BNP PARIBAS
FORTIS

PKI@BNPPF Certificate Policy

version 1.0

Date of publication: August 27, 2012

Effective date: August 29, 2012

Table of contents

1. Introduction

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

The ITU-T X.509 standard defines a CP as “a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements”.

The term CPS is defined by the American Bar Association Guidelines as: "A statement of the practices which a 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, the CPS shall focus in more detail on the question "*how*" these obligations are met by the Isabel CA and the other parties involved in the PKI .

1.1. OVERVIEW

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

An PKI@BNPPF Certificate is a certificate issued by an Isabel CA for specific purposes of BNP Paribas Fortis.

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@BNPPF Certificates.
2. Describes the applicability of PKI@BNPPF 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@BNPPF Certificates.
4. Describes the PKI@BNPPF 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@BNPPF Certificate Subjects and Relying Parties must assure themselves, by reviewing this document, any other information they deem necessary, that any PKI@BNPPF 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@BNPPF Certificate issued by an Isabel CA, a Relying Party is agreeing with the provisions and stipulations of this policy.

1.2. IDENTIFICATION

1.2.1. NAME

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

1.2.2. OBJECT IDENTIFIER

The Object Identifier associated with the “PKI@BNPPF Certificate Policy” is 2.16.56.1.9.48.1.1.

1.2.3. UNIFORM RESOURCE IDENTIFIER

The PKI@BNPPF Certificate Policy will be publicly available on the BNP Paribas Fortis Easy Banking Business web site.

1.2.4. DOCUMENT VERSION HISTORY

Revision of this document has been made as follows:

Date	Changes	Version
August 27th 2012	Initial version	1.0

1.3. COMMUNITY AND APPLICABILITY

1.3.1. CERTIFICATION AUTHORITIES

According to ITU-T X.509, a CA is “an authority trusted by one or more users to create and assign certificates, and optionally, the CA may create the users’ key”.

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

After a certificate request is filed by the PKI@BNPPF RA to the Isabel CA has been verified by the Isabel CA, a PKI@BNPPF 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@BNPPF RAs operating under the control and the authority of an Isabel CA accept PKI@BNPPF Certificate Applications for a PKI@BNPPF Certificate from PKI@BNPPF Certificate Subscribers.

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

Only Registration Authorities authorized by BNP Paribas Fortis are permitted to submit certificate requests to an Isabel CA for the issuance of PKI@BNPPF Certificates. BNP Paribas Fortis will post a list of authorized Registration Authorities on its Easy Banking Business website.

1.3.3. END ENTITIES

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

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

A BNP Paribas Fortis Customer mandates PKI@BNPPF Certificate Subscribers and PKI@BNPPF Certificate Subjects.

The Subject attribute in the PKI@BNPPF Certificate is used to name or otherwise identify the PKI@BNPPF 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@BNPPF CP :

1. A PKI@BNPPF 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 BNP Paribas Fortis Customer and BNP Paribas Fortis.

1.3.4. VALIDATION AUTHORITIES

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

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

Website support for 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@BNPPF CP and its revisions.
2. Determining the suitability and the correct implementation of the PKI@BNPPF CP.
3. The definition of the review requirements and processes relating to the implementation of the CP.

The Policy Authority for the present PKI@BNPPF CP is: BNP Paribas Fortis,see 1.3.7 Contact details.

1.3.6. APPLICABILITY

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

Relying Parties must have a contractual relationship with BNP Paribas Fortis.

If a PKI@BNPPF Certificate Subject wants to have any limitations (financial or otherwise) applicable to transactions authenticated by the PKI@BNPPF 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 BNP Paribas Fortis Security Manager acts as the Policy Authority for the present PKI@BNPPF CP. It is responsible for all aspects of the present PKI@BNPPF 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@BNPPF CP. should be addressed to the representative of its Policy Authority:

Business Information & Security Officer
FORTIS BANK NV/SA
Warandeberg/Montagne de Parc 3
B-1000 Brussels
Belgium
mailto : rpb.information.security.incident.management@bnpparibasfortis.com

2. General provisions

2.1. OBLIGATIONS

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

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

Those entities are:

1. Isabel CA
2. PKI@BNPPF RAs
3. PKI@BNPPF Certificate Subscribers and Subjects
4. PKI@BNPPF Certificate Relying Parties
5. BNP Paribas Fortis Repository
6. Policy Authority
6. Legal entity BNP Paribas Fortis

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

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

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

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

2.1.1. ISABEL CERTIFICATION AUTHORITIES OBLIGATIONS

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

2.1.1.1. NOTIFICATION OF CERTIFICATE ISSUANCE

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

2.1.1.2. PUBLISH PKI@BNPPF CERTIFICATE IN AN ISABEL REPOSITORY

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

2.1.1.3. ACCURACY OF REPRESENTATIONS

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

2.1.1.4. PROCESS CERTIFICATE REVOCATION REQUESTS

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

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

An Isabel CA publishes revocation information about the PKI@BNPPF 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@BNPPF CP and respects the timing specified in section “2.6.2 – Frequency of publication”.

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

2.1.1.6. NOTIFICATION OF REVOCATION OF A CERTIFICATE

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

The Isabel Certification Authority ensures that the revocation information is available to all parties.

2.1.1.7. STANDARDS COMPLIANCE

Issued PKI@BNPPF 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 ensure the handling of personal and confidential data in compliance with the Belgian Law on the protection of the Privacy.

2.1.2. ISABEL RAS OBLIGATIONS

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

2.1.2.1. PROTECTION OF RA PRIVATE KEY

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

2.1.2.3. INDEMNIFY PARTIES FOR DAMAGES

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

2.1.2.4. ARCHIVING AND SECURITY

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

2.1.3. PKI@BNPPF CERTIFICATE SUBSCRIBER AND SUBJECT OBLIGATIONS

PKI@BNPPF 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 an PKI@BNPPF Certificate.

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

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

PKI@BNPPF Certificate Subscriber and PKI@BNPPF Certificate Subject have following obligations:

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

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

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

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

2.1.3.2. GUARANTEE CONFIDENTIALITY OF PRIVATE KEY

An PKI@BNPPF 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@BNPPF 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@BNPPF CERTIFICATE USAGE

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

1. the section “1.3.6 – Applicability” of the present PKI@BNPPF CP.

2. any agreement made or to be made between BNP Paribas Fortis and the BNP Paribas Fortis Customer.

When the Subject suspects that his Private Key has been compromised, he must request the revocation of his PKI@BNPPF Certificate and cease generating digital signatures 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@BNPPF REVOCATION SERVICE ABOUT PRIVATE KEY/PIN COMPROMISE – PKI@BNPPF SECURE SIGNING CARD LOSS

A PKI@BNPPF Certificate Subject or a PKI@BNPPF Certificate Subscriber must immediately notify the PKI@BNPPF Registration Authority 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@BNPPF Secure Signing Card.
3. The suspected or known compromise loss or disclosure of the Subject's PIN code.

Alternatively, if the PKI@BNPPF Registration Authority can not 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@BNPPF RA ABOUT CHANGE OF STATUS

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

2.1.3.6. USE A HARDWARE SECURE SIGNATURE CREATION DEVICE

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

2.1.3.7. RESTRICTION ON PUBLIC KEY USAGE

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

The PKI@BNPPF Certificate Subject or Subscriber may not submit a certificate request containing the Public Key in a third party Certificate to an Isabel CA, even if the third party 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 PKI SERVICES

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

A Relying Party can only rely on a PKI@BNPPF 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@BNPPF Certificate before relying on this certificate.

A Relying Party must verify following attributes in a PKI@BNPPF 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@BNPPF Certificate in accordance with section "7.1.2 – Certificate extensions",
5. The signature of the CA.

The attributes of a PKI@BNPPF Certificate can be found in section "7.1 – Certificate Profile" of the present PKI@BNPPF CP.

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

1. The verification of the digital signature on the PKI@BNPPF Certificate fails, or the verification of the PKI@BNPPF Certificate itself fails or
2. This PKI@BNPPF Certificate has expired or
3. This PKI@BNPPF Certificate has been revoked or
4. The PKI@BNPPF 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@BNPPF 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 BNP Paribas Fortis Customers, Relying Parties and Subjects" and in the section "2.2 – Liability" of the present PKI@BNPPF CP.

2.1.5. REPOSITORY OBLIGATIONS

Isabel makes available and maintains an Electronic Repository for PKI@BNPPF Certificates and PKI@BNPPF 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@BNPPF Certificates that have been issued by the Isabel Certification Authority in compliance with the present PKI@BNPPF CP.
2. The Certificate Revocation List published in accordance with the present PKI@BNPPF CP.
3. The Self-signed Certificate of the Isabel Certification Authority.
4. The current version of this document PKI@BNPPF 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 BNP Paribas Fortis 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@BNPPF Certificate issued, were issued in accordance with the provisions of the present PKI@BNPPF 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 BNP Paribas Fortis Subscribers, Subjects, Customers and Relying Parties. The warranties apply to BNP Paribas Fortis Subscribers, Subjects, Customers and Relying Parties.

2.2.1.2. EXCLUSION OF ISABEL'S LIABILITY TOWARDS BNP PARIBAS FORTIS 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 BNP Paribas Fortis 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@BNPPF CP, in which case BNP Paribas Fortis 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@BNPPF 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@BNPPF 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@BNPPF Certificate issued by Isabel where such Relying Party failed to verify with the Validation Authority that the relevant PKI@BNPPF Certificate has not been revoked,
4. a Relying Party's reliance on any PKI@BNPPF Certificate issued by Isabel where such Relying Party knew or reasonably should have known that the relevant PKI@BNPPF Certificate has been revoked but where the Relying Party nonetheless accepts and places reliance on such PKI@BNPPF 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@BNPPF 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@BNPPF Registration Authority to comply with its obligations under the present PKI@BNPPF CP or any agreement (if any) between a Relying Party and that PKI@BNPPF Registration Authority, as the case may be,
8. any loss or compromise of any PKI@BNPPF Registration Authority's Private Key,
9. any failure by any Revocation Service to comply with its obligations under the applicable PKI@BNPPF CP;
10. any loss or compromise of any Revocation Service Private Key
11. any failure by any other party, including any PKI@BNPPF Registration Authority, to comply with any of its stated obligations towards a Relying Party,
12. any other use of the PKI@BNPPF Certificate, Private Key and/or software, than the use allowed by the present PKI@BNPPF CP;
13. any modifications or changed situations, not notified to Isabel;
14. any misuse or abuse by BNP Paribas Fortis Subscribers, Subjects, Customers and/or Relying Parties.

2.2.1.3. INDIRECT AND CONSEQUENTIAL LOSS TOWARDS BNP PARIBAS FORTIS 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 BNP Paribas Fortis 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 BNP PARIBAS FORTIS 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 BNP Paribas Fortis 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@BNPPF Certificate set forth below. The aggregate liability of Isabel to any and all persons shall, for the entire of all signatures and transactions related to such PKI@BNPPF 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 BNP Paribas Fortis 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 BNP Paribas Fortis Subscriber, Subject, Customer, or Relying Party, that are caused by reliance on or use of a PKI@BNPPF 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@BNPPF 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. LIMITATIONS 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@BNPPF RA LIABILITY

2.2.2.1. WARRANTIES AND LIMITATIONS ON WARRANTIES

BNP Paribas Fortis warrants only that any PKI@BNPPF Certificate issued, is issued in accordance with the provisions of this PKI@BNPPF 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, BNP Paribas Fortis 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 BNP Paribas Fortis Subscribers, Subjects, Customers and Relying Parties.

2.2.2.2. EXCLUSION OF BNP PARIBAS FORTIS'S LIABILITY TOWARDS BNP PARIBAS FORTIS SUBSCRIBERS, SUBJECTS, CUSTOMERS AND RELYING PARTIES

BNP Paribas Fortis shall, unless otherwise stated below, not be liable for any loss or damage suffered by, claims made against or costs incurred by BNP Paribas Fortis 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 BNP Paribas Fortis Subjects Private Key, unless BNP Paribas Fortis failed to comply with the requirements set out in this CP, in which case BNP Paribas Fortis 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 BNP Paribas Fortis 's failure to do so,
2. any inaccurate or incorrect information contained in any PKI@BNPPF Certificate issued by the Isabel CA, unless BNP Paribas Fortis failed to use all reasonable efforts to ensure the accuracy and correctness of such information or unless BNP Paribas Fortis failed to verify the authenticity of all documentary evidence of such information according to the present PKI@BNPPF CP, in which case BNP Paribas Fortis 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 BNP Paribas Fortis 's failure to do so,
3. a Relying Party's reliance on any revoked PKI@BNPPF Certificate issued by the Isabel CA where such Relying Party failed to verify that the relevant PKI@BNPPF Certificate has not been revoked,
4. a Relying Party's reliance on any PKI@BNPPF Certificate issued by the Isabel CA where such Relying Party knew or reasonably should have known that the relevant PKI@BNPPF Certificate has been revoked but where the Relying Party nonetheless accepts and places reliance on such PKI@BNPPF 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@BNPPF Certificate, Private Key and/or software, than the use allowed by this PKI@BNPPF CP;
8. any modifications or changed situations, not notified to the PKI@BNPPF RA;
9. any misuse or abuse by Subscribers, Subjects, Customers and/or Relying Parties.

2.2.2.3. INDIRECT AND CONSEQUENTIAL LOSS TOWARDS BNP PARIBAS FORTIS SUBSCRIBERS, SUBJECTS, CUSTOMERS AND RELYING PARTIES

Even if BNP Paribas Fortis has been advised of the possibility of such damages, BNP Paribas Fortis 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 BNP Paribas Fortis 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 BNP PARIBAS FORTIS'S LIABILITY TOWARDS BNP PARIBAS FORTIS SUBSCRIBERS, SUBJECTS, CUSTOMERS AND RELYING PARTIES

Provided BNP Paribas Fortis is liable, under no circumstances the entire liability of BNP Paribas Fortis to all parties, including but not limited to BNP Paribas Fortis 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@BNPPF Certificate set forth below. The aggregate liability of BNP Paribas Fortis to any and all persons concerning a PKI@BNPPF Certificate shall, for the entire of all signatures and transactions related to such PKI@BNPPF 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@BNPPF Certificate services.

This limitation on damages applies to loss and damages of all types, incurred by any person, including without limitation a BNP Paribas Fortis Subscriber, Subject, Customer, or Relying Party, that are caused by reliance on or use of a PKI@BNPPF Certificate issued, managed, used, revoked by an Isabel CA, or such a PKI@BNPPF 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@BNPPF Certificate shall be the same regardless of the number of digital signatures, transactions, or claims related to such PKI@BNPPF 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 BNP Paribas Fortis will be obligated to pay more than the aggregate liability cap for each PKI@BNPPF Certificate.

2.2.2.5. FORCE MAJEURE EVENTS

If BNP Paribas Fortis 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 BNP Paribas Fortis 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 BNP Paribas Fortis to perform any such obligations which are affected by the Force Majeure Event.

2.2.2.6. LIMITATIONS ON BNP PARIBAS FORTIS'S EXCLUSION OR LIMITATION OF LIABILITY

Nothing in this document shall limit or exclude BNP Paribas Fortis's liability for the following:

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

2.2.3. LIABILITY OF THE BNP PARIBAS FORTIS CUSTOMER, SUBSCRIBER, SUBJECT, RELYING PARTY

By accepting or using a PKI@BNPPF Certificate, the BNP Paribas Fortis Customer, Subscriber, Subject and/or Relying Party agree to indemnify and hold BNP Paribas Fortis, Isabel 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 BNP Paribas Fortis, Isabel and her agent(s) and subcontractors may incur, that are caused by the use or publication of a PKI@BNPPF Certificate and that arises from:

1. failure to execute its obligations as described in the present PKI@BNPPF CP;
2. falsehood or misrepresentation of fact by the BNP Paribas Fortis Customer, Subscriber or Subject;
3. failure by the BNP Paribas Fortis Customer, Subscriber or Subject to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive BNP Paribas Fortis, a PKI@BNPPF RA or any person receiving or relying on the PKI@BNPPF Certificate;
4. failure to protect the BNP Paribas Fortis 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@BNPPF Certificate, private key and/or software, than the use allowed by BNP Paribas Fortis.

All BNP Paribas Fortis Customers, Subscribers, Subjects, Relying Parties accept that the use of a PKI@BNPPF Certificate outside the BNP Paribas Fortis Community (see section "1.3 – Community and Applicability") without the explicit authorization of BNP Paribas Fortis, or the use of a PKI@BNPPF Certificate after a certain use has been forbidden by BNP Paribas Fortis 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 a breach of the present PKI@BNPPF CP.

2.3. FINANCIAL RESPONSIBILITY

BNP Paribas Fortis insures its professional financial liability risks arising out of its activities and liabilities with respect to the provision by it of services linked to PKI@BNPPF Certificates with a reputable insurer. Isabel N.V./S.A. shall have an adequate insurance against professional and civil liability in connection with the performance of its obligations as CA.

2.3.1. INDEMNIFICATION BY BNP PARIBAS FORTIS CUSTOMERS, RELYING PARTIES AND SUBJECTS AND BY BNP PARIBAS FORTIS

BNP Paribas Fortis Customers and/or Relying Parties and/or PKI@BNPPF Certificate Subjects must indemnify any parties (including the Isabel Certification Authority and PKI@BNPPF RAs) and/or BNP Paribas Fortis 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@BNPPF CP will have no valid claim against Isabel in the event of a damage.

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

2.3.3. ADMINISTRATIVE PROCESS

BNP Paribas Fortis accounts and annual report are published and audited yearly in accordance with the Belgian laws.

2.4. INTERPRETATION AND ENFORCEMENT

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

2.4.1. GOVERNING LAW

The laws of Belgium shall govern the enforceability, construction, interpretation, and validity of the present PKI@BNPPF CP.

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@BNPPF Certificate Subscriber or Subject don't allow the inclusion of specific provisions of the present PKI@BNPPF CP, then with respect to that PKI@BNPPF Certificate Subscriber or Subject only, these specific provisions of this CP shall be deemed null and void as if not included and the first paragraph of the present section shall be applicable.

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

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

2.4.3. DISPUTE RESOLUTION PROCEDURES

All parties involved, Isabel CA, PKI@BNPPF RA, BNP Paribas Fortis 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.

2.5. FEES

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

Refunds are only applicable in case this is explicitly agreed.

2.6. PUBLICATION AND REPOSITORY

2.6.1. PUBLICATION OF INFORMATION

The information to be published is:

1. The present PKI@BNPPF CP.
2. The PKI@BNPPF Certificates which are accepted, and therefore declared to contain correct information, by the Subject.
3. The Certificate Revocation Lists for PKI@BNPPF Certificates.
4. The Isabel CA self-signed certificate and cross-certificates.
5. BNP Paribas Fortis general terms and conditions for certification services.
6. The BNP Paribas Fortis 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@BNPPF Certificates publication is guaranteed within 24 hours after their acceptance by their Subject. Typically, PKI@BNPPF Certificates are published within 0.5 hour after they have been accepted.

The Certificate Revocation Lists (CRL) are updated typically within 0.5 hours after a change and are reissued at least once every 24 hours.

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

The issuance of the PKI@BNPPF CP is handled in section “8 – SPECIFICATION ADMINISTRATION” of the present PKI@BNPPF 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@BNPPF CP may be accessed in **read-only mode** by:

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

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

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

1. The PKI@BNPPF RAs
2. The PKI@BNPPF Certificate Subscribers and Subjects
3. The BNP Paribas Fortis Policy Authority

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

The validation service may be accessed only by the PKI@BNPPF CP Customer

2.6.4. REPOSITORIES

The PKI@BNPPF Certificates and the Certificate Revocation Lists for PKI@BNPPF 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

BNP Paribas Fortis will carry out audits of all its procedures and their compliance with the present PKI@BNPPF CP. An audit can be carried out to check Isabel N.V./S.A.'s compliance with the performance of its obligations as CA.

2.7.1. FREQUENCY OF ENTITY COMPLIANCE AUDIT

The frequency of those audits is determined by :

1. BNP Paribas Fortis internal policies.
2. The governing Belgian legal framework.
3. Other parties mandated to execute an audit on behalf of their relation with BNP Paribas Fortis.

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 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 BNP Paribas Fortis and Isabel S.A./N.V..

The auditors shall have a contractual relationship with BNP Paribas Fortis for the performance of the audit, and be sufficiently organizationally separated from the audited Isabel CA, PKI@BNPPF RA or any other BNP Paribas Fortis or 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@BNPPF RA operations.
6. The compliance to PKI@BNPPF CP.
7. The compliance to Belgian regulations.

2.7.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Audit reports will be evaluated by BNP Paribas Fortis. Any discrepancies with the PKI@BNPPF 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 BNP Paribas Fortis Security Manager only.

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@BNPPF 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 BNP Paribas Fortis and a Third Party, and it may have been revealed under non-disclosure agreement.

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

1. PKI@BNPPF Certificates and the information contained therein.
2. The Isabel Certification Authorities self-signed certificates.

2.8.2. TYPES OF INFORMATION NOT CONSIDERED CONFIDENTIAL

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

As the present PKI@BNPPF 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@BNPPF Certificate Subject or the PKI@BNPPF Certificate Subscriber who has requested the revocation of the Subject’s certificate will be notified about the revocation of the PKI@BNPPF Certificate.

The revocation reason is not communicated to Relying Parties.

2.8.4. RELEASE TO LAW ENFORCEMENT OFFICIALS

Isabel CA and PKI@BNPPF 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@BNPPF RAs are allowed to release confidential information about an PKI@BNPPF Certificate Subscriber/Subject upon the request or with the approval of that PKI@BNPPF 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 BNP Paribas Fortis or Isabel. This holds for any information published by BNP Paribas Fortis and Isabel, in a public or private relation.

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

There are 2 types of PKI@BNPPF 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@BNPPF Certificate.

3.1.2. NEED FOR NAMES TO BE MEANINGFUL

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

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@BNPPF Certificates within the X.500 namespace(s) for which Isabel has been authorised.

3.1.6. RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS

PKI@BNPPF RAs can not verify nor guarantee that trademarks, service marks or any other protected signs mentioned in PKI@BNPPF Certificates can legitimately be used without infringement on any Intellectual Property right. No RA nor any CA within the 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@BNPPF RA is obliged to authenticate the identity of a candidate BNP Paribas Fortis Customer before Subscribers of this BNP Paribas Fortis Customer are allowed to apply for PKI@BNPPF Certificates.

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

3.1.9. AUTHENTICATION OF INDIVIDUAL IDENTITY

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

3.2. ROUTINE REKEY

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

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

3.4. REVOCATION REQUEST

BNP Paribas Fortis Customers must call upon the PKI@BNPPF RA to request the revocation of their PKI@BNPPF Certificate. If unavailable, use can be made of the Card Stop revocation service.

3.4.1. AUTHENTICATION BY THE PKI@BNPPF REVOCATION SERVICE

The PKI@BNPPF revocation service must identify and authenticate the Subject to generate a revocation request. Handwritten filled form must be used as a mean of authentication.

PKI@BNPPF revocation service generates a revocation request based on information submitted on paper by the Subject.

3.4.2. AUTHENTICATION BY THE PKI@BNPPF REGISTRATION AUTHORITY

The PKI@BNPPF Registration Authority is operated by the BNP Paribas Fortis Operations Teams

PKI@BNPPF Registration Authority generates a revocation request based on information submitted on paper [correct from an operational perspective?] 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@BNPPF Registration Authority. 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@BNPPF RA's Private Key and verified with the PKI@BNPPF RA's certificate.

4. OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

A PKI@BNPPF RA acts upon a certificate application to validate an applicant's identity. Subsequently, the PKI@BNPPF 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@BNPPF RA uses documented procedures and adopts its own practices.

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

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

4.2. CERTIFICATE ISSUANCE

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

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

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

4.3. CERTIFICATE ACCEPTANCE

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

Acceptance of the PKI@BNPPF Certificate is done by (1) either explicit notification of acceptance, either (2) the use of the PKI@BNPPF 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@BNPPF 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@BNPPF Certificate is to permanently end the operational period of such 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 Digital Certificate.
- The Subscriber, the Subject, Isabel or BNP Paribas Fortis has breached a material obligation under this PKI@BNPPF CP.

- Either the Subscriber's, Isabel or BNP Paribas Fortis obligations under this PKI@BNPPF 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 BNP Paribas Fortis receive a lawful and binding order from a government or regulatory body to revoke the PKI@BNPPF Certificate.
- There has been a modification of the information pertaining to the Subscriber that is contained within the PKI@BNPPF Certificate.

4.4.2. WHO CAN REQUEST REVOCATION

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

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

4.4.3. PROCEDURE FOR REVOCATION REQUEST

The Isabel CA processes securely PKI@BNPPF Certificate revocation requests issued by the PKI@BNPPF 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@BNPPF 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@BNPPF RA’s record all current events concerning a PKI@BNPPF Certificate in audit logs. Those events are recorded for a period of ten years, in particular for the purpose of providing evidence of certification or revocation for legal proceedings. See also ref [2] in the section 9.2 – Appendix B – References of the present CP, 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@BNPPF Certificates.
- All events related to the preparation of a PKI@BNPPF Secure Signing Card.
- All requests and reports relating to revocation, as well as the resulting action.

An Isabel CA guarantees that all registration events including applications for PKI@BNPPF Certificates, such Certificate Re-key or renewal are recorded and in particular:

- Document(s) presented by the PKI@BNPPF Certificate Subscriber to the PKI@BNPPF RA to support registration in accordance with the agreement between the PKI@BNPPF RA and the BNP Paribas Fortis Customer.
- Storage location of copies identification documents, including the signed PKI@BNPPF Certificate Application.

- Any specific choices in the Subscriber's application.
- Identity of BNP Paribas Fortis Customer accepting the PKI@BNPPF 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@BNPPF 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@BNPPF Certificates must be guaranteed.

4.5.5. AUDIT LOG BACKUP PROCEDURES

Isabel ensures 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 BNP Paribas Fortis.

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 BNP Paribas Fortis 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@BNPPF Certificates
- Isabel Certificate Revocation List
- PKI@BNPPF Certificate Policy
- All events and requests leading to changes to PKI@BNPPF Certificates and Certificate Revocation List

4.6.2. RETENTION PERIOD FOR ARCHIVE

All information related to PKI@BNPPF 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@BNPPF Certificate Subject shall have access to archived information relating to himself, without compromising the general confidentiality obligations of the Isabel CA and PKI@BNPPF RAs. All requests to obtain archived information must be addressed to the BNP Paribas Fortis 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 BNP Paribas Fortis for all PKI@BNPPF Certificate related activities.

On termination of an Isabel CA activities, Isabel will act as stipulated by the Belgian National Law, see ref [2] in the section 9.2 – Appendix B – References of the present CP.

In case of termination of a PKI@BNPPF RA, BNP Paribas Fortis 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@BNPPF 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 BNP Paribas Fortis 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 BNP Paribas Fortis 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 PKI.

6.1.2. PRIVATE KEY DELIVERY TO ENTITY

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

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

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

6.1.3. PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

BNP Paribas Fortis 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 Isabel 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@BNPPF Certificate and associated at a PKI@BNPPF 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@BNPPF 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@BNPPF Certificate Subject Private Key is stored within a PKI@BNPPF 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.

BNP Paribas Fortis Subscriber Private Keys must be under sole control of BNP Paribas Fortis Subscriber.

6.2.3. PRIVATE KEY ESCROW

Isabel CA Private Keys are not escrowed.

BNP Paribas Fortis Subscriber Private Key are not escrowed.

6.2.4. PRIVATE KEY BACKUP

Isabel CA Private Keys are backed up.

BNP Paribas Fortis Subscriber Private Key must not be backed up.

6.2.5. PRIVATE KEY ARCHIVAL

BNP Paribas Fortis 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.

BNP Paribas Fortis Private Keys are deactivated when the PKI@BNPPF 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.

BNP Paribas Fortis Subscribers Private Keys are destroyed when destroying the PKI@BNPPF Secure Signing Card.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. PUBLIC KEY ARCHIVAL

PKI@BNPPF 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 BNP Paribas Fortis Subject's Activation Data, consisting of an initial PIN code for the PKI@BNPPF Secure Signing Card, is done centrally by the Isabel CA. The Isabel CA guarantees that the initial PIN code is transmitted securely to the BNP Paribas Fortis 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

BNP Paribas Fortis 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@BNPPF Secure Signing Card, and its initial PIN code can be at the same place except after pickup by the BNP Paribas Fortis Customer.

During the installation, the BNP Paribas Fortis 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@BNPPF 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 BNP Paribas Fortis for the PKI@BNPPF RAs.

6.6. LIFE CYCLE TECHNICAL CONTROLS

Lifecycle technical controls are implemented according to internal policies of Isabel for the Isabel CA and BNP Paribas Fortis for the PKI@BNPPF RAs.

6.7. NETWORK SECURITY CONTROLS

Network security controls are implemented according to internal policies of Isabel for the Isabel CA and BNP Paribas Fortis for the PKI@BNPPF RAs.

6.8. CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

No stipulation.

7. Certificate, CRL, OCSP Profiles

7.1. CERTIFICATE PROFILE

The profile of a PKI@BNPPF 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@BNPPF Certificates delivered by Isabel Certification Authorities must be compliant to ITU-T X.509 v3. c.f. ref [3] in the section “9.2 – Appendix B – References” of the present PKI@BNPPF 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 may only appear if the version is 3. This field is a sequence of one or more certificate extensions.

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

Here is the list of the standard certificate extensions (as defined in ITU-T X.509) that are used in Isabel Certificates delivered by an Isabel 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 an PKI@BNPPF 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-BNP Paribas Fortis contract type: “PKI@BNPPF” *For Internal use only*
SerialNumber (OID 2.5.4.5)	NC	This field represents the PKI@BNPPF 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)}
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@BNPPF CP: 2.16.56.1.9.48.1.1 The field also contains an attribute that is a URI to the full version of the PKI@BNPPF CP referring to the Easy Banking Business website of BNP Paribas Fortis.

Certificate Extension Field	Criticality	Value or Value Format
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@BNPPF 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@BNPPF Certificate can be considered as an element for identification on which basis the PKI@BNPPF Certificate is issued.

7.1.5. NAME CONSTRAINTS

Name Constraint extension is not used in an PKI@BNPPF Certificate.

7.1.6. CERTIFICATE POLICY OBJECT IDENTIFIER

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

7.1.7. USAGE OF POLICY CONSTRAINTS EXTENSION

Policy constraint extension is not used in an PKI@BNPPF 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 PKI@BNPPF Certificate Policy referring to the Easy Banking Business website of BNP Paribas Fortis.

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 BNP Paribas Fortis, the CRL is kept internal, OCSP is the preferred means available to BNP Paribas Fortis 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@BNPPF CP should be addressed to its Policy Authority specified in section “1.3.7 – Contact details” of the present PKI@BNPPF CP.

BNP Paribas Fortis may amend the present PKI@BNPPF CP at any time.

8.2. PUBLICATION AND NOTIFICATION POLICIES

The present PKI@BNPPF Certificate Policy is under direct control of the Policy Authority, see “1.3.5 – Policy Authorities”. The senior management of BNP Paribas Fortis is committed to ensuring that the practices in the present PKI@BNPPF CP are properly implemented.

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

The Policy Authority will produce recommendations for change to the present PKI@BNPPF Certificate Policy, which will be subject to a process of consultation within BNP Paribas Fortis and authorisation by the General Manager “Multichannel Banking” before any changes are implemented.

The present PKI@BNPPF Certificate Policy and its future versions are published at the URI referring to the Easy Banking Business website of BNP Paribas Fortis.The date of publication and the effective date and the version number shall be indicated on the title page of the present PKI@BNPPF 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@BNPPF Certificate Policy will also be published at the above URI.

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

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

8.3. PKI@BNPPF CERTIFICATE POLICY APPROVAL PROCEDURES

The Policy Authority for the present PKI@BNPPF Certificate Policy and the General Manager “Multichannel Banking” must approve changes to the present document.

9. Appendixes

9.1. APPENDIX A – DEFINITIONS

9.1.1. ACRONYMS

Acronym	Description
CA	Certification Authority
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@BNPPF Certificates the Activation Data consists of an initial PIN code sent to the Subscriber on creation of his PKI@BNPPF 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.
BNP Paribas Fortis	Fortis Bank SA/NV, Montagne du Parc 3, 1000 Brussels – Belgium, with company register at Brussels, RPM/RPR no BE0403.199.702.
PKI@BNPPF Certificate	A Digital Certificate that has been issued by an Isabel CA to a PKI@BNPPF Certificate Subscriber.
PKI@BNPPF Certificate Relying Party	A PKI@BNPPF Certificate Relying Party is a physical person or a function that is or belongs to a BNP Paribas Fortis Customer and that relies on the information contained in a PKI@BNPPF Certificate, and/or digital signatures verified using this certificate and/or any other information published by an Isabel CA issuing PKI@BNPPF Certificates.
PKI@BNPPF Certificate Request	Submission of validated PKI@BNPPF Certificate Application information by a PKI@BNPPF RA to an Isabel CA to issue a PKI@BNPPF Certificate
PKI@BNPPF 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@BNPPF Certificate Subject has been issued a PKI@BNPPF Certificate in the scope of his/her activities and decrypts or/and signs with the Private Key associated to that PKI@BNPPF Certificate on behalf of the BNP Paribas Fortis Customer to which he/she belongs. A PKI@BNPPF 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@BNPPF Certificate Subscriber	A physical person, empowered by a BNP Paribas Fortis Customer, to apply for a PKI@BNPPF Certificate in the name of one or more physical person(s) or function(s) subject(s).
BNP Paribas Fortis Customer	An entity that signed a BNP Paribas Fortis contract with BNP Paribas Fortis with the intention of receiving services and/or products from BNP Paribas Fortis.
PKI@BNPPF RA	See PKI@BNPPF Registration Authority.
PKI@BNPPF Registration Authority	An RA, appointed by BNP Paribas Fortis, that operates under the authority and the control of an Isabel CA for PKI@BNPPF Certificates.
PKI@BNPPF 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@BNPPF Secure Signing Card.
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.

Term	Description
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	Isabel NV/SA, Keizerinlaan 13-15, 1000 Brussels – Belgium with company register at Brussels, RPR/RPM no BE0455.530.509.
Isabel Repository	Is an entity around the Isabel CA which provides for the publication of the Certificates and the Certification Revocation List.
Personal Identification Number	A secret code (PIN) that is used to protect against unauthorised access to a Private Key.
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@BNPPF 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@BNPPF Certificate Subject.
Subscriber	See PKI@BNPPF Certificate Subscriber.
Validation Authority	An authority that provides PKI@BNPPF Certificates' Relying Parties with a way of obtaining PKI@BNPPF 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 2527: 'Internet X.509 Public Key Infrastructure – CP and Certification Practices Framework'	Internet Engineering Task Force (IETF)	March 1999
[5]	Banking – Public Key Infrastructure Policy and Practices framework – ISO/TC68/SC2/WG8 N 001	International Standards Organisation	22 October 2002