

FEDICT
Federale Overheidsdienst Binnenlandse Zaken
Service Public Fédéral Intérieur

Component Overview

15 July 2003

Ref: EID-DEL-006 v2.0

Certipost
A branch of Belgacom and the Belgian Post group

Table of Contents

1.	DOCUMENT CONTROL	3
1.1.	DOCUMENT CHANGE CONTROL	3
1.2.	REFERENCES	3
2.	EXECUTIVE SUMMARY	4
2.1.	WHAT IS THE PURPOSE OF THIS DOCUMENT	4
2.2.	HOW IS THIS DOCUMENT ORGANIZED	4
3.	XKMS RESPONDER	5
3.1.	SUPPORTED XKMS/X-BULK FEATURES	5
3.2.	FEATURES UNDEFINED IN XKMS/X-BULK STANDARDS	6
3.2.1.	<i>Inclusion of the certificate serial number provided by the RRN</i>	6
3.2.2.	<i>Uniqueness of certificate request</i>	6
3.2.3.	<i>Suspend status</i>	6
3.2.4.	<i>Certificate acceptance</i>	7
4.	BACKEND SERVICES	7
4.1.	SIGNING ENGINE	7
4.1.1.	<i>Certification engine</i>	8
4.1.2.	<i>CRL Engine</i>	8
4.1.3.	<i>OCSP Engine</i>	9
4.2.	CRL PUBLICATION	10
4.3.	CERTIFICATES PUBLICATION AGENT	10
4.4.	CERTIFICATE REVOCATION	10
4.5.	AUTOMATIC REVOCATION AGENT	11
5.	VALIDATION SERVICES	12
5.1.	CRL AND DELTA CRL WEB SERVER	12
5.2.	OCSP	12
5.3.	LDAP DIRECTORY	12
5.3.1.	<i>Information available in LDAP server</i>	12
5.4.	VALIDATION SERVICES ACCESS CONTROL	14
6.	PUBLIC WEB SERVICES	14
6.1.	CA GENERIC INFORMATION	15
6.2.	CERTIFICATE STATUS CHECKING INTERFACE	15
6.3.	CRL AND ΔCRL DOWNLOAD INTERFACE	15
6.4.	PUBLICATION AND MAINTENANCE OF DOCUMENT REPOSITORY	16

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:

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

2. Executive summary

2.1. What is the purpose of this document

This document gives the functional specifications of the components that will be used to offer the services for the eID CA operation.

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 document provides the functional specifications for the XKMS Responder together with usage recommendations in chapter 3. Chapter 4 describes the functionalities of the Backend services. Public web and validation services are described in chapters 5 and 6.

3. XKMS Responder

3.1. Supported XKMS/X-Bulk features

Standard certificates operations are supported by the two parts of the XML Key Management Specification (XKMS): The XML Key Information Service Specification (X-KISS) and the XML Key Registration Service Specification (X-KRSS) as well as The X-Bulk Specification.

Services provided by the responder are:

XKMS Register

- Request
- Suspend
- UnSuspend
- Revoke

X-KISS Locate

- Search function

X-KISS Validate

- Validate function

X-Bulk BulkRegister

- Batch certificate creation

X-Bulk BulkStatus

- Check whether a pending batch is completed or not.

X-Bulk BulkRegister needs to be used for certificate requests. There is a requirement to have dateOfBirth and placeOfBirth as per RFC3039 included in the certificates. As dateOfBirth and placeOfBirth attributes cannot be part of the subject field of a certificate it has, according to X.509 to be set in the subjectDirectoryAttributes extension.

However, the Subject Directory Attributes extension is not supported by XKMS unless included in a PKCS#10 file included in an X-Bulk BulkRegister request.

As only certificates requests making part of the same XKMS X-Bulk Batch are guaranteed to be issued under the same Operational CA, XKMS X-Bulk Batch is mandatory to be used for certificate registration.

The XKMS/X-Bulk compliant messages sent to the CA are signed using a “GlobalSign Enterprise Administration” certificate that will be delivered to the RRN¹ and need to be renewed yearly. These certificates are issued by GlobalSign and are used for authentication/signature for data exchange between the RA and the CA

3.2. Features undefined in XKMS/X-Bulk standards

3.2.1. Inclusion of the certificate serial number provided by the RRN

The XKMS responder will allow inclusion of an external certificate serial number. The certificate serial number is included in the XKMS/X-Bulk request, the CA will use it as specified. If no certificate serial number is present, a number will automatically be allocated by the CA according the allocation scheme of the CA operator.

The external serial number provided by the RNN, shall be a max. 32 digits number in Hexadecimal representation (128 Bits).

3.2.2. Uniqueness of certificate request

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.

3.2.3. Suspend status

New requested certificates can be set in “Suspended” status immediately after issuance, depending on the values specified in the XKMS or X-BULK requests by the RRN.

¹ RRN: Rijksregister – Register National

The certificates in this state can be Activated/Unsuspected through the XKMS-X-Bulk function.

3.2.4. Certificate acceptance

The RRN formats the elements of the certificate requests. The CA does not perform any operation that would modify the data within a request and is entirely relying on the RRN's input for certificate creation. Therefore, all certificates for which a valid request signed by the RRN exists are considered as implicitly accepted.

4. Backend services

The CA database is parsed by agents on regular time intervals in order to execute the tasks requested by the RRN:

- Certification (+/- 1 Sec)
- Publication (Varying from immediate to +/- 1 Sec)
- Revocation (Varying from immediate to CRL issuance frequency)

The time intervals for each task will be defined in a way to achieve the service level agreement requirements.

If flagged records are found, the database information is then processed according to the agent's role: Signing engine creates certificates, CRLs or delta CRLs; newly generated certificates are pushed in the LDAP server; CRLs or delta CRLs are published on the website; etc.

4.1. Signing Engine

An eID dedicated signing engine (SE) instance will be configured for the project. It periodically parses the database for pending certificate requests. If certificate requests are pending, it processes them using built in configuration scripts and posts the corresponding certificates back to the CA database. Citizen CA keys generated during the eID Key Generation Process are required for the CA operation and are loaded in the hardware signing module (HSM) which is bound to the SE according to the Key Management Procedures.

In order to achieve efficient CRL splitting, the system will be designed to have multiple Citizen CA keys running.

The signing engine is implemented in such a way that it supports handling UTF-8 strings for the attributes within the Subject Distinguished Name extension of the end-user certificates.

4.1.1. Certification engine

The Certification engine will parse the CA database for valid pending certificates requests. If requests are found, it will perform the certification using the HSM, based on the certificate profiles. The SE is configured to double check certification requests prior to certificate issuance by using formatting rules as defined in the configuration file (e.g. subject distinguished name fields that are required or optional). In case the submitted request is invalid, the XKMS/X-Bulk responder will return an error message for that entry.

For the eID project, certificate generation is distributed across multiple operational CAs to achieve efficient CRL Splitting. All entering certification requests within the same batch ID will be issued under the same randomly chosen CA.

Dynamic Subject Directory Attributes are only supported if included in the PKCS#10 formatted certificate requests.

4.1.2. CRL Engine

The CRL engine will create Certificate Revocation Lists for revoked end-user certificates at fixed time intervals.

In order to be in compliance with IETF RFC 2459, a new CRL will be issued each time a delta CRL is issued. This in combination with the delta CRLs requirement to be issued every 3 hours, supercedes the requirement that CRLs will be issued each 24 hours. Both a CRL and a delta CRL will be issued for each operational CA every 3 hours.

The CRL engine is compliant with the RFC2459 which specifies in 5.2.4. delta CRL indicator §2: "When a delta-CRL is issued, the CAs MUST also issue a complete CRL." and repeated in §3 "a delta-CRL MUST NOT be issued without a corresponding complete CRL. The value of CRLNumber for both the delta-CRL and the corresponding complete CRL MUST be identical."

The decision to base the delta CRL each time on the previously issued complete CRL was based on the consideration that delta CRL users can have a simplified update mechanism.

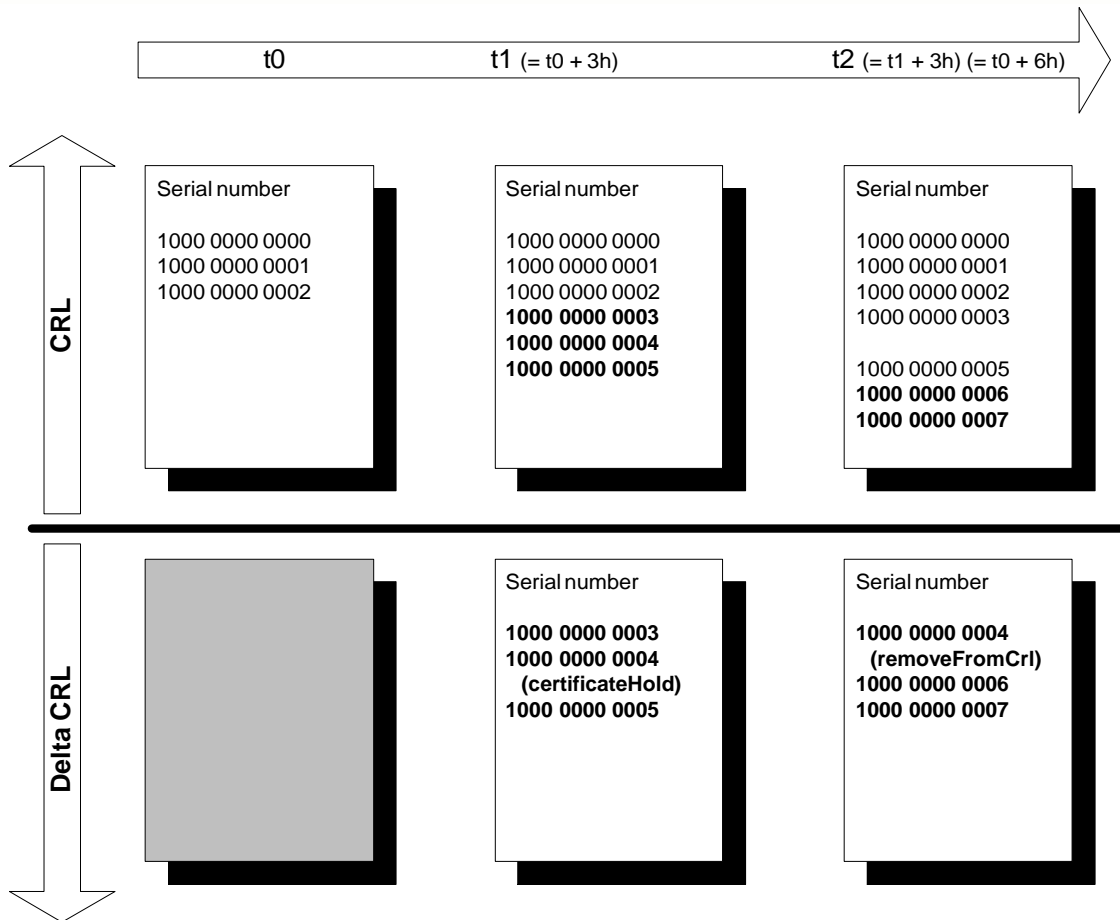
base CRL at time t

+ delta CRL at time t+1 = base CRL at time t+1

+ delta CRL at time t+2 = base CRL at time t+2

etc.

Or as simplified graphical representation:



A newly issued delta CRL will refer to the previously issued CRL (T-3h).

CRLs and delta CRLs will be generated in binary format as it is the de facto best accepted format by popular applications. Base 64 format will thus not be available. The suspended certificates (including those suspended upon issuance) are indicated as a revoked certificate in the CRL with a CRLReason entry "certificateHold (6)". Revoked certificates are indicated as revoked without CRLReason.

In order to avoid inconsistency of CRLs rebuilt from ΔCRLs, certificates that have been placed on hold (Suspended) and then released from hold (un-suspended) will be listed in the delta CRL with as revocation reason removeFromCRL. The concept of suspended certificates is represented by certificate nr 1000 0000 0004 in the graphical representation.

4.1.3. OCSP Engine

The OCSP engine submits OCSP replies to the HSM for signing.

Since a shared infrastructure is used, a shared self-signed OCSP root key (2048 bits) will be used to perform this task.

This self-signed key can however be cross-certified by the eID hierarchy. The corresponding X.509 certificate chain will be returned within the OCSP answer. The returned chain will then start from the OCSP responder certificate up to the CA that signed the validated certificate.

4.2. CRL Publication

A database job will check on a regular basis if a new CRL or delta CRL is issued. In case a new CRL or delta CRL is available in the CA Database it will extract CRL and delta CRL and publish it to the public server location(s) that will be available through HTTP protocol. The CA operator reserves the right to push CRLs and delta CRLs to multiple web servers to allow load distribution.

The CRLs and delta CRLs will be pushed to the CA local LDAP server.

The CRL Publication engine will send a notification email to the following mailing list each time a new CRL or delta CRL is published.

4.3. Certificates publication agent

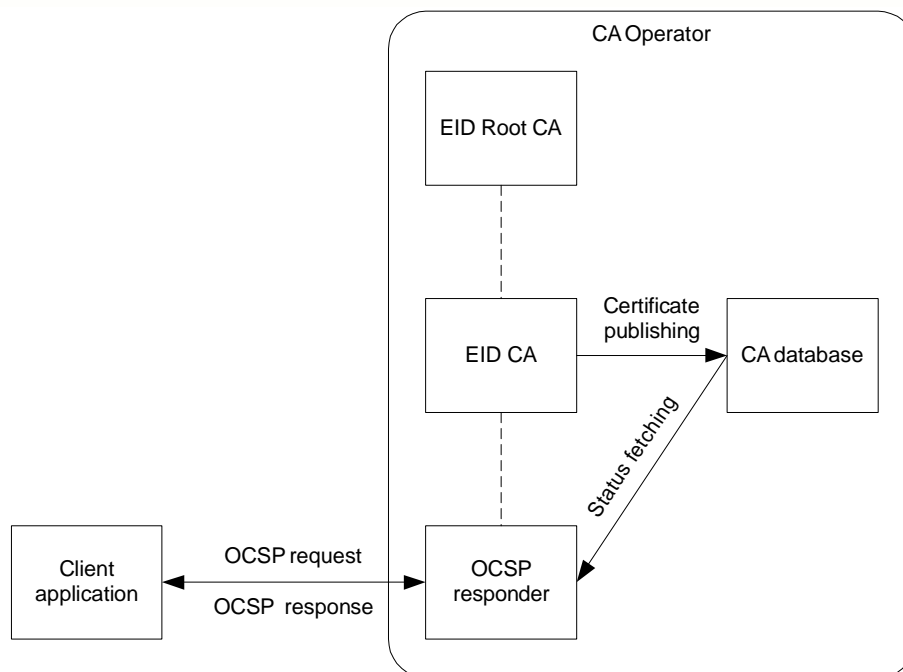
The certificate publication agent supports publication to LDAP servers using LDAP V2 commands.

Certificates are posted directly from the LDAP agents triggered by new issuance. The certificates status changes are reflected in the LDAP in such a way that only valid certificates are available. eID CA Certificates will be manually inserted in the LDAP server.

4.4. Certificate revocation

Upon certificate revocation, the CA database is immediately updated to reflect the exact status.

As there is a direct connection between the OCSP responder and the database, certificates status changes in the database are immediately reflected in OCSP answers. The online validation services OCSP and web validation interface will thus immediately return the updated certificate status.



There will be a gap between the time a certificate is set as revoked in the CA database and the time it is reflected in the corresponding CRL or delta CRL.

4.5. Automatic revocation agent

A database agent will parse the CA database on a regular basis. When it encounters certificates that have been set to suspended state for more than the grace period of one week, it will automatically set their status to 'Revoked'.

The automatic revocation agent will ignore certificates that have been suspended at issuance time and which have not yet been activated. This is done to ensure that certificates are not automatically revoked in the time lapse between the certificate issuance and activation of the Citizen's eID card.

The CA will send a notification email containing the list of automatically revoked certificates serial numbers to a mailing list.

5. Validation Services

5.1. CRL and delta CRL web server

The CRL web server is a logical entity of the secure web servers and hosts the most recent Certificates Revocations Lists (CRLs) generated by the CA agent. The CRL distribution points set in the certificate are referring to this server. Relying parties can download updated CRLs and delta CRLs from this location. The CRL download interface will point to this location for the download of the last issued CRLs and delta CRLs.

The download of the last issued CRLs and delta CRLs from the web server are subject to SLA.

5.2. OCSP

The OCSP responder is implemented as per IETF RFC2560, is OCSP V1 compliant.

Suspended certificates will be marked as revoked in the reply since the "Suspended" status is currently not supported by OCSP.

Summarized, the following OCSP responses are possible:

Good	if the certificate is issued by the CA and if the certificate is valid
Revoked	if the certificate is issued by the CA and the status of the certificate is revoked or the certificate is suspended
Unknown	if the certificate is not issued by the CA

5.3. LDAP Directory

The Government branch in the CA Operator's shared LDAP server gets the newly issued certificates pushed by the certificate publication agent and makes them available to the world through a permanent internet connection. The shared LDAP server supports LDAP V2 and LDAP V3 commands.

5.3.1. Information available in LDAP server

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.

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.

As addressed in 6.2, the LDAP will also contain CRL and Δ CRLs.

To connect to the LDAP server the following settings should be used:

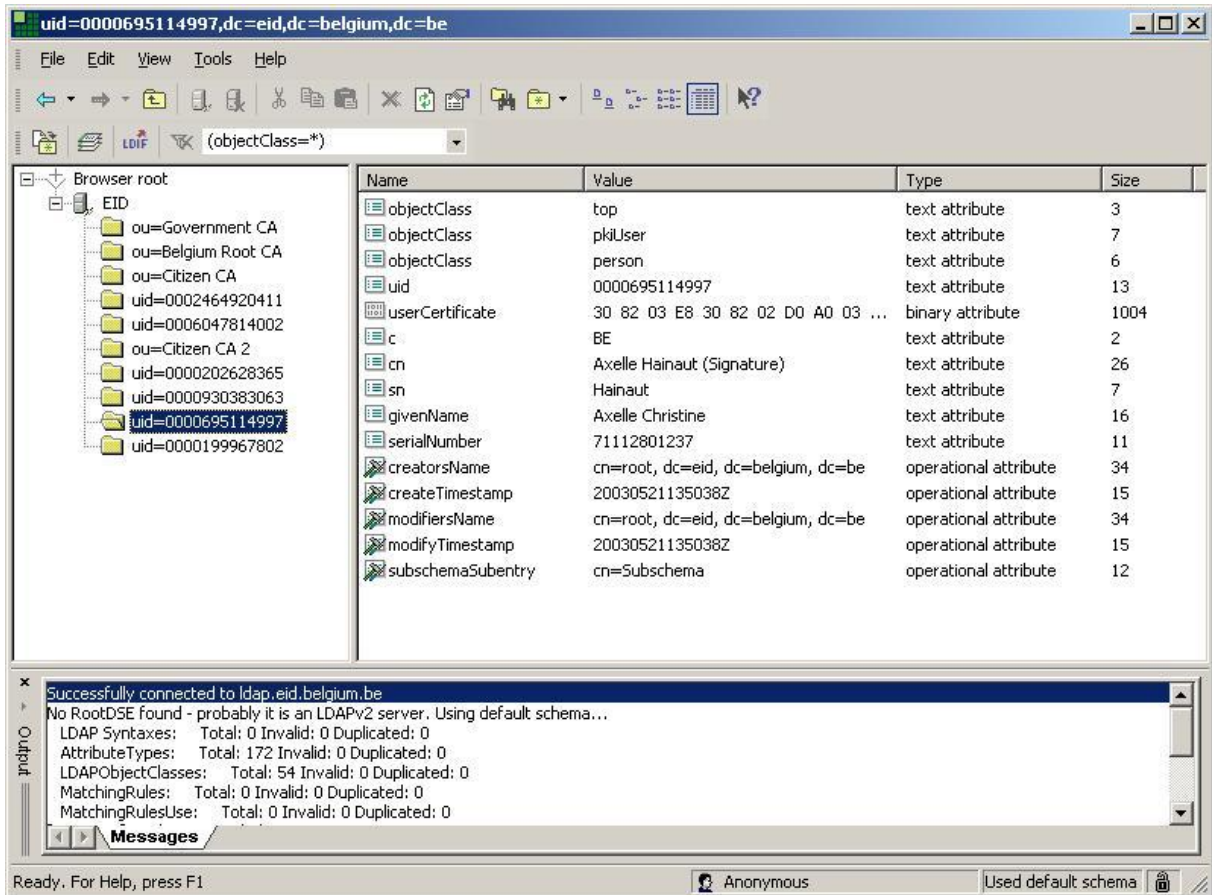
- Host: ldap.eid.belgium.be
- Port: 389
- Base: dc=eid, dc=belgium, dc=be
- Binding: anonymous
- Protocol: LDAP v2

The screenshot shows an LDAP browser window with the following details:

- Address Bar:** ldap://ldap.eid.belgium.be:389/dc=eid,dc=belgium,dc=be??base??(objectClass=*)
- Directory Tree:**
 - Browser root
 - EID
 - ou=Government CA
 - ou=Belgium Root CA
 - ou=Citizen CA
 - uid=0002464920411
 - uid=0006047814002
 - ou=Citizen CA 2
 - uid=0000202628365
 - uid=0000930383063
 - uid=0000695114997
 - uid=0000199967802

- Table of Attributes:**

Name	Value	Type	Size
ou	Government CA	entry	1942
ou	Belgium Root CA	entry	958
ou	Citizen CA	entry	4385
uid	0002464920411	entry	1022
uid	0006047814002	entry	845
ou	Citizen CA 2	entry	109804
uid	0000202628365	entry	1079
uid	0000930383063	entry	1103
uid	0000695114997	entry	1095
uid	0000199967802	entry	1079
o	Belgium	text attribute	7
objectClass	organization	text attribute	12
creatorsName	cn=root, dc=eid, dc=belgium, dc=be	operational attribute	34
createTimestamp	20030307182324Z	operational attribute	15
modifiersName	cn=root, dc=eid, dc=belgium, dc=be	operational attribute	34
modifyTimestamp	20030307182324Z	operational attribute	15
subschemaSubentry	cn=Subschema	operational attribute	12
- Messages:**
- Successfully connected to ldap.eid.belgium.be
- No RootDSE found - probably it is an LDAPv2 server. Using default schema...
- LDAP Syntaxes: Total: 0 Invalid: 0 Duplicated: 0
- AttributeTypes: Total: 172 Invalid: 0 Duplicated: 0
- LDAPObjectClasses: Total: 54 Invalid: 0 Duplicated: 0
- MatchingRules: Total: 0 Invalid: 0 Duplicated: 0
- MatchingRulesUse: Total: 0 Invalid: 0 Duplicated: 0
- Status Bar:** Ready. For Help, press F1 | Anonymous | Used default schema



5.4. Validation services access control

The results returned by the LDAP server are limited to 10 entries.

Only the RRN can issue general queries on the certificate repository using a username/password authentication schema.

The CA operator takes note of their rights to limit access to the validation services. It has however been chosen not to limit access to the validation services during the initial phase of the project. It could however be done in a later stage.

6. Public Web Services

A secure web server will host the certificate validation, CRL and delta CRL download interfaces. It will also give the ability to access CA specific information such as CP and CPS. It will be configured with SSL capabilities.

The web application will be compatible with Internet explorer 5.01 as well as with above and Netscape 4.5 and above. The domain names are resolved by FedICT.

6.1. CA generic information

A section of the web site will allow parties involved in the PKI to retrieve CA specific information. It includes:

- Publication of maintenance window
- Explanation about the way to obtain all CRL information including possible splitting mechanisms
- A hyperlink to external resources (not hosted by the CA Operator)

6.2. Certificate status checking interface

A certificate status checking application will be implemented. It will consist in a web forms allowing a relying party to enter a certificate serial number in a web form and get page with a "Valid Certificate" or "Invalid Certificate" message in return.

Other search criteria such as National Registry Number and First/Last name are not foreseen.

The query result will be returned under SSL/TLS connection to authenticate information source.

6.3. CRL and Δ CRL download interface

A simple web interface will be implemented in order to allow relying parties to download current CRLs and delta CRLs and previous up to one year in the past.

The web based application will ask the user to submit a form containing:

- Certificate serial number of the certificate for which the user wants to download the CRL (In order to determine which CA issued it)
- Desired date of the CRL. This is optional

On submit, the application will determine the CA under which the certificate has been issued, extract the corresponding CRL and delta CRLs from the database and provide him with hyperlinks for download.

Only the download of last issued CRLs for every operational CA is subject to SLA. As retrieval of archived CRLs is delivered as a data retrieval service, it is not covered by an SLA.

6.4. Publication and maintenance of document repository

The CA is responsible of maintaining its document repository. CP, CPS and other CA related documents will be published on the public web server. These documents will be made available on the public website within 24 hours after release (<http://repository.eid.belgium.be>).

The CA certificates can be downloaded at <http://certs.eid.belgium.be>