Hierarchy and Certificate Profiles
- EID-DEL-006: eID CA Component Overview
- EID-DEL-008: eID CA Technical Analysis Customer Interface
- EID-DEL-010: eID CA 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.

2.2. How is this document organized

This document provides the technical specification of the eID PKI hierarchy and certificate profiles from chapter 3 to 8 including the changes which were applied over time. Chapter 9 describes the CA configuration settings, chapter 10 the applied naming conventions and chapter 11 the date new CA's were released on the production environment. *Annex 1 (EID-DEL-004 Annex_1_eID certificate profile V7.04*) provides the last specifications of the certificate profiles applicable at the time this document was created.

3. Structure and organisation

3.1. Structure

A distinction can be made between the hierarchy present on the eID smart cards and the one used for administration and government purposes. The first will be referred to as the eID hierarchy and the latter the Admin Hierarchy.

eID hierarchy

The eID hierarchy is a hybrid hierarchy that consists of a combination of 2 and 3 layer models. The hierarchy present on the smart cards (eID cards) consists of 2 levels, a Self-Signed Belgium Root CA and an operational Citizen CA or Foreigner CA. The Authority Information Access (AIA) 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).

The RRN[1] eID signing certificate is exclusively used to sign all the data on each eID-card issued under the Belgian Root CA hierarchy. The signature will be placed at the creation of the card and each time the data on the card is updated. Such a signature allows official government instances (e.g. RRN itself, municipalities, police, …) to verify the integrity of the data on each eID card[2].

Since January 2008 a second Belgium Root CA tree has been taken in production. The first Belgium Root is near "end-of-live" and phasing out. 26 October 2008 is the final date where it is possible to issue certificates under the first Belgium Root CA tree. After this date the Belgium Root CA2, as it is named, will be fully operational.

As of 2014, two additional BRCA (BRCA3 / BRCA4) are provided, in the context of the 10-year valid end-user certificates. There are respectively SHA-1 and SHA-2-algoritmic root certificates generated.

As of 2016, the production of new certificates is only done under BRCA4 with the SHA-2-algoritmic. Re-issuing is still possible under BRCA2 / BRCA3.

Note: further in this document, if referred to the "Belgium Root CA" it will be applicable for all PKI trees unless otherwise stated.

[1] RRN is an acronym for Rijksregister – Registre National

[2] The CA has no further involvement that the generation of such a RRN eID Signing Certificate

PKI (Admin & Gov)hierarchy

The 2-Level Admin hierarchy consists of a Self-Signed Belgium Root CA and an operational Administration CA, Government CA and Government AA[3].

The Administration CA certificate is used for signing the eID Role Certificates and the CRL of the Administration CA.

The eID Role Certificates assure the electronic identity of a specific application. It can be used exclusively for authentication purposes towards the Belgian eID-card, using an external authentication with certificate verification. This certificate verification is the process whereby the eID card verifies the digital signature of a certificate coming from an external application. The Certificate itself is also verified by the eID Card with data that resides on the eID Card.

If the role identifier retrieved from the Certificate corresponds with one that is programmed in the eID card, then the external card application will get access to the corresponding data and functions in the eID card.

The Government CA and AA certificates are used for signing the SSL Server Certificates needed by the Government, the RRN eID Server Signing Certificates (until 2004) and the CRL of the Government CA and AA.

The SSL Server Certificates assure the electronic identity of servers. It can be used for securing applications on a high level in a client-server or browser-server model, for example for electronic transactions with public authorities.

As the Self-Signed Belgium Root CA is part of both the eID and Admin hierarchy, it will only be further specified within the eID hierarchy to avoid double specifications.

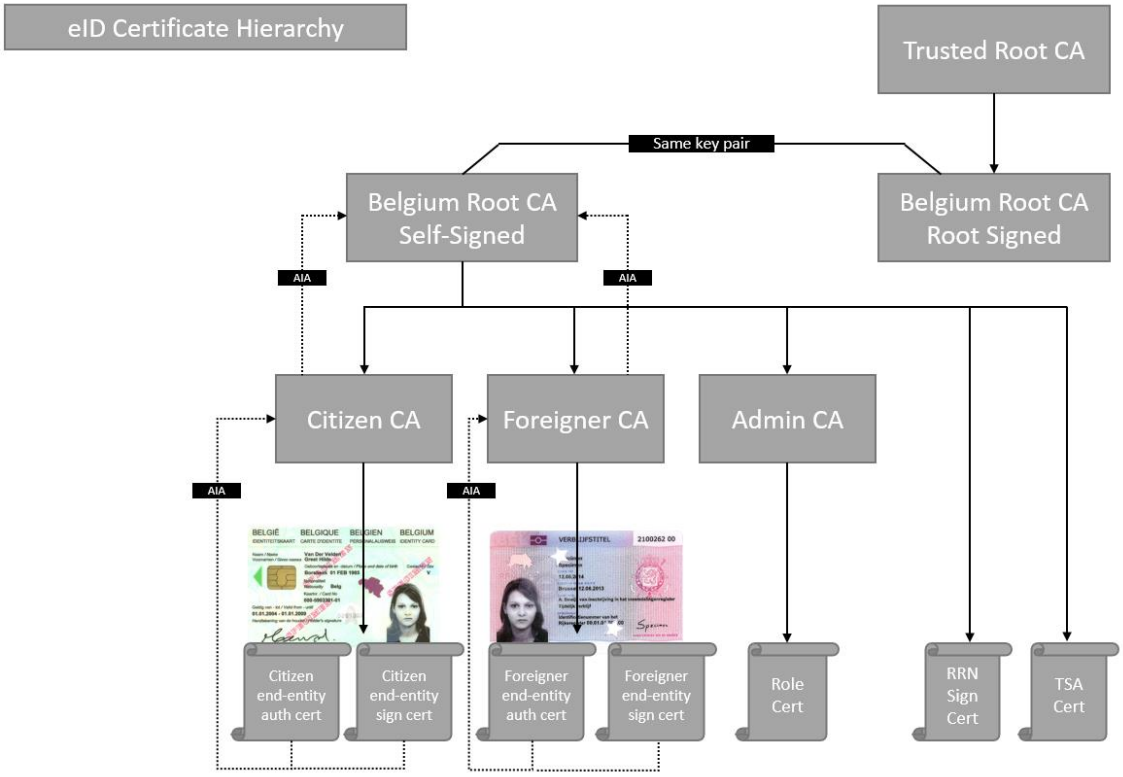
As of 2016 no new government CA were created.

As of 11/01/2016 all non-natural persons certificates under all government CA were revoked.

As of 2016 government CA 2011 / 201401 /201402 have been replaced by a self-signed version. Only existing person certificates are still active until revocation or expiration.

[3] Second government CA to issue certificate for more restricted use

Figure 1 details the structure of the eID and Admin hierarchy.



3.2. Organisation

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

The Belgium Root CA is root signed by the Digicert cybertrust global root (BRCA 2 / 3 / 4) under the terms of a RootSigning™ contract.

The CA operator manages the Belgium Root CA, CA key pairs and associated certificates in compliance with the Key Management Policy.

The eID hierarchy certificates are ruled by the different published "eID" CPS-documents that are maintained by the CA at the following location (https://repository.eid.belgium.be).

4. Signature algorithm

4.1. Key pairs

The key pairs in this hierarchy are generated using the RSA cryptographic algorithm. The lifetime of keys is specified as the period of validity of certificates associated to the keys.

4.2. Hashing algorithm

The hashing algorithm used is Secure Hash Algorithm – 1 (SHA-1) for all certificates under BRCA1, BRCA2 and BRCA3.

With BRCA4, SHA256 is used to provide additional security.

5. Certificate profiles

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

Note: All the URI's specified in the certificate profiles are resolved by BOSA[4].

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

Annex 1 (EID-DEL-004 Annex_1_eID certificate profile V7.04) gives an overview of the most recent specification of the certificate profiles.

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

5.1. Version

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

Version	
All certificates	Version 3 – Value = "2"

5.2. 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[5] can assign a serial number to the eID hierarchy certificates. BOSA can assign a serial number to the Admin hierarchy certificates.

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

The CA operator created the serial number for the RootSigned Belgium Root CA certificate.

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

Serial Number	
Belgium Root CA RootSigned certificate	Generated by the CA at the time of Key Generation Process
eID hierarchy certificates	
Admin hierarchy certificates	

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

[5] RRN is an acronym for Rijksregister – Registre National

5.3. Signature

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

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

5.4. Issuer

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

Issuer		
Certificate	Releases	Field attributes
Belgium Root CA 1 Root Signed certificate	<10/2013	C : BE O : GlobalSign nv-sa OU: Root CA CN: GlobalSign Root CA
Belgium Root CA 2/3/4 Root Signed certificate	>=10/2013	CN : Cybertrust Global Root O : Cybertrust, Inc
eID hierarchy <u>Root certificate</u> Belgium Root CA Self-signed certificate	 <2008 >=2008 >=06/2013	 C: BE, CN: Belgium Root CA C: BE, CN: Belgium Root CA2 C: BE, CN: Belgium Root CA3 C: BE, CN: Belgium Root CA4
<u>Operational CA certificates</u> Citizen CA, Foreigner CA	<2008 >=2008 >=06/2013	C: BE, CN: Belgium Root CA C: BE, CN: Belgium Root CA2 C: BE, CN: Belgium Root CA3 C: BE, CN: Belgium Root CA4

End user certificates Citizen	<2005 >=2005	C: BE, CN: Citizen CA C: BE, CN: Citizen CA, Serial Number: <yyyy><ss>[6]
Foreigner		C: BE, CN: Foreigner CA, Serial Number: <yyyy><ss>
End user certificates Citizen		C: BE, CN: Citizen CA, Serial Number: <yyyy><ss>[7] O: Certipost N.V. / S.A. L: Brussels
Foreigner	>=2017	C: BE, CN: Foreigner CA, Serial Number: <yyyy><ss> O: Certipost N.V. / S.A. L: Brussels
PKI hierarchy Operational CA certificates Administration CA, Government CA & AA	<2008 >=2008 >=20132014	C: BE, CN: Belgium Root CA C: BE, CN: Belgium Root CA2 C: BE, CN: Belgium Root CA3 C: BE, CN: Belgium Root CA4
End user certificates Administration	<2006 >=2006	C: BE, CN: Administration CA C: BE, CN: Administration CA, Serial Number: <yyyy><ss>
Government (CA)	<2006 >=2006	C: BE, CN: Government CA C: BE, CN: Government CA, Serial Number: <yyyy><ss>
Government (AA)	All	C: BE, CN: Government AA, Serial Number: <yyyy><ss>
Government CA 2011	>02/2016	Serial Number: 2011 CN: Government CA C: BE
Government CA 201401 / 201402	>02/2016	Serial Number: 2014<ss> CN: Government CA C: BE

[6] See paragraph 10.1 Serial number to reference a CA

[7] See paragraph 10.1 Serial number to reference a CA

5.5. Validity

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

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

Validity				
	Release	Not before	Not after	Validity period[8]
Belgium Root CA Root Signed certificate	BRCA	27/01/2003	27/01/2014	11 yr
	BRCA2	10/10/2013	12/05/2025	11 yr, 7 mth
	BRCA3	10/10/2013	12/05/2025	11 yr, 7 mth
	BRCA4	10/10/2013	12/05/2025	11 yr, 7 mth
	BRCA4	26/06/2016	22/10/2032	11yr 7 mth
eID hierarchy				
Root certificate				
Belgium Root CA Self-Signed certificate	BRCA		11 years	
	BRCA2		14 yr, 2 mth	
	BRCA3		14 yr, 7 mth	
	BRCA4		19 yr, 3 mth	
Operational CA certificates			6y 5m	
Citizen CA	2003/1		6y 2m	
	2003/2		6y 8m	
	>2004 - <2014		11 yr, 8m	
	>=2014			
Foreigner CA	>=2006		6y 8m	
	>=2015		11y 8m	

[8] Certificate validity periods defined during key ceremony.

PKI hierarchy		
Operational CA certificates		
Administration CA (1024)	2003	6 years
	2004	6y 8m
	2005	6y 8m
	2006	6y 8m
	2007	6y 8m
	2008	6y 3m
	>=2008	6y 8m
Administration CA (2048)	>2005 - <2014	6y 8m
	>=2014	11y 8m
Government CA / AA	>=2006	6y 8m
	Release	Standard validity period[9]
eID hierarchy		
End user certificates		
Citizen	2003/1	5 years
	2003/2	5 years
	2004	5 years
	2005	5y 3m
	2006	5y 3m
	2007	5y 3m
	2008	5y 3m
	>=2014	10y 3m
Foreigner	>=2006	5y 3m
	>=2015	10y 3m
RRN signing	>=2005 <2014	6y 8m
	>=2014	11y 5m
PKI hierarchy		
End user certificates		
Administration (1024 bits)	>=2003	6y 8m
Administration (2048 bits)	>=2005 - <2014	6y 8m
	>=2014	11y 5m

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

Government (CA) RRN signing Server Applications Persons Government (AA) Identity providers	 < 2005 <2007 >=2007 >2008 2006 >=2007 >2008 2006 >=2007 >2008 2006 >=2007 >2008	 6 years 1 year 1 y 3 m TBD by BOSA 1 year 1 y 3 m TBD by BOSA 1 year 1 y 3 m TBD by BOSA 1 year 1 y 3 m TBD by BOSA
OCSP Certificates	<2006 >=2006	1year 1y 3m

5.6. Subject

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

Subject		
Certificate	Release	Field attributes
Belgium Root CA Root Signed certificate	<2008 >=2008 < 2014 >=2014	C : BE, CN: Belgium Root CA C : BE, CN: Belgium Root CA2 C : BE, CN: Belgium Root CA3 C : BE, CN: Belgium Root CA4
eID hierarchy <u>Root certificate</u> Belgium Root CA Self-signed crt	<2008 >=2008-2013 >=2013	C: BE, CN: Belgium Root CA C: BE, CN: Belgium Root CA2 C: BE, CN: Belgium Root CA3 C: BE, CN: Belgium Root CA4

Operational CA certificates		
Citizen CA	<2005	C: BE, CN: Citizen CA
	>=2005	C: BE, CN: Citizen CA, Serial Number: <yyyy><ss>[10]
	>=2017	C: BE, CN: Citizen CA, Serial Number: <yyyy><ss>[11] O: Certipost N.V. / S.A. L: Brussels
Foreigner CA	<2017	C: BE, CN: Foreigner CA, Serial Number: <yyyy><ss>
	>=2017	C: BE, CN: Citizen CA, Serial Number: <yyyy><ss>[12] O: Certipost N.V. / S.A. L: Brussels
End user certificates		
Citizen, Foreigner	>=2005	See Table "End use certificate Subject field (eID Hierarchy)"
RRN signing		C:BE, CN:RRN, O:RRN
PKI hierarchy		
Operational CA	<2006	C: BE, CN: Administration CA
Administration CA,	>=2006	C: BE, CN: Administration CA Serial Number: <yyyy><ss>
	<2006	C: BE, CN: Governement CA
Government CA	>=2006	C: BE, CN: Covernement CA Serial Number: <yyyy><ss>
	>=2006	C: BE, CN: Governement AA
Government AA		Serial Number: <yyyy><ss>

[10] See paragraph 10.1 Serial number to reference a CA

[11] See paragraph 10.1 Serial number to reference a CA

[12] See paragraph 10.1 Serial number to reference a CA

End user certificates		
Administration		
Role 3 & 4	<2012	C:BE, CN:RNN-Rekeying-<yyyy>, O:RRN
Role 7	All	C:BE, CN:RRN-Change address-<yyyy>, O:RRN
Role 1 & 2	>=2006	C:BE, CN:RNN-Extensions, O:RRN
Role 1 & 3 & 4	>=2013	C:BE, CN:RNN-ROLE-134-<yyyy>, O:RRN
AIO	>2012	C:BE, CN:RNNAIO2048, O:RRN
	>=2014	C:BE, CN:RNN-EXTENSIONS-<yyyy>, O:RRN
RRN signing	<2005	C:BE, CN:RRN, O:RRN
Time stamping	All	C:BE, CN: Time stamping Authority, O:Belgium Federal Government, SN: <yyyy>
Government (CA)		
Server	All	C:BE, CN: <Provided by PKCS10 request>
Applications	All	C:BE, CN: <Provided by PKCS10 request>
Persons	All	C:BE, CN:< Provided by PKCS10 request>
Government (AA)		
Identity providers	All	C:BE, CN: <Provided by PKCS10 request>

End user certificate Subject fields definition (eID hierarchy)			
Field	**Length**	**Description**	**Example**
C *(countryName)*	2	countryName is a dynamic element corresponding to the two letter country code ISO3166 standard. The country code is provided with the certificate creation request by the RRN. It is not checked by the CA.	C=BE
CN *(commonName)*	Max 255 Min 1	Concatenation of • <given name>: first given name of the card holder • <surname>: surname of the eID card owner	CN=John Smith (Authentication) CN=John Smith (Signature)

		• (<purpose>): (Authentication) or (Signature)	
surname	Max 255 Min 1	Surname of the eID card owner	S=Smith
givenName	Max 255 Min 1	1 or 2 given names of the eID card owner (This field may not appear in case the owner has no given name)	G=John William
subjectSerialNumber	Max 255 Min 1	This is a unique number provided by the RRN ("Rijksregisternummer" – 11 digits long).	SN=12345678901

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

5.7. 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	
RootSigned Belgium Root CA1 & 2 **RootSigned Belgium Root CA3 & 4**	RSA 2048 bits key RSA 4096 bits key
eID hierarchy	
Root certificate	
Self-signed Belgium Root CA1 & 2	RSA 2048 bits key
Self-signed Belgium Root CA3 & 4	RSA 4096 bits key
Operational CA certificates	
Citizen CA, Foreigner CA <2014	RSA 2048 bits key
Citizen CA, Foreigner CA >=2014	RSA 4096 bits key
End user certificates	
RRN signing	RSA 1024 bits key
RRN signing >=2008	RSA 2048 bits Key
Citizen, Foreigner <2014	RSA 1024 bits key
Citizen, Foreigner CA >=2014	RSA 2048 bits key
PKI hierarchy	
Operational CA certificates	
Administration CA (2048)	RSA 2048 bits key
Administration CA (1024)	RSA 1024 bits key
Government CA, Government AA	RSA 2048 bits key
End user certificates	
Administration (2048)	
Role certificates	RSA 2048 bits key
Administration (1024)	
Role certificates	RSA 1024 bits key
Government (CA)	
All, including RRN Server Signing (until 2004))	Provided by PKCS10 request
Government (AA)	Provided by PKCS10 request
All	

5.8. Key usage extension

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

Key usage extension									
Key usage extension	Digital Signature	Non Repudiation	Key Encipherment	Data Encipherment	Key Agreement	Key Certificate Signing	Crl Signing	Encipher Only	Decipher Only
Root signed Belgium Root CA certificate	NA[13]	NA	NA	NA	NA	A	A	NA	NA
eID hierarchy									
Root certificate									
Self-signed Belgium Root CA	NA	NA	NA	NA	NA	A	A	NA	NA
Operational CA certificates									
Citizen CA, Foreigner CA	NA	NA	NA	NA	NA	A	A	NA	NA
End user certificates									
Citizen, Foreigner Authentication crt	A	NA	NA	NA	NA	NA	NA	NA	NA
Citizen, Foreigner Signature crt	NA	A	NA	NA	NA	NA	NA	NA	NA
RRN signing certificate	A	A	NA	NA	NA	NA	NA	NA	NA
PKI hierarchy									
Operational CA certificates									
Administration CA	NA	NA	NA	NA	NA	A	A	NA	NA
Government CA, Government AA	NA	NA	NA	NA	NA	A	A	NA	NA
End user certificates									
Role certificates	A	NA	NA	NA	NA	NA	NA	NA	NA
Government (CA) certificates									
RRN signing certificate (until 2004)	A	A	NA	NA	NA	NA	NA	NA	NA
Server	A	A	A	A	NA	NA	NA	NA	NA
Applications	A	A	A	A	NA	NA	NA	NA	NA
Persons	A	A	A	A	NA	NA	NA	NA	NA
Time Stamping	A	A	NA	NA	NA	NA	NA	NA	NA
Government (AA) certificates	A	A	A	A	NA	NA	NA	NA	NA
Identity providers									
OCSP responder certificate	A	NA	NA	NA	NA	NA	NA	NA	NA

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

[13] NA: Not asserted, A: Asserted

5.9. Authority and Subject Key Identifiers

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

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

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

5.10. NetscapeCertType

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

- bit-0 SSL client - this cert is certified for SSL client authentication use
- bit-1 SSL server - this cert is certified for SSL server authentication use
- bit-2 S/MIME - this cert is certified for use by clients
- bit-3 Object Signing - this cert is certified for signing objects such as Java applets and plugins
- bit-4 Reserved - this bit is reserved for future use
- bit-5 SSL CA - this cert is certified for issuing certs for SSL use
- bit-6 S/MIME CA - this cert is certified for issuing certs for S/MIME use
- bit-7 Object Signing CA - this cert is certified for issuing certs for Object Signing

NetscapeCertType Key usage extension								
Netscape Key usage	bit-0 - SSL client	bit-1 - SSL server	bit-2 - S/MIME	bit-3 - Object Signing	bit-4 - Reserved	bit-5 - SSL CA	bit-6 - S/MIME CA	bit-7 - Object Signing CA
Root signed Belgium Root CA certificate	NA	NA	NA	NA	NA	NA	A	A
eID hierarchy								
Root certificate								
Self-signed Belgium Root CA	NA	NA	NA	NA	NA	A	A	A
Operational CA certificate								
Citizen CA, Foreigner CA	NA	NA	NA	NA	NA	A	A	A
End user certificates								
Citizen, Foreigner Authentication crt	A	NA	A	NA	NA	NA	NA	NA
Citizen, Foreigner Signature crt	NA	NA	A	NA	NA	NA	NA	NA
RRN signing certificate	-	-	-	-	-	-	-	-
PKI hierarchy								
Operational CA certificate								
Administration CA	NA	NA	NA	NA	NA	A	A	A
Government CA, Government AA	NA	NA	NA	NA	NA	A	A	A
End user certificates								
Role certificates	-	-	-	-	-	-	-	-
Government (CA) certificates								
RRN signing certificate (until 2004)								
Server	NA	A	A	NA	NA	NA	NA	NA
Applications	A	NA	A	A	NA	NA	NA	NA
Persons	A	NA	A	NA	NA	NA	NA	NA
Time Stamping	NA	NA	NA	NA	NA	NA	NA	NA
Government (AA) certificates	A	A	A	A	NA	NA	NA	NA
Identity providers								

5.11. 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 or by Microsoft products. As such the Policy Mapping has not been implemented.

5.12. 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 5.11, the Policy Constraint has not been implemented.

5.13. Certificate policies

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

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

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

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

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

Certificate Policies				
	Policy Identifier	Policy Qualifiers	Policy Qualifier Id	Qualifier
Root signed Belgium Root CA certificate	2.16.56.1.1.1 2.16.56.9.1.1 2.16.56.10.1.1 2.16.56.12.1.1	NA	CPS	http://repository.eid.belgium.be
eID hierarchy Root certificate Self-signed Belgium Root CA	2.16.56.1.1.1 2.16.56.9.1.1 2.16.56.10.1.1 2.16.56.12.1.1	NA	CPS	http://repository.eid.belgium.be

Operational CA certificates				
Citizen CA	2.16.56.1.1.1.2 2.16.56.9.1.1.2 2.16.56.10.1.1.2 2.16.56.12.1.1.2	NA	CPS	https://repository.eid.belgium.be
Foreigner CA	2.16.56.1.1.1.7 2.16.56.9.1.1.7 2.16.56.10.1.1.7 2.16.56.12.1.1.7	NA	CPS	https://repository.eid.belgium.be
End user certificates				
Citizen Authentication certificate	2.16.56.1.1.1.2.2 2.16.56.9.1.1.2.2 2.16.56.10.1.1.2.2 2.16.56.12.1.1.2.2	NA	CPS	https://repository.eid.belgium.be
Citizen Signature certificate	2.16.56.1.1.1.2.1 2.16.56.9.1.1.2.1 2.16.56.10.1.1.2.1 2.16.56.12.1.1.2.1	NA	CPS	https://repository.eid.belgium.be
Foreigner Authentication certificate	2.16.56.1.1.1.7.2 2.16.56.9.1.1.7.2 2.16.56.10.1.1.7.2 2.16.56.12.1.1.7.2	NA	CPS	https://repository.eid.belgium.be
Foreigner Signature certificate	2.16.56.1.1.1.7.1 2.16.56.9.1.1.7.1 2.16.56.10.1.1.7.1 2.16.56.12.1.1.7.1	NA	CPS	https://repository.eid.belgium.be
RRN signing certificate	2.16.56.1.1.1.4 2.16.56.9.1.1.4 2.16.56.10.1.1.4 2.16.56.12.1.1.4	NA	CPS	http://repository.eid.belgium.be
Admin hierarchy				
Operational CA certificates	2.16.56.1.1.1.1	NA	CPS	http://repository.eid.belgium.be
Administration CA	2.16.56.9.1.1.1 2.16.56.10.1.1.1 2.16.56.12.1.1.1			

Government CA (until 2004) Government AA	2.16.56.1.1.1.3 2.16.56.9.1.1.3 2.16.56.10.1.1.3 2.16.56.12.1.1.3	NA	CPS	http://repository.eid.belgium.be
End user certificates				
Role certificates	2.16.56.1.1.1.1.1 2.16.56.9.1.1.1.1 2.16.56.10.1.1.1.1 2.16.56.12.1.1.1.1	NA	CPS	http://repository.pki.belgium.be
Government (CA) certificates				
RRN signing (until 2004)	2.16.56.1.1.1.3.1 2.16.56.9.1.1.3.1 2.16.56.10.1.1.3.1 2.16.56.12.1.1.3.1	NA	CPS	http://repository.eid.belgium.be
Server (from 2004)	2.16.56.1.1.1.3.2 2.16.56.9.1.1.3.2 2.16.56.10.1.1.3.2 2.16.56.12.1.1.3.2	NA	CPS	http://repository.eid.belgium.be
Applications	2.16.56.1.1.1.3.3 2.16.56.9.1.1.3.3 2.16.56.10.1.1.3.3 2.16.56.12.1.1.3.3	NA	CPS	http://repository.eid.belgium.be
Persons	2.16.56.1.1.1.3.4 2.16.56.9.1.1.3.4 2.16.56.10.1.1.3.4 2.16.56.12.1.1.3.4	NA	CPS	http://repository.pki.belgium.be
Time Stamping	2.16.56.9.1.1.3.5 2.16.56.10.1.1.3.5 2.16.56.12.1.1.3.5	NA	CPS	http://repository.pki.belgium.be
Government (AA) certificates				
Identity providers	2.16.56.1.1.1.6.2 2.16.56.9.1.1.6.2 2.16.56.10.1.1.6.2 2.16.56.12.1.1.6.2	NA	CPS	http://repository.pki.belgium.be

5.14. 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		
	CA	Path Lenght Constraint
Root signed Belgium Root CA certificate	TRUE	None
eID hierarchy		
Root certificate		
Self-signed Belgium Root CA	TRUE	None
Operational CA certificate		
Citizen CA, Foreigner CA	TRUE	0
End user certificates		
Citizen, Foreigner Authentication	FALSE	-
Citizen, Foreigner Signature	FALSE	-
RRN signing certificate	FALSE	None
Admin hierarchy		
Operational CA certificate		
Administration CA	TRUE	0
Government CA, Government AA	TRUE	0
End user certificates		
Role certificates	FALSE	None
Government certificates	FALSE	None

5.15. 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 (CDP)		
	Releases	Distribution Point
Root signed Belgium Root CA certificate Root signed Belgium Root CA 2 / 3 / 4 certificate	All	http://secure.globalsign.net/crl/root.crl CDP present in RootSigned certificate only http://Crl.omniroot.com/ctglobal.crl
eID hierarchy		
Root certificate		
Self-signed Belgium Root CA	<2008	http://crl.eid.belgium.be/belgium.crl
	>=2008	http://crl.eid.belgium.be/belgium2.crl
	<2014	
	>=2014	http://crl.eid.belgium.be/belgium3.crl
		http://crl.eid.belgium.be/belgium4.crl
Operational CA certificates		
Citizen CA	<2008	http://crl.eid.belgium.be/belgium.crl
	>=2008	http://crl.eid.belgium.be/belgium2.crl
Foreigner CA	<2014	
	>=2014	http://crl.eid.belgium.be/belgium3.crl
		http://crl.eid.belgium.be/belgium4.crl
End user certificates		
Citizen certificates	2003/1	http://crl.eid.belgium.be/eidc0001.crl
	2003/2	http://crl.eid.belgium.be/eidc0002.crl
	2004	http://crl.eid.belgium.be/eidc2004-1.crl
	>=2005	http://crl.eid.belgium.be/eidc<yyyy><ss>[14].crl
Foreigner certificates		http://crl.eid.belgium.be/eidf<yyyy><ss>.crl
RRN signing certificate	<2008	http://crl.eid.belgium.be/belgium.crl
	>=2008	http://crl.eid.belgium.be/belgium2.crl
	>=2014	http://crl.eid.belgium.be/belgium3.crl
		http://crl.eid.belgium.be/belgium4.crl

[14] See paragraph 10.2 CRL and delta CRL names

Admin hierarchy		
Operational CA certificates		
Administration CA	<2008	http://crl.eid.belgium.be/belgium.crl
Government CA	>=2008	http://crl.eid.belgium.be/belgium2.crl
	>=2014	http://crl.eid.belgium.be/belgium3.crl
Government AA		http://crl.eid.belgium.be/belgium4.crl
End user certificates	2003	none
Administration certificates	2004	http://crl.pki.belgium.be/government.crl
Role certificates	>=2005	http://crl.pki.belgium.be/government2004-1.crl
Government (CA) certificates	All	http://crl.pki.belgium.be/government<yyyy>.crl
		http://crl.pki.belgium.be/governmentAA<yyyy>.crl
Government (AA) certificates		

5.16. Freshest CRL - Delta CRL Distribution Point

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

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

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

5.17. 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		
	Access Method	Access Location
Root signed Belgium Root CA certificate		
eID hierarchy		
Root certificate		
Self-signed Belgium Root CA	None	None
Operational CA certificate		
Citizen CA, Foreigner CA	None	None
>2017	id-ad-ocsp (OCSP)	http://ocsp.eid.belgium.be/2
	id-ad-caIssuers (HTTP)	http://certs.eid.belgium.be/belgiumrs4.crt
End user certificates		
Citizen, Foreigner certificates		
<2008	id-ad-ocsp (OCSP)	http://ocsp.eid.belgium.be
>=2008 <2014		
>=2014		http://ocsp.eid.belgium.be/2
		http://certs.eid.belgium.be/belgiumrs.crt
<2008	id-ad-caIssuers (HTTP)	http://certs.eid.belgium.be/belgiumrs2.crt
>=2008 <2014		http://certs.eid.belgium.be/belgiumrs3.crt
>=2014		http://certs.eid.belgium.be/belgiumrs4.crt
>2017		http://certs.eid.belgium.be/<issuingca>
RRN signing certificate	none	none
Admin hierarchy		
Operational CA certificate		
Administration CA	None	None
Government CA, Government AA	None	None
End user certificates		
Role certificates	None	None
Government certificates	None	None

RFC5280 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 has no practical use to put accessMethod caIssuers in the Admin hierarchy and the eID Operational CA certificates. The LDAP access method will not be used in any of the eID certificate profiles described in this document.

5.18. Subject Directory attributes

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

No subject directory attributes will be present in the eID certificates

5.19. Qualified Certificate Statement

The Qualified Certificate Statement, identified by the OID { id-etsi-qcs 1 } is present in end-user signature certificates as per ETSI TS 101 862 V1.3.2.
As from 05/2017 the Qualified Certificate Statements, identified by the OIDs { id-etsi-qcs 4 } { id-etsi-qcs 5 } { id-etsi-qcs 6 } are present in end-user signature certificates.

6. OCSP Certificate

Each year, a shared OCSP key pair will be generated under the shared security environment of Verizon.

Each operational CA for which an OCSP responder service shall be available will sign the key-pair of the OCSP server, so that there are as many OCSP certificates as there are operational CA's enabled for OCSP. All these OCSP certificates are using the same key-pair.

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

7. CRL profiles

The CRLs and Δ CRLs will be created according to the profiles as described in the chapters 7.1 and 7.2. All CRLs and Δ CRLs are signed by the issuing CA.

7.1. CRL Profile

Version	v2
Signature	Sha256RSA
Issuer	<subject CA>
ThisUpdate	<creation time>
NextUpdate	<creation time> + 7 days
RevokedCertificates	
UserCertificate	<certificate serial number>
RevocationDate	<revocation time>

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

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

7.2. Δ CRL Profile

Version	v2
signature	Sha256RSA
Issuer	<subject CA>
thisUpdate	<creation time>
nextUpdate	<creation time> + 7 days
RevokedCertificates	
userCertificate	<certificate serial number>
revocationDate	<revocation time>
crlEntryExtensions	
CRL Reason Code	certificateHold(6) (for suspended certificates) removeFromCrl(8) (to unsuspend certificates) Note: otherwise not included
crlExtensions	
Authority Key Identifier	non-critical <subject key identifier CA>
CRL Number	non-critical <The CA operator assigned unique number>
Delta CRL Indicator	critical <base CRL Number>

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

8. 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 a unique 10 digits UID randomly assigned by the CA.[15]

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 ΔCRLs as they are also signed by the CA's.

On request of the Belgian Government, the access to the LDAP-service is suspended.

[15] More information about the LDAP services can be found in EID-DEL-006 eID CA Component Overview

9. CA configuration settings

The table below specifies the configuration settings on the CA's these configuration settings are explained hereafter

CA configurations settings								
Setting	Auto-revocation	Unique DN check	Group	Variable validity	Delta CRL creation			
Root certificate								
Belgium Root CA	NA	NA		NA	NA			
eID hierarchy								
Operational CA certificates								
Citizen CA	A	A	G1[16]	A	A			
Foreigner CA	NA	A	G1	A	A			
PKI hierarchy								
Operational CA certificates								
Administration CA	NA	NA		NA	NA			
Government CA	NA	NA		NA	A			
Government AA	NA	NA		NA	A			

9.1. Auto-revocation

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

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

9.2. Unique DN check

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

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

1) Un-suspended
2) Generated with a 'Valid' status.

The unique DN check applies to all certificates issued under the CA's belonging to the same unique DN group.

9.3. Variable validity

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

The variable validity feature is only available through XKMS interface.

9.4. Delta CRL

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

10. Naming conventions

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

10.1. Serial number to reference a CA

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

Remark: The CA's created for the year 2008 the following scheme with respect to the serial numbers:

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

10.2. CRL and delta CRL names

<CRL and delta CRL names>			
CA	**type**	**Format**	**Example**
Citizen CA	Base CRL	eidc<serial number>.crl	eidc201721.crl
	Delta CRL	eidcd<serial number>.crl	eidcd201721.crl
Foreigner CA	Base CRL	eidf<serial number>.crl	eidf201721.crl
	Delta CRL	eidfd<serial number>.crl	eidfd201721.crl
Government CA	Base CRL	government<serial number>.crl	government2010.crl
	Delta CRL	governmentd<serial number>.crl	governmentd2010.crl
Government AA	Base CRL	governmentAA<serial number>.crl	governmentAA2010.crl
	Delta CRL	governmentAAd<serial number>.crl	governmentAAd2010.crl

10.3. CA certificate file names

<CA certificates file name>		
CA	**Format**	**Example**
Root signed Belgium Root CA	belgiumrs.crt	
Self-signed Belgium Root CA	belgiumrca.crt	
Root signed Belgium Root CA (2 /3 / 4)	belgiumrs<x>.crt	belgiumrs4.crt
Self-signed Belgium Root CA (2 /3 / 4)	belgiumrca<x>.crt	belgiumrca4.crt
Citizen CA	citizen<serial number>.crt	citizen201721.crt
Foreigner CA	foreigner<serial number>.crl	foreigner201721.crt
Government CA	government<serial number>.crl	government2005.crt
Government AA	governmentAA<serial number>.crl	governmentAA2006.crt

11. Release dates

Every year new operational CA certificates are created during a key ceremony. The first end user certificates under these new operational CA's are issued after bootstrap of these CA's on the eID production environment. The date of the bootstrap defines the date of the first possible appearance of end user certificates under a modified PKI structure. As an operational CA there is only one release a year, the releases are given the name of the year.

The following release dates apply:

Releases		
Release	**Release date**	**Operational CA bootstrapped**
2003	27/01/2003	Citizen CA Government CA
	10/04/2003	Citizen CA2
2004	15/04/2004	Citizen2004 CA Government2004 CA
2005	21/01/05	Citizen200501 CA
	19/02/05	Government2005 CA
	5/06/2005	Citizen200502 to Citizen200615 CA's
2006	15/06/2006	Citizen200601 to Citizen200620 CA's
	22/06/2006	Government2006 CA GovernmentAA2006 CA
	31/11/2006	Foreigner200601 CA
2007	06/03/2007	Citizen200701 to Citizen200720 CA's Foreigner200701 to Foreigner200705 CA's Goverment2007 CA GovermentAA2007 CA
2008	16/12/2007	Citizen200801 to Citizen200804 CA's Foreigner200801 to Foreigner200804 CA's Goverment2008 CA GovermentAA2008 CA
2008	28/08/2013	Citizen200805 to Citizen200808

2008	14/08/2013	Citizen200809 to Citizen200816 CA's Foreigner200805 CA
2009	22/01/2009	Citizen200901 to Citizen200912 Foreigner200901 to Foreigner200903 Government2009 CA GovernmentAA2009 CA
2010	14/01/2010	Citizen201001 to Citizen201012 Foreigner201001 to Foreigner201002 Government2010 GovernmentAA2010
2011	03/02/2011	Citizen201101 to Citizen201108 Foreigner201101 to Foreigner201102 Government2011 GovernmentAA2011
2012	20/02/2012	Citizen201201 to Citizen201212 Foreigner201201 to Foreigner201204 GovernmentCA201201 to GovernmentCA201202 GovernmentAA201201 to GovernmentAA201202
2013	17/12/2012	Citizen201301 to Citizen201312 Foreigner201301 to Foreigner201304 GovernmentCA2013 GovernmentAA2013
2014	23/10/2013	Citizen201401 to Citizen201420 Foreigner201401 to Foreigner201405 GovernmentCA201401 / 201402 GovernmentAA201401 / 201402
2015	24/10/2014	Citizen201501 to Citizen201520 Foreigner201501 to Foreigner201505 GovernmentCA201501 GovernmentAA201501
2016	25/11/2015	Citizen201601 to Citizen201640 Foreigner201601 to Foreigner201610

2017	28/11/2016	Citizen201701 to Citizen201720 Foreigner201701 to Foreigner201705
2017	12/05/2017	Citizen201721 to Citizen201730 Foreigner201721 tot Foreigner201722

This page is intentionally left blank

Annex 1:

Certificate profile specifications

See EID-DEL-004 Annex_1_eID certificate profile V7.04