Isabel Certificate Policy

version 3.1

Date of publication: March 8, 2019

Effective date: March 8, 2019

Table of contents

VERSION HISTORY

Published Version	Date	Major Changes
1.1	30/6/2003	
2.0	1/7/2015	Aligned with RFC 3647
3.0	23/1/2017	Takes Root-CA upgrade into account
3.1	22/2/2019	Private Key storage requirements and correction of referred URL's

1. Introduction

The trust made in a digital certificate depends on the rules that are followed to issue and to manage this certificate. Those rules are formalised in policy documents: the Certificate Policy (CP) and the Certification Practice Statement (CPS).

The ITU-T X.509 standard defines a CP as “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”.

The term CPS is defined by the American bar association guidelines as "a statement of the practices which a CA employs in issuing certificates."

1.1. OVERVIEW

The present Isabel CP intends to provide the rules that govern Isabel PKI.

The present Isabel CP states the obligations, practices and procedures which Isabel Certification Authority (CA), Registration Authorities (RAs), Isabel Customers, Isabel Certificate Subjects and Isabel Certificate Relying Parties undertake to fulfil in the scope of the application, issuance, acceptance, usage and revocation of Isabel certificates.

An Isabel Certificate is a certificate issued by Isabel 2048-bit CA or by Isabel 4096-bit CA.

The present Isabel CP is based on the Internet Engineering Task Force (IETF) RFC 3647: ‘Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework – November 2003’ [4] that provides a standard and internationally recognised framework for CPs and CPS.

The present CP is thus structured in alignment with RFC 3647.

This CP shall be used by an Isabel Certificate Relying Party in order to determine the level of assurance and trustworthiness that may be attributed to an Isabel Certificate.

This CP shall also be governed by contracts and agreements, made between Isabel and Isabel Customers. Any CP shall take precedence over agreements between the Isabel and an Isabel Customer, unless agreed otherwise.

References to this CP shall be done as following : Isabel CP v. [version number], section [number].

1.2. DOCUMENT NAME AND IDENTIFICATION

The present CP is named “Isabel Certificate Policy”.

The ASN.1 Object Identifier (OID) associated with this CP is 2.16.56.1.9.2.

1.3. PKI PARTICIPANTS

1.3.1. CERTIFICATION AUTHORITIES

According to ITU-T X.509, a CA is “an authority trusted by one or more users to create and assign certificates, and optionally, the CA may create the users’ key”. The Isabel CA that issues certificates in accordance with this CP, shall also respect the related CPS.

In the Isabel PKI, Isabel CA may accept Isabel Certificate Requests for Isabel Certificate Subjects whose identity has been authenticated by an RA of Isabel PKI.

After a certificate request is verified, Isabel CA issues an Isabel Certificate binding the Isabel Certificate Subject’s identity to his/her public key.

Only one CA is authorized by Isabel to issue Isabel Certificates: it is Isabel CA.

1.3.2. REGISTRATION AUTHORITIES

According to RFC 3647, an RA is “responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates”.

In Isabel PKI, RAs operating under the control and the authority of an Isabel CA accept Isabel Certificate Applications for an Isabel Certificate from Isabel Certificate Subscribers.

RAs in Isabel PKI authenticate the identity of the Isabel Certificate Subject and perform verification of the information contained in the Isabel Certificate Application in accordance with this CP and related CPS as well as their internal procedures. If the verified information is correct, the RA sends an Isabel Certificate request to Isabel CA to issue an Isabel Certificate for the Isabel Certificate Subject.

Only Registration Authorities authorized by Isabel are permitted to submit certificate requests to Isabel CA for the issuance of Isabel Certificates.

1.3.3. END ENTITIES

In the scope of the present Isabel CP, end entities in the Isabel Public Key Infrastructure consist of :

1. Isabel Certificate Subscriber
2. Isabel Certificate Subject
3. Isabel Certificate Relying Party

The Subject attribute in the Isabel Certificate is used to name or otherwise identify the Isabel Certificate Subject with:

1. Either a name and first name for a Physical Person Subject.
2. Either a function name for a Function Subject.
3. Either an application name for an Application Subject.

In the scope of the present Isabel CP :

1. an end entity may not be a CA or an RA in the Isabel PKI,
2. a signature of a Function Subject is a technical signature, i.e. it may only be used for integrity reasons, not for transaction authorisation.

1.3.4. VALIDATION AUTHORITIES

In the Isabel PKI, an Isabel Validation Authority provides any relying party with a way of obtaining Isabel Certificate revocation status information.

Certificate Revocation Lists (CRLs) containing the serial numbers of revoked Isabel Certificates as well as the revoked Isabel Certificates themselves are published in an Isabel directory.

Online Certificate Status Protocol (OCSP) responders provide revocation status for Isabel Certificates.

1.3.5. POLICY AUTHORITY

A Policy Authority is the entity responsible for:

1. The specification, validation and publication of the Isabel CP and its revisions.
2. Determining the suitability and the correct implementation of the Isabel CP.
3. Definition of the review requirements and processes relating to the implementation of the CP.

The Policy Authority for the present Isabel CP is the Isabel Security Manager.

1.4. CERTIFICATE USAGE

Isabel Certificates issued in accordance with the present CP may only be used by Relying Parties who are part of an Isabel Customer and for the following purposes: verifying digital signature, non-repudiation, enciphering keys and enciphering data.

Isabel Certificates may not be used by Relying Parties who are not part of an Isabel Customer.

If an Isabel Certificate Subscriber wants to have any limitations (financial or otherwise) applicable to transactions authenticated by the Isabel Certificate, that certificate Subscriber must have a signed agreement with each bank agreeing to such limitations.

1.5. POLICY ADMINISTRATION

1.5.1.1. SPECIFICATION ADMINISTRATION ORGANISATION

The Policy Authority reviews the present Isabel CP on a regular basis to take into account changes in legislation, technology and security risks.

The Policy Authority is responsible for all aspects of the present Isabel CP, including its drafting, validation, registration, publication, maintenance and update.

The continued use of an Isabel certificate after publication of a new version of the CP shall imply the acceptance of this new version by the Subject.

1.5.1.2. POLICY AUTHORITY CONTACT PERSON

The Isabel Security Manager acts as the Policy Authority for the present Isabel CP.

All questions and comments regarding Isabel CP should be addressed to:

Isabel Security Manager
Isabel NV/SA
Keizerinlaan / Bd de l'Impératrice 13-15
B-1000 Brussels
Belgium
Tel: +32 (0)2/545.17.11
Fax: +32 (0) 2/545.17.19
E-mail: policyauthority@isabel.eu
Web: www.isabel.eu

1.5.1.3. PERSON DETERMINING CPS SUITABILITY FOR THE POLICY

The Isabel Security Manager determines the suitability of the Isabel CPS to the present Isabel CP.

1.5.1.4. CP APPROVAL PROCEDURES

Isabel may amend this CP at any time.

No amendment will have retrospective effect.

The Policy Authority for the present Isabel CP and the Isabel general manager must approve changes to the present document.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. GLOSSARY

Term	Description
Application	In the context here, it is the Application which can be the Subject of a Certificate. Such an Application is a software application that is publishing signed information based on an automated process (any time) and as such doesn't allow for human intervention for generating a signature. Examples of such Applications are websites making digitally signed proposals to customers or digitally signed emails for a sales or marketing campaign.
Authentication	The process of validating identity based on the possession of a trusted credential.
Bank Registration Authority	A bank operating as RA for the Isabel PKI
Certificate	The public key of a Subject, together with the identity of the Subject and some other information, rendered unforgeable by encipherment with the private key of the CA which issued the Certificate.

Term	Description
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.
Certificate Revocation List	A list of numbers of revoked certificates digitally signed by the issuing CA.
Certification Authority	An authority trusted by users to issue and manage certificates. Optionally, the CA may create the users' key pair.
Granted bank	A granted bank is a bank that works with Isabel Subscribers but for which they were not the bank RA
Hardware Security Module	Hardware cryptographic module used to generate and store Private Keys and generate digital signatures.
Isabel Certificate	A Certificate that has been issued by an Isabel CA.
Isabel Certificate Relying Party	An Isabel Certificate Relying Party is a physical person or an application that is or belongs to an Isabel Customer and that relies on the information contained in an Isabel Certificate, and/or digital signatures verified using this certificate and/or any other information published by an Isabel CA issuing Isabel Certificates.
Isabel Certificate Request	Submission of validated Isabel Certificate Application information by an RA of Isabel PKI to an Isabel CA to issue an Isabel Certificate
Isabel Certificate Subject	A physical person, an application or a function (e.g. "accountant") identified in a certificate as the holder of the Private Key associated with the Public Key given in the certificate.
Isabel Certificate Subscriber	A physical person, empowered by an Isabel Customer, to apply for an Isabel Certificate on behalf of one or more physical person(s), application(s) or function(s) subject(s). A physical person Subject may be an Isabel Certificate Subscriber acting on its own behalf.
Isabel Certification Authority	A CA operated by Isabel. Isabel CA is also referred as the technical organization around the Certification Authority, which is operated by the company Isabel NV/SA.
Isabel Customer	An entity that signed a contract with Isabel with the intention of receiving services and/or products from Isabel that includes the use of an Isabel Certificate.
Isabel Registration Authority	An RA that is operated by Isabel under the authority and the control of an Isabel CA.

Term	Description
Isabel Secure Signing Card	A smart card storing the Private Key of a Subject and used by this Subject to create a digital signature. The digital signature is created inside the Isabel Secure Signing Card.
Isabel User	A physical person who uses Isabel products/services in the scope of a contract binding Isabel and the Isabel Customer to which the User belongs.
Isabel Validation Authority	An authority that provides Isabel Certificates Relying Parties with a way of obtaining Isabel Certificate revocation status information.
Personal Identification Number	A secret code (PIN) that is used to protect against unauthorized access to a Private Key.
PKI Contract	Isabel Customer contract signed by an Isabel Customer
Policy Authority	The entity responsible for the specification and validation of CPs and for determining the suitability of the CPS to those CPs.
Private Key	The portion of a public-private key pair to be kept secret and which should be known only to the Subject.
Public Key	The portion of a public-private key pair that may be publicly known or distributed without reducing the security of the cryptography system.
Public Key Infrastructure	A structure of hardware, software, people, processes and policies that employs digital signature technology to facilitate a verifiable association between the public component of an asymmetric Public Key with a specific Subject that possesses the corresponding Private Key.
Registration Authority	An entity that is responsible for the identification and authentication of certificate subjects, but that does not sign or issues certificates. A RA may assist in the certificate application process, revocation process or both, as stated in the applicable CP or the present CPS.
Self-signed certificate	Certificate signed with the Private Key for which the Public Key is in the Certificate. Typically used for CA root certificates, where the root key is in a Certificate signed with the corresponding Private Key.

1.6.2. ACRONYMS

Acronym	Description
CA	Certification Authority
CP	Certificate Policy

Acronym	Description
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
URI	Uniform Resource Identifier

2. Publication and Repository Responsibilities

This section describes provisions applicable to the CA's obligations to publish information with respect to its practices, the frequency of such publication, access control to published information and requirements governing the use of repositories.

2.1. PUBLICATION OF ISABEL CA INFORMATION

The Isabel CA information to be published is:

1. The Isabel CP.
2. The Isabel Certification Practice Statement (internally only).
3. The Isabel Certificates which are accepted, and therefore declared to contain correct information, by the Subject.
4. The Certificate Revocation Lists (CRLs) for Isabel Certificates.
5. The Isabel CA self-signed certificate.

This information shall be published online but may be published in other forms.

2.2. REPOSITORIES

Isabel owns and operates an LDAP directory for internal usage. It contains the certificates.

There is a public directory to publish the CRLs.

The access protocol to those repositories is HTTPS based.

Two OCSP servers have been implemented in order to manage certificate status information:

- https://pki.isabel.be/ocsp for 2048-bit CA and
- https://pki.isabel.be/ocsp2 for 4096-bit CA.

2.3. TIME AND FREQUENCY OF PUBLICATION

Isabel Certificates publication is guaranteed within 24 hours after the acceptance of the smart card by the Subject.

The Certificate Revocation Lists (CRL) for Isabel Certificates are reissued at least once every 24 hours.

The Isabel CP and CPS are under version control and a new release of the present CP is published after updates.

Isabel CP is published to Isabel website (https://www.isabel.eu/content/dam/isabel6/contrib6/documents/en-US/certificate-policy.pdf).

However, Isabel CPS is published internally only.

2.4. ACCESS CONTROL ON PUBLISHED INFORMATION

Information	Access Rights	Access by
CP	Read	Anybody
CP	Write / Update	Policy Authority
CPS	Read	Isabel Internal staff working on the PKI or with a need to know
CPS	Write / Update	Policy Authority
Certificates	Read-Only	RA, Isabel Subscribers and Isabel Relying Parties
CRLs	Read-Only	Restricted Isabel Relying Parties
CRLs	Write	Isabel CA
OCSP	Read-Only	Isabel Relying Parties
OCSP	Write	Isabel CA
CA self-signed certificate	Read-Only	Anybody

Isabel insures that appropriate access controls are in place to enforce these access rights and prevent unauthorized writing, modifying, or deleting certificates, CRLs and other information of Isabel PKI.

3. IDENTIFICATION AND AUTHENTICATION

3.1. INITIAL REGISTRATION

This section describes the identification and authentication provisions in the scope of the initial registration of an Isabel Certificate Subject.

There are 3 types of Isabel Certificate Subject under the present Isabel CP:

1. Physical person Subjects: the Subject is represented by the physical person who is identified in the certificate
2. Function Subjects: the Subject is represented by one physical person who is empowered to represent the function that is identified in the certificate (function representative).
3. Application Subjects: the Subject is represented by one or several physical person(s) who is/are empowered to represent the application that is identified in the certificate

3.1.1. TYPES OF NAMES

An Isabel CA must use X.500 Distinguished Name (DN) format for Subject and Issuer name fields in an Isabel Certificate.

3.1.2. NEED FOR NAMES TO BE MEANINGFUL

An RA in Isabel PKI must guarantee the meaningfulness of the DN information entered in the subject field of an Isabel Certificate within the X.500 name space for which Isabel has been authorised.

The Common Name field that is used as part of the X.500 DN for the Isabel Certificate Subject is represented by:

1. The Subject’s Last Name and First Name for physical person Subjects
2. The Function Name for function Subjects
3. The Application Name for application Subjects

In case an organization is mentioned, the naming information must conform to the "legal name" of the organization, as it is registered according to applicable laws and regulations.

3.1.3. ANONYMITY OF SUBSCRIBERS

Isabel Certificate Subscribers cannot be anonymous.

3.1.4. RULES FOR INTERPRETING VARIOUS NAME FORMS

Only names in the form of X.500 DN are used in Isabel Certificates.

3.1.5. UNIQUENESS OF NAMES

An RA in Isabel PKI must guarantee the uniqueness of the DN in the Subject field of an Isabel Certificate within the X.500 name space for which Isabel has been authorised.

The uniqueness of names for the Isabel Certificate Subjects is achieved thanks to the tools used by the RAs agents that prevent the encoding of the same Last Name/First Name or Function Name for two (2) Isabel Certificate Subjects who are within the same Organisation.

If an Isabel Certificate Subject has the same Last Name/First Name or Function Name than another Isabel Certificate Subject in his/her organisation, it is up to the RA agent of Isabel PKI to append letters or digits at the end of the Last Name/First Name or Function Name of the Isabel Certificate Subject when encoding the Isabel Certificate Subject's information.

3.1.6. RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS

RAs of Isabel PKI cannot verify nor guarantee that trademarks, service marks or any other protected signs mentioned in Isabel Certificates can legitimately be used without infringement on any Intellectual Property right. No RA nor any CA within the Isabel PKI shall be obliged to perform such a possible infringement investigation. Nevertheless, if an RA of Isabel PKI suspects any intellectual property right infringement, it has the right to suspend and/or terminate the registration procedure and to verify at first view whether or not an intellectual property right may be violated. The RA of Isabel PKI has the right to request disclosure of all legal documents that demonstrate title or the legitimate use of any such examined right.

3.2. INITIAL IDENTITY VALIDATION

3.2.1. METHOD TO PROVE POSSESSION OF PRIVATE KEY

Isabel Certificate Subject for Application Subject proves it is in possession of its private key by signing the corresponding certificate request. Isabel CA verifies the signature with the Subject' public key associated with the private key used to sign.

Isabel Certificate Subject for physical person Subject proves he/she is in possession of his/her private key by activating the smart card in which the private key is securely stored.

3.2.2. AUTHENTICATION OF ORGANIZATION IDENTITY

An RA of Isabel PKI is obliged to authenticate the identity of a candidate Isabel Customer before Subscribers of this Isabel Customer are allowed to apply for Isabel Certificates.

The authentication of a candidate Isabel Customer's identity is achieved in the scope of the subscription process ruling the signature of an Isabel PKI contract between this Isabel candidate Isabel Customer and Isabel.

3.2.3. AUTHENTICATION OF INDIVIDUAL IDENTITY

The authentication of an individual's identity is achieved in the scope of the Isabel Certification Process.

3.2.3.1. THE FIRST AUTHENTICATION STAGE

This is the stage where the Isabel Certificate Subscriber applies for an Isabel Certificate at an RA of Isabel PKI. The Isabel Certificate Subscriber must provide authenticating pieces together with his/her duly completed Isabel Certificate application to the RA of Isabel PKI.

In cases where the certification process is initiated by a mandatory via a power of attorney, additional documents will be required.

3.2.3.2. THE SECOND AUTHENTICATION STAGE

A second authentication of the Isabel Certificate Subscriber is performed by the RA of the Isabel PKI during the distribution process.

3.2.4. NON VERIFIED SUBSCRIBER INFORMATION

Isabel Certificate Subscriber information that is not collected by the RA during the initial registration process might be verified afterwards.

3.2.5. VALIDATION OF AUTHORITY

N/A

3.2.6. CRITERIA FOR INTEROPERATION

There is currently no cross-certification of Isabel CA.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

This section describes the identification and authentication provisions in the scope of the renewal of an Isabel Certificate for an Isabel Certificate Subject who has already been registered.

3.3.1. IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

A non-revoked Isabel Certificate is renewed automatically by the issuing Isabel CA at the approach of the end of the Isabel Certificate's validity period.

The identification and authentication for a routine re-key is based on the previous private authentication key. This authentication is automatically verified by the CA for authenticity. Then the certificates are renewed automatically.

The same Public Key is re-certified in the scope of this Isabel Certificate renewal process.

The Isabel CA authenticates its own certificate renewal requests.

3.3.2. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

The identification and authentication for a re-key after revocation uses the same process as the initial identity validation (cf. section 3.2).

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

This section describes the identification and authentication provisions in the scope of the revocation of an Isabel Certificate.

Isabel offers Isabel Customers several channels for requesting the revocation of an Isabel Certificate depending on the circumstances.

3.4.1. AUTHENTICATION BY A GRANTED BANK OR ISABEL RA

The RA of Isabel PKI authenticates the revocation request transmitted by the Isabel Subject or by the authorized legal representative and will initiate the revocation to the Isabel CA after positive authentication.

3.4.2. AUTHENTICATION BY AN ISABEL REVOCATION SERVICE

Isabel has a Revocation Service which is available to its Isabel Customers 24 by 7. This service is operated by Card Stop. This service guarantees that the revocation will be initialised within one (1) hour after the request of the Isabel Customer.

Card Stop

Tel: +32 (0)70/344.344

Fax: +32 (0)70/355.355

3.4.3. AUTHENTICATION BY THE ISABEL CA

The Isabel CA authenticates a revocation request on the basis of a digital signature generated by the RA of the Isabel PKI or by the Isabel Revocation Service.

Once the revocation request is authenticated by Isabel CA, Isabel CA revokes the Isabel Certificate and updates the Certificate Revocation List (CRL) with the revoked Isabel certificate. The CRL is signed by Isabel CA to guarantee its integrity.

4. CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

When applying for an Isabel Certificate, the Isabel Certificate Subscriber must respect the conditions and obligations of the applicable CP and any applicable contractual agreement.

During this application process, the identification and authentication process of chapter 3 above must be applied.

This application process results in the issuance of an Isabel Certificate as well as the publication of the Isabel Certificate in the Isabel Repository.

The application for an Isabel Certificate can be initiated in 2 different contexts:

4.1.1. ISABEL CERTIFICATE APPLICATION FOR A NEW SUBJECT

In the case the Isabel Certificate Subscriber belongs to a candidate Isabel Customer:

- the candidate Isabel Customer must go through the authentication described in section 3.2.2 of the present CP.
- The Isabel Certificate Subscriber who applies for an Isabel Certificate must go thru the authentication described in section 3.2.3 of the present CP

In the case the Isabel Certificate Subscriber belongs to an existing Isabel Customer:

- The Isabel Certificate Subscriber who applies for an Isabel Certificate must go thru the authentication described in section 3.2.3 of the present CP.

4.1.2. ISABEL CERTIFICATE APPLICATION FOR AN EXISTING SUBJECT

The Isabel Certificate Subscriber who applies for an Isabel Certificate must authenticate by signing the Isabel Certificate Request with his/her current private authentication.

4.2. CERTIFICATE APPLICATION PROCESSING

The procedure for processing certificate applications includes:

- Identification and authentication procedures to validate the certificate application.
- Approval or rejection of the certificate application by an RA of the Isabel PKI.
- If approved, initiate the certification request to the Isabel CA.

4.3. CERTIFICATE ISSUANCE

The provisions related to the certificate issuance are stated in the corresponding section of Isabel CPS.

4.4. CERTIFICATE ACCEPTANCE

During the step of activation of the smart card, the end user must check that the information written down on his/her smart card matches with the information displayed on the Isabel web portal and coming from Isabel eAdmin server (company name, user last name, user first name, userID and card ID). Then the end user must click on the button “I agree” or “Cancel”.

4.5. KEY PAIR AND CERTIFICATE USAGE

An Isabel Certificate Subject may only use his/her Private Key and Isabel Certificate for allowed key usage purposes in consistency with the applicable certificate key usage field, in compliance with the provisions stated in the relevant CP and in any agreement made or to be made between Isabel and the Isabel Customer.

The Isabel Certificate Subject must stop using the private key after the expiration or revocation of the certificate.

4.6. CERTIFICATE RENEWAL

A certificate has a limited validity period.

Prior to the end of this validity period, an Isabel Certificate

1. Is automatically renewed for Physical person Subjects
2. Is automatically renewed for Function Subjects

For Application Subjects, a new key pair has to be generated in compliance with the initial procedures for certification.

4.7. CERTIFICATE RE-KEY

A certificate re-key means issuing new public and private key pairs and a certificate to a Subscriber. An Isabel Certificate re-key occurs

- when the key pairs are compromised
- when the usage period of the key pairs has expired
- when the Isabel Certificate is revoked
- when the Isabel Certificate has expired

Isabel Certificate re-key must follow the initial procedures of certificate application and issuance.

4.7.1. ISABEL SMART CARD RENEWAL

In the case an Isabel Certificate Subject encounters a situation where he is no longer in position to use his/her Isabel smart card and needs a new one, then the Isabel Certificate Subscriber has to follow 4.1.2 Isabel Certificate Application for an existing Subject.

4.8. CERTIFICATE MODIFICATION

To correct certificate data, the Isabel Subscriber / RA must revoke the Isabel Certificate and request a new Isabel Certificate with the corrected data. No modification can be performed on an issued Isabel Certificate.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

The revocation of an Isabel Certificate is definitive and irreversible.

4.9.1. CIRCUMSTANCES FOR REVOCATION

The revocation of an Isabel Physical Person, Function or Application Subject Certificate shall always occur after a final decision by an RA of Isabel PKI or an Isabel Revocation Service.

Circumstances for the revocation of an Isabel Certificate are detailed in section 3.4 of Isabel CPS.

4.9.2. WHO CAN REQUEST REVOCATION

The revocation of an Isabel Physical Person, Function or Application Subject Certificate may be requested by:

1. The physical person who is identified in a Physical Person Subject Certificate.
2. The physical person who represents a Function or Application Certificate.
3. Any physical person empowered by an Isabel Customer to request revocation of its Subject Certificates.
4. Any RA of Isabel PKI.
5. The Isabel CA that has issued the certificate.

4.9.3. PROCEDURE FOR REVOCATION REQUEST

The procedure for revocation request is described in section 3.4 of this CP.

4.9.4. REVOCATION REQUEST GRACE PERIOD

No grace period is allowed.

4.9.5. CIRCUMSTANCES FOR SUSPENSION

Certificate suspension is not supported in the Isabel PKI.

4.9.6. CRL ISSUANCE FREQUENCY

The Certificate Revocation Lists (CRL) for Isabel Certificates are reissued at least once every 24 hours.

4.10. CERTIFICATE STATUS SERVICES

Two OCSP servers have been implemented in order to manage certificate status information:

- https://pki.isabel.be/ocsp for 2048-bit CA and
- https://pki.isabel.be/ocsp2 for 4096-bit CA.

4.11. END OF SUBSCRIPTION

The requirements to put an end to the subscription of the PKI Contract are detailed in the Terms and Conditions related to that PKI Contract.

4.12. KEY ESCROW AND RECOVERY

Isabel CA private keys are not escrowed.

No private key of Isabel PKI is escrowed.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1. PHYSICAL CONTROLS

All Isabel PKI components are hosted in datacentres that are certified TIA 942 Tier III+

An independent third party performs an annual onsite physical inspection of these datacentres in order to evaluate that the physical and environmental security measures of the facility are compliant with ISO 27002 controls related to several areas such as physical perimeter entry controls, HVAC systems, power distribution, UPS systems, etc.

5.2. PROCEDURAL CONTROLS

The provisions related to the procedural controls are stated in the corresponding section of Isabel CPS.

5.3. PERSONNEL CONTROLS

The provisions related to the personnel controls are stated in the corresponding section of Isabel CPS.

5.4. AUDIT LOGGING PROCEDURES

The provisions related to the audit logging procedures are stated in the corresponding section of Isabel CPS.

5.5. RECORDS ARCHIVAL

The provisions related to the record archival are stated in the corresponding section of Isabel CPS.

5.6. KEY CHANGEOVER

An Isabel CA ensures that its private signing keys are not used beyond the end of their life cycle. When an Isabel CA private key has reached the end of its life, its certificate is revoked.

A routine re-key of Isabel CA applies in following situations:

- When Isabel CA has been compromised; or
- When Isabel CA has experienced a key integrity issue

A compromise involves revocation of the CA’s certificate and a re-key procedure will be triggered.

Isabel CA key pair generation and replacement is performed during a key ceremony.

5.7. COMPROMISE AND DISASTER RECOVERY

The provisions related to the compromise and disaster recovery are stated in the corresponding section of Isabel CPS.

5.8. CA OR RA TERMINATION

On termination of an Isabel CA activities or Isabel RA activities, Isabel will act as stipulated by the Belgian National Law, i.e. [2].

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. KEY PAIR GENERATION

The Isabel key generation process is Isabel proprietary.

The generation process has been audited for its quality and robustness. It is continuously monitored.

6.1.2. PRIVATE KEY DELIVERY TO SUBSCRIBER

The different processes available to Isabel Customers for key delivery are described in details in section 4.3 of this CP.

6.1.3. PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

Once generated, the public key of the key pair is sent to the CA for certification.

6.1.4. CA PUBLIC KEY DELIVERY TO RELYING PARTIES

Isabel operates in a closed community and thus, there is no CA public key delivery outside of Isabel Customers.

6.1.5. KEY SIZES

The size of the RSA Public Key (modulus n) for a physical person or a function is at least 1024 bits.

The size of the RSA Public Key (modulus n) for Applications (outside of the PKI) is at least 1024 bits

The size of the RSA Public Key (modulus n) for Applications within the PKI system is 2048 bits

The size of the keys of the Isabel 2048-bit CA is 2048 bits and of the Isabel 4096-bit CA is 4096 bits.

6.1.6. PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

The parameters used to compute the RSA public key (e,n) are n which is the multiplication of p and q, two distinct random large prime and *e* which is a random integer such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n))=1$, where $\phi(n) = (p-1) * (q-1)$. The p and q should be checked to make sure they are prime numbers.

6.1.7. KEY USAGE PURPOSES

The key usage field indicates the purpose for which the certified public key is to be used. The different values for this field are described in the ITU-T Rec X.509:

	Key Usage Field	Description
a	DigitalSignature	For verifying digital signatures that have purposes other than those in b, f or g below
b	nonRepudiation	For verifying digital signatures used in providing non-repudiation services that protect against the signing entity falsely denying some action (excluding certificate or CRL signing as in f or g below)
c	keyEncipherment	For enciphering keys or other security information (e.g. for key transport).
d	dataEncipherment	For enciphering user data, but not keys or other security information as in c above
e	keyAgreement	For use as a public key agreement key
f	KeyCertsign	For verifying a CA’s signature on certificates. For use in CA certificates only
g	cRLSign	For verifying a CA’s signature on CRLs
h	encipherOnly	Public key agreement key for use only in enciphering data when used with keyAgreement bit also set (meaning with other key usage bit set undefined)
i	decipherOnly	Public key agreement key for use only in deciphering data when used with keyAgreement bit also set (meaning with other key usage bit set undefined).

If this extension is flagged critical, then the certificate shall be used only for one of the purposes indicated.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

Isabel Certificate Subject’s private key is stored within the following cryptographic modules

- an Isabel smart card for a physical person or function which is EAL4+ certified
- a third party Hardware Security Module (HSM) that is certified FIPS 140-2 level 3 for applications
- Isabel TRD (Tamper Resistant Device)*

6.2.2. PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

The provisions related to the private key multi-person control are stated in the corresponding section of Isabel CPS.

* Isabel TRD solution is in the process to be decommissioned.

6.2.3. PRIVATE KEY ESCROW

Isabel CA private keys are not escrowed.

No private key of Isabel PKI is escrowed.

6.2.4. PRIVATE KEY BACKUP

The provisions related to the private key backup are stated in the corresponding section of Isabel CPS.

6.2.5. PRIVATE KEY ARCHIVAL

Isabel private keys are not archived.

6.2.6. PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

Isabel CA private key is generated within the HSM during the CA key ceremony. There is no transfer of Isabel CA private key.

Isabel Subject's private key is loaded into the cryptographic module in a secure way. Details are considered as company confidential.

6.2.7. PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

Isabel CA private key is stored in an HSM which is certified FIPS 140-2 level 3.

Isabel Subject's private key for physical person is stored in an Isabel Secure Signing Card which is EAL4+ certified.

6.2.8. METHOD OF ACTIVATING PRIVATE KEY

Isabel Subject's private key is activated by a PIN code.

Isabel Secure Signing Cards are "burned" after entering successively more than five (5) invalid PIN codes.

6.2.9. METHOD OF DEACTIVATING PRIVATE KEY

Isabel Subject's private key is de-activated when the Isabel Secure Signing Card is removed from the card reader.

Isabel CA private key can be de-activated if the HSM is tampered.

6.2.10.METHOD OF DESTROYING PRIVATE KEY

Isabel Subject's private key is destroyed when the chip of Isabel Secure Signing Card is physically destroyed or damaged.

For the destruction of Isabel CA private key, see HSM specifications.

6.2.11.CRYPTOGRAPHIC MODULE RATING

Isabel HSM are certified FIPS 140-2 level 3.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. PUBLIC KEY ARCHIVAL

The provisions related to the public key archival are stated in the corresponding section of Isabel CPS.

6.3.2. CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

The key pair period is

- 50 years for Isabel CA
- 10 years for an Application Subject
- 4 months for a function Subject
- 4 months for a physical person Subject

6.4. ACTIVATION DATA

6.4.1. ACTIVATION DATA GENERATION AND INSTALLATION

The generation of the Subject’s initial temporary activation data (Isabel PIN code) is done by Isabel PKI system.

During the Isabel Secure Signing Card activation process, the Subject must change his/her temporary Isabel PIN code into a final Isabel PIN code of his/her choice.

6.4.2. ACTIVATION DATA PROTECTION

The Subject is responsible for the confidentiality of his/her activation data (Isabel PIN code).

6.4.3. OTHER ASPECTS OF ACTIVATION DATA

Isabel does not backup, escrow nor archive Subject’s activation data.

6.5. COMPUTER SECURITY CONTROLS

The provisions related to the computer security controls are stated in the corresponding section of Isabel CPS.

6.6. LIFE CYCLE TECHNICAL CONTROLS

The provisions related to the life cycle technical controls are stated in the corresponding section of Isabel CPS.

6.7. NETWORK SECURITY CONTROLS

The provisions related to the network security controls are stated in the corresponding section of Isabel CPS.

6.8. TIME-STAMPING

Clock of Isabel PKI equipment (CA, logs, etc.) is synchronised with Isabel's time server, which is synchronised with an external NTP server.

7. CERTIFICATE AND CRL PROFILES

7.1. CERTIFICATE PROFILE

7.1.1. PROFILE OF CERTIFICATE ISSUED TO A PHYSICAL PERSON BY 2048-BIT ISABEL CA

Certificate Field	Value or Value Format
version	INTEGER {V3(2)} (Note: integer value 2 corresponds to v3 certificates)
SerialNumber	INTEGER {0..MAX}
signature	*AlgorithIdentifier sha-1WithRSAEncryption OID ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}*
issuer	*CN=Isabel Certification Authority; O=CA; L=ISABEL; C=BE*
validity	*notBefore*=UTCTime *notAfter*=UTCTime Valid 4 months
subject	*CN*=Lastname Firstname*; O=Organisation name; L=ISABEL; C=BE* *Some OU fields can optionally be present.*
subjectPublicKeyInfo	*AlgorithmIdentifier rsaEncryption OID ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)* pkcs-1(1) 1*}*

7.1.2. PROFILE OF CERTIFICATE ISSUED TO A PHYSICAL PERSON BY 4096-BIT ISABEL CA

Certificate Field	Value or Value Format
version	INTEGER {V3(2)} (Note: integer value 2 corresponds to v3 certificates)
SerialNumber	INTEGER {0..MAX}
signature	*AlgorithIdentifier sha-256WithRSAEncryption OID ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}*

Certificate Field	Value or Value Format
issuer	*CN=Isabel Certification Authority Root; O=CA; L=ISABEL; C=BE*
validity	*notBefore*=UTCTime *notAfter*=UTCTime Valid 4 months
subject	*CN*=Lastname Firstname*; O=Organisation name; L=ISABEL; C=BE* *Some OU fields can optionally be present.*
subjectPublicKeyInfo	*AlgorithmIdentifier rsaEncryption OID ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)* pkcs-1(1) 1*}*

7.1.3. PROFILE OF CERTIFICATE ISSUED TO A FUNCTION BY 2048-BIT ISABEL CA

Certificate Field	Value or Value Format
version	INTEGER {V3(2)} (Note: integer value 2 corresponds to v3 certificates)
SerialNumber	INTEGER {0..MAX}
signature	*AlgorithIdentifier sha-1WithRSAEncryption OID::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}*
issuer	*CN=Isabel Certification Authority; O=CA; L=ISABEL; C=BE*
validity	*notBefore*=UTCTime *notAfter*=UTCTime Valid 8 months
subject	*CN*=Function Name; *O=Organisation name; L=ISABEL; C=BE* *Some OU and/or GN fields can optionally be present.*
subjectPublicKeyInfo	*AlgorithmIdentifier rsaEncryption OID ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)* pkcs-1(1) 1*}*

7.1.4. PROFILE OF CERTIFICATE ISSUED TO A FUNCTION BY 4096-BIT ISABEL CA

Certificate Field	Value or Value Format
version	INTEGER {V3(2)} (Note: integer value 2 corresponds to v3 certificates)
SerialNumber	INTEGER {0..MAX}
signature	*AlgorithIdentifier sha-256WithRSAEncryption* *OID::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}*
issuer	*CN=Isabel Certification Authority Root; O=CA; L=ISABEL; C=BE*
validity	*notBefore*=UTCTime *notAfter*=UTCTime Valid 8 months
subject	*CN*=Function Name; *O=Organisation name; L=ISABEL; C=BE* *Some OU and/or GN fields can optionally be present.*
subjectPublicKeyInfo	*AlgorithmIdentifier rsaEncryption* *OID ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)* pkcs-1(1) 1*}*

7.1.5. PROFILE OF CERTIFICATE ISSUED TO AN APPLICATION BY 2048-BIT ISABEL CA

Certificate Field	Value or Value Format
version	INTEGER {V3(2)} (Note: integer value 2 corresponds to v3 certificates)
SerialNumber	INTEGER {0..MAX}
signature	*AlgorithIdentifier sha-1WithRSAEncryption* *OID ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}*
issuer	*CN=Isabel Certification Authority; O=CA; L=ISABEL; C=BE*

Certificate Field	Value or Value Format
validity	*notBefore*=UTCTime *notAfter*=UTCTime Valid 10 years
subject	*CN*=Application Name; *O=Organisation name; L=ISABEL; C=BE* *Some OU fields can optionally be present.*
subjectPublicKeyInfo	*AlgorithmIdentifier rsaEncryption OID ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)* pkcs-1(1) *1}*

7.1.6. PROFILE OF CERTIFICATE ISSUED TO AN APPLICATION BY 4096-BIT ISABEL CA

Certificate Field	Value or Value Format
version	INTEGER {V3(2)} (Note: integer value 2 corresponds to v3 certificates)
SerialNumber	INTEGER {0..MAX}
signature	*AlgorithIdentifier sha-256WithRSAEncryption OID ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}*
issuer	*CN=Isabel Certification Authority Root; O=CA; L=ISABEL; C=BE*
validity	*notBefore*=UTCTime *notAfter*=UTCTime Valid 10 years
subject	*CN*=Application Name; *O=Organisation name; L=ISABEL; C=BE* *Some OU fields can optionally be present.*
subjectPublicKeyInfo	*AlgorithmIdentifier rsaEncryption OID ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)* pkcs-1(1) *1}*

7.1.7. VERSION NUMBER

All Isabel Certificates delivered by Isabel CA must be compliant to ITU-T X.509 v3.

7.1.8. CERTIFICATE EXTENSIONS

The extensions defined for X.509v3 certificates provide methods for associating additional attributes with users or public keys and for managing the certificate hierarchy. This field may only appear if the version is 3. This field is a sequence of one or more certificate extensions.

An application MUST reject the certificate if it encounters a critical extension it does not recognise; however, a non-critical extension may be ignored if it is not recognised.

Here is the list of the standard certificate extensions (as defined in ITU-T X.509) that are used in Isabel Certificates delivered by an Isabel CA and a description on how they are used, including if those extensions are critical (C) or non-critical (NC).

For a more complete description of those certificate extensions, c.f. ITU-T X.509v3.

7.1.8.1.EXTENSIONS OF CERTIFICATES FOR PHYSICAL PERSON AND FUNCTION

Following table summarizes the MANDATORY extensions and their value for an Isabel Certificate issued to a physical person or to a function:

Certificate Extension Field	Criticality	Value or Value Format
KeyUsage	NC	This field gives a list of permitted usages for the key. BIT STRING ::= {digitalSignature(0), nonRepudiation(1), keyEncipherment(2), dataEncipherment(3)}
ExtKeyUsage	NC	This field gives more acceptable usages of the key. It’s a list of OIDs. KeyPurposeID ::= {id-kp-clientAuth (1.3.6.1.5.5.7.3.2), id-kp-emailProtection (1.3.6.1.5.5.7.3.4)}
authorityKeyIdentifier	NC	This field identifies the CA public key to be used to verify the signature applied on the certificates. OCTET STRING ::= {43 41 30 32} (“CA02”) for 2048-bit CA OCTET STRING ::= {43 41 30 34} (“CA04”) for 4096-bit CA

Certificate Extension Field	Criticality	Value or Value Format
CertificatePolicies	NC	This field contains a sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers. These policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used. Has the value {joint-iso-ccitt(2) allocation per country (16) Belgium (56) isabel (1) certification-policies(9) standard(4)} The field also contains an attribute that is a URI to the full version of the CP.
subjectPublicKeyInfo OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) allocation per country (16) Belgium(56) Isabel(1) 8}	NC/C	This field is a proprietary Isabel extension *For Internal use only* This field is Critical for revoked certificates.
SerialNumber (OID 2.5.4.5)	NC	This field represents the Isabel Secure Signing Card's Identifier (CardID).
AuthorityInfoAccess	NC	This field gives a pointer to an on-line certificate revocation status service. The value is: https://pki.isabel.be/ocsp for 2048-bit CA and https://pki.isabel.be/ocsp2 for 4096-bit CA.

7.1.8.2. EXTENSIONS OF CERTIFICATES FOR APPLICATION

Following table summarizes the MANDATORY extensions and their value for an Isabel Certificate issued to an application:

Certificate Extension Field	Criticality	Value or Value Format
KeyUsage	NC	This field gives a list of permitted usages for the key. BIT STRING ::= {digitalSignature(0), nonRepudiation(1), keyEncipherment(2), dataEncipherment(3)}
ObjectKeyIdentifier	NC	Key ID

Certificate Extension Field	Criticality	Value or Value Format
authorityKeyIdentifier	NC	This field identifies the CA public key to be used to verify the signature applied on the certificates. OCTET STRING ::= {43 41 30 32} ("CA02") for 2048-bit CA OCTET STRING ::= {43 41 30 34} ("CA04") for 4096-bit CA
CertificatePolicies	NC	This field contains a sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers. These policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used. Has the value {joint-iso-ccitt(2) allocation per country (16) Belgium (56) isabel (1) certification-policies(9) standard(4)} The field also contains an attribute that is a URI to the full version of the CP.
subjectPublicKeyInfo OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) allocation per country (16) Belgium(56) Isabel(1) 8}	NC/C	This field is a proprietary Isabel extension *For Internal use only* This field is Critical for revoked certificates.

7.1.9. ALGORITHM OBJECT IDENTIFIERS

sha-1WithRSAEncryption
OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

sha-256WithRSAEncryption
OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

rsaEncryption
OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.1.10.NAME FORMS

Cf. sections above on Certificate profiles

7.1.11.NAME CONSTRAINTS

Name Constraint extension is not used in Isabel Certificates.

7.1.12.CERTIFICATE POLICY OBJECT IDENTIFIER

C.f. Section 1.2 of the current CP.

7.1.13.USAGE OF POLICY CONSTRAINTS EXTENSION

Policy constraint extension is not used in Isabel Certificates.

7.1.14.POLICY QUALIFIERS SYNTAX AND SEMANTIC

A policy qualifier is defined for the certificate policy defined in the certificate policies extension.

This qualifier is a URI to the full version of the CP:

https://www.isabel.eu/content/dam/isabel6/contrib6/documents/en-US/certificate-policy.pdfProcessing semantics for the critical CP extensionCertificate policies extension is marked as non-critical.

7.2. CRL PROFILE

7.2.1. CRL PROFILE OF 2048-BIT ISABEL CA

The profile of a CRL produced by an Isabel CA is the following:

Certificate Field	Value or Value Format
version	INTEGER {V2(1)} (Note: integer value 1 corresponds to v2 CRLs)
Issuer	CN=Isabel Certification Authority; O=CA; L=ISABEL; C=BE
ThisUpdate	UTCTime. Indicates the time at which the CRL has been produced.
NextUpdate	UTCTime. Indicates when the next CRL will be produced (at the latest).
Signature	AlgorithIdentifier sha-1WithRSAEncryption OID ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
RevokedCertificates	The list of certificates that are revoked.

7.2.1. CRL PROFILE OF 4096-BIT ISABEL CA

The profile of a CRL produced by an Isabel CA is the following:

Certificate Field	Value or Value Format
version	INTEGER {V2(1)} (Note: integer value 1 corresponds to v2 CRLs)
Issuer	CN=Isabel Certification Authority Root; O=CA; L=ISABEL; C=BE
ThisUpdate	UTCTime. Indicates the time at which the CRL has been produced.
NextUpdate	UTCTime. Indicates when the next CRL will be produced (at the latest).
Signature	AlgorithIdentifier sha-256WithRSAEncryption OID ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
RevokedCertificates	The list of certificates that are revoked.

7.2.2. VERSION NUMBER

All Isabel CRLs must be compliant to ITU-T X.509 v2.

7.2.3. CRL AND CRL ENTRY EXTENSIONS

Isabel CRL extensions are:

CRL Extension Field	Criticality	Value or Value Format
authorityKeyIdentifier	NC	This field identifies the CA public key to be used to verify the signature applied on the certificates. OCTET STRING ::= {43 41 30 32} (“CA02”) for 2048-bit CA OCTET STRING ::= {43 41 30 34} (“CA04”) for 4096-bit CA
CrlNumber	NC	INTEGER. The number of the CRL

CRL entries can also contain extensions. Those used in the Isabel CRL entries are listed here:

CRL Entry Extension Field	Criticality	Value or Value Format
ReasonCode	NC	This extension specifies the reason why the entry was revoked. Possible values are: CRLReason ::= ENUMERATED { unspecified (0), keyCompromise (1), caCompromise (2), affiliationChanged (3), superseded (4), cessationOfOperations (5)} Other values are permitted but not used.

8. Compliance audit and other assessments

8.1. FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

The frequency and circumstances of those audits is determined by :

1. Isabel internal policies.
2. The governing Belgian legal framework.
3. Other parties with a right to audit based on their relationship with Isabel.

8.2. IDENTITY / QUALIFICATIONS OF ASSESSORS

A competent independent professional firm that complies with appropriate national and international standards and codes of practice and that has expertise in the domain of PKI can qualify as an independent assessor.

8.3. ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY

The assessors must be independent from Isabel and the Isabel PKI infrastructure.

The assessors shall have a contractual relationship with Isabel for the performance of the audit, and be sufficiently organizationally separated from the audited Isabel CA, Isabel RA or any other Isabel PKI component to provide an unbiased, independent evaluation.

8.4. TOPICS COVERED BY ASSESSMENT

The assessment will determine the compliance of the PKI services with this CPS and the relevant CP. It will determine the business risks of non-compliance with the CPS and CP in accordance with the agreed control objectives.

Assessment will cover all or part of the following topics:

1. The Isabel CA infrastructure.
2. The Isabel CA management.
3. The Isabel CA key management policies and procedures.
4. The Isabel CA operations.
5. The Isabel RA operations.
6. The compliance to Isabel policies, CP and CPS.
7. The compliance to Belgian regulations.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Assessment results will be evaluated by Isabel.

Isabel will undertake to resolve any deficiencies or non-conformities identified as a result of an assessment within an agreed timescale dependent upon the severity of the risk or risks involved.

8.6. COMMUNICATION OF RESULTS

For security reasons, the assessment results are addressed to the Isabel Security Manager and his manager.

Assessment results are considered as strictly confidential information.

Assessment results will not be made public, unless this would be requested by the national law.

9. Other business and legal matters

9.1. FEES

9.1.1. CERTIFICATE ISSUANCE OR RENEWAL FEES

Fees for Isabel Certificates and related services, and their modalities are set forth in contractual agreements agreed between Isabel Certificate Customers and Isabel.

9.1.2. CERTIFICATE ACCESS FEES

Fees for Isabel Certificates access, and their modalities are set forth in contractual agreements agreed between Isabel Certificate Customers and Isabel.

9.1.3. REVOCATION OR STATUS INFORMATION ACCESS FEES

Fees for Isabel Certificates revocation or status information access, and their modalities are set forth in contractual agreements agreed between Isabel Certificate Customers and Isabel.

9.1.4. FEES FOR OTHER SERVICES

Fees for Isabel PKI services, and their modalities are set forth in contractual agreements agreed between Isabel Certificate Customers and Isabel.

9.1.5. REFUND POLICY

Refunds are only applicable in case and as set forth in contractual agreements agreed between Isabel Certificate Customers and Isabel.

9.2. FINANCIAL RESPONSIBILITY

9.2.1. INSURANCE COVERAGE

Isabel will use all reasonable efforts to have sufficient insurance to cover its potential liability in regard to the provision of services under this CP.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. SCOPE OF CONFIDENTIAL INFORMATION

The following information is considered as confidential:

- Information collected by the RAs of Isabel PKI to identify and authenticate Customers and Subscribers.
- Subject’s private key and key activation data.

- Isabel CA's private key.
- Audit trail records of the PKI
- Isabel CPS and operating procedures.

9.3.2. INFORMATION NOT CONSIDERED CONFIDENTIAL

Isabel Certificates and Isabel CP are not considered as confidential information.

9.3.3. RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

Individuals allowed to access confidential information should not disclose them.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. PRIVACY PLAN

Isabel's privacy plan protects sensitive Customer information in accordance with all European Union directives, regulations and Belgian laws.

9.4.2. INFORMATION TREATED AS PRIVATE

Information pertaining to Subscribers is treated as private.

9.4.3. INFORMATION NOT DEEMED PRIVATE

Public information is not deemed as private.

9.4.4. RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

It is afforded the appropriate level of protection in accordance with all European Union directives, regulations and Belgian laws.

9.4.5. NOTICE AND CONSENT TO USE PRIVATE INFORMATION

When the law requires it, a notice and consent to use private information is used.

9.4.6. DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

Isabel is allowed to release confidential information based on a Belgian court order that is duly signed by a competent judge.

9.4.7. OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

There are no other circumstances for Isabel to release its confidential information.

9.5. INTELLECTUAL PROPERTY RIGHTS

All information provided in this document is part of the Intellectual Property Rights of Isabel. This holds for any information published by Isabel, in a public or private relation.

These rights hold beyond any contractual relationship that might exist with Isabel.

The Certificates and means of access and signature, including the public key, are the exclusive property of Isabel. Any use of the Certificates and means of access and signature outside the agreed functionalities of the Isabel system must be laid down in a contract with Isabel. When all Certificates related to the same Public Key have expired or have been revoked, the Subject, Subscriber or Customer may not, after the said expiry or revocation, use the data relating to the corresponding signature creation in order to sign or have such data certified by another certification service provider.

9.6. REPRESENTATIONS AND WARRANTIES

Warranties (if any) are in the PKI contract or any other relevant agreements between Isabel and its Customers.

9.7. DISCLAIMERS OF WARRANTIES

Disclaimers of warranties (if any) are in the PKI contract or any other relevant agreements between Isabel and its Customers.

9.8. LIMITATION OF LIABILITY

Isabel liabilities are set out in the PKI contract or any other relevant agreements between Isabel and its Customers. Except as provided in those agreements, and to the fullest extent permissible by law, Isabel do not accept any liability.

All persons use the Internet at their own risk. Isabel is not liable for matters outside its own control including the availability or working of the Internet, or telecommunications or other infrastructure or systems.

Other liability issues are dealt with in contracts between relevant parties.

9.9. INDEMNITIES

Isabel Customers and/or Third Parties who rely on an Isabel Certificate and/or Isabel Certificate Subjects must indemnify any parties (including Isabel CA, RAs and Revocation Services) and/or Isabel for any damage resulting from a disrespect of their obligations.

A Relying Party who is found to have acted in a manner inconsistent with his/her obligations as stated in the present CP will have no valid claim against Isabel in the event of a damage.

Isabel is not liable for any consequence due to the violation by a Relying Party of his/her obligations.

9.10. TERM AND TERMINATION

If Isabel ceases its PKI activity, Isabel will act as stipulated by the applicable Belgian / European Laws and its PKI contract.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

All official notices required under this CP, shall be in writing and sent by registered mail or fax, or by an email message signed with an advanced electronic signature.

9.12. AMENDMENTS

Comments, questions and change requests to the present Isabel CP should be addressed to its Policy Authority specified in section 1.3.5 of the present Isabel CP.

Isabel may amend this CP at any time.

No amendment will have retrospective effect.

9.13. DISPUTE RESOLUTION PROCEDURES

All parties involved in the Isabel PKI, including the Isabel CA, RA, Customers, Subscribers, Subjects and Relying Parties, shall in good faith and to their reasonable efforts try to find an amicable solution for any claims, disputes or discussions between them.

When no amicable solution to a dispute can be found within a reasonable time, all disputes will be submitted to the exclusive jurisdiction of the Courts of Brussels.

9.13.1.NAME CLAIM DISPUTE RESOLUTION PROCEDURE

Isabel CA is authorised to resolve any dispute related to DNs used in the Subject field of Isabel Certificates within the X.500 namespace(s) for which Isabel has been authorised.

9.14. GOVERNING LAW

The laws of Belgium shall govern the enforceability, construction, interpretation, and validity of the present Isabel Certification Practice Statement.

9.15. COMPLIANCE WITH APPLICABLE LAW

Please refer to 9.14.

9.16. MISCELLANEOUS PROVISIONS

Any PKI contract or agreement referring to this CP will specify that the terms of this CP will continue to apply in the event of severance, survival, merger or notice affecting any party.

9.16.1.SEVERABILITY, SURVIVAL, MERGER, NOTICE

To the extent that any court of competent jurisdiction or similar body holds any of the terms and conditions of this document to be invalid, unenforceable or illegal, those terms and conditions shall be severed from the remainder of this document, which shall remain in force. Those terms and conditions shall be replaced by a clause which comes as close as possible to the intention of the clause that is invalid.

In case, exceptionally, the laws of a territory governing a foreign Isabel Certificate Subscriber or Subject don't allow the inclusion of specific provisions of this CP, then with respect to that Isabel Certificate Subscriber or Subject only, these specific provisions of this CP shall be deemed null and void as if not included and the first paragraph of the present section shall be applicable.

The provisions that by nature need to survive the termination of the validity of this CP, shall so survive.

In case of merger Isabel S.A./N.V. shall to its best efforts ensure the continuity of the CA operations referred herein.

9.17. OTHER PROVISION

Not stipulated

10. APPENDIX - REFERENCES

	Title	Owner	Date
[1]	'Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic Signatures'	European Parliament and European Council	13 December 1999
[2]	'Wet houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische hantekeningen en certificatiediensten'	Belgian Parliament	9 July 2001
[3]	ITU-T Recommendation X.509	ITU-T	June 1997
[4]	RFC 3647: 'Internet X.509 Public Key Infrastructure – CP and Certification Practices Framework'	Internet Engineering Task Force (IETF)	November 2003
[5]	Banking – Public Key Infrastructure Policy and Practices framework – ISO/TC68/SC2/WG8 N 001	International Standards Organisation	22 October 2002
[14]	FIPS PUB 140-2	NIST	December 2002
[17]	NIST Special Publication 800-57: Recommendation for Key Management – Part 2: Best Practices for Key Management Organization	NIST	February 2005