PKI@KBC Certificate Policy

version 1.0

Date of publication: October 22, 2007

Effective date: October 29, 2007

Table of contents

TABLE OF CONTENTS 2

1. INTRODUCTION 6

1.1. Overview 6

1.2. Identification 6

1.2.1. Name 6

1.2.2. Object identifier 6

1.2.3. Uniform Resource Identifier 7

1.2.4. Document version history 7

1.3. Community and Applicability 7

1.3.1. Certification Authority 7

1.3.2. Registration Authorities 7

1.3.3. End entities 8

1.3.4. Validation Authorities 8

1.3.5. Policy Authorities 8

1.3.6. Applicability 8

1.3.7. Contact details 9

2. GENERAL PROVISIONS 10

2.1. Obligations 10

2.1.1. Isabel Certification Authority Obligations 10

2.1.2. PKI@KBC RAs Obligations 11

2.1.3. PKI@KBC Certificate Subscriber and Subject obligations 12

2.1.4. Relying Party obligations 13

2.1.5. Repository obligations 15

2.2. Liability 15

2.2.1. CA Liability 15

2.2.2. PKI@KBC RA Liability 17

2.2.3. Liability of the PKI@KBC Customer, Subscriber, Subject, Relying Party 19

2.3. Financial responsibility 20

2.3.1. Indemnification by PKI@KBC Customers, Relying Parties and Subjects 20

2.3.2. Fiduciary Relationships 20

2.4. Interpretation and enforcement 20

2.4.1. Governing law 20

2.4.2. Severability, Survival, Merger, Notice 21

2.4.3. Dispute resolution procedures 21

2.5. Fees 21

2.6. Publication and repository 21

2.6.1. Publication of Isabel CA information 21

2.6.2. Frequency of publication 22

2.6.3. Access Control 22

2.6.4. Repositories 22

2.7. Compliance audit 22

2.7.1. Frequency of entity compliance audit 22

2.7.2. Identity/qualification of auditors 23

2.7.3. Auditor's relationship to audited party ... 23
2.7.4. Topics covered by audit ... 23
2.7.5. Actions taken as a result of deficiency ... 23
2.7.6. Communication of results ... 23
2.8. Confidentiality ... 24
2.8.1. Types of information to be kept confidential ... 24
2.8.2. Types of information not considered confidential ... 24
2.8.3. Disclosure of certificate revocation information ... 24
2.8.4. Release to law enforcement officials ... 24
2.8.5. Release as part of civil discovery ... 24
2.8.6. Disclosure upon Subscriber/Subject request ... 24
2.8.7. Other information release circumstances ... 25
2.9. Intellectual Property Rights ... 25

3. IDENTIFICATION AND AUTHENTICATION ... 26
3.1. Initial Registration ... 26
3.1.1. Types of names ... 26
3.1.2. Need for names to be meaningful ... 26
3.1.3. Rules for interpreting various name forms ... 26
3.1.4. Uniqueness of names ... 26
3.1.5. Name claim dispute resolution procedure ... 26
3.1.6. Recognition, authentication and role of trademarks ... 27
3.1.7. Method to prove possession of private key ... 27
3.1.8. Authentication of organization identity ... 27
3.1.9. Authentication of individual identity ... 27
3.2. Routine Rekey ... 27
3.3. Rekey after Revocation ... 27
3.4. Revocation Request ... 27
3.4.1. Authentication by the Revocation Services ... 28
3.4.2. Authentication by the PKI@KBC Revocation Service ... 28
3.4.3. Authentication by the Card Stop Revocation Service ... 28
3.4.4. Authentication by the Isabel CA ... 28

4. OPERATIONAL REQUIREMENTS ... 29
4.1. Certificate Application ... 29
4.2. Certificate Issuance ... 29
4.3. Certificate Acceptance ... 29
4.4. Certificate Suspension and Revocation ... 29
4.4.1. Circumstances for revocation ... 29
4.4.2. Who can request revocation ... 30
4.4.3. Procedure for revocation request ... 30
4.4.4. Revocation request grace period ... 30
4.4.5. Circumstances for suspension ... 30
4.4.6. Who can request suspension ... 30
4.4.7. Procedure for suspension request ... 30
4.4.8. Limits on suspension period ... 30
4.4.9. CRL issuance frequency ... 31
4.4.10. CRL checking requirements ... 31
4.4.11. On-line revocation/status checking availability ... 31
4.4.12. On-line revocation checking requirements ... 31

4.4.13. Other forms of revocation advertisements available 31
4.4.14. Checking requirements for other forms of revocation advertisements 31
4.4.15. Special requirements re key compromise 31
4.5. Security Audit Procedures 31
4.5.1. Types of data recorded 31
4.5.2. Frequency of processing log 32
4.5.3. Retention period for audit log 32
4.5.4. Protection of audit log 32
4.5.5. Audit log backup procedures 32
4.5.6. Audit collection system (internal vs external) 32
4.5.7. Notification to event-causing subject 32
4.5.8. Vulnerability assessments 32
4.6. Records Archival 33
4.6.1. Types of event recorded 33
4.6.2. Retention period for archive 33
4.6.3. Protection of archive 33
4.6.4. Archive backup procedures 33
4.6.5. Requirements for time-stamping of records 33
4.6.6. Archive collection system (internal or external) 33
4.6.7. Procedures to obtain and verify archive information 33
4.7. Key changeover 34
4.8. Compromise and Disaster Recovery 34
4.9. CA/RA Termination 34

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS 35
5.1. Physical Controls 35
5.2. Procedural Controls 35
5.2.1. Trusted roles 35
5.2.2. Number of persons required per task 35
5.2.3. Identification and authentication for each role 35
5.3. Personnel Controls 35

6. TECHNICAL SECURITY CONTROLS 36
6.1. Key Pair Generation and Installation 36
6.1.1. Key pair generation 36
6.1.2. Private key delivery to entity 36
6.1.3. Public key delivery to certificate issuer 36
6.1.4. CA public key delivery to users 36
6.1.5. Key sizes 36
6.1.6. Public key parameters generation 37
6.1.7. Parameter quality checking 37
6.1.8. Hardware/software key generation 37
6.1.9. Key usage purposes (as per X.509 v3 key usage field) 37
6.2. Private Key Protection 37
6.2.1. Standards for cryptographic module 37
6.2.2. Private key (n out of m) multi-person control 37
6.2.3. Private key escrow 37
6.2.4. Private key backup 37
6.2.5. Private key archival 38
6.2.6. Private key entry into cryptographic module 38

6.2.7. Method of activating private key 38
6.2.8. Method of deactivating private key 38
6.2.9. Method of destroying private key 38
6.3. Other Aspects of Key Pair Management 38
6.3.1. Public key archival 38
6.3.2. Usage periods for the public and private keys 38
6.4. Activation Data 39
6.4.1. Activation data generation and installation 39
6.4.2. Activation data protection 39
6.4.3. Other aspects of activation data 39
6.5. Computer Security Controls 39
6.6. Life Cycle Technical Controls 39
6.7. Network Security Controls 39
6.8. Cryptographic Module Engineering Controls 39

7. CERTIFICATE, CRL, OCSP PROFILES 40
7.1. Certificate Profile 40
7.1.1. Version number 41
7.1.2. Certificate extensions 41
7.1.3. Algorithm Object Identifiers 42
7.1.4. Name forms 42
7.1.5. Name constraints 42
7.1.6. Certificate Policy Object Identifier 42
7.1.7. Usage of Policy Constraints extension 43
7.1.8. Policy qualifiers syntax and semantic 43
7.1.9. Processing semantics for the critical certificate policy extension 43
7.2. CRL profile 43
7.3. OCSP profile 43

8. SPECIFICATION ADMINISTRATION 44
8.1. Specification change procedures 44
8.2. Publication and notification policies 44
8.3. PKI@KBC Certificate Policy approval procedures 44
8.4. Term and Termination 44

9. APPENDIXES 45
9.1. Appendix A – Definitions 45
9.1.1. Acronyms 45
9.1.2. Glossary 46
9.2. Appendix B – References 48

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 applications with common security requirements”.

The term CPS is defined by the American Bar Association Guidelines as: "A statement of the practices which a Certification Authority (CA) employs in issuing certificates".

Whereas the CP states mainly “*which*” the basic obligations are of the CA and the other parties involved in the PKI practice, the CPS shall focus in more detail on the question "*how*" these obligations are met by the CA and the other parties involved in the PKI practice.

1.1. OVERVIEW

The present “PKI@KBC Certificate Policy” states the applicability of, and the set of rules applicable to the “PKI@KBC Certificates”. It defines the requirements for issuance, management and use of the public key certificates designated as PKI@KBC Certificates and associated cryptographic technology used for authentication, confidentiality, data integrity and non-repudiation security services.

A PKI@KBC Certificate is a certificate issued by an Isabel CA for specific purposes of KBC.

The present CP:

1. Describes the entities that are part or use the services of the Isabel Public Key Infrastructure in the scope of the application for, issuance, acceptance, use and revocation of PKI@KBC Certificates.
2. Describes the applicability of PKI@KBC Certificates to third parties.
3. Describes the obligations and liabilities of the entities that participate in the application for, issuance, acceptance, use and revocation of PKI@KBC Certificates.
4. Describes the PKI@KBC Certificate profile.
5. Provides a glossary of terms and a list of reference documents.

As stated in sections 1.3.6 and 2.1.4, PKI@KBC Certificate Subjects and Relying Parties must assure themselves, by reviewing this document, any other information they deem necessary, that any PKI@KBC Certificate issued or other service provided by Isabel CA under this Policy is suitable for the intended use.

By relying on information contained in a PKI@KBC Certificate issued by an Isabel CA, a Relying Party is agreeing with the provisions and stipulations of this.

1.2. IDENTIFICATION

1.2.1. NAME

The present CP is named “PKI@KBC Certificate Policy”.

1.2.2. OBJECT IDENTIFIER

The Object Identifier associated with the “PKI@KBC Certificate Policy” is 2.16.56.1.9.46.1.1.

1.2.3. UNIFORM RESOURCE IDENTIFIER

The PKI@KBC Certificate Policy will be publicly available on the web site of KBC at following URL : https://www.kbc.com/certificate-policy.

1.2.4. DOCUMENT VERSION HISTORY

Revisions of this document have been made as follows:

Date	Changes	Version
June 19, 2007	New Version	0.1
July 11, 2007	Finale draft by Isabel	0.4
July 20, 2007 July 25, 2007	Corrected with comments from KBC CA liability updated	0.5
October 15, 2007	Final Version	1.0

1.3. COMMUNITY AND APPLICABILITY

1.3.1. CERTIFICATION AUTHORITY

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".

In the Isabel Public Key Infrastructure, the Isabel Certification Authority may accept Certificate Requests for Certificate Subjects whose identity has been authenticated by a PKI@KBC Registration Authority (RA).

After a certificate request which is filed by the PKI@KBC RA to the Isabel CA has been verified by the Isabel CA, a PKI@KBC Certificate, binding the Certificate Subject's identity to his/her Public Key, is issued.

1.3.2. REGISTRATION AUTHORITIES

According to RFC 3647 [4], an RA is "An entity that 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.".

In the Isabel Public Key Infrastructure, PKI@KBC RAs operating under the control and the authority of an Isabel CA accept PKI@KBC Certificate Applications for a PKI@KBC Certificate from PKI@KBC Certificate Subscribers.

PKI@KBC RAs must authenticate the identity of the PKI@KBC Certificate Subject and must perform verification of the information contained in the PKI@KBC Certificate Application. If the verified information is correct, the PKI@KBC RA sends a PKI@KBC Certificate request to the appropriate Isabel CA to issue a PKI@KBC Certificate for the PKI@KBC Certificate Subject.

Only Registration Authorities authorized by KBC are permitted to submit certificate requests to an Isabel CA for the issuance of PKI@KBC Certificates. KBC will post a list of authorized Registration Authorities on its website https://www.kbc.be.

1.3.3. END ENTITIES

In the scope of the present PKI@KBC Certificate Policy, end entities in the Public Key Infrastructure consist of:

1. PKI@KBC Certificate Subscriber
2. PKI@KBC Certificate Subject
3. PKI@KBC Certificate Relying Party

A PKI@KBC Customer mandates PKI@KBC Certificate Subscribers and PKI@KBC Certificate Subjects.

The Subject attribute field in the PKI@KBC Certificate is used to name or otherwise identify the PKI@KBC Certificate Subject with:

1. Either a name and first name for a Physical Person Subject.
2. Either a function name for a Function Subject.

In the scope of the present PKI@KBC Certificate Policy:

1. a PKI@KBC Certificate Subject may not be a CA or an RA in the Isabel Public Key Infrastructure,
2. a signature of Function Subject is a technical signature, i.e. it may only be used for integrity reasons, not for transaction authorisation, unless specified otherwise in the contract between the PKI@KBC Customer and KBC.

1.3.4. VALIDATION AUTHORITIES

In the Isabel Public Key Infrastructure, the Validation Authority provides any Relying Party with a way of obtaining PKI@KBC Certificate revocation status information.

On-Line Certificate Status Protocol (OCSP) responders provide revocation status for PKI@KBC Certificates.

Website support for manual verification of revocation status of individual certificates will be provided in the future.

1.3.5. POLICY AUTHORITIES

A Policy Authority is the entity responsible for:

1. The specification, validation and publication of the PKI@KBC Certificate Policy and its revisions.
2. Determining the suitability and the correct implementation of the PKI@KBC CP.
3. The definition of the review requirements and processes relating to the implementation of the CPs.

The Policy Authority for the present PKI@KBC CP is: see "1.3.7 – Contact details".

1.3.6. APPLICABILITY

PKI@KBC Certificates issued in accordance with the present CP may only be used by Relying Parties who are part of a PKI@KBC Customer AND for following purposes: verifying digital signatures, non repudiation, enciphering keys and enciphering data.

Relying Parties must have a contractual relationship with KBC.

If a PKI@KBC Certificate Subject wants to have any limitations (financial or otherwise) applicable to transactions authenticated by the PKI@KBC Certificate, that Subject must have a signed agreement with each Relying Party agreeing to such limitations.

1.3.7. CONTACT DETAILS

1.3.7.1. SPECIFICATION ADMINISTRATION ORGANISATION

The KBC Security Manager acts as the Policy Authority for the present PKI@KBC CP. It is responsible for all aspects of the present PKI@KBC CP, including its specification, validation, registration, publication, maintenance and interpretation.

1.3.7.2. POLICY AUTHORITY CONTACT PERSON

All questions and comments regarding the present PKI@KBC CP should be addressed to the representative of its Policy Authority:

KBC Security Manager
KBC Group NV/SA
ELB / Leubrust
Brusselsesteenweg 100
B-3000 Leuven
Belgium
E-mail: kbc.marketing.ebanking@kbc.be
Web: www.kbc.be

2. General provisions

2.1. OBLIGATIONS

This section describes the obligations of the entities that participate, within the Isabel PKI, to the application for, issuance, acceptance, use, publication and revocation of PKI@KBC Certificates.

PKI@KBC Certificate Relying Parties must understand the provisions of this section before relying on a PKI@KBC Certificate.

Those entities are:

1. Isabel CA
2. PKI@KBC RAs
3. PKI@KBC Certificate Subscribers and Subjects
4. PKI@KBC Certificate Relying Parties
5. Isabel Repository
6. Policy Authority
7. legal entity KBC

To request a PKI@KBC Certificate to the Isabel CA for a PKI@KBC subscriber, the PKI@KBC RA must accept the obligations described hereafter.

To issue a PKI@KBC Certificate, the Isabel CA must accept the obligations described hereafter.

By accepting an issued PKI@KBC Certificate, a PKI@KBC Certificate Subject accepts the obligations and statements described hereafter.

By making use of a PKI@KBC Certificate, a PKI@KBC Certificate Relying Party accepts its obligations and the statements described hereafter.

2.1.1. ISABEL CERTIFICATION AUTHORITY OBLIGATIONS

The Isabel CA issuing PKI@KBC Certificates in the Isabel Public Key Infrastructure, has the following obligations:

2.1.1.1. Notification of Certificate issuance

The Isabel CA ensures that the PKI@KBC Certificate Subject is notified about the issuance of his/her PKI@KBC Certificate.

2.1.1.2. Publish PKI@KBC Certificate in an Isabel Repository

The Isabel CA publishes a PKI@KBC Certificate it has issued after the certificate has been accepted by the PKI@KBC Certificate Subject.

2.1.1.3. Accuracy of representations

By publishing a PKI@KBC Certificate that references this CP, the Isabel CA guarantees, to all who reasonably rely on the information contained in the PKI@KBC Certificate, that it has issued the PKI@KBC Certificate to the named PKI@KBC Certificate Subject in accordance with the provisions in the present PKI@KBC CP.

2.1.1.4. PROCESS CERTIFICATE REVOCATION REQUESTS

The Isabel CA processes securely PKI@KBC Certificate revocation requests issued by PKI@KBC RAs under its control. Publication of the revocation is specified in section “2.6.2 – Frequency of publication”.

2.1.1.5. PUBLISH PKI@KBC CERTIFICATE REVOCATION INFORMATION IN AN ISABEL REPOSITORY

The Isabel CA publishes revocation information about the PKI@KBC Certificate it has revoked in an Isabel repository in the form of an updated Certificate Revocation List (CRL).

The Isabel CA complies with the provisions stated in the section “2.6 – Publication and repository” of the present PKI@KBC CP and respects timing specified in section “2.6.2 – Frequency of publication”.

This mechanism allows PKI@KBC Certificate Relying Parties to obtain timely and unambiguous knowledge of the revocation status of any PKI@KBC Certificate issued by the Isabel CA.

2.1.1.6. NOTIFICATION OF REVOCATION OF A CERTIFICATE

The Isabel Certification Authority ensures that the entity (either the PKI@KBC Certificate Subject or the PKI@KBC Certificate Subscriber) that has requested the revocation of a PKI@KBC Certificate to a PKI@KBC Registration Authority and any other parties who reasonably rely on that PKI@KBC Certificate are notified of the PKI@KBC Certificate revocation.

The Isabel Certification Authority ensure that the revocation information is available to parties

2.1.1.7. STANDARDS COMPLIANCE

Issued PKI@KBC Certificates must comply with the standard X.509 version 3.

2.1.1.8. ARCHIVING AND SECURITY

The Isabel Certification Authority respects its archiving duties in a most secure manner in order to secure the availability of documents and/or other information for evidence, and in order to safeguard confidentiality and integrity of such documents and other information. In general, it assures the physical security of information, protects the access thereto and instructs its personnel.

2.1.1.9. PERSONAL DATA PROTECTION

The Isabel CA shall be prudent in the handling of personal and confidential data in line with the Belgian Law on the protection of the Privacy.

2.1.2. PKI@KBC RAS OBLIGATIONS

A PKI@KBC RA, approved and operating within the Isabel Public Key Infrastructure, has the following specific obligations:

2.1.2.1. PROTECTION OF RA PRIVATE KEY

A PKI@KBC RA must protect and guarantee the sole possession and the confidentiality and safety of its Private Key and the confidentiality of the associated Activation Data.

2.1.2.2. RESTRICTION ON RA PRIVATE KEY USE

A PKI@KBC RA uses its Private Key only for purposes associated with its RA function.

2.1.2.3. INDEMNIFY PARTIES FOR DAMAGES

A PKI@KBC RA indemnifies parties for any damage resulting from a disrespect of its obligations, within the limits specified in section “2.2 – Liability” of the present PKI@KBC Certificate Policy.

2.1.2.4. ARCHIVING AND SECURITY

The PKI@KBC RA respects its archiving duties in a most secure manner in order to secure the availability of documents and/or other information for evidence, and in order to safeguard confidentiality and integrity of such documents and other information. In general, it assures the physical security of information, protects the access thereto and instructs its personnel.

2.1.2.5. APPROVAL

Each PKI@KBC RA has an approval for operation from KBC. KBC has a list of approved PKI@KBC RAs. By performing activities as a PKI@KBC RA for an Isabel CA, the PKI@KBC RA certifies that he has accepted this responsibility and has agreed to operate in compliance with the present CP.

2.1.3. PKI@KBC CERTIFICATE SUBSCRIBER AND SUBJECT OBLIGATIONS

PKI@KBC Certificate Subscribers and Subjects are in general obliged to respect the statements, conditions and procedures of the present CP, which they shall be deemed to have accepted by using a PKI@KBC Certificate.

PKI@KBC Certificate Subscribers and Subjects agree to uphold these obligations throughout the operational period of the PKI@KBC Certificate.

A Subscriber shall sign an agreement with a PKI@KBC RA at or prior to the time of issuance of the Certificate. The PKI@KBC RA retains a copy of the agreement. Subscribers are bound by rights and obligations to KBC through their contractual agreement with the PKI@KBC RA.

PKI@KBC Certificate Subscriber and PKI@KBC Certificate Subject have the following obligations:

2.1.3.1. OBTAIN THE NECESSARY INFORMATION TO CORRECTLY AND SAFELY USE THE ISABEL PKI SERVICES

A PKI@KBC Certificate Subject is obliged to obtain from the PKI@KBC RA that has issued his/her PKI@KBC Certificate:

1. A notification about his/her obligations
2. A notification about the requirements regarding the protection of his/her Private Key
3. A notification about the precise guarantees that are offered by the Isabel PKI services

The publication of the present PKI@KBC CP to the PKI@KBC Certificate Subjects and PKI@KBC Certificate Relying Parties should be considered as a notification. The use of the PKI@KBC Certificate by the Subject shall imply the acceptance of the statements in the mentioned notifications.

2.1.3.2. GUARANTEE CONFIDENTIALITY OF PRIVATE KEY

A PKI@KBC Certificate Subject must protect and guarantee the sole possession and the confidentiality and safety of his/her Private Key and the confidentiality of the Activation Data.

In general, the Subject shall take necessary precautions to prevent loss, disclosure to any party, modification or unauthorized use of key materials and PKI@KBC Secure Signing Card with its associated Activation Data.

Every use of the Private Key of the Subject shall be deemed to be a use by the Subject until sufficiently demonstrated otherwise.

2.1.3.3. Restriction on private key and PKI@KBC Certificate usage

A PKI@KBC Certificate Subject may only use his/her Private Key and PKI@KBC Certificate for allowed key usage purposes, in compliance with the provisions stated in:

1. the section “1.3.6 – Applicability” of the present PKI@KBC CP.
2. any agreement made or to be made between KBC and the PKI@KBC Customer.

When the Subject suspects that his Private Key has been compromised, he must request the revocation of his PKI@KBC Certificate and cease generating digital signature with this Private Key.

When all certificates related to the same Public Key have been revoked or are expired, the Public Key becomes invalid and the Subject is not allowed to use the corresponding Private Key; this is a.o. to generate a digital signature, nor to decrypt.

2.1.3.4. Notification to the PKI@KBC Revocation Service or the PKI@KBC RA about private key/PIN compromise – PKI@KBC Secure Signing Card Loss

A PKI@KBC Certificate Subject or a PKI@KBC Certificate Subscriber must immediately notify either the PKI@KBC Revocation Service or the PKI@KBC RA about:

1. The suspected or known compromise, loss or disclosure of the Subject’s Private Key.
2. The suspected or known loss of the Subject’s PKI@KBC Secure Signing Card.
3. The suspected or known compromise loss or disclosure of the Subject’s PIN code.

Alternatively, if neither the PKI@KBC Revocation Service nor the PKI@KBC RA can be reached, Card Stop Revocation Service may be notified in accordance with section “3.4 – Revocation Request”.

2.1.3.5. Notification to the PKI@KBC RA about change of status

A PKI@KBC Certificate Subject or a PKI@KBC Certificate Subscriber must immediately notify his/her PKI@KBC RA about any change in the information provided in the application for the Subject’s PKI@KBC Certificate.

2.1.3.6. Use a hardware Secure Signature Creation Device

A PKI@KBC Certificate Subject must use hardware Secure Signature Creation Device to store and use his/her Private Key: the PKI@KBC Secure Signing Card.

2.1.3.7. Restriction on Public Key Usage

The PKI@KBC Certificate Subject or Subscriber may not submit a certificate request containing the Public Key in a PKI@KBC Certificate to a third party CA, even if the PKI@KBC Certificate has expired or has been revoked.

The PKI@KBC Certificate Subject or Subscriber may not submit a certificate request containing the Public Key contained in any other Certificate to an Isabel CA, even if the other Certificate has expired or has been revoked.

2.1.4. RELYING PARTY OBLIGATIONS

A Relying Party has specifically the following obligations:

2.1.4.1. Obtain the necessary information to correctly and safely use the Isabel PKI services

A Relying Party is obliged to obtain, from the Isabel CA that has issued the PKI@KBC Certificate he intends to rely on, a notification about the precise guarantees, liabilities and obligations that are offered by the Isabel PKI services in accordance with the section “2.2 – Liability” of the present PKI@KBC CP.

The Relying Party must read and accept the notified statements. In general, the Relying Party shall accept this CP before making use of any PKI@KBC Certificate issued by an Isabel CA, including all applicable liability limitations and warranties. Furthermore, a Relying Party must be aware of and abide by all rules, regulations and statutes applicable to all information contained in a PKI@KBC Certificate.

2.1.4.2. OBTAIN AND VERIFY THE ISABEL CA SELF-SIGNED CERTIFICATE

A Relying Party is obliged to obtain and verify the validity of the Isabel CA Self-signed certificate at the root of the chain of certificates needed to verify the validity of a PKI@KBC Certificate.

A Relying Party is obliged to verify and accept the content and the validity of the Isabel CA Self-signed Certificate before relying on this certificate.

A Relying Party must verify following attributes in the Isabel CA Self-signed Certificate:

1. The issuer (Isabel CA),
2. The validity period,
3. The key and certificate usage and limitations,
4. The signature of the CA.

A Relying Party must accept the Isabel CA Self-signed Certificate, in compliance with provision set in “4.3 – Certificate Acceptance”.

2.1.4.3. RESTRICTION ON PKI@KBC CERTIFICATE USAGE

A Relying Party can only rely on a PKI@KBC Certificate for allowed usage purposes, and within the limitations as to functional use and value, in compliance with the provisions stated in the section “1.3.6 – Applicability” of the present CP.

A Relying Party is obliged to verify and accept the content and the validity of a PKI@KBC Certificate before relying on this Certificate.

A Relying Party must verify following attributes in a PKI@KBC Certificate:

1. The issuer (Isabel CA),
2. The validity period,
3. The revocation status,
4. The key and certificate usage and limitations as specified in the PKI@KBC Certificate in accordance with section “7.1.2 – Certificate extensions”,
5. The signature of the CA.

The attributes of a PKI@KBC Certificate can be found in section “7.1 – Certificate Profile” of the present PKI@KBC CP.

A Relying Party may not rely on a PKI@KBC Certificate when:

1. The verification of the digital signature of the Isabel CA on the PKI@KBC Certificate fails, or the verification of the PKI@KBC Certificate itself fails or
2. This PKI@KBC Certificate has expired or
3. This PKI@KBC Certificate has been revoked or
4. The PKI@KBC Certificate is used for not-allowed purposes or is not used within the limitations of use.

2.1.4.4. VERIFY SIGNATURES

A Relying Party is obliged to check a digital signature with the PKI@KBC Certificate certifying the Public Key associated to the Private Key used to generate the digital signature.

2.1.4.5. DISRESPECT OF RELYING PARTY OBLIGATIONS

The Relying Party shall be well aware of the provisions stated in the section “2.3.1 – Indemnification by PKI@KBC Customers, Relying Parties and Subjects” and in the section “2.2 – Liability” of the present PKI@KBC CP.

2.1.5. REPOSITORY OBLIGATIONS

Isabel makes available and maintains an Electronic Repository for PKI@KBC Certificates and PKI@KBC Certificate Revocation information.

Isabel protects this Electronic Repository against unauthorized modifications on a best effort basis.

This electronic repository will at least contain:

1. The PKI@KBC Certificates that have been issued by the Isabel Certification Authority in compliance with the present PKI@KBC CP.
2. The Certificate Revocation List published in accordance with the present PKI@KBC CP.
3. The Self-signed Certificate of the Isabel Certification Authority.
4. The current version of this document PKI@KBC Certificate Policy

The Electronic Repository is permanently (24/24) available for direct consultation in an electronic way.

The Electronic Repository is not consultable by non PKI@KBC Customers nor their representatives.

2.2. LIABILITY

2.2.1. CA LIABILITY

2.2.1.1. WARRANTIES AND LIMITATIONS ON WARRANTIES

Isabel warrants only that any PKI@KBC Certificate issued, were issued in accordance with the provisions of the present PKI@KBC CP for that level of assurance. In addition other warranties may exist by operation of law.

Unless otherwise agreed and within the limits of the applicable law, Isabel disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided, and further disclaim any and all liability for negligence and lack of reasonable care on the part of PKI@KBC Subscribers, Subjects, Customers and Relying Parties. The warranties apply to PKI@KBC Subscribers, Subjects, Customers and Relying Parties.

2.2.1.2. EXCLUSION OF ISABEL'S LIABILITY TOWARDS PKI@KBC SUBSCRIBERS, SUBJECTS, CUSTOMERS AND RELYING PARTIES

Limitations of liability shall include an exclusion of indirect, special, incidental, and consequential damages.

Isabel shall, unless otherwise stated below, not be liable for any loss or damage suffered by, claims made against or costs incurred by PKI@KBC Subscribers, Subjects, Customers and/or Relying Parties to the extent that such loss, damage, claims or costs arise from the following:

1. any loss or compromise of Isabel's Private Key, unless Isabel failed to comply with the requirements set out in this PKI@KBC CP, in which case Isabel will (subject to any other restrictions or exclusions below) be liable to a Relying Party to the extent that such Relying Party is able to demonstrate that it suffered loss or damage as a result of Isabel's failure to do so,

2. any inaccurate or incorrect information contained in any PKI@KBC Certificate issued by Isabel, unless Isabel failed to use all reasonable efforts to ensure the accuracy and correctness of such information or unless Isabel failed to verify the authenticity of all documentary evidence of such information according to the present PKI@KBC CP, in which case Isabel will (subject to any other restrictions or exclusions below) be liable to a Relying Party to the extent that such Relying Party is able to demonstrate that it suffered loss or damage as a result of Isabel's failure to do so,
3. a Relying Party's reliance on any revoked PKI@KBC Certificate issued by Isabel where such Relying Party failed to verify with the Validation Authority that the relevant PKI@KBC Certificate has not been revoked,
4. a Relying Party's reliance on any PKI@KBC Certificate issued by Isabel where such Relying Party knew or reasonably should have known that the relevant PKI@KBC Certificate has been revoked but where the Relying Party nonetheless accepts and places reliance on such PKI@KBC Certificate,
5. any unavailability of the Validation Authority, repository for any reason whatsoever,
6. any incorrect or inaccurate information contained in Isabel’s CRL, used by the Validation Authority, unless Isabel failed to update its CRL in accordance with the procedures specified in the present PKI@KBC CP, in which case Isabel will, subject to any other restrictions or exclusions below, be liable to a Relying Party to the extent that such Relying Party is able to demonstrate that it suffered loss or damage as a result of Isabel's failure to do so,
7. any failure by any PKI@KBC Registration Authority to comply with its obligations under the applicable PKI@KBC CP or any agreement (if any) between a Relying Party and that PKI@KBC Registration Authority, as the case may be,
8. any loss or compromise of any PKI@KBC Registration Authority’s Private Key,
9. any failure by any Revocation Service to comply with its obligations under the applicable PKI@KBC CP,
10. any loss or compromise of any Revocation Service Private Key,
11. any failure by any other party, including any PKI@KBC Registration Authority, to comply with any of its stated obligations towards a Relying Party,
12. any other use of the PKI@KBC Certificate, Private Key and/or software, than the use allowed by the present PKI@KBC CP;
13. any modifications or changed situations, not notified to Isabel;
14. any misuse or abuse by PKI@KBC Subscribers, Subjects, Customers and/or Relying Parties.

2.2.1.3. Indirect and Consequential Loss towards PKI@KBC Subscribers, Subjects, Customers and Relying Parties

Even if Isabel has been advised of the possibility of such damages, Isabel shall under no circumstances be liable for:

1. any indirect or consequential loss or damage;
2. any loss of profits;
3. any punitive damages;
4. consequences of actions and claims brought against the PKI@KBC Subscribers, Subjects, Customers and Relying Parties by third parties ;
5. any loss of goodwill;
6. any loss of anticipated savings;
7. any loss of revenue;
8. any loss of business;

9. any business interruption; or
10. loss of information or data.

2.2.1.4. LIMITATIONS ON ISABEL'S LIABILITY TOWARDS PKI@KBC SUBSCRIBERS, SUBJECTS, CUSTOMERS AND RELYING PARTIES

Provided Isabel is liable, under no circumstances the entire liability of Isabel to all parties, including but not limited to PKI@KBC Subscribers, Subjects, Customers, or Relying Parties, in respect of any single claim or series of related claims, exceed the applicable liability cap for such PKI@KBC Certificate set forth below. The aggregate liability of Isabel to any and all persons concerning a PKI@KBC Certificate shall, for the entire of all signatures and transactions related to such PKI@KBC Certificate, be limited to 2.500 EUR. This liability cap of 2.500 EUR is applicable between Isabel on the one hand and on the other hand PKI@KBC Subscribers, Subjects, Customers and Relying Parties.

This limitation on damages applies to loss and damages of all types, incurred by any person, including without limitation a PKI@KBC Subscriber, Subject, Customer, or Relying Party, that are caused by reliance on or use of a PKI@KBC Certificate Isabel issues, manages, uses, revokes, or such a certificate that expires. This limitation on damages applies as well to liability under contract, tort, and any other form of liability claim. The liability cap on each PKI@KBC Certificate shall be the same regardless of the number of digital signatures, transactions, or claims related to such certificate. In the event the liability cap is exceeded, the liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court or competent jurisdiction. In no event Isabel will be obligated to pay more than the aggregate liability cap for each certificate.

2.2.1.5. FORCE MAJEURE EVENTS

If Isabel is prevented, hindered or delayed from or in performing any of its obligations, whether under this document or under any other relevant document, by a force majeure event, such as war, terrorism, insurrection, strikes, social conflict, accident, fire, flood or incidents relating to third parties (such as delays in transport or delivery, equipment breakdown or problems with data communication connections, then Isabel shall not be liable for:

1. any failure or delay by it to perform any such obligations to the extent that such failure is a result of the force majeure event; and
2. any loss or damage of whatsoever nature suffered by, claims of whatsoever nature made against or costs of whatsoever nature incurred by Relying Parties arising from such failure or delay by Isabel to perform any such obligations which are affected by the force majeure event.

2.2.1.6. LIMITATION ON ISABEL'S EXCLUSION OR LIMITATION OF LIABILITY

Nothing in this document shall limit or exclude Isabel's liability for the following:

1. death or personal injury resulting from Isabel's negligence; or
2. fraud by Isabel.

2.2.2. PKI@KBC RA LIABILITY

2.2.2.1. WARRANTIES AND LIMITATIONS ON WARRANTIES

KBC warrants only that any PKI@KBC Certificate issued, is issued in accordance with the provisions of this PKI@KBC CP for that level of assurance. In addition other warranties may exist by operation of law.

Unless otherwise agreed and within the limits of the applicable law, KBC disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided, and further disclaim any and all liability for negligence and lack of reasonable care on the part of Subscribers, Subjects, Customers and Relying Parties.

2.2.2.2. Exclusion of KBC's liability towards Subscribers, Subjects, Customers and Relying Parties

KBC shall, unless otherwise stated below, not be liable for any loss or damage suffered by, claims made against or costs incurred by Subscribers, Subjects, Customers and/or Relying Parties to the extent that such loss, damage, claims or costs arise from the following:

1. any loss or compromise of PKI@KBC Subjects Private Key, unless KBC failed to comply with the requirements set out in this CP, in which case KBC will (subject to any other restrictions or exclusions below) be liable to a Relying Party to the extent that such Relying Party is able to demonstrate that it suffered loss or damage as a result of KBC's failure to do so,
2. any inaccurate or incorrect information contained in any PKI@KBC Certificate issued by the Isabel CA, unless KBC failed to use all reasonable efforts to ensure the accuracy and correctness of such information or unless KBC failed to verify the authenticity of all documentary evidence of such information according to the PKI@KBC CP, in which case KBC will (subject to any other restrictions or exclusions below) be liable to a Relying Party to the extent that such Relying Party is able to demonstrate that it suffered loss or damage as a result of KBC's failure to do so,
3. a Relying Party's reliance on any revoked PKI@KBC Certificate issued by the Isabel CA where such Relying Party failed to verify that the relevant PKI@KBC Certificate has not been revoked,
4. a Relying Party's reliance on any PKI@KBC Certificate issued by the Isabel CA where such Relying Party knew or reasonably should have known that the relevant PKI@KBC Certificate has been revoked but where the Relying Party nonetheless accepts and places reliance on such PKI@KBC Certificate,
5. any unavailability of Isabel's CRL, repository, for any reason whatsoever,
6. any incorrect or inaccurate information contained in Isabel's CRL,
7. any other use of the PKI@KBC Certificate, Private Key and/or software, than the use allowed by this PKI@KBC CP;
8. any modifications or changed situations, not notified to the PKI@KBC RA;
9. any misuse or abuse by Subscribers, Subjects, Customers and/or Relying Parties.

2.2.2.3. Indirect and Consequential Loss towards Subscribers, Subjects, Customers and Relying Parties

Even if KBC has been advised of the possibility of such damages, KBC shall under no circumstances be liable for any indirect or consequential loss or damage, such as, but not limited to:

1. any loss of profits;
2. any punitive damages;
3. consequences of actions and claims brought against the Subscribers, Subjects, Customers and Relying Parties by third parties ;
4. any loss of goodwill;
5. any loss of anticipated savings;
6. any loss of revenue;
7. any loss of business;
8. any business interruption; or
9. loss of information or data.

2.2.2.4. Limitations on KBC's liability towards Subscribers, Subjects, Customers and Relying Parties

Provided KBC is liable, under no circumstances the entire liability of KBC to all parties, including but not limited to Subscribers, Subjects, Customers, or Relying Parties, in respect of any single claim or series of related claims, exceed the applicable liability cap for such PKI@KBC Certificate set forth below. The aggregate liability of KBC to any and all persons concerning a PKI@KBC Certificate shall, for the entire of all signatures and transactions related to such PKI@KBC Certificate, be limited to the greater of the following two amounts: 2.500 EUR, or a sum equivalent to a year of fees due for the PKI@KBC Certificate services.

This limitation on damages applies to loss and damages of all types, incurred by any person, including without limitation a Subscriber, Subject, Customer, or Relying Party, that are caused by reliance on or use of a PKI@KBC Certificate issued, managed, used, revoked by an Isabel CA, or such a PKI@KBC Certificate that expires. This limitation on damages applies as well to liability under contract, tort, and any other form of liability claim. The liability cap on each PKI@KBC Certificate shall be the same regardless of the number of digital signatures, transactions, or claims related to such PKI@KBC Certificate. In the event the liability cap is exceeded, the liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court or competent jurisdiction. In no event KBC will be obligated to pay more than the aggregate liability cap for each PKI@KBC Certificate.

2.2.2.5. Force Majeure Events

If KBC is prevented, hindered or delayed from or in performing any of its obligations, whether under this document or under any other relevant document, by a Force Majeure Event, such as war, terrorism, insurrection, strikes, social conflict, accident, fire, flood or incidents relating to third parties (such as delays in transport or delivery, equipment breakdown or problems with data communication connections, then KBC shall not be liable for:

1. any failure or delay by it to perform any such obligations to the extent that such failure is a result of the Force Majeure Event; and
2. any loss or damage of whatsoever nature suffered by, claims of whatsoever nature made against or costs of whatsoever nature incurred by Relying Parties arising from such failure or delay by KBC to perform any such obligations which are affected by the Force Majeure Event.

2.2.2.6. Limitations on KBC’s exclusion or limitation of liability

Nothing in this document shall limit or exclude KBC's liability for the following:

1. death or personal injury resulting from KBC’s or Isabel’s negligence; or
2. fraud by KBC or Isabel.

2.2.3. LIABILITY OF THE PKI@KBC CUSTOMER, SUBSCRIBER, SUBJECT, RELYING PARTY

By accepting or using a PKI@KBC Certificate, the Customer, Subscriber, Subject and/or Relying Party agree to indemnify and hold KBC and her agent(s) and subcontractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, that Isabel and her agent(s) and subcontractors may incur, that are caused by the use or publication of a PKI@KBC Certificate and that arises from:

1. failure to execute its obligations as described in the present PKI@KBC CP;
2. falsehood or misrepresentation of fact by the Customer, Subscriber or Subject;
3. failure by the Customer, Subscriber or Subject to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive KBC, a PKI@KBC RA, a PKI@KBC Revocation Service or any person receiving or relying on the PKI@KBC Certificate;
4. failure to protect the Subscribers or Subjects private key, to use a trustworthy system, or to otherwise, take the precautions necessary to prevent the compromise, loss, disclosure, modification or unauthorized use of such private key;

5. any other use of the PKI@KBC Certificate, private key and/or software, than the use allowed by KBC.

All Customers, Subscribers, Subjects, Relying Parties accept that the use of a PKI@KBC Certificate outside the PKI@KBC Community (see section “1.3 – Community and Applicability”) without the explicit authorization of KBC, or the use of a PKI@KBC Certificate after a certain use has been forbidden by KBC in a cease and desist letter, will give rise to the liability as described above and that such forbidden use will be ipso facto be considered as an unfair trade practice in the meaning of the Act of 14 July 1991 and/or a breach of the present PKI@KBC CP.

2.3. FINANCIAL RESPONSIBILITY

All KBC Group companies are insured for their Professional Liability up to an amount of 50 mio EUR per loss and in the aggregate, after a deductible of 1.250.000 EUR per loss. On simple demand of Isabel, KBC will ask her insurer to issue an Insurance Certificate stating the insured amount. Cover will always be subject to the original policy’s conditions.

Isabel will also insure her Professional iability risks arising out of her activities and liabilities with respect to PKI@KBC with a reputable insurer and provide an Insurance Certificate upon first demand of a KBC Group Company.

2.3.1. INDEMNIFICATION BY PKI@KBC CUSTOMERS, RELYING PARTIES AND SUBJECTS

PKI@KBC Customers and/or Relying Parties and/or PKI@KBC Certificate Subjects must indemnify any parties (including the Isabel Certification Authority, PKI@KBC RAs and Revocation Services) and/or KBC 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 PKI@KBC CP will have no valid claim against Isabel in the event of damage.

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

2.3.2. FIDUCIARY RELATIONSHIPS

The relationship between KBC and PKI@KBC Certificate Subjects and between KBC and PKI@KBC Certificate Relying Parties is not that of agent and principal. Neither PKI@KBC Certificate Subjects nor Relying Parties have any authority to bind KBC, by contract or otherwise, to any obligation.

2.4. INTERPRETATION AND ENFORCEMENT

In the event of any conflict or inconsistencies between the present PKI@KBC Certificate Policy and contractual agreements binding PKI@KBC Customers, PKI@KBC Certificate Subscribers and Subjects to KBC: the dispositions of the present PKI@KBC CP shall prevail on the contractual agreement and any specific newly agreed agreement, unless stated otherwise and insofar that they are applicable to PKI@KBC Certificates.

2.4.1. GOVERNING LAW

The laws of Belgium shall govern the enforceability, construction, interpretation, and validity of the present PKI@KBC Certificate Policy.

2.4.2. 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 PKI@KBC Certificate Subscriber or Subject don't allow the inclusion of specific provisions of this PKI@KBC CP, then with respect to that PKI@KBC Certificate Subscriber or Subject only, these specific provisions of this PKI@KBC 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 PKI@KBC CP, shall so survive.

In case of merger of one of the KBC Group Companies which are acting as a PKI@KBC RA, KBC shall to its best efforts ensure the continuity of the PKI@KBC RA operations referred herein.

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

2.4.3. DISPUTE RESOLUTION PROCEDURES

All parties involved, including the Isabel CA, PKI@KBC 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. Parties can always agree upon arbitration before Cepina or SGOA (Stichting Geschillen Oplossing Automatisering).

2.5. FEES

Fees for PKI@KBC Certificates and related services, and their modalities are set forth in contractual agreements agreed between PKI@KBC Customers/Subscribers/Subjects and KBC.

Refunds are only applicable in case this is explicitly agreed.

2.6. PUBLICATION AND REPOSITORY

2.6.1. PUBLICATION OF ISABEL CA INFORMATION

The Isabel CA information to be published is:

1. The PKI@KBC CP.
2. The PKI@KBC Certificates which are accepted, and therefore declared to contain correct information, by the Subject.
3. The Certificate Revocation List.
4. The Isabel CA self-signed certificate.
5. PKI@KBC general terms and conditions for certification services.
6. The PKI@KBC model contracts for certification services.

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

2.6.2. FREQUENCY OF PUBLICATION

PKI@KBC Certificates publication is generally guaranteed within 24 hours after their acceptance by their Subject. PKI@KBC Certificates are normally published within 0.5 hour after they have been accepted.

The Certificate Revocation List (CRL) is normally updated and reissued within 0.5 hours after a change and is reissued at least once every 24 hours, even if there is no change.

The PKI@KBC CP is under version control as stipulated in this document.

The issuance of the PKI@KBC CP is handled in section “8 – Specification Administration” of the present PKI@KBC CP.

2.6.3. ACCESS CONTROL

The Isabel CA shall insure that appropriate access controls are in place to prevent unauthorized writing, modifying, or deleting certificates, policy documents, CRLs and other items placed in the Repository.

The present PKI@KBC CP may be accessed in **read-only mode** by:

1. The Isabel Certification Authority
2. The PKI@KBC RAs
3. The PKI@KBC Certificate Subscribers and Subjects
4. The PKI@KBC Certificate Relying Parties

The present PKI@KBC CP may be accessed in write/update mode by the Policy Authority c.f. section “8 – Specification Administration”.

The PKI@KBC Certificates may be accessed in **read-only mode** by:

1. The PKI@KBC RAs
2. The PKI@KBC Certificate Subscribers and Subjects
3. The PKI@KBC Policy Authority

The PKI@KBC Certificates, the Certificate Revocation List for PKI@KBC Certificates may be accessed in **write/update mode** by the Isabel Certification Authority.

The Validation Service may be accessed only by the PKI@KBC Customer.

2.6.4. REPOSITORIES

The PKI@KBC Certificates and the Certificate Revocation List for PKI@KBC Certificates are published in an Isabel directory.

The management of the Isabel directory is the responsibility of Isabel S.A./N.V., but not of the Isabel Certification Authority.

2.7. COMPLIANCE AUDIT

KBC will carry out audits of all the procedures related to PKI@KBC and their compliance with the present CP.

2.7.1. FREQUENCY OF ENTITY COMPLIANCE AUDIT

The frequency of those audits is determined by:

1. KBC internal policies.
2. The governing Belgian legal framework.

3. Other parties mandated to execute an audit on behalf of their relation with KBC.

2.7.2. IDENTITY/QUALIFICATION OF AUDITORS

Auditor(s) will be chosen as independent parties with expertise in the domain of Public Key Infrastructure.

The auditor(s) shall have qualifications in accordance with professional practices and as mandated by law, if applicable. The auditor(s) as a core task have to perform audits on the CA or the Information System Security, and must be thoroughly familiar with PKI policies (CPSs and CPs).

2.7.3. AUDITOR'S RELATIONSHIP TO AUDITED PARTY

The auditors must be independent from KBC and Isabel S.A./N.V..

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

2.7.4. TOPICS COVERED BY AUDIT

Audits will be carried out regarding:

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 PKI@KBC RA operations.
6. The compliance to PKI@KBC CP.
7. The compliance to Belgian regulations.

2.7.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Audit reports will be evaluated by KBC. Any discrepancies with the PKI@KBC CP or other irregularities will be prioritised and corrective actions will be planned taking into account the residual risk. A consecutive audit can be performed in order to review the requested corrections.

2.7.6. COMMUNICATION OF RESULTS

The findings of an audit will be stated in a report which is addressed to the KBC Internal Audit Manager but can be shared (in extenso or summarized) with

- the responsible business (at all levels of the organisation),
- the internal auditors covering the involved business domain,
- the external auditors,
- the members of the Audit Committee,
- the regulator

of the entities of the KBC group making use of PKI@KBC, as well as every third party having audit rights on the activities of these entities as far as PKI@KBC is related to that activity.

Audit report information will not be made public, unless this would be requested by the national law. Audit information must be considered as strict confidential information within the framework of this CP.

2.8. CONFIDENTIALITY

2.8.1. TYPES OF INFORMATION TO BE KEPT CONFIDENTIAL

All information related to the application, issuance, acceptance and revocation of PKI@KBC Certificate is considered confidential and under restricted access except if listed in section "2.8.2 – Types of information not considered confidential".

This information might be part of a bilateral agreement between KBC and a Third Party, and it may have been revealed under non-disclosure agreement.

The following information is restricted to PKI@KBC Certificate Subscribers, Subjects and Relying Parties:

1. PKI@KBC Certificates and the information contained therein.
2. The Isabel Certification Authority Self-signed certificate.

2.8.2. TYPES OF INFORMATION NOT CONSIDERED CONFIDENTIAL

The present PKI@KBC CP is publicly available, and hence not part of the confidentiality obligations under this section.

As the present PKI@KBC CP is not classified as a confidential document, it does not contain confidential information.

2.8.3. DISCLOSURE OF CERTIFICATE REVOCATION INFORMATION

The reasons for the revocation of a certificate are formalised in the ITU-T X.509 standard with the CRL entry extension field 'Reason code'.

The PKI@KBC Certificate Subject or the PKI@KBC Certificate Subscriber who has requested the revocation of the Subject's certificate will be notified about the revocation of the PKI@KBC Certificate itself.

The revocation reason is not communicated to Relying Parties.

2.8.4. RELEASE TO LAW ENFORCEMENT OFFICIALS

Isabel CA and PKI@KBC RAs are allowed to release confidential information based on an order that is duly signed by a judge or officer in the course of a criminal investigation or as otherwise may be required by law.

2.8.5. RELEASE AS PART OF CIVIL DISCOVERY

No stipulation.

2.8.6. DISCLOSURE UPON SUBSCRIBER/SUBJECT REQUEST

Isabel CA and PKI@KBC RAs are allowed to release confidential information about a PKI@KBC Certificate Subscriber/Subject upon the request or with the approval of that PKI@KBC Certificate Subscriber/Subject.

2.8.7. OTHER INFORMATION RELEASE CIRCUMSTANCES

No provision.

2.9. INTELLECTUAL PROPERTY RIGHTS

All information provided in this document is part of the intellectual property rights of KBC or Isabel. This holds for any information published by KBC and Isabel, in a public or private relation.

These rights hold beyond any contractual relationship that might exist with KBC. The PKI@KBC Certificates and means of access and signature, including the public key, are the exclusive property of Isabel. Any use of the PKI@KBC Certificates and means of access and signature outside the agreed functionalities of the PKI@KBC system must be laid down in a contract with KBC. 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.

3. Identification and authentication

This chapter describes the procedures used to authenticate a PKI@KBC Certificate Subscriber prior to certificate issuance. It also describes how parties requesting rekey or revocation are authenticated and addresses naming practices, including name ownership recognition and name dispute resolution.

3.1. INITIAL REGISTRATION

This section describes the identification and authentication provisions in the scope of the initial registration of a PKI@KBC Certificate Subject.

There are 2 types of PKI@KBC Certificate Subject:

- Physical person Subject: the Subject is represented by the physical person who is identified in the certificate.
- Function Subject: the Subject is represented by one physical person who is empowered to represent the function that is identified in the certificate (function representative).

3.1.1. TYPES OF NAMES

An Isabel CA must use X.500 Distinguished Name format for Subject and Issuer name fields in a PKI@KBC Certificate.

3.1.2. NEED FOR NAMES TO BE MEANINGFUL

A PKI@KBC RA must guarantee the meaningfulness of the Distinguished Name information entered in the subject field of a PKI@KBC Certificate within the X.500 name space for which Isabel has been authorised.

The Isabel CA does not issue anonymous or pseudonymous certificates.

3.1.3. RULES FOR INTERPRETING VARIOUS NAME FORMS

Distinguished Names in Certificates shall be interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.4. UNIQUENESS OF NAMES

Isabel CA must guarantee the uniqueness of the Distinguished Name in the Subject field of a PKI@KBC Certificate within the X.500 name space for which Isabel has been authorised and which has been reserved for PKI@KBC.

See “7 – Certificate, CRL, OCSP profiles”.

3.1.5. NAME CLAIM DISPUTE RESOLUTION PROCEDURE

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

3.1.6. RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS

PKI@KBC RAs can not verify nor guarantee that trademarks, service marks or any other protected signs mentioned in PKI@KBC 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.

3.1.7. METHOD TO PROVE POSSESSION OF PRIVATE KEY

No stipulation.

3.1.8. AUTHENTICATION OF ORGANIZATION IDENTITY

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

The authentication of a candidate Customer's identity is achieved in the scope of the subscription process ruling the signature of a PKI@KBC Service/Product contract between this PKI@KBC Customer and KBC. The contract further details the authenticating procedure and pieces that must be provided to the PKI@KBC RA by the candidate Customer in the scope of this subscription process.

3.1.9. AUTHENTICATION OF INDIVIDUAL IDENTITY

The identification of the applying PKI@KBC Customer is carried out according to a documented procedure that is implemented by the PKI@KBC RAs.

3.2. ROUTINE REKEY

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

3.3. REKEY AFTER REVOCATION

The PKI@KBC Certificate Subject who has had his/her PKI@KBC Certificate revoked and wants to apply for a new PKI@KBC Certificate needs to go through the whole PKI@KBC Certificate Process again and be authenticated.

In this case a new PKI@KBC Secure Signing Card is issued and delivered to the Subscriber.

3.4. REVOCATION REQUEST

KBC offers to its customers two ways of requesting the revocation of a PKI@KBC Certificate:

- the Customer must call upon the PKI@KBC Revocation Service;
- if unavailable, use can be made of the Card Stop Revocation Service.

3.4.1. AUTHENTICATION BY THE REVOCATION SERVICES

PKI@KBC Revocation Service and Card Stop Revocation Service must identify and authenticate the Subject to generate a revocation request. Handwritten filled form must be used as a mean of authentication.

3.4.2. AUTHENTICATION BY THE PKI@KBC REVOCATION SERVICE

The PKI@KBC Revocation Service is operated by the KBC Help Desk

PKI@KBC Revocation Service generates a revocation request based on information submitted on paper by the Subject.

3.4.3. AUTHENTICATION BY THE CARD STOP REVOCATION SERVICE

The Card Stop Revocation Service is only to be used in case of unavailability of the PKI@KBC Revocation Service. The Card Stop Revocation Service is operated by:

Card Stop

Tel: +32 (0)70/344.344

Fax: +32 (0)70/344.355

Card Stop Revocation Service generates a revocation request based on information submitted by phone by the Subject.

A handwritten confirmation must be done afterwards as a means of authentication and confirmation. This does not prevent the publication of the updated CRL.

3.4.4. AUTHENTICATION BY THE ISABEL CA

The Isabel CA authenticates a revocation request on basis of a digital signature generated with the PKI@KBC RA or the PKI@KBC Revocation Service agent’s Private Key and verified with the PKI@KBC RA or the PKI@KBC Revocation Service agent’s certificate.

4. Operational requirements

4.1. CERTIFICATE APPLICATION

A PKI@KBC RA acts upon a certificate application to validate an applicant's identity. Subsequently, the PKI@KBC RA either approves or rejects the certificate application. Such approval or rejection does not necessarily have to be justified to the applicant or any other party.

The PKI@KBC RA uses documented procedures and adopts its own practices.

The Isabel CA processes securely PKI@KBC Certificate Requests issued by PKI@KBC RAs under its control and publishes in accordance with section ”2.6.2 – Frequency of publication”. The Isabel CA accepts such PKI@KBC Certificate Requests only from formally approved PKI@KBC RAs.

The Isabel CA rejects any certificate request that does not appear to comply with all the stipulations of this PKI@KBC CP.

4.2. CERTIFICATE ISSUANCE

Further to validation and approval of a certificate application, the PKI@KBC RA sends a certificate issuance request to the Isabel CA.

Requests from the PKI@KBC RA are granted approval provided that they are validly made and they contain valid subscriber data, formatted according the Isabel CA specifications.

Issued PKI@KBC Certificates are delivered to the Subject. The Subject receives its PKI@KBC Secure Signing Card and is invited to download from the Isabel repository its own PKI@KBC Certificate.

4.3. CERTIFICATE ACCEPTANCE

The Isabel CA must obtain the acceptance of the PKI@KBC Certificate Subject for his/her PKI@KBC Certificate.

Acceptance of the PKI@KBC Certificate is done by (1) either explicit notification of acceptance, either (2) the use of the PKI@KBC Certificate by the Subject, (3) either automatically after the 10th day after the publication in the Repository without notification of remarks by the Subject.

Upon download of his PKI@KBC Certificate, the Subject also installs and accepts the Isabel CA Self-signed certificate.

4.4. CERTIFICATE SUSPENSION AND REVOCATION

4.4.1. CIRCUMSTANCES FOR REVOCATION

Revocation of a PKI@KBC Certificate is to permanently end the operational period of the certificate prior to reaching the end of its stated validity period. Isabel CA will revoke a digital certificate if:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the Private Key associated with the certificate.

- The Subscriber, Isabel or KBC has breached a material obligation under this PKI@KBC CP.
- Either the Subscriber's, Isabel or KBC obligations under this PKI@KBC CP are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised.
- Isabel or KBC receive a lawful and binding order from a government or regulatory body to revoke the PKI@KBC Certificate.
- There has been a modification of the information pertaining to the Subscriber that is contained within the PKI@KBC Certificate.

4.4.2. WHO CAN REQUEST REVOCATION

The revocation of a Physical Person or Function Subject PKI@KBC Certificate may be requested by:

- The physical person who is identified in a Physical Person Subject PKI@KBC Certificate.
- The physical person who represents a Function PKI@KBC Certificate.
- Any physical person empowered by a PKI@KBC Customer to request revocation of its Subject PKI@KBC Certificates.
- The PKI@KBC RA.
- The Isabel CA that has issued the certificate.

4.4.3. PROCEDURE FOR REVOCATION REQUEST

The Isabel CA processes securely PKI@KBC Certificate revocation requests issued by the PKI@KBC RAs under its control and publishes the revocation in accordance with section "2.6.2 – Frequency of publication".

4.4.4. REVOCATION REQUEST GRACE PERIOD

No grace period shall be allowed.

4.4.5. CIRCUMSTANCES FOR SUSPENSION

No stipulation

4.4.6. WHO CAN REQUEST SUSPENSION

No stipulation

4.4.7. PROCEDURE FOR SUSPENSION REQUEST

No stipulation

4.4.8. LIMITS ON SUSPENSION PERIOD

No stipulation

4.4.9. CRL ISSUANCE FREQUENCY

The updated Certificate Revocation List shall be published in accordance with section “2.6.2 – Frequency of publication” after revocation of a PKI@KBC Certificate.

4.4.10. CRL CHECKING REQUIREMENTS

No stipulation

4.4.11. ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

Isabel CA provides an on line revocation/status checking service.

4.4.12. ON-LINE REVOCATION CHECKING REQUIREMENTS

The on line revocation checking service provides status information based on the last issued CRL.

4.4.13. OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

No stipulation.

4.4.14. CHECKING REQUIREMENTS FOR OTHER FORMS OF REVOCATION ADVERTISEMENTS

No stipulation.

4.4.15. SPECIAL REQUIREMENTS RE KEY COMPROMISE

No stipulation.

4.5. SECURITY AUDIT PROCEDURES

Security audit procedure must follow stipulations in “2.7 – Compliance audit”.

4.5.1. TYPES OF DATA RECORDED

The Isabel CA and PKI@KBC RA s record all current events concerning a PKI@KBC Certificate in audit logs. Those events are recorded for a period of one to ten years, in particular for the purpose of providing evidence of certification or revocation for legal proceedings. See also [2] for Belgian National Regulations events recording requirements.

Events concerning significant CA environmental, key management and certificate management are recorded and in particular:

- All events related to the life-cycle of CA keys.
- All events related to the life-cycle of PKI@KBC Certificates.
- All events related to the preparation of a PKI@KBC Secure Signing Card.

- All requests and reports relating to revocation, as well as the resulting action.

An Isabel CA guarantee that all registration events including applications for certificates, certificate Re-key or renewal are recorded and in particular:

- Document(s) presented by the PKI@KBC Certificate Subscriber to the PKI@KBC RA to support registration in accordance with the agreement between the PKI@KBC RA and the PKI@KBC Customer.
- Storage location of copies identification documents, including the signed PKI@KBC Certificate Application.
- Any specific choices in the Subscriber's application.
- Identity of PKI@KBC Customer accepting the PKI@KBC Certificate application.
- Method used to validate identification documents, if any.
- Name of receiving CA and/or submitting RA, if applicable.

The details of the events and data to be recorded are documented as internal Isabel procedures.

4.5.2. FREQUENCY OF PROCESSING LOG

Isabel CA authorized personnel review audit logs on a regular basis, at least on a weekly basis.

4.5.3. RETENTION PERIOD FOR AUDIT LOG

All information related to PKI@KBC Certificates is archived during at least 10 years.

4.5.4. PROTECTION OF AUDIT LOG

The confidentiality and integrity of current and archived events concerning PKI@KBC Certificates must be guaranteed.

4.5.5. AUDIT LOG BACKUP PROCEDURES

Isabel insures that audit logs are backed up on a regular basis.

4.5.6. AUDIT COLLECTION SYSTEM (INTERNAL VS EXTERNAL)

The audit collection system is internal to the Isabel CA system and KBC.

4.5.7. NOTIFICATION TO EVENT-CAUSING SUBJECT

No stipulation.

4.5.8. VULNERABILITY ASSESSMENTS

Security audits shall be conducted on a regular basis on Isabel CA and PKI@KBC systems and procedures according to policies internal to the Isabel CA system.

4.6. RECORDS ARCHIVAL

4.6.1. TYPES OF EVENT RECORDED

Following items are archived:

- PKI@KBC Certificates
- Isabel Certificate Revocation List
- PKI@KBC Certificate Policy
- All events and requests leading to changes to PKI@KBC Certificates and Certificate Revocation List

4.6.2. RETENTION PERIOD FOR ARCHIVE

All information related to PKI@KBC Certificates is archived during at least 10 years.

4.6.3. PROTECTION OF ARCHIVE

Electronic and paper based archives are protected with physical and logical access control mechanisms to prevent unauthorised access. Archives are protected against environmental threats such as temperature, fire, flood, humidity and magnetism.

4.6.4. ARCHIVE BACKUP PROCEDURES

Multiple copies of the archives exist to guarantee availability.

On a regular basis, archives are re-written on state-of-the-art media to guarantee the retention period and to avoid obsolete media types infrastructures.

4.6.5. REQUIREMENTS FOR TIME-STAMPING OF RECORDS

Archived information is digitally signed and time stamped.

4.6.6. ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

The archive collection system is internal to the Isabel CA system.

4.6.7. PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

A PKI@KBC Certificate Subject shall have access to archived information relating to himself, without compromising the general confidentiality obligations of the Isabel CA and PKI@KBC RAs. All requests to obtain archived information must be addressed to the KBC Security Manager in writing.

Archive information must be verified on a regular basis to ensure availability of archived information during the retention period.

4.7. KEY CHANGEOVER

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.

4.8. COMPROMISE AND DISASTER RECOVERY

Isabel CA has put in place policies and procedures that in the event of a disaster, including compromise of a CA's private signing key, operations are restored as soon as possible.

No further stipulations.

4.9. CA/RA TERMINATION

In case of termination of CA operations for any reason whatsoever, Isabel will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies in agreement with KBC for all PKI@KBC Certificate related activities.

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

In case of termination of a PKI@KBC RA, KBC will provide timely notice to Isabel CA.

5. Physical, procedural and personnel security controls

5.1. PHYSICAL CONTROLS

No stipulation.

5.2. PROCEDURAL CONTROLS

5.2.1. TRUSTED ROLES

The Isabel CA requires the roles defined in the following sections to be fulfilled by trusted personnel.

5.2.1.1. CA OPERATOR

These persons will act as operators on the Isabel CA system using the CA workstation under dual control. There will be two pools of CA Operators.

5.2.1.2. CA SYSTEM ADMINISTRATOR

These persons administer the Isabel CA system using the console.

5.2.1.3. CA SECURITY OFFICER

These persons implement the CA policies, ensure compliance to PKI@KBC CP and check audit logs.

5.2.2. NUMBER OF PERSONS REQUIRED PER TASK

No stipulation.

5.2.3. IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

Representatives of each trusted role are authenticated with a digital signature generated with their Private Key stored inside a smart card.

5.3. PERSONNEL CONTROLS

Personnel controls must be implemented according to Isabel and KBC internal policies.

6. Technical security controls

6.1. KEY PAIR GENERATION AND INSTALLATION

The Isabel CA uses appropriate cryptographic devices to perform CA key management tasks. Those cryptographic devices are known as Hardware Security Modules (HSMs).

Such devices meet formal requirements, which guarantee, amongst other things, that device tampering is immediately detected; and private keys cannot leave devices unencrypted. Hardware and software mechanisms that protect CA private keys are documented.

6.1.1. KEY PAIR GENERATION

Isabel CA securely generates and protects its own private key(s), using a trustworthy system, and takes necessary precautions to prevent the compromise or unauthorized usage of it.

Generation of PKI@KBC Subject's key pair is done centrally by the Isabel CA using a trustworthy system and following a documented procedure.

The Isabel CA must guarantee the uniqueness of a key pair within the Isabel PKI.

6.1.2. PRIVATE KEY DELIVERY TO ENTITY

Isabel CA shall deliver PKI@KBC Subject private key stored on a PKI@KBC Secure Signing Card to the local PKI@KBC RA branch of the PKI@KBC Certificate Subscriber.

Isabel CA delivers securely the Activation Data of the PKI@KBC Secure Signing Card directly to the Subject if this is a physical person, and the Subscriber if the Subject is a function.

The PKI@KBC Secure Signing Card and corresponding PIN-code can *never* be at the same place, at the same time, except after pickup of the PKI@KBC Secure Signing Card by the PKI@KBC Subscriber.

6.1.3. PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

PKI@KBC Subject key pairs are generated centrally using a "Key Generator" relying on a trustworthy system. The public key is delivered to the CA electronically in a message insuring its integrity and provenience (done internally at Isabel CA).

6.1.4. CA PUBLIC KEY DELIVERY TO USERS

The Isabel CA public key is published in the repository. This repository is accessible to entities in read only mode 24 / 7.

6.1.5. KEY SIZES

The size of the Public Key (modulus n), certified by a PKI@KBC Certificate and associated at a PKI@KBC Secure Signing Card, must be at least 1024 bits.

The size of the Isabel CA keys must be at least 2048 bits.

6.1.6. PUBLIC KEY PARAMETERS GENERATION

The Isabel key generation process is Isabel proprietary information.

The generation process has been audited on its quality.

The quality of generation process parameters is continuously monitored.

6.1.7. PARAMETER QUALITY CHECKING

The Isabel CA shall use a hardware key generation component checking.

6.1.8. HARDWARE/SOFTWARE KEY GENERATION

The Isabel CA shall use a hardware key generation component ensuring a security level at least as high as the PKI@KBC Secure Signing Card storing the private key after its generation.

6.1.9. KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)

End entity certificate use is restricted by using certificate extensions on key usage and extended key usage. Any usage of the certificate inconsistent with these extensions is not permitted.

6.2. PRIVATE KEY PROTECTION

Isabel supports the use of secure devices and tamperproof equipment to securely issue, manage and store certificates. Isabel uses accredited trustworthy hardware to prevent compromise of its private key.

6.2.1. STANDARDS FOR CRYPTOGRAPHIC MODULE

PKI@KBC Certificate Subject Private Key is stored within a PKI@KBC Secure Signing Card, which is evaluated EAL 4+.

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

CA Private Keys are under triple control.

PKI@KBC Subscriber Private Keys must be under sole control of PKI@KBC Subscriber.

6.2.3. PRIVATE KEY ESCROW

Isabel CA Private Keys are not escrowed.

PKI@KBC Subscriber Private Key are not escrowed.

6.2.4. PRIVATE KEY BACKUP

Isabel CA Private Keys are backed up.

PKI@KBC Subscriber Private Key must not be backed up.

6.2.5. PRIVATE KEY ARCHIVAL

PKI@KBC Subscriber Private Keys are not archived.

6.2.6. PRIVATE KEY ENTRY INTO CRYPTOGRAPHIC MODULE

The Isabel CA Private Keys are loaded into the cryptographic module in a secure way.

6.2.7. METHOD OF ACTIVATING PRIVATE KEY

The Isabel CA Private Keys are protected with a PIN or a password.

6.2.8. METHOD OF DEACTIVATING PRIVATE KEY

Isabel CA Private Keys are deactivated by powering off the equipment.

PKI@KBC Private Keys are deactivated when the PKI@KBC Secure Signing Card is removed from the smart card reader.

6.2.9. METHOD OF DESTROYING PRIVATE KEY

An Isabel CA Private Key is destroyed in a secure way when the key is no longer used by the Isabel CA.

PKI@KBC Subscribers Private Keys are destroyed when destroying the PKI@KBC Secure Signing Card.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. PUBLIC KEY ARCHIVAL

PKI@KBC Certificates and therefore the Public Key they certify must be archived during at least 10 years.

6.3.2. USAGE PERIODS FOR THE PUBLIC AND PRIVATE KEYS

No provision.

6.4. ACTIVATION DATA

Generation of PKI@KBC Subject's Activation Data, consisting of an initial PIN code for the PKI@KBC Secure Signing Card, is done centrally by the Isabel CA. The Isabel CA guarantees that the initial PIN code is transmitted securely to the PKI@KBC Subscriber. After delivery, the Subject is responsible to guarantee the confidentiality of his/her PIN code. Isabel does not backup, escrow nor archive Subject's initial PIN codes.

6.4.1. ACTIVATION DATA GENERATION AND INSTALLATION

PKI@KBC Subject initial PIN code generation is done in a secure way and transmitted to the Subject in a secure way. At no moment the Private Key, i.e. PKI@KBC Secure Signing Card, and its initial PIN code can be at the same place except after pickup by the PKI@KBC Customer.

During the installation, the PKI@KBC Subscriber will be prompted to change the initial PIN code assigned by the Isabel CA with a personally assigned PIN code.

6.4.2. ACTIVATION DATA PROTECTION

The PIN code is protected in confidentiality and integrity until its delivery to and acceptance by the PKI@KBC Certificate Subscriber.

6.4.3. OTHER ASPECTS OF ACTIVATION DATA

No stipulation

6.5. COMPUTER SECURITY CONTROLS

Computer security technical controls are implemented according to internal policies of Isabel for the Isabel CA and KBC for the PKI@KBC RAs.

6.6. LIFE CYCLE TECHNICAL CONTROLS

Lifecycle technical controls are implemented according to internal policies of Isabel for the Isabel CA and KBC for the PKI@KBC RAs.

6.7. NETWORK SECURITY CONTROLS

Network security controls are implemented according to internal policies of Isabel for the Isabel CA and KBC for the PKI@KBC RAs.

6.8. CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

No stipulation.

7. Certificate, CRL, OCSP profiles

7.1. CERTIFICATE PROFILE

The profile of a PKI@KBC Certificate issued to a physical person or to a function Subject is the following:

Certificate Field	Value or Value Format
Version	INTEGER {V3(2)} (Note: integer value 2 corresponds to v3 certificates)
SerialNumber	INTEGER {0..MAX} The form of the number is yyyydddnnnnn where • yyyy is the year the certificate was produced • ddd is the number of the day in the year • nnnnn is a sequence number for that day
Signature	*AlgorithIdentifier sha-1WithRSAEncryption* *OBJECT IDENTIFIER ::= {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
subject (Normal)	• mandatory field: CN= <Lastname>+<Firstname>, for physical persons <Functionname>, for functions • mandatory field OU= <User ID> • mandatory field: OU= <Technical ID of the Subscribing Entity> • mandatory field: OU= <ISO Country Code of the Subscribing Entity>+<Enterprise number of the Subscribing Entity> • mandatory field: O= <Name of the Subscribing Entity> • L= Isabel • C=BE
subjectPublicKeyInfo	*AlgorithmIdentifier rsaEncryption* *OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1}*

7.1.1. VERSION NUMBER

All PKI@KBC Certificates delivered by the Isabel Certification Authority comply with ITU-T X.509 v3. c.f. ref [3] in the section “9.2 – Appendix B – References” of the present PKI@KBC CP.

7.1.2. 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 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 PKI@KBC Certificates delivered by an Isabel Certification Authority 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.

Following table summarizes the MANDATORY extensions and their value for a PKI@KBC Certificate issued to a physical person or to a function:

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 ::= {4341 3032} (“CA02”)
subjectPublicKeyInfo OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) allocation per country (16) Belgium(56) Isabel(1) 8.1}	NC	This field is a proprietary Isabel extension *For Internal use only*
subjectContractInfo OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) allocation per country (16) Belgium(56) Isabel(1) 8.2}	NC	This field represents the Isabel-KBC contract type: “PKI@KBC” *For Internal use only*
SerialNumber (OID 2.5.4.5)	NC	This field represents the PKI@KBC Secure Signing Card’s Identifier (CardID).
KeyUsage	NC	This field gives a list of permitted usages for the key. BIT STRING ::= {digitalSignature(0), nonRepudiation(1), keyEncipherment(2), dataEncipherment(3)}

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) policy-specification(…)}, which is for this PKI@KBC CP: 2.16.56.1.9.46.1.1 The field also contains an attribute that is a URI to the full version of the PKI@KBC CP: http://www.isabel.be/PKI/Policies/Standard.htm
ExtKeyUsage	NC	This field gives more acceptable usages of the key. It's a list of OIDs. KeyPurposeID ::= {id-kp-clientAuth, id-kp-emailProtection}
AuthorityInfoAccess	NC	This field gives a pointer to an on-line certificate revocation status service. The value is: https://pki.isabel.be/ocsp

7.1.3. ALGORITHM OBJECT IDENTIFIERS

sha-1WithRSAEncryption
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) 1}

7.1.4. NAME FORMS

Entity	Name Form
PKI@KBC Certificate Subject	*See higher.*
Isabel Certification Authority	*CN=Isabel Certification Authority; O=CA; L=ISABEL; C=BE*

Any e-mail address, nor the names it contains, in the PKI@KBC Certificate can be considered as an element for identification on which basis the PKI@KBC Certificate is issued.

7.1.5. NAME CONSTRAINTS

Name Constraint extension is not used in a PKI@KBC Certificate.

7.1.6. CERTIFICATE POLICY OBJECT IDENTIFIER

C.f. Section 1.2 – Identification of the current PKI@KBC Certificate Policy.

7.1.7. USAGE OF POLICY CONSTRAINTS EXTENSION

Policy constraint extension is not used in a PKI@KBC Certificate.

7.1.8. 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: http://www.isabel.be/PKI/Policies/Standard.htm for the PKI@KBC Certificate Policy.

7.1.9. PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICY EXTENSION

Certificate policies extension is marked as non-critical, c.f. 7.1.2.

7.2. CRL PROFILE

For the purposes of PKI@KBC, the CRL is kept internal, OCSP is the preferred means available to PKI@KBC Customers for validation information.

7.3. OCSP PROFILE

The Isabel CA maintains a record of the OCSP profile it uses in an internal technical document. This will be made available at the discretion of the Isabel CA.

8. Specification Administration

8.1. SPECIFICATION CHANGE PROCEDURES

Comments, questions and change requests to the present PKI@KBC CP should be addressed to its Policy Authority specified in section “1.3.7 – Contact details” of the present PKI@KBC CP.

KBC may amend the present PKI@KBC CP at any time.

8.2. PUBLICATION AND NOTIFICATION POLICIES

The present PKI@KBC Certificate Policy is under direct control of the Policy Authority: see “1.3.5 – Policy Authorities”. The senior management of KBC is committed to ensuring that the practices in the present PKI@KBC Certificate Policy are properly implemented.

The Policy Authority, to take account of changing circumstances, legislation, technology and security risks, reviews the present PKI@KBC Certificate Policy on a regular basis.

The Policy Authority will produce recommendations for change to the present PKI@KBC Certificate Policy, which will be subject to a process of consultation within KBC and authorisation by the KBC Manager Distribution Channels before any changes are implemented.

The present PKI@KBC Certificate Policy and its future versions are published at following URI: https://www.kbc.com/certificate-policy. The date of publication and the effective date and the version number shall be indicated on the title page of the present PKI@KBC Certificate Policy. The version published following this URL is the only valid version within the time period of that publication.

Notifications related to the present PKI@KBC Certificate Policy will also be published at the above URI.

The continued use of an PKI@KBC Certificate after publication of a new version of the PKI@KBC Certificate Policy shall imply the acceptance of this new version by the Subject.

The latest version of the present PKI@KBC CP will be available on-line. Older versions are archived by KBC.

8.3. PKI@KBC CERTIFICATE POLICY APPROVAL PROCEDURES

The Policy Authority for the present PKI@KBC Certificate Policy and the KBC Manager Distribution Channels must approve changes to the present document.

8.4. TERM AND TERMINATION

This PKI@KBC CP remains in force until notice of the opposite is communicated by KBC in the repository.

9. Appendixes

9.1. APPENDIX A – DEFINITIONS

9.1.1. ACRONYMS

Acronym	Description
CA	Certification Authority
CBFA	Commissie voor het Bank-, Financie- en Assurantiewezen Commission Bancaire, Financière et des Assurances
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
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
URL	Uniform Resource Locator

9.1.2. GLOSSARY

Term	Description
Activation Data	Any data used to protect the Private Key, e.g. password, PIN code,... For PKI@KBC Certificates the Activation Data consists of an initial PIN code sent to the Subscriber on creation of his PKI@KBC Secure Signing Card, and which must be changed upon first use.
Authentication	The process of establishing identity based on the possession of a trusted credential.
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.
Certification Practice Statement	A statement of the practices which a CA employs in issuing certificates.
Digital 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.
Isabel Certification Authority	A CA operated by Isabel. Isabel CA is also referred as the technical organisation around the Certification Authority, which is operated by the company Isabel NV/SA.
Isabel Repository	Is an entity around the Isabel CA which provides for the publication of the Certificates and the Certification Revocation List.
KBC	Is the company KBC Groep NV, with registered offices at 2, Havenlaan 1080 Brussels, Belgium and the KBC Group Companies or KBC Affiliated Companies within the meaning of Article 11 of the Companies Code, and all other companies in which KBC Group NV has a direct or indirect participation.
Personal Identification Number	A secret code (PIN) that is used to protect against unauthorised access to a Private Key.
PKI@KBC Certificate	A Digital Certificate that has been issued by an Isabel CA to a PKI@KBC Certificate Subscriber.
PKI@KBC Certificate Relying Party	A PKI@KBC Certificate Relying Party is a physical person or a function that is or belongs to a PKI@KBC Customer and that relies on the information contained in a PKI@KBC Certificate, and/or digital signatures verified using this certificate and/or any other information published by an Isabel CA issuing PKI@KBC Certificates.
PKI@KBC Certificate Request	Submission of validated PKI@KBC Certificate Application information by a PKI@KBC RA to an Isabel CA to issue a PKI@KBC Certificate

Term	Description
PKI@KBC Certificate Subject	A physical person 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. The PKI@KBC Certificate Subject has been issued a PKI@KBC Certificate in the scope of his/her activities and decrypts or/and signs with the Private Key associated to that PKI@KBC Certificate on behalf of the PKI@KBC Customer to which he/she belongs. A PKI@KBC Certificate Subject is represented by: - In the case of a Physical Person Subject: the Subject is represented by the physical person who is identified in the certificate. - In the case of a Function Subject: the Subject is represented by a physical person who is empowered to represent the function that is identified in the certificate (function representative).
PKI@KBC Certificate Subscriber	A physical person, empowered by a PKI@KBC Customer, to apply for a PKI@KBC Certificate in the name of one or more physical person(s) or function(s) subject(s).
PKI@KBC Customer	An entity that signed a PKI@KBC contract with KBC with the intention of receiving services and/or products from KBC.
PKI@KBC RA	See PKI@KBC Registration Authority.
PKI@KBC Registration Authority	An RA, appointed by KBC, that operates under the authority and the control of an Isabel CA for PKI@KBC Certificates.
PKI@KBC 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 PKI@KBC Secure Signing Card.
Policy Authority	The entity responsible for the specification and validation of 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. An RA may assist in the certificate application process, revocation process or both, as stated in the applicable CP.
Relying Party	See PKI@KBC Certificate Relying Party.
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.
Subject	See PKI@KBC Certificate Subject.
Subscriber	See PKI@KBC Certificate Subscriber.
Validation Authority	An authority that provides PKI@KBC Certificates Relying Parties with a way of obtaining PKI@KBC Certificate revocation status information.

9.2. APPENDIX B – 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, Certificate Policy and Certification Practices Framework'; Obsoletes: 2527	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