

FEDICT

Federale Overheidsdienst Binnenlandse Zaken
Service Public Fédéral Intérieur

Functional Analysis Customer Services

15 July 2003

Ref: EID-DEL-010 v2.0

Certipost

A branch of Belgacom and the Belgian Post group

Table of Contents

1.	DOCUMENT CONTROL	4
1.1.	DOCUMENT CHANGE CONTROL	4
1.2.	REFERENCES	4
2.	EXECUTIVE SUMMARY	5
2.1.	WHAT IS THE PURPOSE OF THIS DOCUMENT	5
2.2.	HOW IS THIS DOCUMENT ORGANIZED	5
3.	TECHNICAL SOLUTION – EID INFRASTRUCTURE	6
3.1.	DELIVERABLES	6
3.2.	GENERAL	6
3.2.1.	<i>Service Level Agreement</i>	6
3.2.2.	<i>Infrastructure sharing</i>	6
3.2.3.	<i>Dependency on Electronic ID Manufacture</i>	7
3.2.4.	<i>Duration</i>	7
3.2.5.	<i>Volumes</i>	7
3.2.6.	<i>Hierarchy</i>	8
3.2.6.1.	Hierarchy model	8
3.2.6.2.	Hierarchy description	8
3.2.6.3.	Key Generation	8
3.3.	CERTIFICATE DEFINITION	10
3.3.1.	<i>General</i>	10
3.3.2.	<i>Certificates</i>	10
3.3.2.1.	Certificate profile	10
3.3.2.2.	Certificate Lifecycle	11
3.3.2.3.	Lifetime of the certificates	11
3.4.	CERTIFICATE OPERATIONS	11
3.4.1.	<i>Description</i>	11
3.4.2.	<i>Issuance</i>	11
3.4.2.1.	Overview	11
3.4.2.2.	Serial number	12
3.4.2.3.	Verification of uniqueness of data	12
3.4.2.4.	Status of the certificate after issuing	12
3.4.2.5.	Delivery and acceptance of issued certificates	12
3.4.3.	<i>Suspension and Activation</i>	12
3.4.3.1.	Overview	12
3.4.3.2.	Revocation of suspended certificates	13
3.4.3.3.	Publishing status of suspended certificates	13
3.4.4.	<i>Revocation</i>	13
3.4.4.1.	Overview	13
3.4.4.2.	Publishing status of revoked certificates	13
3.4.5.	<i>Renewal</i>	13
3.5.	PUBLICATION OF CERTIFICATE REVOCATION LISTS (CRL) AND DELTA CRL	14
3.5.1.	<i>Conformity to standards</i>	14

3.5.2.	<i>CRLs, delta CRLs and CA's</i>	14
3.5.3.	<i>Format of the CRL</i>	14
3.5.4.	<i>CRL Issuance frequency</i>	14
3.5.5.	<i>CRL and delta CRL Time-Stamping</i>	14
3.5.6.	<i>CRL and delta CRL publication service</i>	14
3.5.7.	<i>Certificate Revocation lists and service-levels</i>	15
3.6.	ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)	15
3.6.1.	<i>Conformity to standards</i>	15
3.6.2.	<i>Web interface to the OCSP responder</i>	15
3.6.3.	<i>OCSP and service-levels</i>	15
3.7.	ARCHIVING SERVICES	16
3.7.1.	<i>Description Archiving Services</i>	16
3.7.2.	<i>Storage Media and integrity of the Media</i>	16
3.7.3.	<i>Information archived and duration of archive</i>	16
3.7.4.	<i>Retrieval of archived items</i>	17
3.8.	CERTIFICATE LOOKUP SERVICES	17
3.8.1.	<i>Description Certificate Lookup services</i>	17
3.8.2.	<i>Repository format</i>	17
3.8.3.	<i>Duration of information stored in the Repository</i>	17
3.8.4.	<i>Retrieval of certificates</i>	17
3.8.5.	<i>Restriction on use</i>	18
4.	LIST OF FIGURES AND TABLES	18

1. Document control

1.1. Document change control

Last revised version: V2.0

Last revision date: 15/07/2003

Final author: Stefan Wijnen

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 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 industry standards and 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 CA Components, the reader should be aware that other documents exists describing certain topics of the eID project:

- § EID-DEL-004: eID Hierarchy and Certificate Profiles
- § EID-DEL-006: Component Overview
- § EID-DEL-008: Technical Analysis Customer Interface
- § EID-DEL-048: Service Level Agreement
- § EID-DEL-049: Service Level Management
- § R&S-DEL-005: Role and Server Certificate Profiles

2. Executive summary

2.1. What is the purpose of this document

This document gives an overview of the certification services that will be present in the eID project towards the customer.

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

2.2. How is this document organized

This functional analysis will present the proposed technical solution with some references to other documents with more details around a specific domain. Those documents are defined in chapter 1.2.

3. Technical solution – eID Infrastructure

This section outlines the criteria used for the design of the proposed Technical Architecture.

3.1. Deliverables

The Technical Architecture is designed towards delivery of the following certificates with associated services: delivery, publication and maintenance during the pilot phase of authentication- and signature certificates according to the X.509 version 3 norm together with the associated trust-services:

- Delivery of the authentication- and signature certificates for the prototype and the test-cards. (pilot phase only)
- Delivery of the physical connections and integration with the RRN¹. (pilot phase only)
- Delivery of the authentication- and signature certificates.
- Maintaining the life cycle of the certificates.
- Publication of Certification Revocation Lists (CRL) and Delta CRL.
- OCSP services.
- Archiving services.
- Certificate lookup services.

3.2. General

3.2.1. Service Level Agreement

FedICT² has chosen for an availability of 99,0% for the pilot phase and availability of 99,5% for the rollout as the scenario to be executed. All further information in this document will take this scenario into account³.

3.2.2. Infrastructure sharing

The E-ID CA services will be delivered on PKI components shared with existing customers.

¹ RRN: Rijksregister – Registre National

² FedICT: The Federal public service for ICT

³ Further details about the and SLM can be found in EID-DEL-049 Service Level Management

3.2.3. Dependency on Electronic ID Manufacture

The smart card manufacturer is bound to follow the procedures and definitions of the Certificate Authority Operator (certificate issuer) with regards to the format and content of the information-exchange.

3.2.4. Duration

The maintenance of the certificates, publication of CRLs; delta CRLs and OCSP services are guaranteed for 5 years after issuance.

Archived information will be maintained for a maximum of 30 years after expiration date of the certificates with lookup possibilities.

3.2.5. Volumes

The estimated volumes are defined as follows:

- 100.000 certificates with associated trust-services for the pilot.
- 16.000.000 certificates with associated trust-services for the rollout.

These are not upper limits.

3.2.6. Hierarchy

3.2.6.1. Hierarchy model

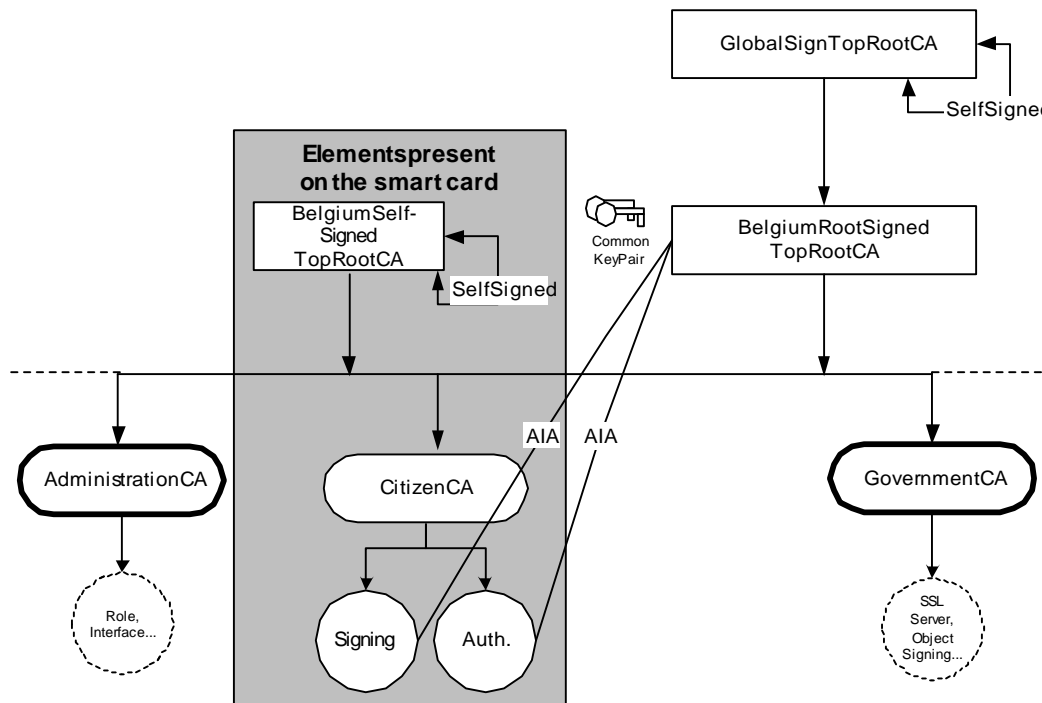


Figure 1: eID CA hierarchy

3.2.6.2. Hierarchy description

The Administration and Government CA are out of the scope of the eID project. Additional resources on these CAs can be found in the role and server project⁴.

3.2.6.3. Key Generation

The root key generation ceremony will take place in adequate manner and environment to ensure the security, confidentiality and integrity of the root keys generated. The procedures and policies are performed under dual control with split knowledge involving members of Ubizen Management and Ubizen staff and include:

- CA Key Generation,

⁴ The exact specifications of the Hierarchy and the entire certificate profiles are defined R&S-DEL-005 Role and Server Certificates Profiles.

- CA Key Release, activation and de-activation,
- CA Key Storage, back-up and recovery,
- End of CA Key lifecycle,
- Interoperability of the Hierarchy

RootSign™ is a solution where GlobalSign certifies the root of an existing CA (or PKI infrastructure) to extend the certification path to GlobalSign's root, which is embedded in most popular browser stores, and therefore facilitates certificate validation of certificates, which are issued by the customer's PKI infrastructure.



Figure 2: Certification Path - the new chain once a CA is RootSigned by GlobalSign

RootSign™ signs the public key of the CA's self-signed root and therefore a transition is established to end the certificate validation chain to GlobalSign's root, which is indeed embedded in most popular browsers. In the hierarchy model outlined in 3.2.6.1 GlobalSign will sign the CA TOP ROOT with its GlobalSign Partner CA root. This means all certificates issued under the Hierarchy will benefit from the RootSign™ solution.

GlobalSign's top root is currently embedded in the following products: Netscape Communicator version 4.6 and higher, Microsoft Internet Explorer version 5.0.1 (June 1999) and higher, Microsoft Windows NT Service Pack 6, Microsoft Windows 98 SR2 and more recent versions of Microsoft Windows, current Opera Browsers, current Mozilla and derivate Browsers. GlobalSign enjoys an 85+% browser market penetration (where the GlobalSign's top root is embedded by default).

In older browser software, the GlobalSign Root CA Certificate can easily be installed. Since GlobalSign has a large installed base, a lot of users will already have done this.

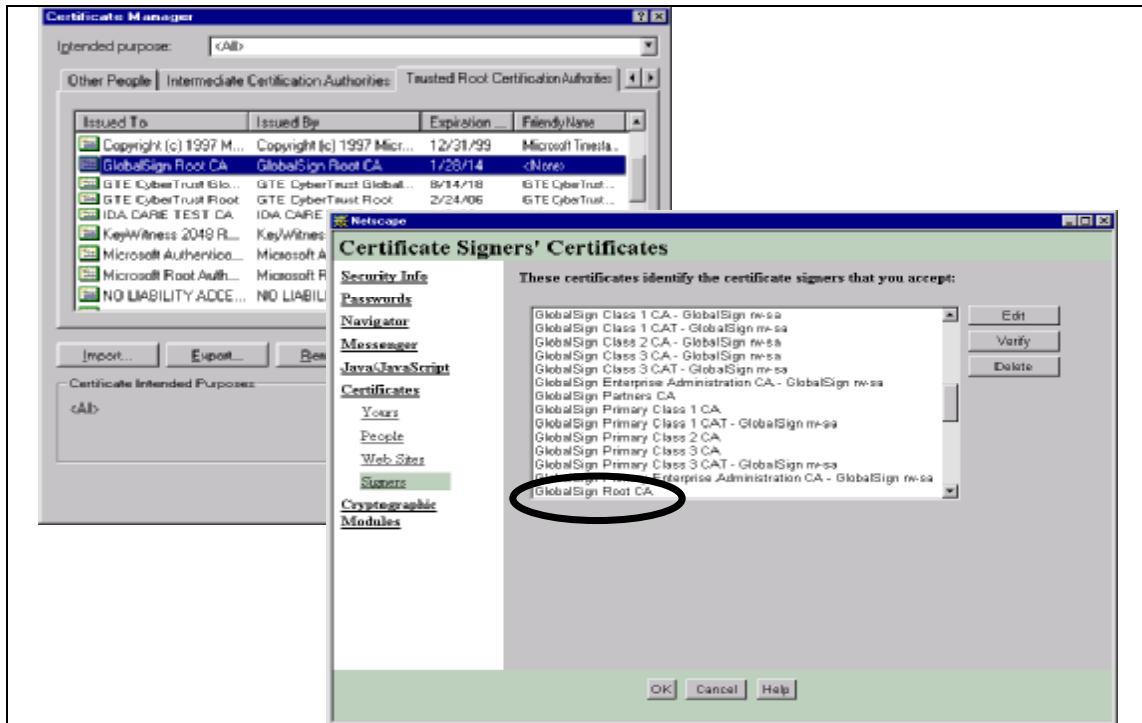


Figure 3: GlobalSign Root CA Certificates in I.E. 5.0 and Netscape 4.7

3.3. Certificate definition

3.3.1. General

The CA operator must deliver the authentication- and signature certificates for each ID card. The delivery of the webserver certificates and object authentication certificates is out of the scope of the eID project⁵.

3.3.2. Certificates

3.3.2.1. Certificate profile

The signature certificates will be technically conform the Qualified Certificate Profile norm – Reference RFC 3039.

⁵ More information on this kind of certificates can be found in R&S-DEL-005 Role and Server certificates profiles.

3.3.2.2. Certificate Lifecycle

The Authentication certificates will have the same life cycle as the signature certificates (e.g. revocation of both certificates will happen through two simultaneous demands within the same XKMS request⁶).

3.3.2.3. Lifetime of the certificates

The commercial lifetime of the certificates is five years. Shorter technical lifetimes are fully supported, with a renewal principle. This could be the case because of security considerations with the length of the RSA keys⁷.

3.4. Certificate operations

3.4.1. Description

The goal of the certificate operations is the maintenance of the lifecycle of the certificates. The management of the certificates during their complete lifecycle comprises:

- Issuance,
- Suspension,
- Reactivation (Unsuspend)
- Revocation,
- Renewal

Besides these operations that directly influence the certificates, 2 other services are provided by the CA operator:

- Status verification (Certificate Status Service) – see chapter 3.6,
- Directory Service – see chapter 3.8.

3.4.2. Issuance

3.4.2.1. Overview

The CA Operator will issue certificates on the request of the RRN. The certificates will only be issued to the RRN, not to any other party.

⁶ All the XKMS and X-BULK commands are specified in EID-DEL-008 Technical Analysis Customer Interface

⁷ The exact lifetime of the certificates is defined in EID-DEL-004 eID Hierarchy and Certificate Profiles.

3.4.2.2. Serial number

The CA Operator expects to receive, next to the certificate-signing request, a unique serial number from the RRN. After verification (see 3.4.2.3), the CA Operator will assign this number to the SerialNumber field in the certificate.

3.4.2.3. Verification of uniqueness of data

The CA will verify the submitted certification data prior to processing for the following validity tests:

- Uniqueness of serial number provided by the RRN
- Completeness and integrity of the data provided by the RRN
- Uniqueness of the subject field of valid certificates within a single certificate profile.

Negative verification of the above will result in an error code to be returned by the XKMS responder within the <processinfo> element, more precisely in a newly defined <reason> element.

Uniqueness of public keys within the PKI a.k.a “Key Clash” verification is performed by the RRN.

The uniqueness of the subject field will be guaranteed by inserting “(Authentication)” or “(Signature)” in the CN of the Citizens certificates.

3.4.2.4. Status of the certificate after issuing

Upon request, the certificate will be immediately suspended at creation. The certificate will only be activated after trigger from the RRN (when the eID card is activated).

3.4.2.5. Delivery and acceptance of issued certificates

The issued certificates will be delivered to the RRN. The RRN confirms the acceptance of the certificate delivered by the CA Operator.

3.4.3. Suspension and Activation.

3.4.3.1. Overview

The CA Operator will suspend certificates at the request of the RRN and will confirm the suspension to the RRN.

3.4.3.2.Revocation of suspended certificates

The CA Operator will automatically revoke certificates that have been suspended for over a week, without intervention of the RRN, except if it concerns the initial suspension (the suspension done at creation of the certificate, see §3.4.2.4). This means that the certificate cannot be activated anymore and the status of the certificate changes from 'Suspended' to 'Revoked'.

The CA Operator will notify the RRN of suspended certificates that are revoked because of this.

3.4.3.3.Publishing status of suspended certificates

GlobalSign will publish the status of suspended certificates in the OCSP service and in subsequent CRLs and/or delta CRLs.

The OCSP response for a suspended certificate will have the status of revoked (status of suspended is not supported in the OCSP standard). In CRLs or delta CRLs the suspended certificate serial number will be published.

3.4.4. Revocation

3.4.4.1.Overview

The CA Operator will revoke certificates at the request of the RRN and will confirm the revocation to the RRN.

3.4.4.2.Publishing status of revoked certificates

The CA Operator will publish the status of revoked certificates in the OCSP service and in subsequent CRLs and/or delta CRLs.

The OCSP response for a revoked certificate will have the status of revoked. In CRLs or delta CRLs the revoked certificate serial number will be published.

3.4.5. Renewal

The CA Operator offers within its public services renewal of certificates. In that context, renewal means re-certification via XKMS.

3.5. Publication of Certificate Revocation Lists (CRL) and delta CRL

3.5.1. Conformity to standards

The CA Operator's CRL engine will use CRL Version 2 structures as defined in RFC 2459 including Delta CRLs.

3.5.2. CRLs, delta CRLs and CA's

The CA Operator will publish CRLs and delta CRLs (where appropriate) for the Citizen CA's involved in the project according to its Key Management Procedures and Key Management Policies.

3.5.3. Format of the CRL

The CRL profile is defined in EID-DEL-004⁸.

The CRLs might be split up to limit the size of a single CRL⁹.

3.5.4. CRL Issuance frequency

The CA Operator will schedule the issuance of CRLs and delta CRLs and will follow the indicated frequency:

- CRL Publishing every 3 hours,
- Delta CRL Publishing every 3 hours, at the same time a CRL is published,
- Base CRL of a delta CRL never older than 14 calendar days.

Publishing happens at fixed time-intervals.

3.5.5. CRL and delta CRL Time-Stamping

All CRLs and delta CRLs are by default time stamped (in accordance with RFC 2459).

3.5.6. CRL and delta CRL publication service

The CA Operator will provide download capabilities of the CRLs and delta CRLs using the following methods:

⁸ EID-DEL-004 eID Hierarchy and Certificate Profiles

⁹ The splitting mechanism has been addressed in EID-DEL-006 Component Overview.

- The CRLs are published in the directory service that can be queried using S-LDAP v3/v2.
- A website within the .be domain will be set up. This website is publicly accessible using HTTP and HTTPS protocols. The website includes:
 - Information about CRL and delta CRLs including possible splitting mechanisms,
 - All CRLs and delta CRLs published during the last year (at least),
 - A simple web-interface to facilitate the downloading of the CRLs and delta CRLs.

Please note that the CA Operator will not offer CRL and Delta CRLs through the FTP protocol because:

- The standard FTP protocol is inherent insecure, especially active FTP sessions. There is no accepted standard (there are several) to access FTP servers over SSL.
- There are scalability and load-balancing issues.

3.5.7. Certificate Revocation lists and service-levels

The time between receipt of the CRL downloading request at the CA Operator local network and the start of the download of the CRL or delta CRL will be less than 10 seconds.

The CA Operator's technical architecture is designed to support the requested monthly unavailability of less than 1% during the pilot phase and 0.5% during the rollout phase of the total number of minutes in the calendar month. This excludes however unavailability of (parts of) the Internet and unavailability of local infrastructure at the service requestor. The CA Operator has taken precautions to minimise possible unavailability of its Internet connection as reflected in the redundant ISP that services it.

3.6. Online Certificate Status Protocol (OCSP)

3.6.1. Conformity to standards

The CA Operator's OCSP responder delivers OCSP answers conform RFC 2560 over both HTTP and HTTPS.

3.6.2. Web interface to the OCSP responder

A simple web-interface will be set up on a web server within the .be domain. The web-interface allows entering a certificate-number after which the status of the certificate is displayed. The web-interface is publicly available.

3.6.3. OCSP and service-levels

The response time to a single OCSP request originating on the CA network will be less than 1 second.

The response time to a single status request through the web interface initiated on the CA network will be less than 5 seconds.

The CA Operator's technical architecture is designed to support the requested monthly unavailability of less than 1% during the pilot phase and 0.5% during the rollout phase of the total number of minutes in the calendar month. This excludes however unavailability of (parts of) the Internet and unavailability of local infrastructure at the service requestor.

3.7. Archiving services

3.7.1. Description Archiving Services

The CA Operator will establish an offline archive procedure to archive the requested information for the requested duration.

3.7.2. Storage Media and integrity of the Media

All information will be archived on DLT tapes. However, the CA Operator reserves the right to change to other storage media in the future as new technology becomes more appropriate.

Data is not necessarily stored in its original form. It might be transformed to a common, simpler format to guarantee retrieval with common tools over a long period of time. However, at all times the content and context of the information will be intact.

All information on the tapes is refreshed every two years. This means that the data is retrieved, verified and refreshed on new tapes. This prevention is taken in order to ensure the integrity of the storage media, guaranteeing successful retrieval with no data loss. The two years gap is in accordance with best practises.

3.7.3. Information archived and duration of archive

The CA Operator will archive at least the following items:

- All certificates for a period of 30 years after expiration. This includes the CA certificates.
- Audit trails for the following items:
 - Issuance of certificates for a period of 30 years after issuance.
 - Revocation of certificates for a period of 30 years after revocation.
- All CRLs and delta CRLs for a period of 30 years after publishing.

The items can be time-stamped if so required.

3.7.4. Retrieval of archived items

Belgacom has based its pricing for the archival retrieval on the following assumptions:

- The archive is stored offline and is only accessible to authorized personnel of the CA Operator or the RRN,
- Only a manual retrieval procedure is required,
- Between the request for retrieval of an item and retrieving the item a window of 1 working day is allowed,
- A maximum of 30 retrieval requests per year.

The exact procedure for request for retrieval will be addressed in a separate document as part of the CA procedures.

3.8. Certificate lookup services

3.8.1. Description Certificate Lookup services

The CA Operator will provide a public repository with all the certificates issued together with a web-front end.

3.8.2. Repository format

All issued certificates, together with the CRLs, will be available on the Repository Server which provides (S)LDAP V3 services conform RFC 2251 and RFC 2830 (Transport Layer Security). The certificates together with the CRLs follow the LDAP scheme outlined in RFC 2587.

3.8.3. Duration of information stored in the Repository

The CA Operator guarantees the availability of the repository during the contract and for an additional 5 years after termination of the contract.

3.8.4. Retrieval of certificates

The interface to the repository is provided via:

- Native LDAP v3 access using the LDAP protocol with optional TLS extensions,

A distinction between authorised access by the RRN and public access to those interfaces will be made:

- Authorised RRN queries will be able to access the repository over both interfaces without restriction. The CA Operator will provide the necessary network- and access- controls to authenticate and authorise the RRN.

- Public access to the repository will be limited to retrieving 10 certificates. The CA Operator will implement the necessary access controls to enforce this.

3.8.5. Restriction on use

We understand it is allowed to restrict public access to the repository:

- To 30 LDAP queries per user per week.

Although this might not be present immediately, we reserve the right to do this at a later stage.

4. List of Figures and Tables

List of Figures

Figure 1:	eID CA hierarchy	8
Figure 2:	Certification Path - the new chain once a CA is RootSigned by GlobalSign	9
Figure 3:	GlobalSign Root CA Certificates in I.E. 5.0 and Netscape 4.7	10