CREDOC
SERVICES

Certification Authority

Policy & Practice Statement

Document Approval

IT MGR	**SPONSOR BUSINESS**	**CHIEF SECURITY OFFICER**	**LEGAL DEPT**
NAME: PIETER BOONE **DATE:**	**NAME: PH.SIX** **DATE:**	**NAME: PASCALE VAN OVERMEIR** **DATE:**	**NAME:** **DATE:**
SIGNATURE:	**SIGNATURE:**	**SIGNATURE:**	**SIGNATURE:**

Document Identification

DOCUMENT N° SOA	CA CPS&CP	**REVISION**	VERSION 1.0
DEPARTMENT	*IT*	**DOCUMENT TYPE**	SERVICE MGT
AUTHOR		**CREATION DATE**	03 SEPTEMBER 2007
CHECKED BY	*IT-MGR / CA ADMIN*	**PRINT DATE**	17 JANUARY 2008

Document History

Date	Author	Revision	Description of Change

Related Documents

Document Number	Document Type	Title	Stored

Contact

Department	Contact Person	Tel. / Mobile	E-mail
BUSINESS			
MGT			
IT			

CREDOC
Bergstraat - Rue de la Montagne 30-32
B - 1000 Brussel - Bruxelles
België - Belgique

Author:
Office:
Telephone: **+32 (0)2 / 505.08.11**
E-mail:

Table of Contents

1. INTRODUCTION

1.1. OVERVIEW

This document describes the set of rules and operational practices used by Credoc-CA, the Certification Authority for the Koninkelijke Federatie van het Belgische Notariaat - Fédération Royale du Notariat belge (FRNB) [1] for issuing certificates. This document is based on the structure suggested by the RFC 2527 [2].

Certification Practice Statement (CPS) details rules of certification practice stated in certification policy (CP) and describes the process of public key certification and the applicability range of the certificates resulting from this certification. The nature, aim, and role of certification practice statement is particularly important from the point of view of a subscriber and a relying party.

CP - Certification Policy - describes general rules of certification practice, defines certification parties, their responsibilities and obligations, types of certificates, authentication procedures and applicability range. Certification policy states what level of trust can be applied to a given type of a certificate by Credoc. CPS describes how Credoc secures the level of trust by the policy.

CPS describes a set of four main and several additional certification policies applied by Credoc to issuance of certificates to authorities and end-users. These policies represent different levels of credibility corresponding to public key certificates. The applicability ranges of certificates issued in compliance with the policies might be the same. However, responsibility of a certification authority and certificate users is different.

CPS was created, assuming the reader is generally familiar with the notions concerning certificates, electronic signature and public key infrastructure.

1.1.1. General Definitions

Activation Data
Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase)

CA - Certification Authority
An authority trusted by one or more users to create and assign public key certificates.

Certificates - or Public Key Certificates
A data structure containing the public key of an end entity and some other information, which is digitally signed with the private key of the CA which issued it.

CP - Certificate Policy

A named set of rules that indicates the applicability of a certificate to a particular community and /or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

CPS - Certification Practice Statement
A statement of the practices which a certification authority employs in issuing certificates.
CRL - Certificate Revocation Lists
A CRL is a time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.

CSO – Chief Security Officer

PKI - Public Key Infrastructure
A term generally used to describe the laws, policies, standards, and software that regulate or manipulate certificates and public and private keys. All of this implies a set of standards for applications that use encryption.

Policy Qualifier
Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

RA - Registration Authority
An entity that is responsible for identification and authentication of certificate subjects, but does not sign or issue certificates.

RbR Not – azerty
DataBase with all relevant data of Belgium Notary

Relying Party
A holder of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

Subscriber
For certificates issued to individuals, same as certificate subject. In the case of certificates issued to resources (such as web servers), the person responsible for the certificate for that resource.

Remark:
Within this document the words „MUST", „MUST NOT", „REQUIRED", „SHALL", SHALL NOT", „SHOULD", „SHOULD NOT", „RECOMMENDED", „MAY", „OPTIONAL" are to be interpreted as in RFC 2119 [3].

1.2. IDENTIFICATION

- Title: Credoc-CA Certificate Policy (CP) and Certification Practice Statement (CPS).
- Version: 0.0
- Date: 09.06.2007
- OID assigned: 1.3.6.1.4.1.2614.5548.1.1.1.3
- Expiration: This document is valid until further notice, or next version.

1.3. COMMUNITY AND APPLICABILITY

Credoc-CA provides PKI services for Koninklijke Federatie van het Belgische Notariaat - Fédération Royale du Notariat belge (FRNB) in general [for the Belgian Notaries and notarian employees]

1.3.1. Certification Authorities

Credoc-CA doesn't issue certificates to subordinate – understand : external partner or party - Certification Authorities at this time.

1.3.2. Registration Authorities (RA)

The Credoc-CA also performs the role of a RA.
RA can also be performed by Belgian Notaries by means of 'e-notariaat' / 'e-notariat' web portal.
Strong identification & authentification is always required, by means of the Real card, as stated in the policies of Credoc.

1.3.3. End entities

The Credoc-CA issues certificates for people, hosts and host applications/services involved in the notarial entities, also known as 'études' for test purposes and business/'production'.

1.3.4. Applicability

The issued certificate types and suitability are as follows:

- Personnel,
- Server and
- Application certificates: authentication and communication

encryption.

1.3.5. User Restrictions

Certificates issued by the Credoc-CA are only valid in the context of the KFBN – FRNB notarian applications, and communication with e-notariaat / e-notariat web portal and applications and communications enabled by this web portal (i.e. governmental authorities). Any other usage including financial transactions is strictly forbidden without written approval of Credoc.
The ownership of a Credoc-certificate does not imply automatic access to any kind of computing resources.

1.4. CONTACT DETAILS

The Credoc-CA is managed by management of Credoc Services cvba-scrl (Brussels).
The contact person for questions related to this document or Credoc-CA in general is:

Credoc Services cvba – scrl
CSO PKI
Bergstraat - Rue de la Montagne 30-34
1000 - Brussels
Belgium

Phone:	(+ 32) (0)5050840
Fax:	(+ 32) (0)5050855
E-Mail:	Credoc_CA@credoc.be

2. GENERAL PROVISIONS

2.1. OBLIGATIONS

2.1.1. CA Obligations

Credoc–CA is solely responsible for the issuance and management of certificates referencing this document.

Credoc-CA will:

- handle certificate requests and issue new certificates:
  - issue certificates based on validated requests
  - accept certification requests validated by the RA
  - deliver the certificate to end entity
  - notify end entities three and one week in advance that the certificate is going to expire
- handle certificate revocation requests and certificate revocation:
  - accept revocation requests from RA's or end entities
  - issue and publish Certificate Revocation Lists (CRLs) according to the rules described in this document

2.1.2. RA Obligations

RA’s must sign an agreement to adhere to the procedures described in this document

Authorised RA's will:

- authenticate entities requesting a certificate according to the procedures described in this document
- determine if the person has the right to have a Credoc-CA certificate
- submit validated, signed certificate requests to Credoc-CA
- create and submit validated revocation requests to the Credoc-CA
- follow the policies and procedures described in this document

2.1.3. Subscriber Obligations

In requesting a certificate, subscribers agree to:

- read and accept the policies and procedures published in this document
- only to provide true and accurate information to Credoc–CA, and only such information as he/she is entitled to submit for the purpose of this document;
- use the certificate exclusively for authorized and legal purposes, consistent with this document;
- by using the authentification procedures described in this document subscribers accept restrictions to liability described in section 2.2:
- by using the authentification procedures described in this document describers accept the statements relating to confidentiality of information in section 2.8;
- generate a key pair using a trustworthy method
- keep the private key safe and protected
- use a strong passphrase to protect the private key

- notify the Credoc-CA/RA:
  - in case of possible private key compromise, key destruction or loss
  - when the certificate is no longer required
  - when the information in the certificate becomes wrong or inaccurate

2.1.4. *Relying Party Obligations*

In using a certificate issued by Credoc–CA relying parties agree to:

- read and accept the policies and procedures published in this document
- use the certificate exclusively for authorized and legal purposes, consistent with this document;
- see paragraph 4.4.9 on CRL checking requirements for relying parties
- use the certificates for permitted purposes only, as defined in this document;

2.1.5. *Repository Obligations*

Credoc–CA maintains an online accessible repository of certificate revocation information. The repository is operated at a 'best – effort' basis, where the intended availability is continuous.

Credoc-CA will publish all information described in section 2.6.1 on its web server
http://pki.credoc.be/

2.2. LIABILITY

2.2.1. *CA Liability*

Credoc-CA:

- guarantees only to control the identity of the subjects requesting a certificate or revocation request according to the procedures described in this document; no other liability, neither implicit nor explicit is accepted
- is run on a best effort basis and does not give any guarantees about the service security or suitability
- will not be held liable for any problems arising from its operation or use made of certificates it issues
- denies any financial or any other kind of responsibilities for damages or impairments resulting from its operation. Credoc accepts no liability for or in connection with the certification services and the parties using or relying on them shall hold Credoc Services cvba-scrl free and harmless from liability resulting from such use or reliance.

2.2.2. *RA Liability*

Section 2.2.1 applies mutatis mutandis to the liability of the RA

2.3. FINANCIAL RESPONSIBILITY

No financial responsibility is accepted.
See section 2.2 Liability.

2.4. Interpretation and Enforcement

This document must be treated according to Belgian law and Belgian Law on Third Services Providers [Wet tot vaststelling van een juridisch kader voor sommige verleners van vertrouwensdiensten, 15 mei 2007]. Legal disputes arising from the operation of the Credoc-CA will be treated according to Belgian Law.

Credoc–CA shall be entitled to terminate the certification services at any time. The Credoc–CA will make all reasonable efforts to notify all its subscribers, and any relying parties known to Credoc Services to be currently and actively relying on certificates issued by the Credoc CA on such termination. All certificates issued by the Credoc CA that reference this document will be revoked not later than the time of termination

Credoc CSO resolves all disputes related to interpretation and enforcement of conditions and rules described in this document.

2.5. Fees

To be defined in accordance with the Credoc executive management

2.5.1. *Certificate issuance or renewal fees*

See section 2.5.

2.5.2. *Certificate access fees*

See section 2.5.

2.5.3. *Revocation or status information access fees*

See section 2.5.

2.5.4. *Fees for other services such as policy information*

See section 2.5.

2.5.5. *Refund policy*

See section 2.5.

2.6. Publication and Repositories

2.6.1. *Publication of CA Information*

Credoc-CA publishes the following information through its secure online repository:

- the Credoc-CA certificate
- the latest CRL signed by the Credoc CA;
- a copy of this document and copies of all previous documents
- other relevant information (i.e. user guide explaining how RA should approve certificate requests))

2.6.2. Frequency of Publication

New information will be published as soon as available.
CRLs will be published as soon as issued and at least every month.
New versions of this document are published as soon as they have been approved.

2.6.3. Access Controls

Credoc-CA does imposes strong access control restrictions to the information available at its web site, but which excludes the CA certificate, latest CRL and a copy of this document containing the CP and CPS.

The Credoc-CA web site is maintained in a best effort basis. Excluding maintenance shutdowns and unforeseen failures the site should be available on a 24 hours per day, 7 days per week basis. Credoc-CA may impose a more restricted access control policy to the repository at its discretion.

2.6.4. Repositories

The Credoc-CA online repository, which contains all information specified in 2.6.1, is available at :

http://pki.credoc.be/

2.7. Compliance Audit

The Credoc-CA may be audited by other trusted CA's , or any other internationally recognised auditor to verify its compliance with the rules and procedures specified in this document. Any costs associated to such an audit must be covered by the requesting party.

2.7.1. Frequency of entity compliance audit

No stipulation.

2.7.2. Identity/qualifications of auditor

No stipulation.

2.7.3. Auditor's relationship to audited party

No stipulation.

2.7.4. Topics covered by audit

No stipulation.

2.7.5. Actions taken as a result of deficiency

No stipulation.

2.7.6. Communication of results

No stipulation.

2.8. Confidentiality

Credoc-CA collects personal information about the subscribers (e.g. full name, notarial office organisation, telephone number, e-mail-address and in case of a RA a copy of the handwritten signature, or electronic signature). These data will be protected according to the Belgian Law on Privacy, and FRNB-KFBN Policies.

2.8.1. Types of information to be kept confidential

All information about subscribers that is not present in the certificate and CRL is considered confidential and will not be released outside.
Under no circumstances does the Credoc CA have access to the private keys of any subscriber to whom it issues a certificate.

2.8.2. Types of information not considered to be confidential

Information included in issued certificates and CRLs (Full Name, email-address, notary office) issued by the Credoc-CA is not considered confidential.

2.8.3. Disclosure of certificate revocation/suspension information

If a certificate has to be revoked because of private-key-compromise Credoc-CA may notify:

- the person holding the certificate (person or host or service)
- known relying parties
-

no information about the reason for a revocation is published

2.8.4. Release to law enforcement officials

In case of law enforcement, officials will be allowed to inspect the collected personal information after exhibition of regular warrant. Otherwise , see section 2.8.2

2.8.5. Release as part of civil discovery

In case of civil discovery, personal information will not be revealed. Otherwise , see section 2.8.2

2.8.6. Disclosure upon owner's request

Personal information will be revealed upon owner's request. Otherwise , see section 2.8.1

2.8.7. Other information release circumstances

Information about the holder of a certificate may be released to site-managers of relying parties under certain circumstances. In each case the holder of the certificate has to give his/her accordance. Otherwise , see section 2.8.2

2.9. INTELLECTUAL PROPERTY RIGHTS

This document is based on the following sources:

- RFC 2527 [2]
- ETSI TS 101 456 v1.4.1. (2006 – 1)

- Belgian Law on Trusted Third Services Providers [Wet tot vaststelling van een juridisch kader voor sommige verleners van vertrouwensdiensten, 15 mei 2007]
- Belgian Law on Privacy [Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens Gecoördineerde versie, zoals laatst gewijzigd door de wet van 11 december 1998, B.S., 3 februari 1999]

Besides, the sources of intellectual property rights , this document is also linked with the Credoc Services ' "Information Security Policy"[QMS # 1.1.1.0.1.5], applicable throughout the organisation.

The Credoc Services cvba – scrl -CA claims no intellectual property rights on issued certificates, practice/policy specifications, names or keys.

3. IDENTIFICATION AND AUTHENTICATION

3.1. INITIAL REGISTRATION

3.1.1. Types of Names

To each entity the Credoc-CA assigns a Distinguished Name (DN, X.500) that identifies each entity uniquely. The DN is inserted in the subject field of the issued certificate to bind the entity to the certificate. The DN must be a non-empty printable string.
Following naming attributes may be used in entities' DN. See also 7.1.4

E =<notary email>
CN=<notary name>
OU=<IT provider name> Server
T =Office Server
S = <RbRNot Office ID>
O =<notary office name>
C =BE

Key usage:
Digital signature, key encipherment, data encipherment, key agreement

AIA:
http://pki.credoc.be/kfbn-frnbIssuingCAClassA.crt

3.1.1.1. Country

- Necessity: Mandatory
- Comment
  - For personal certificates, this is the country of residence of the subscriber.
  - For server/application certificates, it is the country where the server/application is located.

3.1.1.2. Organisation

- Necessity: Mandatory

- Comment:
  - For personal certificates and server/application certificates the name of the Organization is "Notary_Office_name" (i.e.“etude”).

3.1.1.3. Organizational Unit

- Necessity: Mandatory
- Comment:
  - For personal certificates, this is the official name of the notary or notary employee (employing the subscriber).
  - For server/application certificates, it is a “etude” code (reference name in RBR not) of the notarial unit or notarial office running the server/application.

3.1.1.4. State (locality)

- Necessity: Mandatory
- Comment:
  - is the official identification of the notary office in the RBR Not database of the “Chambre nationale des notaires Belge”

3.1.1.5. Name (Common Name)

- Necessity: Mandatory
- Comment:
  - For personal certificates it is the first name followed by the surname as presented in the RBR Not database of the “Chambre nationale des notaires Belge” - “Nationale Kamer van Belgische Notarissen” belongs to.
  - For application certificates it is the fully qualified hostname where the application is running prefixed with the name of the application „service/“.

3.1.2. Need for names to be meaningful

The Subject Name in a certificate must have a reasonable association with the authenticated name of the subscriber.

- For a user certificate, the CN must include the full name of the subscriber, as registered into Credoc Services RBR Not db.
- For server and host certificates, the OU, must be formed from the fully qualified domain name registered in Credoc Services database. In this case it can be an alias.
- For a service certificate, the CN must be related to the type of service the certificate is identifying.

3.1.3. Rules for interpreting various name forms

See Section 3.1.1 and 3.1.2

3.1.4. Uniqueness of Names

The distinguished name for each certificate must be unique. In case of real subject name duplication, additional numbers and/or letters will be appended to the distinguished name to guarantee uniqueness.
Certificates must apply to unique individuals or resources (servers).

IMPORTANT
Users must, nor other resources (servers) not share certificates.
In case of multiple servers in an office, multiple certificates requests should be installed.

3.1.5. Name claim dispute resolution procedure

Name claim disputes will be solved by the Credoc–CA

3.1.6. Recognition, authentication and role of trademarks

No stipulation

3.1.7. Method to Prove Possession of Private Key

Credoc-CA is currently not proving the possession of the private key relating to certificate requests.
In fact, Credoc CA has installed procedures to delete all created private keys.

3.1.8. Authentication of Notary Identity

Credoc-CA/RA verifies the identity of Notary (also RA) by checking:

- that the Notary is known to be part of the RBR Not or Notarian community.

3.1.9. Authentication of Individual Identity

Authorised RA (if not Credoc Services cvba-scrl) are verifying the identity of a person by
- personal contact checking the identity card, comparing photograph and registering the number of the identity piece or keeping a copy of the identity card [procedures is also known as : ‘Face to Face” identification]
- if the RA is located at a distant organization there are two different options:
    - the RA keeps a copy of the identity card and sends the request per email to Credoc-CA/RA signed with his/her personal certificate; or
    - the RA sends the copy of the identity card, manually signed per post to the Credoc-CA/RA.

  IMPORTANT:
  If any doubts exist that the copy couldn't be correct the Credoc-RA can contact the RA of the notary office to get some further proof. The Credoc-RA then calls the requestor, using the indicated (-pre-registered-) telephone number (it must belong to the notary office or database with authentification source data range of the assigned notary office and must not be a private number of the individual). During the call, the ‘question and answer’ procedure can be used, to un-questionably identification of the Notary (RA).

For natural persons the subject name must be conforming to the name in the identity card.

In case the entity to be certified is a machine or a service the person in charge – Notary of the notarian office - has to fulfil the process defined in the section above and give prove that he/she is adequately authorised.

The Credoc-RA shall record the issuance of each certificate, containing:

- the identity of the person performing the identification
- the number and type of the identity card or the number of the copy of the identity card which corresponds to the serial number of the certificate.
- whether the contact was personal or by post and phone
- the date and time of the verification or in case any reasons why the verification failed
- the name of the RA which signed the copy of the identity card or the electronic request.

3.2. Routine Rekey

Rekey before expiration can be accomplished by submitting a rekey request based on a new public key. It will be checked with the distant RA if the requestor has still the right to receive a certificate. Rekey after expiration follows the same authentication procedure as for a new certificate.

3.3. Rekey After Revocation

Rekey after revocation follows the same rules as an initial registration.

3.4. Revocation Request

Certificate revocation requests should be submitted by written form signed manually, submitting a request via ‘e-notariaat’ web portal, or Email
sent to:
Credoc_CA@credoc.be

signed with a valid Credoc-CA certificate.
The CA inspects the signature electronically or based on the declaration of identity mentioned in 3.1.9

4. OPERATIONAL REQUIREMENTS

4.1. Certification Application

The minimum key length for all certificates is 2048 bits. The default validity period is 3 years.
Certificate requests are sent by e-mail to Credoc_CA@credoc.be, or submit by use of ‘e-notariaat’-web portal.
Depending on if the requester is a person or a machine or a service the procedures outlined in 3.1.9 are applied.

IMPORTANT:
Non-conforming requests won't be accepted.

4.1.1. Host or Service certificate

Host or service certificate requests must be submitted to the appropriate RA by email.

1. print out Pdf template [website http:///pki.credoc.be] and fill out the requested information. Send the documents by fax [02/ 609 76 68] or send it by mail to CSO PKI , Bergstraat 30-34 , B-1000 BRUSSEL; or

2. send the documents by , electronically signed, e-mail [using notary qualified certificate , i.e. Real smart card]

Credoc CA creates the private key, and guarantees the secure management within the whole CA creation procedure. The Credoc CA provides help for users in the creation of requests with appropriate contents and format on its web site.

4.2. CERTIFICATE ISSUANCE

Credoc-CA issues the certificate if, and only if, the authentication of the subject is successful according to 3.1.9.
Credoc CA guarantees the secure delivery of the certificates to the end-user' or RA-notary.

4.3. CERTIFICATE ACCEPTANCE

Not defined.

4.4. CERTIFICATE SUSPENSION AND REVOCATION

4.4.1. Circumstances for Revocation

A certificate will be revoked in the following circumstances:

- the subscriber's private key has been lost or is suspected to be compromised
- the information in the certificate is wrong or inaccurate
- the subject has failed to comply with the rules in this policy
- the subscriber no longer needs the certificate to access relying parties' resources
- the system to which the certificate has been issued has been retired
- the notary ends profession, or associates with other notary (- office];

4.4.2. Who can request revocation

The revocation of the certificate can be requested by:

- the certificate subscriber or in case of host/application certificates each person which is responsible for the host/service.
- any other entity presenting proof of knowledge of the private key compromise or of the modification of the subscriber's data or relation with Credoc-CA
- Credoc -CA/RA

4.4.3. Procedure for Revocation Request

The entity requesting the certificate must send the revocation request by signed e-mail to the Credoc -CA/RA. If this is not possible the CA/RA must be contacted directly. Authentication can be performed as described in 3.1.9.

4.4.4. Revocation request grace period

There will be no grace period associated with certificate revocation. The Credoc CA handles revocation requests with priority and a certificate will be revoked as soon as possible after circumstances for revocation, as described in section 4.4.1, are established.

4.4.5. Circumstances for Suspension

Due to security measurements, it is not possible to 'suspend' the issued certificate. Once the certificate has been suspended (or requested to be done), it will be 'de facto' revocated.

4.4.6. Who can request suspension

see 4.4.4

4.4.7. Procedure for suspension request

see 4.4.3.

4.4.8. Limits on Suspension Period

see 4.4.4.

4.4.9. CRL Issuance Frequency

CRLs are issued after every certificate revocation or at least every 30 days.

4.4.10. CRL Checking Requirements for Relying Parties

A relying party must verify a certificate against the most recent CRL issued, in order to validate the use of the certificate.

4.4.11. Online Revocation/status Checking Availability

Not Implemented.

4.4.12. Online Revocation Checking Requirements

Not Implemented.

4.4.13. Other Forms of Revocation Advertisement

None.

4.4.14. *Requirements for Relying Parties on Other Forms of Revocation Advertisement*

None.

4.4.15. *Variations of the Above in Case of Private Key Compromise*

Not defined.

4.5. Security Audit Procedures

4.5.1. *Types of Events Audited*

- opening and closing of the cabinet which protects the keys
- (re-)boots of the equipment
- interactive logins on this system

4.5.2. *Processing Frequency of Audit Logs*

The log files are analysed at least once a month.

4.5.3. *Retention Period for Audit Logs*

The minimum retention period is 3 years.

4.5.4. *Protection of Audit Logs*

Only authorised CA personnel is allowed to view and process audit logs. Audit logs are copied to an off-line medium. The audit log files are encrypted.

4.5.5. *Backup Procedures*

Audit log files are copied to an off-line medium, which is saved in safe storage.

4.5.6. *Accumulation System*

The audit log accumulation system is internal to the Credoc-CA.

4.5.7. *Vulnerability Assessments*

Not defined.

4.6. Records Archival

4.6.1. *Types of Events Recorded*

The following events are recorded in either digital or paper-based archives:

- Certification requests
- Revocation requests
- Identity verification procedures
- Issued certificates
- Issued CRLs
- E-mail messages sent and received by the Credoc-CA/RA

4.6.2. Retention Period for Archives

Logs will be kept for a minimum legally required period.

4.6.3. Protection of Archive

Records are backed up on removable media, which are stored in a room with restricted access.

4.6.4. Archive Backup Procedures

See Section 4.6.3

4.6.5. Time-stamping Requirements

All events logged in the event recording (if digital) should have a time stamp to un-questionably prove the existence on a certain time.
Since Credoc Services cvba-scrl has a TSA [Time Stamp Authority], it is appropriate to use this service.

4.6.6. Archive Collection System

The archive system is internal to the Credoc-CA.

4.6.7. Procedures to Obtain and Verify Archive Information

Not defined.

4.7. Key Changeover

CA's private signing key is changed periodically. To avoid interruption of validity of all subordinate keys the new CA-key should be generated 3 years before the old one looses validity. From that point on new certificates are signed by the new CA-key. The new CA-key is posted in the on-line repository.

4.8. Compromise and Disaster Recovery

If the CA private key is compromised - or suspected to be - the CA will:

- inform subscribers, RAs and other relying parties.
- terminate the issuance and distribution of certificates and CRLs
- notify relevant security contacts

4.8.1. Computing resources, software, and/or data are corrupted

If the CA equipment is damaged or rendered inoperative, but the CA private key is not destroyed, CA operation will be reestablished as quickly as possible. If the private key is destroyed the case will be treated as in section 4.8.3.

4.8.2. Entity public key is revoked

See section 4.8.3.

4.8.3. Entity key is compromised

If the private key of the Credoc CA is, or is suspected to be, compromised, the Credoc CA shall:

- make all reasonable effort to inform subscribers and relying partners.
- terminate distribution services for certificates and CRLs issued using the compromised key.
- generate a new CA key pair and certificate and make the latter available in the public repository.

In the case of such a CA key compromise, new certificates will be issued only in accordance with the entity identification procedures defined in section 3.1.

If an RA's private key is compromised, or is suspected to be compromised, the RA informs the Credoc CA and requests a revocation of the RA's certificate.

If an entity private key is compromised or suspected to be compromised, the entity or its administrator must request a revocation of the certificate and make all reasonable efforts to inform any known relying parties.

4.8.4. Secure facility after a natural or other type of disaster

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the Credoc CA will take whatever action it deems appropriate.

4.9. CA TERMINATION

Upon termination the Credoc-CA will:

- notify - based on best efforts- subscribers, RAs and relying parties
- terminate the issuance and distribution of certificates and CRLs
- notify relevant security contacts
- notify widely as possible the end of the service
- destroy all copies of private keys

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

General Remark:
*All following topics concerning ‘***Physical, Procedural, and Personnel Security Controls”** *has been fully described in ‘Physical Security “- document] , that is managed by Credoc management and maintained by Credoc’s CSO.As per company policy , this document is regularly audited.*

Due to confidentiality, this document is not public information.

5.1. PHYSICAL SECURITY CONTROLS

The CA operates in a controlled environment, where access is restricted to authorised people. The CA-machine is additionally protected by physical security measurements, what are known and applied by CA-personnel.

5.1.1. *Site Location*

The Credoc-CA is located at Brussels.

5.1.2. *Physical Access*

Physical access to the hardware infrastructure is restricted to authorised CA-personnel. All removable media is stored in a secure cabinet, with strict limited access by CA-personnel (and with precautions according Credoc IT Policy and 'Physical Security').

5.1.3. *Power and Air Conditioning*

The building has an air conditioning system and the CA machines are connected to an UPS system.

5.1.4. *Water Exposures*

No stipulation.
See "General Remark"

5.1.5. *Fire Prevention and Protection*

The building has a fire alarm system.

5.1.6. *Media Storage*

The Credoc-CA key and Backup copies of CA related information is kept in several removable storage media.

5.1.7. *Waste Disposal*

No stipulation.
See "General Remark"

5.1.8. *Off-site Backup*

No stipulation.
See "General Remark"

5.2. PROCEDURAL CONTROLS

Not defined.
See "General Remark"

5.3. Personnel Security Controls

5.3.1. Background Checks and Clearance Procedures for CA Personnel

CA personnel is recruited in full accordance with the Credoc Services security policy.
See "General Remark"

5.3.2. Background Checks and Security Procedures for other Personnel

No other personnel is authorised to access CA facilities.
See "General Remark"

5.3.3. Training Requirements and Procedures

See "General Remark"

5.3.4. Training Period and Retraining Procedures

Not defined.
See "General Remark"

5.3.5. Frequency and Sequence of Job Rotation

Job rotation is not performed.
See "General Remark"

5.3.6. Sanctions Against Personnel

Not defined.
See "General Remark"

5.3.7. Controls on Contracting Personnel

Not defined.
See "General Remark"

5.3.8. Documentation Supplied to Personnel

- Copies of this document
- Credoc-CA Operation Manual
- Special and personalised training by Pascale

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

Keys for the Credoc-CA are generated by CA staff on a dedicated machine not connected to any kind of network (concerning the root CA-machine, only).

6.1.2. *Private Key Delivery to Entity*

No stipulation.

6.1.3. *Public Key Delivery to Certificate Issuer*

RA generates all public keys.

6.1.4. *CA Public Key Delivery to Users*

The CA certificate chain can be downloaded from the Credoc-CA web site.

6.1.5. *Key Sizes*

- the minimum key length for a personnel or server/service certificate is 2048 bit.
- the CA key (signing of end-entities) length is 2048 bits.

6.1.6. *Public Key Parameters Generation*

Not defined.

6.1.7. *Parameter Quality Checking*

Not defined.

6.1.8. *Hardware/ software key generation*

Key generation is performed by software.

6.1.9. *Key Usage Purposes(as per X.509 v3 key usage field)*

Keys may be used for:

- authentication,
- non-repudiation,
- data encipherment,
- message integrity,
- session establishment

The Credoc-CA private key can only sign certificates and CRLs.

6.2. PRIVATE KEY PROTECTION

6.2.1. *Private Key (n out of m) Multi-person Control*

Not defined.

6.2.2. *Private Key Escrow*

Not defined. The Credoc CA keys are not given in escrow. The Credoc CA is not available for accepting escrow copies of keys of other parties.

6.2.3. Private Key Archival and Backup

The Credoc-CA private key is kept encrypted in multiple copies on CDROMs , or USB flash drive meory stick, in safe places.

The passphrase is, for emergencies in a sealed envelope kept in a secure cabinet. It's controlled from time to time if the envelope is unopened.

Credoc CA has implemented procedures to maintain security regarding the private key archival and backup.

6.3. Other Aspects of Key Pair Management

The Credoc-CA certificate -(signing of end-entities- has currently a validity of 10 years and will expire on 17th October 2017.

6.4. Activation Data

The Credoc-CA private key is protected by a passphrase of at least 15 characters length.

6.5. Computer Security Controls

6.5.1. Specific Security Technical Requirements

- CA operating systems are maintained at a high level of security by applying all the relevant patches
- Monitoring is performed to detect unauthorised software changes
- CA systems configuration is reduced to the base minimum

6.5.2. Computer Security Rating

Not defined.

6.6. Life Cycle Security Controls

Not defined.

6.7. Network Security Controls

- The root CA signing machine is kept off-line (not connected to any kind of network);
- CA machines, other than the signing machine, are protected by a firewall.
- CA machines have - limited by firewall - inbound connectivity

6.8. CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Not defined.

7. CERTIFICATE AND CRL PROFILE

7.1. CERTIFICATE PROFILE

7.1.1. Version Number

X.509 v3.

7.1.2. Certificate Extensions

- CA-certificate:
  - **X509v3 Basic Constraints:** critical CA: TRUE
  - **X509v3 Subject Key Identifier:**
    c9 39 a6 d3 9e 67 e4 05 af c1 30 78 77 33 49 83 75 14 e4 b2
  - **X509v3 Authority Key Identifier:**
    KeyId: 68 60 cd 1d 92 4f 6c 1d e5 03 25 d6 a2 93 39 fa 2f 34 88 56
  - **AIA:** http://pki.credoc.be/RootCA.crt
  - **X509v3 Key Usage:** Critical: Certificate Signing, CRL Signing
  - **X509v3 CRL Distribution Points:** URL: http://pki.credoc.be/RootCA.crl

- User/Host/Service-certificates:
  - **X509v3 Key Usage:** Critical: Digital Signature, Key Encipherment, DataEncipherment
  - **X509v3 Subject Key Identifier:**
    unique identifier of the subject (hash)
  - **X509v3 Subject Key Identifier:**
    c9 39 a6 d3 9e 67 e4 05 af c1 30 78 77 33 49 83 75 14 e4 b2
  - **AIA:** http://pki.credoc.be/KFBN-FRNBIssuingCAClassA.crt
  - **X509v3 CRL Distribution Points:**
    http:// pki.credoc.be/KFBN-FRNBIssuingCAClassA.crl
  - **CRL validity:** 7 days
  - **Certificate Policies:** The OID of the CP/CPS
  - **CPS Policy:** http://pki.credoc.be/credoc-cps.pdf

7.1.3. Algorithm Object Identifiers

Not defined.

7.1.4. Name Constraints

see 7.1.4

7.1.5. Certificate Policy Object Identifier

The certificate policy object identifier (OID) for this document is:
1.3.6.1.4.1.2614.5548.1.1.1.0
Version 1.3
The structure is as follows:
IANA 1.3.6.1.4.1.
FRNB-KFBN 2614.
Internal number 5548.
CA 1.
CP/CPS 1.
Version number, major 1.
Version number, minor 0

7.1.6. Usage of Policy Constraints Extensions

No stipulation

7.1.7. Policy Qualifier Syntax and Semantics

No stipulation

7.2. CRL PROFILE

7.2.1. Version

X.509 v1

7.2.2. CRL and CRL Entry Extensions

Not defined.

8. SPECIFICATION ADMINISTRATION

8.1. SPECIFICATION CHANGE PROCEDURES

Users will not be warned in advance of changes to Credoc-CA 's policy and CPS. Relevant changes will be made as widely available as possible.

8.2. PUBLICATION AND NOTIFICATION PROCEDURES

The Credoc-CA policy is available at

http://pki.credoc.be/ca/credoc-cps.pdf

Previous versions can be found at http://credoc.be/pki/ca/

8.3. CPS APPROVAL PROCEDURES

Not defined.

9. BIBLIOGRAPHY

- Credoc Information Security Policy" [QMS # 1.1.1.0.1.5]

10. APPENDIX A.

This template could be used completely or partly :

10.1. REGISTRATION AUTHORITY AGREEMENT

This forms part of the operating procedures of the Credoc Certification Authority (CA).

1. In acting as a Registration Authority (RA) for Credoc CA I have read and understood and accept the responsibilities and tasks assigned to an RA laid out in Credoc CA Certification Policy and Practice Statement (CP/CPS) document available on the Credoc CA web site –

http://pki.credoc.be/

.

2. I understand that Credoc CA will notify me by email of changes to CP/CPS and I will immediately notify Credoc CA if I am no longer willing to act as an RA under any new CP/CPS.

3. I understand that failure to fulfill my responsibilities and tasks under this agreement may result in the termination of my appointment as an RA.

Signed by .... on .... email:............................