BNP Paribas Fortis Certification Policy

Certification Authority

BNP Paribas Fortis Customer Ephemeral Certification Authority

Review		
Name	Position	Date

Confirmation		
Name	Position	Date
PMA	Governing body	13/02/2018

Versioning			
Version	Date	Author	Type of amendments
0.5	17/10/2016	Cédric Szaniec	First initialisation version
0.6	28/10/2016	Gert Feyt	Changes following meeting with Fortis and Signel (21/10) and following feedback of Fortis lawyers.
1.0	09/11/216	Cédric Szaniec	Version confirmed by the PMA
1.1	18/2/2017	Cédric Szaniec	Taking into account the various remarks by Fortis and consultants
2.0	23/06/2017	Cédric Szaniec	Change from Safran I&S to IDEMIA Adaptation of CP for eIDAS EN 319 411 - 1
2.1	25/06/2017	Cédric Szaniec	Addition of elements for new channel: Easy Banking Business
2.2	16/01/2018	Cédric Szaniec	Change from 'OT Morpho' to 'IDEMIA' and from 'ITP ITG' to 'ITG'. Corrections for Non Conformities resulting from audit ETSI EN 319 411-1 : - Added I.C.6 - Modified and clarified III.A.4 and III.A.5 - Specified IV.J.1

Contents

I. Introduction

I.A. General introduction

This document defines the Certification Policy applicable to the certificates:

- issued by the "BNP Paribas Fortis Customer Ephemeral Certification Authority <N> " certification authorities (hereinafter "BNPPF Instant CA"), acting as Certification Service Provider (CSP);
- in order to respond to the requirements of reliability of core applications (in particular, in the case of online contract applications).

This certification policy (hereinafter "CP") concerns the issue of certificates of electronic signature of documents in PDF, XML (XAdES, XML-DSig) or CMS format.

The BNPPF Instant Fortis CA responds to the requirements of private individuals, users of BNP Paribas Fortis personal certificates (hereinafter holders), and forms part of the BNP Paribas Group's Public Key Infrastructure (PKI) as indicated in Figure 1.

The purpose of this certification policy, part of an ETSI EN 319 411-1 qualification process, is to describe:

- The commitments of the BNPPF Instant CA relating to the definition of rules of issue and to management of certificates issued by BNP Paribas Fortis, and to their implementation
- The terms and conditions of use of certificates issued by the BNPPF Instant CA

This Certification Policy responds to the requirements of the Lightweight Certificate Policy (LCP) defined in standard ETSI EN 319 411-1. The LCP OID is as follows: 0.4.0.2042.1.3.

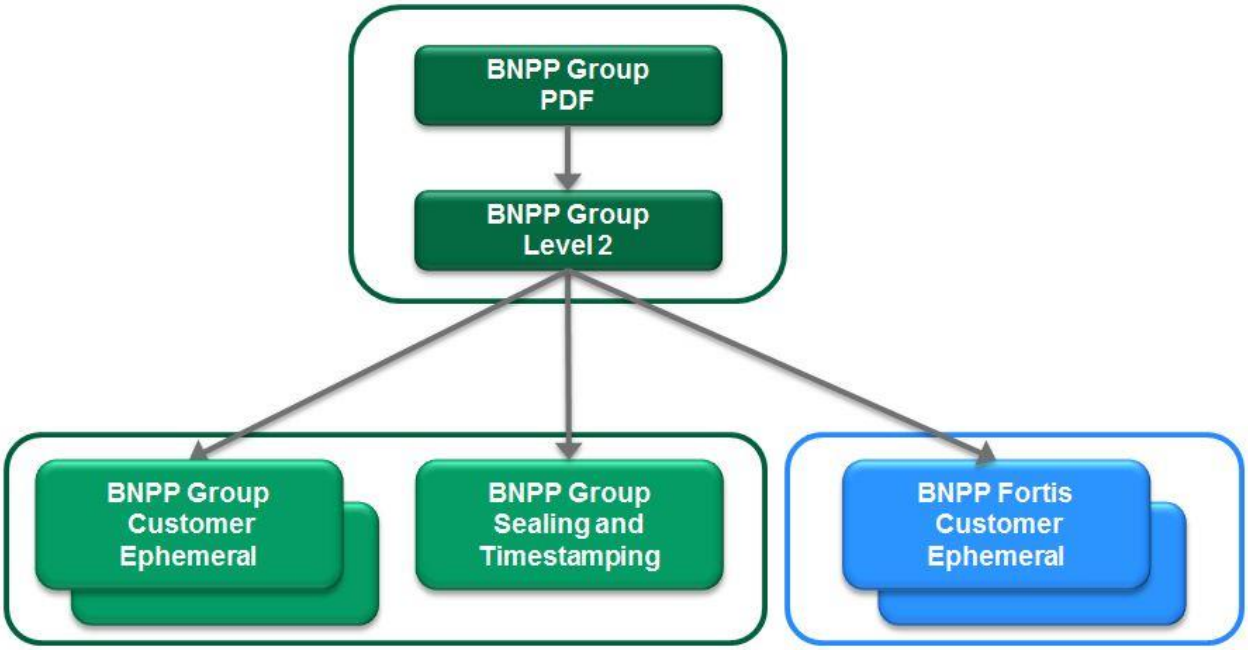


Figure 1: PKI of the BNP Paribas Group

I.B. Identification of the document

This certification policy is identified by its object identifier (OID, footer on each page of the document). Other more explicit information such as, for example, name, version number or date of update, also help identify it.

The OID numbers corresponding to this certification policy indicated in the certificates depend on the technical body of the issuer CA, i.e.:

- For electronic signature certificates:
  - BNPPF Instant CA no. 1: 1.2.250.1.62.10.7.1.1.2

    - BNPPF Instant CA no. 2: 1.2.250.1.62.10.8.1.1.2
- For OCSP certificates:
    - BNPPF Instant CA no. 1: 1.2.250.1.62.10.7.1.2.1
    - BNPPF Instant CA no. 2: 1.2.250.1.62.10.8.1.2.1

The OID branch of BNP Paribas is registered: {iso(1) member-body(2) fr(250) type-org(1) BNP Paribas(62)} Signel (10) BNPPF Instant CA (7 or 8) Certification Policy(1) Certificate Template(1 or 2) Version(1 or 2)

It corresponds to certificates issued from 24 July 2017 onwards.

I.C. Entities operating within the PKI

To clarify and facilitate identification of requirements, and in line with the documents of the ETSI in the area of functional breakdown of the CP of BNPPF Instant CA, the latter is organised around the following entities:

- Certification Authority (CA)
- Registration Authority (RA)
- Holders
- Operator
- User application (application for signature of documents made available by BNP Paribas Fortis)
- PMA (Policy Management Authority): PKI governance body

The scenarios of usage covered by the CP do not require any confiscation functions.

BNPPF Instant CA means a Manager of certificates for management of its PKI, in particular, as interface with the Operator.

In the context of the functions of BNPPF Instant CA certification service provision which it handles directly, BNPPF Instant CA is a service of BNP Paribas Fortis. BNP Paribas Fortis is a legal entity within the meaning of Belgian law, which undertakes to satisfy the following requirements:

- To be a contractual relationship with the end users for which it is responsible for ensuring:
    - the issue and management of certificates, relying, for this, on BNP Paribas' public key infrastructure (PKI);
    - the definition of the rules of issue of certificates issued by the BNPPF Instant CA and their correct application;
    - the definition of the terms and conditions of use of certificates issued by the BNPPF Instant CA;
- Remittance to the holder of certificates issued by the BNPPF Instant CA and for which, through BNP Paribas, IDEMIA is responsible for management of holder certificates.

I.C.1. Certification Authority

The certification authority BNPPF Instant CA is responsible for the provision of services relating to management of certificates throughout their lifetime (generation, diffusion, renewal, revocation, etc.) and relies, for this, on a public key infrastructure (PKI).

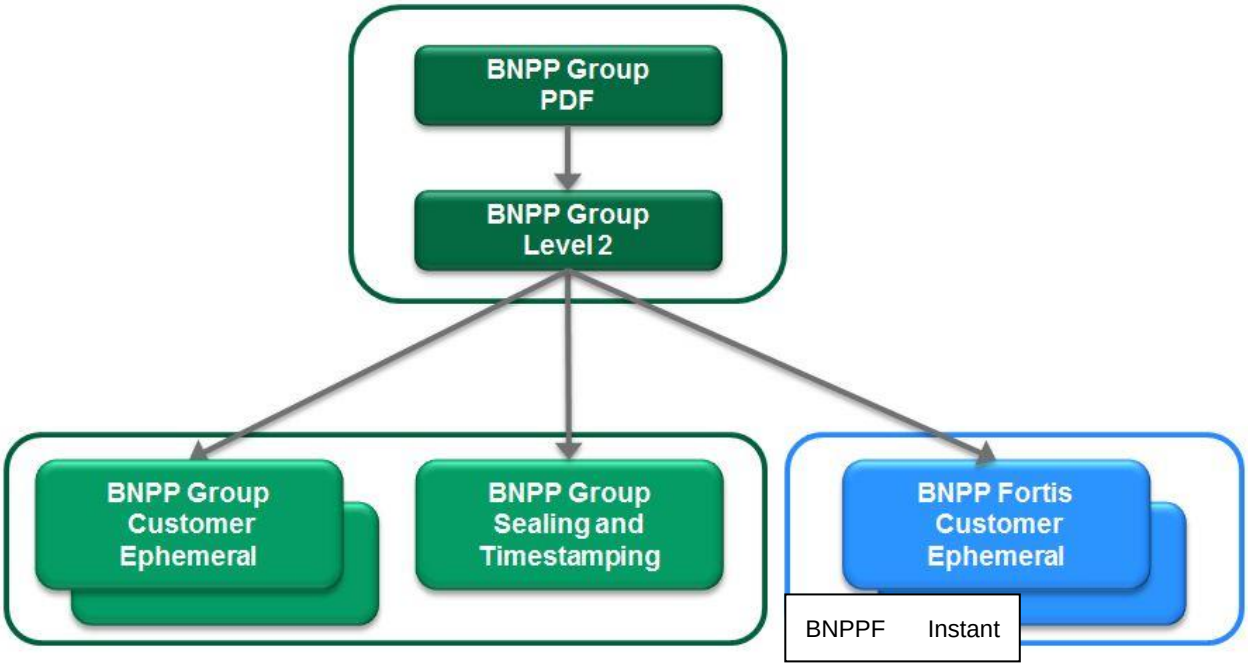
To clarify and facilitate identification of requirements, and in line with the documents of the ETSI (European Telecommunications Standards Institute) on this topic, the functional breakdown of this PKI is as follows:

- **Certificate generation function** – This function generates the certificates (creation of format, electronic signature with associated private key):
    - either by using the tools specific to the technical units or the future certificate holders; or
    - by using the tools of its PKI.
- **Function of remittance to holder** – This function remits to the holder, as a minimum, their certificate or the certification chain.

- **Publication function** – This function provides the various parties concerned with the policies published, the authority certificates and any other relevant information aimed at holders and/or users of certificates, apart from certificate status information.
- **Revocation management function** – This function processes revocation applications and determines the actions to be taken. The results of processing are diffused via the certificate status information function.
- **Certificate status information function** – This function provides users of certificates with information about the status of certificates (revoked status in particular). This function is implemented according to an information publication method which is given material form by a Certificate Revocation List (CRL).
- **PKI administration function** – This function is associated with the role which defines the functional behaviour and technical configuration of the PKI.

All of the functions handled by BNP Paribas' PKI (as a technical department) are executed by IDEMIA's IT department, which acts as a supplier of BNP Paribas. BNP Paribas acts as a supplier of the PKI for the BNPPF Instant CA, a BNP Paribas Fortis service. BNP Paribas Fortis is linked to BNP Paribas via a Master Service Agreement (MSA).

The Certification Practice Statement (CPS) associated with the authorities identified in this document describes the operational organisation of the PKI and the distribution of roles between the various units, according to the functional organisation and definition of the roles described in this policy:



Technically, BNPPF Instant CA is made up of two separate PKI departments. They are identified by a CN with a suffix:

- CN = BNP Paribas Fortis Customer Ephemeral Certification Authority <N>

  Where <N> is 1 or 2

I.C.2. Registration Authority (RA)

The role of the RA is to verify the identity of the requester of a certificate in order to approve the certificate issue application.

This function verifies the identification information of the future holder of a certificate, and any other specific attributes, before sending the corresponding application (generation, revocation) to the appropriate PKI function.

It must apply procedures for identification of private individuals making it possible to issue certificates according to a procedure in compliance with Belgian banking regulations, and notably, with the regulation on the prevention of use of the financial system for the purposes of money laundering or the financing of terrorism (Law of 11 January 1993 on the prevention of use of the financial system for the purposes of money laundering or the financing of terrorism).

There are two steps in the registration procedure for certificates issued by BNPPF Instant CA: the first is completed just once, when the private individual enters into a relationship with the bank and the second, based on information registered during the first step, is completed whenever the private individual applies for an ephemeral certificate, that is, whenever a transaction requiring a signature is necessary.

The BNPPF Instant CA uses two RA units:

- **A functional RA:** responsible for verification of the identity of the private individual and keeping the proof of identity provided by that person, and this, in two steps:
    - Step 1: When the private individual enters into a relationship with the bank which is maintained for the period of time in compliance with Belgian banking regulations. This is a commercial branch of BNP Paribas Fortis, which collects proof of identity. These documents are archived electronically. During this step, one or more means enabling definitive authentication are remitted to or associated with the user.
    - Step 2: On each transaction likely to give rise to issue of a certificate. This is an authentication system which uses the authentication methods associated with the private individual (see previous step) recognised by the bank and a high level of assurance regarding the person's identity.
- **A technical RA:** responsible for the creation of keys and submission of certificate applications to the certification authority. It also generates a file of proof (files of proof of signature confirmation) on each signature by the holder.

The BNP Paribas Fortis functional RA has responsibility for:

- Verifying the identity of the future certificate holder.
    - On initialisation of processes making it possible to become a customer of the bank or agent:
        - Using face to face or equivalent: verification of identity details based on documentary evidence in accordance with the regulations applicable to credit establishments
            - In the case of a Belgian resident, the electronic identity card (or where applicable, another document) issued by the Belgian authorities is used.
            - In the case of a non-resident, the identity card or where applicable, the passport issued by the country of residence is used. In the absence of an identity document, ad hoc processes have been put in place
        - When the identification details are verified, an acceptance process is initiated in order to become a customer of the bank or agent
        - After acceptance
            - **For the Easy Banking Web (EBW) channel**, the bank is responsible for:
                - remitting to the user (mentioned in step 1) the smart bank card (EMV standard) which allows authentication using the M1 protocol and signature using the M2 protocol;
                - remittance of their PIN;
                - remittance of the branded UCR on behalf of BNP Paribas Fortis.
            - **For the Easy Banking Business (EBB) channel**, the bank is responsible for:

        - remitting to or associating with the user (mentioned in step 1), the smart bank card (Isabel standard) which allows authentication and signature, and optionally, remitting their PIN;
        - Activation of the card for the EBB channel is secure: either face to face at the bank or using the Belgian identity card (Belgium eID) using their PIN.
    - All documentary proof of identity is kept in the bank archiving system, and this is made available to all bank branches.

- On initialisation of the process making it possible to take out a contract online.

    - **For the Easy Banking Web (EBW) channel**: during this step, authentication of the customer is unique (SMID: customer number) as a private individual in their banking electronic channel with their bank card (procedure M1).
    - **For the Easy Banking Business (EBB) channel**: during this stage, authentication of the private individual (mentioned in step 1) is unique in the bank electronic channel with their EEB/Isabel card and their PIN:
        - An EBB card provided by BNPP Fortis
        - An Isabel card provided by BNPP Fortis
        - An Isabel card provided by another bank
    - They can then:
        - select a product/service;
        - follow the corresponding instructions necessary to purchase the product/service;
        - proceed with the electronic signature step for the product/service.

- On initialisation of the process making it possible to sign electronically.
    - The private individual:
        - **For the Easy Banking Web (EBW) channel:** enters the M2 challenge from their bank card as a private individual (SMID) in their banking online channel. This step formalises the application for creating a signature certificate.
        - **For the Easy Banking Business (EBB) channel:** uses their EBB or Isabel card in their bank electronic channel and enters their PIN. This step formalises the application for creating a signature certificate.
    - If this application is **valid, a certificate application is sent to the technical RA** which generates a certificate in the name of the private individual (forename, surname).

      Note: At this stage, by clicking on "Cancel" instead of signing with their bank/EBB/Isabel card (authorisation screen), the signature process is cancelled and the user returns to the selected product/service screen. No certificate is generated.

    - This step also enables acceptance of the certificate to be managed:
        - Either the private individual gives their consent (authorisation screen) concerning:
            - the identification data concerning them, taken from the certificate generated;
            - the creation of an electronic signature on their behalf on a specific contractual document;

Note: They may view CGUs and CPs during this step.

This process formalises the electronic signature application. Consequently, the certificate generated is used to sign the document legally binding the customer or agent with the Bank.

- Or the private individual brings an end to the electronic signature process by clicking on "Cancel" instead of giving their consent (authorisation screen). Consequently, the certificate generated is cancelled. The user returns to the signature screen and no signature is generated.

- Keep the verification data of the certificate holder in accordance with the regulation applicable to credit establishments *(Law of 11 January 1993 on prevention of use of the financial system for the purposes of money laundering and financing of terrorism).*

- Keep all of the holder's authentication personal details confidential, in compliance with banking regulations.

  - All information relating to confidential details is stored in the banking archiving system.

I.C.3. Certification operator

The Certification Operator provides technical services, in particular relating to security and hosting, making it possible to satisfy the requirements of this policy.

The role of the Certification Operator is handled by IDEMIA.

I.C.4. Certificate holder

In this certification policy, a certificate holder is a private individual identified by BNP Paribas Fortis (accountholder customer or agent).

I.C.5. Certificate user applications

The certificate user applications are:

- An electronic signature creation application made available to the certificate holder by BNP Paribas Fortis,
- All electronic signature display and approval software.

I.C.6. Policy Management Authority (PMA)

The PMA is the PKI governing body of BNP Paribas, and has the following responsibilities:

- Define, review, approve and apply Certification Policies and Certification Practice Declarations,
- Manage all the risks related to the PKI,
- Manage the events specific to the PKI (for example: key ceremony or end of life),
- Define and manage the trusted staff or entities operating the PKI,
- Manage relationships with external entities,
- Take all the necessary actions to enforce the execution of all the above-listed tasks.

I.D. Usage of certificates

I.D.1. Dual keys and holder certificates

The ephemeral certificates issued in the context of this certification policy are only used in connection with use of electronic signature solutions and approval of documents in a format defined by BNP Paribas Fortis.

The only permitted use is personal signature through the 'Non Repudiation' value (2.5.29.15(1)) of the 'Key Usage' extension.

I.D.2. Dual keys and certificates from the BNPPF Instant CA

The certificates from the BNPPF Instant CA defined by this CP are used to sign the ephemeral signature personal certificates and CRLs.

I.D.3. Dual keys and OCSP certificates

The signature keys of the CA's OCSP department (OID: 1.2.250.1.62.10.7.1.2.1 & 1.2.250.1.62.10.8.1.2.1) are only used to sign the OCSP tokens produced by the certificate status information function.

I.E. Certification policy management

I.E.1. Company managing the certification policy

The entity responsible for the administration and management of this certification policy is ITG in agreement with BNP Paribas Fortis. It is responsible for the preparation, follow-up and amendment, as necessary, of this CP.

ITG is the Group Information Technology function.

I.E.2. Contact point

BNP Paribas Fortis can be contacted for any questions relating to this CP via the Easy Banking Centre (EBC) on 02 762 20 00 (FR) or 02 762 60 00 (NL).

Fintro can be contacted for any questions relating to this CP via Easy Banking Fintro (Web & App) on 02 433 45 20 (FR) or 02 433 45 10 (NL).

The Easy Banking Business Helpdesk can be contacted for any questions relating to this CP via the EBB Helpdesk on 02 565 05 00.

If the response or treatment are still not satisfactory, the Complaints Management Department may be asked to intervene.

I.E.3. Entity determining a CPS's conformity with this certification policy

The PMA (Policy Management Authority), the PKI's governance body, appoints the people (or departments) determining the conformity of the Certification Practice Statement with this Certification Policy.

I.E.4. CP compliance approval procedures

This Certification Policy will be revised periodically by the PMA (Policy Management Authority), this PKI's governance body, in order to ensure its compliance with the security standards expected by the national supervisory body (cf. eIDAS European Regulation No 910/2014).

In addition, the approval of this Certification Policy will occur during a PMA session.

I.F. Definitions and acronyms

The acronyms used in this CP are as follows:

- **AA**: Archiving Authority
- **CA:** Certification Authority
- **RCA:** Root Certification Authority
- **RA:** Registration Authority
- **ANSSI:** Agence Nationale de la Sécurité des Systèmes d'Information
- **CAP**: Client Acceptance Procedure
- **CFU**: Customer Follow-up
- **GTCU:** General Terms and Conditions of Use
- **CRL:** Certificate Revocation List
- **DN**: Distinguished Name
- **CPS:** Certification Practice Statement
- **EMV**: Europay/Mastercard/Visa
- **PKI:** Public Key Infrastructure
- **OID**: Object Identifier
- **OCSP**: Online Certificate Status Protocol
- **PMA**: Policy Management Authority
- **CP:** Certification Policy
- **SGRG:** Security General Reference Guide:
- **RSA**: Rivest Shamir Adleman
- **SMID**: Single Multichannel Identifier
- **UCR**: Unconnected card reader
- **URL**: Uniform Resource Locator

Public Key Infrastructure (PKI)	All physical units, procedures and software making it possible to manage the lifetime of certificates and to offer authentication, assessment and signature services.
Certificate	Electronic file issued by a Certification Authority certifying the identity of a holder (private individual, machine, etc.). The certificate is valid for a given term specified in the certificate.
Certification Authority (AC or CA)	Entity responsible for signing, issuing and maintaining the certificates of a public key infrastructure, in accordance with a certification policy. Applicative entities using the certificates issued by the Certification Authority of the holder of the certificate.
Certification policy (CP)	All rules and requirements to which a certification authority is subject in the setting in place and supply of its services.
Certification Practice Statement (CPS)	Description of practices (organisation, operational procedures, technical and human resources) which the certification authority applies in the context of the provision of its electronic certification services, in accordance with the certification policy or policies which it has undertaken to respect.
Certificate Revocation List (CRL)	List published by the certification authority presenting certificates which are no longer reliable (revoked, invalid, etc.). For simplicity, the authorities' revocation lists (known as ARL) are associated with this.
OCSP responder	Certificate online status service
Dual key	Pair of keys made up of a private key and a public key.

X 509	Standard of the Union internationale des télécommunications (UIT) relating to public key infrastructures (PKI), including the standard formats of its units: electronic certificates, revocation lists, confirmation algorithm, etc.
UTF-8	Encoding of characters defined by Unicode where each character is encoded on a series of one to six 8-bit words (there are currently no characters codes with more than four words).
Distinguished Name (DN)	Element making it possible to identify a holder or a certification authority in a unique way.
Object Identifier (OID)	Universal identifier, represented in the form of a series of whole numbers associated in the context of a PKI to a reference element such as the certification policy or the Certification Practice Statement.
Isabel Card	A type of card from the company Isabel with very secure technology which allows technically secure authentication and high-level legal identification.
EBB Card	A type of card from the company Isabel for the EBB platform with very secure technology which allows technically secure authentication and high-level legal identification.
eID Belgium	A type of identification card from the Belgian government with very secure technology which allows technically secure authentication and high-level legal identification.

II. Responsibilities concerning the provision of information to be published

II.A. Companies responsible for providing information

For the provision of information to be published intended for holders and users of certificates, the BNPPF Instant CA implements, within its PKI, a publication function and a certificate status information function.

This policy specifies the methods of provision and the corresponding URL (web publication servers).

II.B. Information to be published

The BNPPF Instant CA publishes the following information intended for certificate holders and users:

- This certification policy: **http://bnpp.digitaltrust.morpho.com/cp**.

  The lists of revoked certificates: **http://bnpp.digitaltrust.morpho.com/crl/bnpp-fortis-customer-ephemeral1-ca.crl** and **http://bnpp.digitaltrust.morpho.com/crl/bnpp-fortis-customer-ephemeral2-ca.crl**.
- The currently valid certificates of the BNPPF Instant CA: **http://bnpp.digitaltrust.morpho.com/ca/bnpp-fortis-customer-ephemeral1-ca.cer** and **http://bnpp.digitaltrust.morpho.com/ca/bnpp-fortis-customer-ephemeral2-ca.cer**.
- The general terms and conditions for the use of ephemeral certificates.

II.C. Publication deadlines and frequency

The publication deadlines and frequency depend on the information concerned:

- For information linked to the PKI (new version of the CP, general terms and conditions of use), information is published as soon as necessary so that consistency between the information published and the CA's actual commitments is assured at any time. This deadline is no more than 7 business days.
- For certificate status information, refer to IV.I.
- For systems publishing this information, BNP Paribas and IDEMIA make the following commitments regarding availability requirements:
  - For information linked to the PKI (new version of the CP, general terms and conditions of use), systems have availability for working days with a maximum period of unavailability due to interruption of service (failure or maintenance) of 8 hours (working days) and a total maximum tolerated period of unavailability of 2 hours 10 minutes per month excluding scheduled maintenance and excluding cases of force majeure (proven serious security incident).
  - For CA certificates and lists of revoked certificates, systems have availability of 24 hours, 7 days a week, with a maximum tolerated period of unavailability of 2 hours 10 minutes per month excluding scheduled maintenance and cases of force majeure (proven serious security incident).

II.D. Control of access to information published

All information published aimed at certificate users is freely accessible. Access for making changes to the publication systems (additions, deletions, amendments to published information) is strictly limited to the authorised internal functions of the PKI.

III. Identification and authentication

III.A. Naming

III.A.1. Types of names

The names used comply with the specifications set out in the standard X.500.

On each X509 v3 certificate, the issuers and the subject are identified by a Distinguished Name, DN, of the type X.501, the exact format of which is set out in Section VII describing the certificate profile, in accordance with standard ETSI EN 319 412-1.

III.A.2. Need to use explicit names

The names chosen to designate certificate holders must be explicit. The DN respects the structure of the identity used in the BNP Paribas Fortis reference systems and which the bank communicates in its function as technical RA to the operator for signature of the corresponding certificate.

The subject's common name (CN) must represent the identity of the recipient, whose identity will have been verified (cf. §III.B) and may not in any event represent anything other than their identity in connection with their civil status (no machine name, or the identity of another person).

III.A.3. Using pseudonyms for holders

Pseudonyms are not used for holder certificates.

III.A.4. Rules for interpreting various name forms

The functional RA is responsible for the uniqueness of the names of its holders and for settlement of disputes concerning the claim relating to use of a name by said holders.

The functional RA, in the context of relationship entering, carries out transformations concerning the name and first names of the bearer. The name can only contain 40 characters, which must be letters, blanks, dashes, dots or commas, to the exclusion of all others.

For first names, the length of all first names can not exceed 32 characters and can only contain letters, blanks, dashes, dots or commas, to the exclusion of all others.

In addition, the following transformations are applied:

- for lowercase letters, 'abcdefghijklmnopqrstuvwxyzâäàáãåçñéêëèíîìîôöòóõûüùúý' are converted to 'ABCDEFGHIJKLMNOPQRSTUVWXYZAAAAAACNEEEEIIIIOOOOOUUUUY'
- for uppercase letters, 'ÂÄÀÁÃÅÇÑÉÊËÈÍÎÌÎÔÖÒÓÕÛÜÙÚÝ' are converted to 'AAAAAACNEEEEIIIIOOOOOUUUUY'

The detailed rules are indicated in the CPS.

III.A.5. Uniqueness of Names

a) As regards an ephemeral certificate

BNP Paribas Fortis is responsible for the uniqueness of the names of its holders and for settlement of disputes concerning the claim relating to use of a name by said holders.

In order to ensure continuity of the holder's unique identification within the domain of the BNPPF Instant CA, the DN in the "Subject" field of each holder certificate allows unique identification of the corresponding holder within the CA's domain.

For this, this DN must respect the following requirements for holders:

- CN = Identity of subject / private individual, in the form "Givenname Surname"

- SN (surName) = surname of subject / private individual
- givenName = given name of subject / private individual
- SN (serialNumber) = Unique no. (UUID)
- OU= F+ (customer's SMID) or I+(Isabel ID + SMID)
- C=BE

Uniqueness is guaranteed by BNP Paribas Fortis by the addition of a unique number (UUID) – cf. RFC 4122 –) in the SN attribute of the subject (DN) of the certificate.

In the case of a test certificate, the template used is the same as the template of an ephemeral certificate. However, the DN will meet the following requirements:

- CN (commonName) = either the Identity of the subject / natural person, as "First name Last name" with the addition of a "- Test" in suffix, or "MONITORING - TEST"
- SN (surName) = either the name of the subject / natural person with the addition of "- Test" in suffix, or "MONITORING -TEST"
- givenName = either the subject / natural person's first name or "MONITORING -TEST"
- SN (serialNumber) = unique number (UUID)
- OU = F-1
- C = BE

b) As regards an OCSP certificate

The serial number integrated into the subject of the OCSP certificate guarantees its uniqueness.

- CN (commonName) = OCSP Responder <N>

In case of a test certificate, the CN field will contain the suffix "TEST".

c) As regards a certificate from the Instant CA certification authority

The serial number integrated into the subject of the certification authority makes it possible to identify the CA having issued the lightweight certificate.

III.A.6. Identification, authentication and role of registered trademarks

The BNP Paribas trademark is registered by BNP Paribas:

- BNP PARIBAS, a French trademark registered on 3 September 1999 in classes 35, 36 and 38 under number 99810625.
- BNP PARIBAS, a Community trademark registered on 8 October 1999 in classes 35, 36 and 38 under number 1338888.

The BNP Paribas Fortis trademark is a trademark registered in the European Union by BNP Paribas on 17 February 2010 in classes 9, 35, 36 and 41 under number 008373185.

- This trademark was registered with the Bureau Benelux des Marques on 3 January 2013 in classes 35, 36 and 42 under number 0931084.

The Fintro trademark is a trademark registered in the European Union by BNP Paribas Fortis on 10 May 2007 in class 36 under number 004046173.

- This trademark was registered with the Bureau Benelux des Marques by BNP Paribas Fortis on 27 September 2004 in class 36 under number 0764125.

III.B. Initial approval of identity

III.B.1. Method to prove possession of private key

The certificate application generated by the BNP Paribas technical RA is signed using the associated private key, the dual key being generated by the security module of the BNP Paribas technical RA.

The OCSP certificate application generated by an PKI operator is signed using the associated private key, the dual key being generated by the security module of the BNP Paribas CA.

III.B.2. Validation of the identity of the BNP Paribas customer body

Not applicable.

III.B.3. Approval of identity of an individual

a) As regards an ephemeral certificate

Registration of a holder (cf. Section I.C.2 for more detail) for the issue of a certificate is completed by BNP Paribas Fortis in its functional RA function.

The rules for verification of holder identity are left to the discretion of BNP Paribas Fortis in the context of its activity and in its role as functional RA.

The procedure for issue of a certificate is based on the specifications of the technical RA, which uses holder information based on data sent by BNP Paribas Fortis' application to the technical RA.

The procedure for verification of the holder's identity in the form "Given Name Surname" is solely the responsibility of BNP Paribas Fortis in the context of its banking activity.

The common name (CN) of the certificate may only be associated with a private individual and not with a service name, application or similar.

b) As regards an OCSP certificate

Only the certificate manager is authorised to request creation of an OCSP certificate.

III.B.4. Unverified holder information

a) As regards an ephemeral certificate

All certified information is verified.

b) As regards an OCSP certificate

Not applicable

III.B.5. Approval of applicant's authority

a) As regards an ephemeral certificate

Cf. Section III.B.4.

b) As regards an OCSP certificate

Confirmation of the applicant's validity is confirmed on signature of the OCSP certificate application form.

III.B.6. CA cross-certification

Not applicable

III.C. Identification and approval of a key renewal application

III.C.1. Identification and approval for an ordinary renewal

In accordance with the document [RFC 3647], the notion of "certificate renewal" corresponds to the issue of a new certificate for which only the validity dates are changed; all the other information is identical to the previous certificate (including the holder public key).

Renewal does not apply in the context of this CP.

III.C.2. Identification and approval for renewal after revocation

Not applicable

III.D. Identification and approval of a revocation application

a) As regards an ephemeral certificate

The application for revocation of the final certificate can only be initiated by the holder in the context of its online subscription operation. Acceptance of the revocation application is automatic. The holder applies for revocation by cancelling the signature request, particularly if the CN information contained in the lightweight certificate (Given Name - Surname) presented to it is incorrect.

The terms and conditions of this application are specified in Section IV.I.

b) As regards an OCSP certificate

Revocation of an OCSP certificate issued by the BNPPF Instant CA is realised either via a form by the certificate manager following a specific event, or by the PKI operator in the event of contractual breach.

c) As regards a certificate from the BNPPF Instant CA

Approval of a revocation application from a certification authority is an exceptional phenomenon.
The terms and conditions of this application are specified in Section IV.I.

IV. Operational requirements on the lifetime of certificates

IV.A. Certificate application

IV.A.1. Origin of a certificate application

a) As regards an ephemeral certificate

The certificate application can only be issued by a business application of BNP Paribas Fortis in its functional RA function. The business application of BNP Paribas Fortis and the technical RA are firmly authenticated for any holder certificate application.

b) As regards an OCSP certificate

An OCSP certificate may be requested only by the certificate manager in the context of the company's commercial activity.

IV.A.2. Processes and responsibilities for drawing up a certificate application

a) As regards an ephemeral certificate

The certificate application requires firm authentication of the technical units of the functional RA of BNP Paribas Fortis and the technical RA, using secure protocols which use authentication certificates.

- The functional RA verifies the status of these certificates before processing the application.
- The functional RA of BNP Paribas Fortis is responsible for verifying the integrity of the data that it sends to the technical RA.
- The process for drawing up a holder certificate is described in Section I.C.2.

b) As regards an OCSP certificate

At the time of the certificate application issued in the context of the OCSP certificate, the form provided by the certificate manager contains the elements necessary to constitute the DN of the certificate. The PKI Operator can then generate the dual keys and proof of possession of the key to be submitted for signature to the CA.

IV.B. Processing a certificate application

IV.B.1. Execution of the application identification and approval processes

a) As regards an ephemeral certificate

The procedure for identification and confirmation of the holder certificate application is as follows:

- The application is prepared automatically by BNP Paribas Fortis' functional RA in electronic form and sent to BNP Paribas' technical RA.
- Proof of possession of the key is generated and formatted by the technical RA, with the information to be certified, in the form of a certificate application.
- This proof is sent to the certification operator for signature of the certificate.

b) As regards an OCSP certificate

The certificate manager certifies the conformity of the application for creation of any OCSP certificate.

IV.B.2. Acceptance or rejection of the application

a) As regards an ephemeral certificate

The holder expresses acceptance of the certificate application by authorising their initial application with their bank card and their UCR (M2 for Easy Banking Web) or their EBB/Isabel card and their PIN (for Easy Banking Business). The document is presented to it by the core application of BNP Paribas Fortis and the holder gives its consent before signature.

b) As regards an OCSP certificate

Acceptance is given material form by confirmation of the certificate generated by the PKI operator. Rejection is given material form by an e-mail indicating the reason for refusal.

IV.B.3. Duration of preparation of certificate

a) As regards an ephemeral certificate

The certificate is prepared by the CA on receipt of the application by the technical RA and within 24 hours of receipt of the application.

b) As regards an OCSP certificate

The maximum processing period is 24 hours after receipt and approval of the application.

IV.C. Issue of the certificate

IV.C.1. Actions of the CA concerning issue of the certificate to the holder

a) As regards an ephemeral certificate

After authentication of the technical RA vis-à-vis the BNPPF Instant CA, the certification application sent by the technical RA is automatically signed by the BNPPF Instant CA, after verification of the conformity of its content, namely:

- Respect of the syntax of the attributes of the subject (DN), cf. Section III.A.5.
- The security attributes of the application (key size).

b) As regards an OCSP certificate

Following authentication of the origin and verification of the integrity of the application, the BNPPF Instant CA (as the technical department) triggers the certificate generation processes.

IV.C.2. Notification of certificate issuance to the holder

a) As regards an ephemeral certificate

This is an automatic operation at the time of an online contract process.

The certificate is sent to the holder via a signed document remitted at the end of a BNP Paribas Fortis business transaction.

b) As regards an OCSP certificate

The PKI's administrator informs the certificate manager of the correct progress of the operation.

IV.D. Certificate acceptance

IV.D.1. Certificate acceptance procedure

a) As regards an ephemeral certificate

The holder gives their consent by explicitly accepting the CN of the certificate generated in their name, cf. Section I.C.2. They agree to sign the data presented to them by BNP Paribas Fortis' functional RA.

b) As regards an OCSP certificate

ITG formally accepts the certificate by verifying its conformity vis-à-vis the application form.

IV.D.2. Publication of the certificate

The certificates are not published in the context of this CP. The BNPPF Instant CA keeps the certificates issued according to the technical specifications of its PKI.

IV.D.1. Notifying of certificate issuance

See the corresponding section of the CPS.

IV.E. Uses of the dual key of the certificate

IV.E.1. Use of the private key of the certificate by the holder

a) As regards an ephemeral certificate

Use of the private key of the holder and of the associate certificate is strictly limited to the signature service offered by BNP Paribas Fortis. By design, the BNP Paribas Fortis business application does not allow any other use of the private key.

The general terms and conditions of use of the certificate specify the parties' roles and responsibilities.

b) As regards an OCSP certificate

OCSP certificates are CA certificates, see Section I.D.3.

IV.E.2. Use of the private key and of the certificate by the user of the certificate

See Section I.C.2 for a description of the technical RA.

The private key of a lightweight electronic signature certificate is destroyed at the end of the user transaction.

IV.F. Renewal of a certificate

Not applicable in the context of this CP.

IV.G. Issue of a new certificate following a change to the dual key

a) As regards an ephemeral certificate

Issue of a new certificate for a given holder is the responsibility of the functional RA following the same procedure as for an initial certificate.

b) As regards an OCSP certificate

Issue of a new OCSP certificate follows the same procedure as for an initial certificate.

IV.H. Amendment of the certificate

Amendment of a certificate corresponds to the issue of a new certificate for the same public key, following changes to information other than dates of validity and serial number (otherwise, this is a certificate renewal).

Changing certificates is not authorised in this policy.

IV.I. Revocation and suspension of certificates

Suspension does not apply in the context of this CP.

The procedures relating to revocation of a CA are described in the BNPP PDF CA and BNPP LEVEL 2 CA offline CP of the CA, the OID are respectively 1.2.250.1.62.10.1.1.1.1 & 1.2.250.1.62.10.2.1.1.1. The information relating to revocation of final certificates will be given below.

IV.I.1. Possible causes of a revocation

a) As regards an ephemeral certificate

The following circumstances may be at the origin of the revocation of a holder's certificate:

- The holder's information featuring on their certificate does not match their identity
- The holder has abandoned their online application operation

b) As regards an OCSP certificate

Regarding OCSP certificates, the possible causes are as follows:

- Cessation of commercial activity associated with the certification authority
- Compromise, suspected compromise, theft or loss of means of reconstitution of private key
- Non-conformity noted during an audit.

IV.I.2. Origin of a revocation application

a) As regards an ephemeral certificate

Acceptance of the certificate is mandatory before any electronic signature. The holder's identity is presented to the holder from the CN resulting from their certificate. If this identity is incorrect, the holder must refuse this certificate using a "Cancel" functionality in the online application.

b) As regards an OCSP certificate

Only the certificate manager is authorised to submit a revocation application for an OCSP certificate.

IV.I.3. Procedure for processing a revocation application

a) As regards an ephemeral certificate

A holder's revocation application is processed automatically by the technical RA.

b) As regards an OCSP certificate

Revocation of an OCSP certificate is completed by the IDEMIA operating teams under the supervision of ITG.

IV.I.4. Deadline given to holder to submit the revocation application

a) As regards an ephemeral certificate

Due to its nature, a revocation application must be processed urgently. Revocation of the certificate is effective when the certificate serial number is included on the list of revocations of the BNPPF Instant CA, and when this list is access for downloading.

Formulation of the application must be processed during the session time of an online subscription of a BNP Paribas Fortis application.

b) As regards an OCSP certificate

Not applicable

IV.I.5. Deadline for processing a revocation application

a) As regards an ephemeral certificate

The period for processing the revocation shall not be more than six hours, in line with the life of the lightweight certificate.

b) As regards an OCSP certificate

Revocation applications must be processed on receipt by the corresponding certification authority. This revocation is processed within 24 hours of receipt of the application.

IV.I.6. Requirements for verification of the revocation by certificate users

The technical RA is required to verify that the certificate of the BNPPF Instant CA certification authority having issued the holder's certificate is valid.

No requirement on revoked holder certificates is specified.

IV.I.7. CRL drafting frequency

An CRL is generated regularly every 24 hours.

IV.I.8. Maximum deadline for publication of an CRL

An CRL must be published within 30 minutes at the most of its generation.

IV.I.9. Availability of an online system for verification of the revocation and the certificate status

The CA implements an online system for verification of the revocation and the certificate status in accordance with RFC 6960. This service is available 24 hours a day, 7 days a week.

IV.I.10. Requirements for online verification of the revocation of certificates by certificate users

Cf. IV.I.6.

IV.I.11. Other available information resources regarding revocations

Not applicable

IV.I.12. Specific requirements in the case of compromise of the private key

For CA or OCSP certificates, in the case of revocation following compromise of the private key, information will be clearly distributed.

In the case of revocation due to compromise or suspected compromise of a key, the CRL must be updated according to the policy set out in Section IV.J.2. In the case of revocation due to compromise of a key, authorised persons will be notified of the presumed date of the compromise.

The information consisting of ascertaining whether a certificate has revoked status or not must be available 24 hours, 7 days a week to the whole community who need to know this. It must be possible for the status of a certificate to be authenticated and fully protected.

IV.I.13. Possible causes of a suspension

Not applicable

IV.J. Function of information on status of certificates

IV.J.1. Operational characteristics

The function of information on the status of certificates makes several mechanisms available: either a free consultation mechanism for CRL, or an OCSP responder.

Several addresses are implemented by the BNPPF Instant CA in order to verify the status of a certificate:

- For holder certificates:
  - CRL
    - **http://bnpp.digitaltrust.morpho.com/crl/bnpp-fortis-customer-ephemeral1-ca.crl**
    - **http://bnpp.digitaltrust.morpho.com/crl/bnpp-fortis-customer-ephemeral2-ca.crl**
  - OCSP
    - **http://bnpp.digitaltrust.morpho.com/ocsp/bnpp-fortis-customer-ephemeral1-ca**
    - **http://bnpp.digitaltrust.morpho.com/ocsp/bnpp-fortis-customer-ephemeral2-ca**
- For certificates from the BNPPF Instant CA certification authority itself:
  - **http://bnpp.digitaltrust.morpho.com/crl/bnpp-level2-ca.crl**

By their nature, the two certificate status services do not have immediate synchronous information after a revocation. Indeed, the OCSP service responds in real time, whereas the update of a CRL is an asynchronous process. With consequently a delay between the two services.

Concerning the status of ephemeral certificates, the maximum difference between the two services takes into account the frequency of issuance of the CRL, in addition to the publication delay, i.e. 24 hours and 30 minutes

IV.J.2. Availability of function

A CRL must be published within 30 minutes at the most of its generation. The availability rate is, as a minimum, 99.7%, 24/7.

The response time of the certificate status verification server (OCSP) to the request received is less than 10 seconds.

IV.K. End of relationship with the holder

When the relationship between the holder and BNP Paribas Fortis ends, the holder no longer has access to the functional RA, and can therefore no longer apply for any certificates.

IV.L. Confiscation of key and recovery

Confiscation of the private keys of holders and OCSP responders is forbidden.

V. Non-technical security measures

The requirements defined hereinafter in this Section are the minimum requirements which the BNPPF Instant CA must respect.

The CPS describes the means implemented to respect these requirements in the context of hosting of the BNP Paribas PKI with IDEMIA and where applicable, in the context of the other activities associated with certification.

V.A. Physical security measures

V.A.1. Geographic situation and construction of sites

The hosting sites of the BNP Paribas PKI are described in the contract between IDEMIA and its service provider.

The sites containing information to be published are those of the IDEMIA host.

V.A.2. Physical access

Access is strictly limited to persons authorised to enter the premises and traceability of access must be ensured. Outside business hours, security is reinforced by use of physical and logical intrusion detection systems.

Access to hardware (servers, cryptographic boxes, CA's administration post, network's active elements) is restricted to those persons authorised to carry out operations requiring physical access to the hardware (biometric access control, associated rights).

V.A.3. Power and air conditioning

The characteristics of the power and air conditioning systems make it possible to respect the conditions of usage of the PKI's systems as fixed by their suppliers.

They also allow respect of the requirements of this CP and the CA's commitments in terms of availability of its functions, notably the revocation management and certificate status information functions.

V.A.4. Vulnerability to water damage

The systems for protection against water damage also allow respect of the requirements of this CP, and the commitments made by the CA, as authority, in terms of availability of its functions, notably the revocation management and certificate status information functions.

V.A.5. Fire prevention and protection

The systems for fire protection and firefighting allow respect of the requirements of this CP and the commitments made by the CA in terms of availability of its functions, notably the revocation management and certificate status information functions.

V.A.6. Conservation of media

The media (paper, hard disk, CD, etc.) corresponding to the information relating to the PKI's activity (operating, back-up functions, etc.) are treated and kept in a secure environment accessible only to authorised persons.

V.A.7. Decommissioning of media

Paper and magnetic media at the end of their life are systematically destroyed using appropriate means, making it possible to avoid any loss of confidentiality.

The PKI's storage media (server hard disk) are not reused for other purposes before full destruction of information associated with the PKI which they may contain.

V.A.8. Off-site back-ups

Back-ups are stored on the various production sites of the PKI's host: locally on the primary site and remotely via automatic synchronisation mechanisms.

V.B. Procedural security measures

V.B.1. Trusted roles

The following roles are distinguished:

- **The PKI's security officer**: they are responsible for application of the BNPPF Instant CA's certification policy.
- **Physical safety manager**: they are responsible for controls of physical access to the equipment of the CA unit's systems, excluding RA. This manager is appointed by the host partner of IDEMIA.
- **The PKI's technical operators:** they are responsible for the use, configuration and technical maintenance of the equipment, cryptographic boxes and servers. In particular, they develop the progress of the key ceremony on a technical level.
- **Auditor:** person appointed by a competent authority (complying for example with the "Instruction relating to procedure for authorisation of bodies qualifying trustworthy service providers") and whose role is to regularly carry out compliance checks on implementation of functions provided by the unit in relation to the certification policies, the PKI's certification practices declarations and the unit's security policies. The auditor is appointed by the BNP Paribas organisation or IDEMIA.

V.B.2. Number of persons required per task

Depending on the type of operation carried out, the number and capacity of people who necessarily have to be present, as actors or witnesses, may be different.

For security reasons, sensitive functions will be allocated to more than one person. This CP imposes a certain number of requirements concerning this allocation, notably for operations linked to the PKI's security modules; these are described in the CPS.

V.B.3. Identification and authentication for each role

ITG and host of the PKI check the identity and authorisations of all staff before allocating them a role and the corresponding rights. See CPS for more information.

V.B.4. Roles requiring a separation of powers

Several roles may be allocated to the same person, provided the holding of more than one role does not compromise the security of the functions implemented. For trusted roles, it is nevertheless recommended that the same person does not hold more than one role and, as a minimum, the requirements below of not holding more than one role must be respected.

The powers associated with each role must be described in the CA's CPS and comply with the security policy of the unit concerned.

V.C. Security measures vis-à-vis staff

V.C.1. Required qualifications, competences and skills

All staff required to work within PKI units are contractually subject to a security clause.

Each department operating a PKI unit must ensure that the remit of its staff who need to work within the unit match their professional competences.

The CA and the certification operator inform anyone holding trusted roles of the PKI of:

- their responsibilities relating to the PKI's services;

- procedures associated with security of the system and staff supervision.

Each person has, as a minimum, the appropriate documentation concerning the operational procedures and specific tools which they implement as well as the general policies and practices of the unit within which they work.

The appropriate documentation is described in Section V.C.8.

V.C.2. Procedures for verification of records

The PKI's staff are identified and must have no conviction conflicting with their duties.

V.C.3. Requirements in terms of initial training

Operating staff must be trained in the software, hardware and internal operating procedures of the unit for which they work.

V.C.4. Requirements and frequency of in-house training

The staff concerned must receive appropriate information and training prior to any changes to the systems, procedures, organisation, etc., according to the nature of these changes.

V.C.5. Frequency and sequence of rotation between various duties

In terms of career management for a given operator, the rules applicable are those practiced by the employer.

V.C.6. Sanctions in the case of unauthorised actions

The certification authority decides on penalties to be applied when an employee abuses their rights or carries out an operation which does not conform to their remit.

V.C.7. Requirements vis-à-vis the staff of external service providers

For contracted staff working for IDEMIA, they must respect the same conditions as those set out in Sections V.C.1 to V.C.4.

Concerning contracted staff working for BNP Paribas, they must comply with Human Resources and checks imposed by their company.

V.C.8. Documentation provided to staff

The documents which staff must have are as follows:

- Certification Practice Statement specific to the certification area;
- Manufacturers' documents for hardware and software used;
- Certification Policies supported by the unit to which they belong;
- Internal operating procedures.

The certification authority and the certification operator must ensure that their respective staff (as defined in the CPS) have the documents identified above, according to their requirements as set out by the CPS.

V.D. Procedures for constitution of audit data

Daily logging consists of recording events manually or electronically, by entry or automatic generation.

The resulting files, in hard copy or electronic format, must allow traceability and accountability for the operations carried out.

V.D.1. Types of event to be recorded

The PKI of the BNP Paribas Group, hosted with IDEMIA, on a daily basis logs the following events automatically on start-up of a system and in electronic format, concerning systems linked to the functions that it implements in the context of the PKI:

- Creation/modification/deletion of user accounts (access rights) and the corresponding authentication data (passwords, certificates, etc.)
- Start-up and stoppage of IT systems and applications
- Events linked to logging: start-up and stoppage of the daily logging function, modification of daily logging configuration, actions taken following failure of the daily logging function
- Connection/disconnection of users having trusted roles, and the corresponding unsuccessful attempts.

It must be possible for other events to be collected by the IDEMIA security officer, using electronic or manual means. This means those concerning security and which are not produced automatically by the computer systems, notably:

- Physical access
- Actions relating to maintenance and changes to system configuration
- Changes made to staff
- Actions of destruction and re-initialisation of media containing confidential information (keys, activation data, personal information about holders, etc.)

In addition to these daily logging requirements common to all units and all functions of the PKI, events specific to the various functions of the PKI must also be logged daily, notably:

- Receipt of a certificate application (initial and renewal)
- Approval/rejection of a certificate application
- Events linked to signature keys and to CA certificates (generation (key ceremony), back-up/recovery, revocation, renewal, destruction, etc.)
- Generation of holder certificates
- Publication and update of information linked to the CA (CP, CA certificates, general terms and conditions of use, etc.)
- Receipt of a revocation application
- Approval/rejection of a revocation application
- Generation and publication of CRL

Each recording of an event in a log must contain, as a minimum, the following fields:

- Type of event
- Name of operator or reference of system triggering the event
- Date and time of event
- Outcome of event (failure or success).

Accountability for an action lies with the person, body or system having executed it. The name or identifier of the operator must explicitly feature in one of the fields of the event log.

V.D.2. Frequency of processing of event logs

Analysis of the content of event logs must be regular, and at least once a quarter.

V.D.3. Archiving period for event logs

Event logs are kept for 7 years.

V.D.4. Protection of event logs

The BNP Paribas Group's PKI sets in place the required measures to ensure the integrity and availability of the events lots for the unit in question, in accordance with the requirements of this policy.

V.D.5. Procedure for backing up event logs

The BNP Paribas Group's PKI sets in place the required measures to ensure the integrity and availability of the events lots for the unit in question, in accordance with the requirements of this policy.

A back-up copy of event logs is made after each ceremony on the platforms of the BNP Paribas Group's PKI.

V.D.6. System for collection of event logs

The BNP Paribas Group's PKI relies on the internal collection systems of each of its units.

V.D.7. Notification of the logging of an event to the event manager

Not applicable

V.D.8. Assessment of vulnerabilities

The vulnerabilities evaluation process is identical to the risk analysis carried out by IDEMIA and BNP Paribas on its PKI-certified ETSI EN 319 411-1.

Additional intrusion tests are carried out periodically.

V.E. Archiving of data

V.E.1. Type of data to be archived

Archiving makes it possible to:

- Ensure the durability of logs constituted by the various units of the PKI.
- Keep paper documents associated with the certification operations, along with their availability if required.

The data to be archived concern both hard copies and electronic format.

The data to be archived is the following:

- The (executable) software and configuration files of IT equipment
- The CP
- The certificates and CRL as issued or published
- The audit data
- The event logs of the various entities of the PKI
- The paper documents associated with the PKI

V.E.2. Procedure for constitution of archives

For any matter regarding archives associated with customer certificates, reference should be made to the information relating to data stored in the proof file, which is found in the appendices to the CPS.

See the corresponding section of the CPS.

V.E.3. Archiving period for archives

The archiving period of the electronic archives is as follows:

- Archiving period for archives of event logs: 7 years
- Archiving period for archives of certificates, CRL after their expiry: 8 years
- Data linked to the identity of the private individual are kept, as a minimum, for the duration of the relationship with BNP Paribas Fortis, plus a period of 10 years.

V.E.4. Archive recovery period

Archives may be recovered within 5 working days.

V.E.5. Protection of archives

Throughout their archiving, archives and their back-ups are:

- Protected in full
- Accessible to authorised persons
- Accessible for reading and analysis.

The CPS specifies the methods used to archive documents in complete security.

V.E.6. Time-stamping requirements

See the corresponding section of the CPS.

V.E.7. Archive collection system

The archive collection system is the information system of IDEMIA and its host.

V.E.8. Procedures to recover and verify archives

Archives are managed by the BNP Paribas Group's PKI. The recovery process must form the subject of an internal functioning procedure mentioned in the CPS of online CAs. Recovery must be carried out within 5 business days at the most.

V.F. Authority key changeover

The BNPPF Instant CA cannot generate any certificate with an end date after the expiry date of the certificate corresponding to its own. For this, the period of validity of its certificate is longer than that of the certificates which it signs.

Also, when it allows a certification application, the BNPPF Instant CA fixes the life of the certification requested so that it is never valid beyond the end of validity date of the certificate of its dual key used for signature.

V.G. Resumption following compromise and incident

V.G.1. Procedures for feedback and handling of incidents and compromises

The operating teams of IDEMIA implement procedures and methods for feedback and handling of incidents, notably through awareness-raising and training of its staff.

Analysis of the various event logs is controlled by the IDEMIA security officer.

V.G.2. Procedures for resumption in the case of corruption of IT resources (hardware, software and/or data)

Backing up units of the PKI makes it possible to ensure resumption of activity in the case of an incident within 48 hours. This only applies when CRLs need to be generated urgently.

V.G.3. Procedures for resumption in the case of compromise of a unit's private key

In the case of compromise of an authority key, the corresponding certificate is immediately revoked (according to key ceremony completion deadlines).

V.G.4. Procedures for resumption in the case of compromise of a unit's algorithm

In the case of compromise of an algorithm used in an authority certificate, the corresponding certificate is

immediately revoked through completion of the key ceremony.

V.G.5. Capacities for continuation of business following an incident

The various units of the BNP Paribas Group's PKI have the resources necessary making it possible to ensure continuity of their business in compliance with the requirements of this policy.

As regards the online authority, continuity of business consists of restoring the PKI based on back-ups and secrets.

V.H. End of life of the BNP Paribas Group's PKI

One or more units of the PKI may need to cease their business or transfer it to another entity.

Transfer of business is defined as the end of business of a PKI unit not having any effect on the validity of the certificates issued prior to the transfer in question and resumption of this business organised by the CA in collaboration with the new entity.

Cessation of business is defined as the end of business of a PKI unit having an effect on the validity of the certificates issued prior to the cessation concerned.

In the case of cessation of business, BNP Paribas and IDEMIA undertake to implement the human resources making it possible to revoke all CA certificates of the PKI.

Finally, in cases where IDEMIA cannot ensure handling of the costs necessary for continuation of the CA's operations, for example, in the case of cessation of business, BNP Paribas undertakes to cover the necessary costs.

V.H.1. Transfer of business or cessation of business affecting a PKI unit

In order to ensure a constant level of trust during and after such events, the CA has the following obligations:

- to set in place procedures aimed at providing a continuous service, particularly in terms of archiving (notably archiving of holder certificates and information relating to certificates);
- to ensure continuity of the revocation (consideration of a revocation application and publication of CRLs), in accordance with the requirements of availability for its functions defined in this CP;
- to communicate beforehand its intention to transfer business on a given date;
- to implement all resources at its disposal to inform its partners (end users, other units, other PKI, etc.) of its intentions relating to end of business;
- the CA must specify in its CPS that it must notify how the transfer of obligations will happen (archives and logs to another entity) and how certificates which are still valid that need to be revoked will be processed.

V.H.2. Cessation of business affecting the CA

Cessation of activity may be full or partial (for example: cessation of business for a given category of certificates only). Partial cessation of activity must be gradual so that only the obligations referred to in the first three items above are to be executed by the CA, or a third-party entity which resumes the business, on expiry of the last certificate it has issued.

In the event of total cessation of activity, the CA or, if prevented, any entity which substitutes it pursuant to a law, a regulation, a legal decision or an agreement concluded previously with this entity, must ensure revocation of the certificates and publication of ARL in accordance with the commitments made in its CP.

VI. Technical security measures

The requirements defined hereinafter in this Section are the minimum requirements which the BNPPF Instant CA must respect.

The CPS describes the resources deployed in order to respect these requirements.

VI.A. Dual key generation and installation

VI.A.1. Dual key generation

a) Authority keys

Signature keys of the BNPPF Instant CA are generated in fully controlled circumstances, by staff in trusted roles, in the context of "key ceremonies". These ceremonies follow predefined scripts.

The signature keys of the BNPPF Instant CA are generated and implemented in a cryptographic box, the characteristics of which are described in the CPS.

The confidentiality of the keys is in particular ensured by technical measures detailed in the CPS.

b) Holder keys

A holder's dual key is generated by a hardware security module (HSM), the requirements of which are described in Section VI.B.1.

c) OCSP keys

The generation of the dual key of an OCSP certificate is ensured by a hardware security module (HSM), the requirements of which are described in Section VI.B.1.

VI.A.2. Transmission of the private key to its owner

a) Authority keys

See the corresponding section of the CPS.

b) Holder keys

The holder's private key remains under the individual's control via a signature software and can only be used by this software on signature of a document made available by BNP Paribas Fortis. It is destroyed immediately after its used.

c) OCSP keys

Private keys are generated on a security resource (HSM) so that keys never leave the resource and so remain protected in terms of confidentiality and integrity.

VI.A.3. Transmission of the public key to the CA

a) Holder keys

Holder public keys are submitted to the CA based on applications generated by the signature software in a format which makes it possible to prove possession of the key, by signing the application. The signature is verified by the CA. The CA issues a certificate if this verification is correct. Issue is thus protected in full end-to-end at the time of a certificate generation application.

b) OCSP keys

The public keys of OCSP certificates are submitted to the CA based on applications generated by a format which makes it possible to prove possession of the key, by signing the application. The signature is verified by the CA. The CA issues a certificate if this verification is correct.

Issue is thus protected in full end-to-end at the time of a certificate generation application.

VI.A.4. Transmission of the public key from the CA to the certificate users

The BNP Paribas Group's PKI makes available all the authority certificates via its publication service.

The CA may also submit its certificate on a removable device directly to participants of a key ceremony.

VI.A.5. Size of keys

The authorities use keys of 4,096 bits.

Holders use keys of a minimum of 2,048 bits.

The certificates of OCSP responders use keys of a minimum of 2,048 bits.

The CA follows the security recommendations of the ANSSI in the context of the RGS.

VI.A.6. Verification of dual key settings generated and their quality

The dual key generation equipment uses settings respecting the security standards specific to the algorithm corresponding to the dual key (cf. Section VII).

VI.A.7. Lifetime of keys

Cf. Section VI.C.2.

VI.A.8. Key use objectives

Use of a CA private key and of the associated certificate is strictly limited to the signature of certificates and CRLs.

For holder certificates, see I.D.1.

For OCSP certificates, see I.D.3.

VI.B. Security measures for the protection of private keys and for security modules

VI.B.1. Security standards and measures for security modules

a) Authority keys

See the corresponding section of the CPS.

b) Holder keys

The holder's private key is protected by a security box, the resistance level of which is a minimum of FIPS 140-2 level 2.

c) OCSP keys

The holder's private key is protected by a security box, the resistance level of which is a minimum of FIPS 140-2 level 3.

VI.B.2. Check of private key by more than one person

a) Authority keys

See the corresponding section of the CPS.

b) Holder keys

Holder private key is not checked by more than one person.

c) OCSP keys

The private keys of OCSP responders are not checked by more than one person.

VI.B.3. Confiscation of the private key

a) Authority keys

See the corresponding section of the CPS.

b) Holder keys

The private keys of holders are not confiscated.

c) OCSP keys

The private keys of OCSP responders are not confiscated.

VI.B.4. Back-up copy of the private key

a) Authority keys

See the corresponding section of the CPS.

b) Holder keys

Holder private keys do not form the subject of any back-up copy by the CA.

c) OCSP keys

The private keys of OCSP responders form the subject of back-up copies, using the specifications of the security box.

VI.B.5. Archiving of the private key

a) Authority keys

See the corresponding section of the CPS.

b) Holder keys

Holder private keys are not archived in any event.

c) Holder keys

OCSP responder private keys are not archived in any event.

VI.B.6. Transfer of private key to/from security module

Cf. Section VI.B.4.

VI.B.7. Storage of private key in a security module

a) Authority keys

See the corresponding section of the CPS.

b) Holder keys

Holder private keys are stored in a security module responding as a minimum to the requirements in Section XI below.

c) OCSP keys

OCSP keys are stored in a security module responding as a minimum to the requirements in Section XI below.

VI.B.8. Method of activating private keys

a) Authority keys

See the corresponding section of the CPS.

b) Holder keys

Keys are activated once generated.

c) OCSP keys

Keys are activated once generated.

VI.B.9. Method of deactivating private keys

a) Authority keys

See the corresponding section of the CPS.

b) Holder keys

Not applicable.

c) OCSP keys

Not applicable.

VI.B.10. Method of destroying private keys

a) Authority keys

See the corresponding section of the CPS.

b) Holder keys

Destruction of keys is triggered after the signature operation.

c) OCSP keys

Keys are destroyed when the certificate associated with the dual keys has expired.

VI.B.11. Level of security evaluation of the security module

a) Authority keys

The security modules of a CA of the BNP Paribas Group's PKI are evaluated at the level corresponding to the targeted use, as specified in Section XI below.

b) Holder keys

See previous paragraph.

c) OCSP keys

See previous paragraph.

VI.C. Other aspects of dual key management

VI.C.1. Public key archival

a) Authority keys

The public keys of CAs of the BNP Paribas Group's PKI are archived in the context of the archiving of the corresponding certificates.

b) Holder keys

They are not archived.

a) OCSP keys

They are not archived.

VI.C.2. Lifetime of dual keys and certificates

As regards a CA certificate:

- The lifetime of the keys is 23 years.

As regards a lightweight certificate:

- The settings of the lifetime can be set and the lifetime is 1 hour at the most.
- The lifetime of dual keys is limited to its association with a certificate.

As regards an OCSP certificate:

- The lifetime of the keys is 1 year.

The validity of a CA certificate ends after the certificates that it issues are no longer valid.

VI.D. Activation data

VI.D.1. Activation data generation and installation of the HSM

a) As regards authority keys

The generation and installation of the activation data of the PKI's security module occur during the security box initialisation and personalisation phase. The activation data are chosen and entered by the persons responsible for these data themselves.

b) As regards holder keys

The generation and installation of the activation data of the PKI's security module occur during the security box initialisation and personalisation phase. The activation data are chosen and entered by the persons responsible for these data themselves.

They are only known to members of ITP-ITG in the context of the roles allocated to them.

c) As regards OCSP keys

The generation and installation of the activation data of the PKI's security module occur during the security box initialisation and personalisation phase. The activation data are chosen and entered by the persons responsible for these data themselves.

They are only known to members of IDEMIA in the context of the roles allocated to them.

VI.D.2. Protection of activation data of the HSM

The activation data generated for the BNP Paribas Group's PKI security modules are protected in terms of integrity and confidentiality until remittance to their recipient.

VI.D.3. Protection of activation data corresponding to holder private keys

See the corresponding section of the CPS.

VI.D.4. Other aspects relating to activation data

See the corresponding section of the CPS.

VI.E. Security measures for IT systems

VI.E.1. Technical security requirements specific to IT systems

See the corresponding section of the CPS.

VI.E.2. Level of qualification of IT systems

The security module used by the BNP Paribas Group's PKI forms the subject of common criterion certification EAL4+.

VI.F. Security measures associated with system development

The development environments are separate from the production environment.

VI.F.1. Measures associated with security management

Any significant development in a system of a unit of the BNP Paribas Group's PKI must be documented and must feature in the internal functioning procedures of the unit concerned and conform to the compliance assurance maintenance schedule, in the case of evaluated products.

VI.F.2. Level of security evaluation of system lifetime

This policy does not contain any specific requirement on the subject.

VI.G. Network security measures

Interconnections and access to the PKI's resources are controlled by hardware and software allowing segmentation of data, services and users by role and function. These solutions ensure control of incoming and outgoing flows. Changes to open ports, access rights and modifications must be systematically traced in a space for tracking changes to logic access.

VI.H. Time-stamping/dating system

To date these events, the various units of the PKI use the PKI system time, ensuring synchronisation of the PKI system clocks, to the nearest minute as a minimum, and in relation to a reliable UTC time source, to the nearest second as a minimum.

VII. Profiles of certificates, OCSPs and CRLs

VII.A. Profile of certificates

VII.A.1. Version number

Certificates issued in the context of the BNP Paribas Group's PKI comply with the standard X.509 v3.

VII.A.2. Basic fields

Certificates follow the basic format of certificates defined in recommendation x.509v3 and include, as a minimum, the following basic fields:

Field name	Description	Content
Version	Version of certificate X.509	Contains the value 2 to indicate that the certificate is an x.509v3 certificate
SerialNumber	Certificate serial number	Contains a whole value to indicate the certificate serial number; this value must be unique for each certificate issued by the root authority.
Signature	Signature of authority to authenticate it	Sha2WithRSAEncryption
Issuer	Name of authority	Contains the authority's DN (X.500). The issuer is one of the following values: - CN=BNP Paribas Fortis Customer Ephemeral Certification Authority 1, OU=VATBE-0403199702, O=BNP Paribas Fortis, C=BE - CN=BNP Paribas Fortis Customer Ephemeral Certification Authority 2, OU=VATBE-0403199702, O=BNP Paribas Fortis, C=BE
Validity	Certificate validity period	Contains dates/times of activation and expiry of certificate.
Subject	Name of holder	Contains the holder DN (see paragraph III.A.5)
Subject Public Key Info	Subject Public Key Info	Contains the OID of the algorithm and the subject public key
Extensions	List of extensions	See next section

VII.A.3. Extensions of certificate

The certificates issued by the BNPPF Instant CA comprise the following X.509v3 extensions. The CPS specifies the values used.

a) As regards holder certificates

Extension	Critical extension	Description
Authority Key Identifier	N	Identification element of public key of authority signing the certificate
Basic Constraint	Y	Indicates that the certificate is an end entity.
Certificate Policies	N	OID of the CP governing the certificate and Title of CP. The OID possible are as follows: - 1.2.250.1.62.10.7.1.1.2 - 1.2.250.1.62.10.8.1.1.2
Subject Key Identifier	N	Identification element of holder public key
KeyUsage	Y	Description of authorised users of the private key: Non-repudiation
CRL Distribution Point	N	Contains the CRL's URL (see paragraph IV.J.1).
Authority Information Access	N	Information for access to authority certificate.

b) As regards OCSP certificates

Extension	Critical extension	Description
Authority Key Identifier	N	Identification element of public key of authority signing the certificate
Basic Constraint	Y	Indicates that the certificate is an end entity.
Key Usage	Y	Description of authorised users of the private key: digitalSignature
Extended Key Usage	N	Indicates that the certificate signs the OCSP responses (ocspSigning)
Certificate Policies	N	OID of the CP governing the certificate and Title of CP. The OID possible are as follows: - 1.2.250.1.62.10.7.1.2.1 - 1.2.250.1.62.10.8.1.2.1
OCSP no Check	N	Indicates to the OCSP customer to trust the OCSP responder for the lifetime of the certificate.

Extension	Critical extension	Description
Subject Key Identifier	N	Identification element of holder public key

VII.A.4. OID of algorithms

The algorithm identifiers must be registered with a depositary (e.g., an international depository such as the ISO's).

The condensate algorithm used in the context of the BNP Paribas Group's PKI is SHA-2 (OID 2.16.840.1.101.3.4.2.1). The encryption algorithm used in the context of the BNP Paribas Group's PKI is RSA.

Signature is completed in RSA-SHA256, the OID of which is 1.2.840.113549.1.1.11.

VII.A.5. Form of names

In the context of the BNP Paribas Group's PKI, the names allocated to holders and to OCSP certificates comply with standard X.500, as set out in Section III.A of this document.

VII.A.6. OID of certification policies

a) Authority certificates

The actors present at the key ceremony ensure that the certificates issued contain the "Any Policy" OID (2.5.29.32.0).

b) Holder certificates

Holder certificates reference the OID of this certification policy.

c) OCSP certificates

OCSP certificates reference the OID of this certification policy.

VII.A.7. Usage of Policy Constraints extension

This policy does not contain any specific requirement on the subject.

VII.A.8. Policy qualifier syntax and semantics

This policy does not contain any specific requirement on the subject.

VII.A.9. Processing semantics for the critical extensions of the certification policy

This policy does not contain any specific requirement on the subject.

VII.B. CRL profile

VII.B.1. Version number

The CRL issued used version 2 of the format defined in standard ISO [9594-8].

VII.B.2. Basic fields

The basic fields of the CRL issued by the root authority are as follows:

Field	Description
Version	CRL version X.509
Signature	Identifier of the algorithm used to produce the list integrity stamp Sha2WithRSAEncryption applied for this CP.
Issuer	Name of authority of the BNP Paribas Group's PKI. The issuer is one of the following values: - CN=BNP Paribas Fortis Customer Ephemeral Certification Authority 1, OU=VATBE-0403199702, O=BNP Paribas Fortis, C=BE - CN=BNP Paribas Fortis Customer Ephemeral Certification Authority 2, OU=VATBE-0403199702, O=BNP Paribas Fortis, C=BE
This Update	CRL issue date
Next Update	Deadline for issue of this CRL
Revoked Certificates	Revocation registration list. For each revocation, the values associated with the following fields will be specified: - User Certificate (serial number of revoked certificate) - Revocation Date (certificate revocation date).
CRL Extensions	General extensions of CRL

The CRL in its final form is all of the following elements:

Field	Description
tbsCertlist	All the fields described above
signatureAlgorithm	The identifier of the algorithm used to produce the list integrity stamp Sha2WithRSAEncryption applied for this CP.
signatureValue	The result of this algorithm on all fields on tbsCertList

VII.C. CRL extensions and CRL input

The CRL include the basis fields set out in the previous paragraph, along with the following input extensions:

Input extension	Description

Authority Key Identifier	Identifies the public key of the authority having signed the CRL
CRL Number	Gives a sequential growing number for each CRL issued
MS "CA Version"	Microsoft AD CS extension linked to the version of CA keys
MS "CRL Next Publish"	Microsoft AD CS extension linked to the date of next publication
Reason Key	Identifies the reason for revocation of certificate.

VIII. Compliance audit and other assessments

VIII.A. Frequencies and/or circumstances of assessments

A compliance check, in relation to the reference system of ETSI EN 319 411-1 LCP, of the BNP Paribas Group's PKI is carried out every two years. An internal audit will be carried out by BNP Paribas every year.

VIII.B. Identities/qualifications of assessors

Audit of a unit must be assigned by the IDEMIA or BNP Paribas management to a team competent in information system security and in the field of activity of the unit being audited.

Similarly, those carrying out internal audits must satisfy the conditions stipulated in the previous paragraph.

VIII.C. Relations between assessors and assessed entities

The organisation of internal audits is written in the associated CPS.

VIII.D. Subjects covered by the assessments

The compliance checks or internal checks carried out by BNP Paribas concern the whole of the BNP Paribas Group PKI and are aimed at verifying compliance with the commitments and practices defined in this certification policy and in the CPS responding to it, and the ensuing elements (operational procedures, resources implemented, etc.).

VIII.E. Actions taken following conclusions of evaluations

After a compliance control or an internal audit, the assessor provides ITG with a compliance report, accompanied by recommendations.

ITG, by delegation to the actors identified in this policy, is responsible for settling areas of non-compliance as well as for choosing the measure to be applied.

VIII.F. Communication of the results

The results of compliance audits are confidential and can only be communicated to third parties in the case of an explicit request.

Moreover, the results of the compliance audits and audits carried out internally will be communicated to the PMA.

IX. Appendix 1 – Other business and legal issues

IX.A. Tariffs

The pricing applied by BNP Paribas Fortis to the user of the certificate is specified in the general terms and conditions applicable to the BNP Paribas Fortis channel in which the certificate is used.

IX.B. Financial responsibility

The financial responsibility of BNP Paribas Fortis vis-à-vis the user of the certificate is specified in the general terms and conditions applicable to the BNP Paribas Fortis channel in which the certificate is used.

IX.C. Business data privacy

IX.C.1. Scope of confidential information

The types of information considered as confidential are, at least, the following:

- The CPS corresponding to this CP
- The private keys of units and holders of certificates of the BNP Paribas Group's PKI
- The activation data associated with the private keys of the authorities of the BNP Paribas Group's PKI
- All the secrets of the BNP Paribas Group's PKI
- The event logs of the units of the BNP Paribas Group's PKI
- The holder registration file
- The minutes of key ceremonies.

IX.C.2. Information outside the scope of confidential information

Not applicable

IX.C.3. Responsibilities in terms of protection of confidential information

BNP Paribas Fortis, as certification authority, is required to comply with the legislation and regulations in force on Belgian territory.

IX.D. Personal data protection

BNP Paribas Fortis applies the applicable legislation and regulations on personal data privacy, both in terms of collection as well as use of personal data (Belgian Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of private individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) from 25 May 2018.

IX.D.1. Personal data protection policy

It is understood that any collection and any use of personal data by all its units of the BNP Paribas Group's PKI are carried out in strict compliance with the legislation and regulations in force.

IX.D.2. Personal data

Data considered as personal are, at least, the following:

- all data concerning the holder registration file

IX.D.3. Non-personal data

No specific requirement is imposed in this matter.

IX.D.4. Responsibility in terms of personal data protection

For the personal data of certificate users, BNP Paribas Fortis is the controller.

IX.D.5. Notification and consent for use of personal data

The processing of the personal details of certificate users forms the subject of provision of information, notifications and collection of consent, specified in the general terms and conditions applicable to the BNP Paribas Fortis channel in which the certificate is used.

IX.D.6. Conditions of disclosure of personal information to judicial or administrative authorities

See legislation and regulations in force on Belgian territory.

IX.D.7. Other circumstances of disclosure of personal data

See legislation and regulations in force on Belgian territory.

IX.E. Intellectual and industrial property rights

Application of the legislation and regulations in force on Belgian territory.

IX.F. Contractual interpretations and guarantees

The common obligations of the units of the PKI are as follows:

- to protect and guarantee the integrity and confidentiality of their secret and/or private keys;
- to use their security keys (public, private and/or secret) solely for those purposes provided for at the time of their issue and with the tools specified in the conditions fixed by the CA's CP and the ensuing documents;
- to respect and apply the part of the CPS incumbent upon them;
- to submit to the compliance checks carried out by the audit team commissioned by the CA (see Section VIII);
- to respect the agreements or contracts between them or holders;
- to implement the resources (technical and human) necessary to provide the services to which they are committed in conditions guaranteeing quality and security.

IX.F.1. Certification Authority

The CA has the obligation to:

- be able to show users of its certificates that it has issued a certificate for a given holder and that this holder has accepted the certificate, in accordance with the requirements of Section IV.4 above;
- guarantee and maintain the consistency of its CPS with its CP;
- take all reasonable measures to ensure that its holders are aware of their rights and obligations as regards the use and management of keys, certificates or the hardware and software used for the purposes of the PKI. The relationship between a holder and the CA is formalised by a contractual link specifying the parties' rights and obligations and notably, the guarantees furnished by the CA.

IX.F.2. Registration service

See paragraph IX.F.1.

IX.F.3. Certificate holders

The holder is obliged to check and communicate accurate and up-to-date information during the identification process (identity of the private individual for example).

IX.F.4. Certificate users

The certificate user may only use the certificate in the BNP Paribas Fortis channel in which its creation is proposed, and in the context only of relations between the user of the certificate and BNP Paribas Fortis.

IX.F.5. Other participants

No specific requirement is imposed in the context of this CP.

IX.G. Guarantee limit

The responsibility of BNP Paribas Fortis vis-à-vis the user of the certificate is specified in the general terms and conditions applicable to the BNP Paribas Fortis channel in which the certificate is used.

IX.H. Limit of responsibility

The responsibility of BNP Paribas Fortis vis-à-vis the user of the certificate is specified in the general terms and conditions applicable to the BNP Paribas Fortis channel in which the certificate is used.

IX.I. Indemnities

The financial responsibility of BNP Paribas Fortis vis-à-vis the user of the certificate is specified in the general terms and conditions applicable to the BNP Paribas Fortis channel in which the certificate is used.

IX.J. Duration and early end of period of validity of the CP

IX.J.1. Period of validity

The CA's CP must remain applicable at least until the end of life of the last certificate issued in respect of this CP.

IX.J.2. Effects of the end of validity and remaining clauses applicable

No specific requirement is imposed in the context of this CP.

IX.K. Individual notifications and communications between participants

No specific requirement is imposed in the context of this CP.

IX.L. Amendments to the CP

IX.L.1. Amendment procedures

Major amendments made to this CP must be presented during a Policy Management Authority (PMA) meeting for approval of the changes made and this, prior to publication of the new version of the CP.

In the case of minor amendments (misprints, typos, etc.), these amendments do not require formal approval by the PMA to trigger publication of the new version of the CP.

IX.L.2. Mechanism and period of provision of information about amendments

No mechanism is provided for to give information about amendments made.

IX.L.3. Circumstances according to which the OID must be changed

Changing the CP OID is triggered once the amendments made by the CP are major and confirmed by the PMA.

In this case, the last digit of the OID will be modified to reflect major amendments.

IX.M. Provisions on dispute resolution

In the event of any dispute, the holder must contact the points of contact provided in Section I.E.2.

IX.N. Courts with jurisdiction

Application of the legislation and regulations in force on Belgian territory.

IX.O. Compliance with legislation and regulations

Application of the legislation and regulations in force on Belgian territory.

IX.P. Miscellaneous

No specific requirement is imposed in the context of this CP.

IX.Q. Other provisions

No specific requirement is imposed in the context of this CP.

X. Appendix 2 – Documents cited as reference

X.A. Regulation

Not applicable.

X.B. Technical documents

Reference	Purpose of document
FIPS140-2_LEVEL3_CERT	Certificate of qualification FIPS 140-2 level 3 of the nShield security box (firmware 2.50.16).

All the procedures detailed relating to this CP are described in the appendices to the CPS which can be viewed on request by authorised persons (see Section I.E.2).

XI. Appendix 3 – Security requirements for the CA's security module

XI.A. Requirements concerning security objectives

The security module, used by the BNP Paribas Group's PKI to generate and implement its signature keys (for the generation of electronic certificates, CRL), and to generate holder dual keys, must comply with the following security requirements:

- Ensure the confidentiality and integrity of the signature private keys of the CA during their lifetime, and ensure their definite destruction at end of that life;
- Be capable of identifying and authenticating its users;
- Limit access to its services depending on the user and the role which it has been allocated;
- Be capable of carrying out a series of tests to check that it is functioning correctly and enter certain status if it detects an error;
- Make it possible to create a secure electronic signature, to sign the certificates generated by the CA, which does not reveal the private keys of the CA and which cannot be falsified without the knowledge of these private keys;
- Create audit registrations for each modification concerning security;
- Guarantee the confidentiality and integrity of saved data and request, as a minimum, a dual check of back-up and restoration operations.

XI.B. Requirement concerning qualification

The security module used by the BNP Paribas Group's PKI is not qualified according to the process described in the General Security Reference System of the French administration.