
# PKI@BNPPF Certificate Policy

## version 1.0

## Date de publication : 27 août 2012

## Date d'effet : 29 août 2012

# Table des matières

# 1. Introduction

La fiabilité d'un certificat numérique dépend des règles observées pour sa délivrance et sa gestion. Ces règles sont formalisées dans des politiques, à savoir la Certificate Policy (CP) et le Certification Practice Statement (CPS).

Une CP est définie, selon la norme ITU-T X.509, comme « un ensemble déterminé de règles indiquant l'applicabilité d'un certificat à une communauté donnée et/ou une classe d'applications présentant des exigences de sécurité communes ».

Le terme « CPS » est défini par les directives de l'American Bar Association comme suit : « liste des pratiques employées par une autorité de certification (CA) pour délivrer des certificats ».

Si la CP ne fait principalement qu'« *énoncer* » les obligations élémentaires incombant au CA et aux autres parties impliquées dans la PKI, le CPS, lui, se penche plus en détail sur la « *manière* » dont ces obligations sont remplies par le CA Isabel et les autres parties impliquées dans la PKI.

## 1.1. APERÇU

Le présent « PKI@BNPPF Certificate Policy » établit l'applicabilité des « PKI@BNPPF Certificates » ainsi que l'ensemble des règles qui leur sont applicables. Il définit les exigences relatives à la délivrance, à la gestion et à l'utilisation des certificats à clé publique désignés par PKI@BNPPF Certificate et de la technologie cryptographique associée utilisée pour les services d'authentification, de confidentialité, de protection de l'intégrité des données et de non-répudiation.

Un PKI@BNPPF Certificate est un certificat délivré par une CA pour les besoins spécifiques de BNP Paribas Fortis.

La présente CP :

- décrit les entités appartenant ou utilisant les services de l'infrastructure PKI d'Isabel dans le cadre des activités relatives aux demandes, délivrances, acceptations, utilisations et révocations de PKI@BNPPF Certificate ;
- décrit l'applicabilité des PKI@BNPPF Certificate aux tierces parties ;
- décrit les obligations et les responsabilités des entités participant aux activités de demande, d'acceptation, d'utilisation et de révocation de PKI@BNPPF Certificate ;
- décrit le profil d'un PKI@BNPPF Certificate ;
- fournit un glossaire de termes et une liste de documents de référence ;

Comme indiqué aux sections 1.3.6 et 2.1.4, les Sujets ou Parties Utilisatrices d'unPKI@BNPPF Certificate doivent s'assurer, en examinant le présent document ainsi que toute autre information qu'ils jugent utile, que le PKI@BNPPF Certificate délivré ou tout autre service fourni par le CA Isabel au titre de la présente Politique convient aux fins prévues.

En faisant usage des informations incluses dans un PKI@BNPPF Certificate délivré par un CA Isabel, les Parties Utilisatrices signifient leur acceptation des clauses et conditions de la présente politique.

## 1.2. IDENTIFICATION

### 1.2.1. NOM

La présente CP s'intitule « PKI@BNPPF Certificate Policy ».

### 1.2.2. OBJECT IDENTIFIER

L'Object Identifier associé à la « PKI@BNPPF Certificate Policy » est 2.16.56.1.9.48.1.1.

### 1.2.3. UNIFORM RESOURCE IDENTIFIER

La PKI@BNPPF Certificate Policy sera publiée sur le site web Easy Banking Business de BNP Paribas Fortis.

### 1.2.4. HISTORIQUE DES VERSIONS DU DOCUMENT

Le présent document a subi les révisions suivantes :

| Date | Modifications | Version |
|---|---|---|
| 27 août 2012 | Version intiale | 1.0 |

## 1.3. COMMUNAUTÉ ET APPLICABILITÉ

### 1.3.1. CERTIFICATION AUTHORITIES

Selon la norme ITU-T X.509, le CA est une « autorité habilitée par un ou plusieurs utilisateurs à créer et assigner des certificats. Le CA peut aussi éventuellement créer la clé des utilisateurs ».

Dans la Public Key Infrastructure, les Certification Authorities d'Isabel peuvent accepter les demandes de PKI@BNPPF Certificate relatives à des Sujets dont l'identité a été authentifiée par une PKI@BNPPF Registration Authority (RA).

Lorsqu'une demande de certificat soumise par PKI@BNPPF RA au CA Isabel a été contrôlée par ce dernier, un PKI@BNPPF Certificate, associant l'identité du Sujet à sa Clé publique, est délivré.

### 1.3.2. REGISTRATION AUTHORITIES

Aux termes de la norme RFC 3647 [4], le RA est « l'entité responsable d'une ou plusieurs des fonctions suivantes : l'identification et l'authentification des demandeurs de certificat, l'approbation ou le rejet d'une demande de certificat, le lancement d'une procédure de révocation ou de suspension de certificat dans certaines circonstances, le traitement de demandes d'abonnés visant à faire révoquer ou suspendre leur certificat et l'approbation ou le rejet de demandes introduites par des abonnés en vue de faire renouveler leur certificat ou d'obtenir une nouvelle clé ».

Dans l'infrastructure PKI d'Isabel, les PKI@BNPPF RA agissant sous le contrôle et l'autorité d'un CA Isabel acceptent les demandes de PKI@BNPPF Certificate pour un PKI@BNPPF Certificate soumises par des souscripteurs à un PKI@BNPPF Certificate

Les PKI@BNPPF RA RA doivent authentifier l'identité du Sujet au PKI@BNPPF Certificate et vérifier les informations figurant dans la demande de PKI@BNPPF Certificate . Si les informations vérifiées sont exactes, PKI@BNPPF RA envoie une demande de PKI@BNPPF Certificate au CA compétent afin qu'il délivre un PKI@BNPPF Certificate au PKI@BNPPF Certificate Sujet.

Seules les Registration Authorities autorisées par BNP Paribas Fortis ont le droit de soumettre des demandes de certificats à un CA Isabel en vue de la délivrance d'un PKI@BNPPF Certificate. BNP Paribas Fortis publiera sur son site web Easy Banking Business une liste des Registration Authorities autorisées.

### 1.3.3. ENTITÉS FINALES

Dans le cadre de la présente PKI@BNPPF Certificate Policy, les entités finales de l'infrastructure PKI se composent :

1. PKI@BNPPF Certificate du souscripteur ;
2. PKI@BNPPF Certificate du Sujet ;
3. PKI@BNPPF Certificate de la Partie Utilisatrice ;

Les Clients de BNP Paribas Fortis désignent des PKI@BNPPF Certificate Souscripteurs ainsi que des PKI@BNPPF Certificate Sujets.

Le terme « Sujet » est utilisé dans le PKI@BNPPF Certificate pour nommer ou à tout le moins identifier le PKI@BNPPF Certificate Sujet soit par :

1. son nom et son prénom, pour un Sujet personne physique ;
2. un nom de fonction, pour un Sujet fonction ;

Dans le cadre de la présente PKI@BNPPF CP :

1. Un PKI@BNPPF Certificate Sujet ne peut être un CA ou un RA de l'infrastructure PKI d'Isabel ;
2. la signature d'un Sujet fonction est une signature technique, c'est-à-dire qu'elle ne peut être utilisée qu'à des fins de contrôle de l'intégrité, et non pas pour des autorisations de transactions, sauf disposition contraire du contrat conclu entre le Client deBNP Paribas Fortis et BNP Paribas Fortis.

### 1.3.4. VALIDATION AUTHORITIES

Dans l'infrastructure PKI d'Isabel, l'Isabel Validation Authority permet à toute Partie Utilisatrice d'obtenir des informations sur le statut de la révocation de son PKI@BNPPF Certificate.

Les intervenants du On-Line Certificate Status Protocol (OCSP) fournissent le statut de révocation des PKI@BNPPF Certificate.

Un soutien sera assuré à l'avenir, via le site Internet, pour la vérification du statut de révocation des différents certificats.

### 1.3.5. POLICY AUTHORITIES

La Policy Authority est l'entité chargée de :

1. spécifier, valider et publier le PKI@BNPPF CP et ses révisions ;
2. vérifier l'adéquation et l'application correcte du PKI@BNPPF CP ;
3. définir les exigences en matière de contrôle et les processus afférents à l'application de la CP ;

La Policy Authority compétente pour la présente PKI@BNPPF CP est : BNP Paribas Fortis, voir 1.3.7 Coordonnées.

### 1.3.6. CHAMP D'APPLICATION

Les PKI@BNPPF Certificate délivrés conformément à la présente CP peuvent uniquement être utilisés par les Parties Utilisatrices faisant partie d'un Client de BNP Paribas Fortis ET aux fins suivantes : vérification de la signature numérique, non-répudiation, chiffrage de clés et chiffrage de données.

Les Parties Utilisatrices doivent avoir noué une relation contractuelle avec BNP Paribas Fortis.

Si un Sujet du PKI@BNPPF Certificate souhaite faire appliquer l'une ou l'autre limitation (financière ou non) aux transactions authentifiées par le PKI@BNPPF Certificate, il doit avoir conclu avec chaque Partie Utilisatrice un accord signé fixant ces limitations.

## 1.3.7. COORDONNÉES

### 1.3.7.1. ORGANISATION DE L'ADMINISTRATION DE SPÉCIFICATION

Le Security Manager de BNP Paribas Fortis assume le rôle de Policy Authority aux fins du présent PKI@BNPPF CP. Il est chargé de l'ensemble des aspects du présent PKI@BNPPF CP, notamment sa spécification, sa validation, son enregistrement, sa publication, sa maintenance et son interprétation.

### 1.3.7.2. PERSONNE DE CONTACT DE LA POLICY AUTHORITY

Toutes les questions et tous les commentaires relatifs au présent PKI@BNPPF CP doivent être adressés au représentant de sa Policy Authority :

Business Information & Security Officer

FORTIS BANK NV/SA

Warandeberg/Montagne de Parc 3

B-1000 Bruxelles

Belgique

mailto : rpb.information.security.incident.management@bnpparibasfortis.com

# 2. Provisions Générales

## 2.1. OBLIGATIONS

La présente section décrit les obligations des entités participant, au sein de l'infrastructure PKI, à la demande, la délivrance, l'acceptation, l'utilisation, la publication et la révocation de PKI@BNPPF Certificates.

PKI@BNPPF CertificateAvant de faire valoir un PKI@BNPPF Certificate, les Parties Utilisatrices sont tenues d'avoir compris les dispositions de la présente section.

Ces entités sont :

1. CA Isabel
2. PKI@BNPPF RA
3. PKI@BNPPF Certificate Souscripteurs et Sujets
4. PKI@BNPPF Certificate Parties Utilisatrices
5. BNP Paribas Fortis Registre
6. Policy Authority

Entité juridique BNP Paribas Fortis

Pour demander au CA Isabel un PKI@BNPPF Certificate pour un Souscripteur de PKI@BNPPF Certificate, la PKI@BNPPF RA doit accepter les obligations énoncées ci-après.

Pour délivrer un PKI@BNPPF Certificate, le CA Isabel doit accepter les obligations énoncées ci-après.

En acceptant un PKI@BNPPF Certificate qui lui a été délivré, le PKI@BNPPF Certificate Sujet accepte également les obligations et mentions décrites ci-après.

En faisant usage d'un PKI@BNPPF Certificate, la PKI@BNPPF Certificate Partie Utilisatrice signifie qu'elle accepte ses obligations ainsi que les mentions décrites ci-après.

### 2.1.1. OBLIGATIONS DES CERTIFICATION AUTHORITIES D'ISABEL

Le CA Isabel délivrant les PKI@BNPPF Certificates dans l'infrastructure PKI doit respecter les obligations suivantes :

#### 2.1.1.1. NOTIFICATION DE LA DÉLIVRANCE DES CERTIFICATS

Le CA Isabel veille à ce que le PKI@BNPPF Certificate Sujet soit notifié de la délivrance de son PKI@BNPPF Certificate.

#### 2.1.1.2. PUBLICATION DU PKI@BNPPF CERTIFICATE DANS UN REGISTRE D'ISABEL

Le CA Isabel publie le PKI@BNPPF Certificate qu'il a délivré une fois celui-ci accepté par le Sujet du PKI@BNPPF Certificate .

#### 2.1.1.3. EXACTITUDE DES REPRÉSENTATIONS

En publiant un PKI@BNPPF Certificate faisant référence à la présente CP, le CA Isabel garantit à toute personne s'appuyant raisonnablement sur les informations contenues dans le PKI@BNPPF Certificate, qu'il a délivré le PKI@BNPPF Certificate au Sujet du PKI@BNPPF Certificate conformément aux dispositions de la présente PKI@BNPPF CP.

#### 2.1.1.4. TRAITEMENT DES DEMANDES DE RÉVOCATION D'UN CERTIFICAT

Le CA Isabel traite de manière sécurisée les demandes de révocation de PKI@BNPPF Certificate introduites par les PKI@BNPPF RA sous son contrôle. La publication de la révocation est mentionnée à la section “2.6.2 – Fréquence de publication”.

#### 2.1.1.5. PUBLIER LES INFORMATIONS DE RÉVOCATION DES PKI@BNPPF CERTIFICATE DANS UN REGISTRE D'ISABEL

Le CA Isabel publie les informations de révocation des PKI@BNPPF Certificate qu'il a révoqués dans un registre d'Isabel sous la forme d'une Certificate Revocation List (CRL) mise à jour.

Le CA Isabel respecte les dispositions de la section « 2.6 – Publication et registre » de la présente PKI@BNPPF CP. Il respecte les délais fixés à la section «2.6.2 – Fréquence de publication».

Ce mécanisme permet aux Parties Utilisatrices du PKI@BNPP Certificate de connaître, en temps voulu et sans ambigüité, le statut de révocation de tout PKI@BNPPF Certificate délivré par un CA Isabel.

#### 2.1.1.6. NOTIFICATION DE LA RÉVOCATION D'UN CERTIFICAT

L'Autorité de Certification Isabel veille à ce que l'entité (soit le Sujet du PKI@BNPPF Certificate ou un Souscripteur au PKI@BNPPF Certificate) ayant demandé la révocation d'un PKI@BNPPF Certificate à une PKI@BNPPF Registration Authority , ainsi que toute autre partie utilisant raisonnablement ce PKI@BNPPF Certificate, soient notifiées de la révocation du PKI@BNPPF Certificate.

L'autorité de certification Isabel veille à ce que toutes les parties disposent des informations relatives à la révocation.

#### 2.1.1.7. RESPECT DES NORMES

Les PKI@BNPPF Certificates délivrés doivent respecter la norme X.509 version 3.

#### 2.1.1.8. ARCHIVAGE ET SÉCURITÉ

L'autorité de certification Isabel respecte avec le plus grand soin ses obligations d'archivage, afin d'assurer la disponibilité des documents et/ou des autres informations nécessaires à titre de preuve, ainsi que pour garantir la confidentialité et l'intégrité de ces documents et informations. En règle générale, elle assure la sécurité physique des informations, protège l'accès à celles-ci et donne à son personnel les instructions utiles à ces fins.

#### 2.1.1.9. PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Le CA Isabel veille à ce que la manipulation des données à caractère personnel et confidentiel se fasse dans le respect de la loi belge sur la protection de la vie privée.

### 2.1.2. OBLIGATIONS DES RA D'ISABEL

Les PKI@BNPPF RA approuvées et actives au sein de l'infrastructure PKI d'Isabel possèdent les obligations spécifiques suivantes :

#### 2.1.2.1. PROTECTION DE LA CLÉ PRIVÉE DU RA

La PKI@BNPPF RA est tenue de conserver pour elle seule sa Clé privée et d'en garantir la confidentialité et la sécurité, de même que la confidentialité des Données d'activation qui lui sont associées.

#### 2.1.2.2. RESTRICTION DE L'UTILISATION DE LA CLÉ PRIVÉE DU RA

La PKI@BNPPF RA utilise uniquement sa Clé privée aux fins associées à sa fonction de RA.

#### 2.1.2.3. INDEMNISATION DES PARTIES EN CAS DE PRÉJUDICE

La PKI@BNPPF RA indemnise les parties pour tout préjudice causé à la suite d'un manquement à ses obligations, dans les délais fixés à la section « 2.2 – Responsabilité » de la présente PKI@BNPPF Certificate Policy.

#### 2.1.2.4. ARCHIVAGE ET SÉCURITÉ

La PKI@BNPPF RA respecte avec le plus grand soin ses obligations d'archivage, afin d'assurer la disponibilité des documents et/ou autres informations nécessaires à des fins de preuve, ainsi que pour assurer la confidentialité et l'intégrité de ces documents et informations. En règle générale, elle assure la sécurité physique des informations, protège l'accès à celles-ci et donne à son personnel les instructions utiles à ces fins.

#### 2.1.2.5. APPROBATION

Chaque PKI@BNPPF RA a reçu une approbation de BNP Paribas Fortis pour l'exercice de ses fonctions. BNP Paribas Fortis possède une liste des PKI@BNPPF RA approuvés. En exécutant ses tâches de PKI@BNPPF RA pour un CA Isabel, la PKI@BNPPF RA confirme avoir accepté cette responsabilité et avoir accepté d'agir conformément à la présente CP.

### 2.1.3. PKI@BNPPF CERTIFICATE OBLIGATIONS DU SOUSCRIPTEUR ET DU SUJET

Les Souscripteurs et les Sujets PKI@BNPPF Certificate sont, de manière générale, tenus de respecter les déclarations, conditions et procédures de la présente CP, qu'ils sont réputés avoir accepté en faisant usage d'un PKI@BNPPF Certificate.

Les Souscripteurs et Sujets PKI@BNPPF Certificate acceptent de respecter ces obligations pendant la totalité de la période de validité du PKI@BNPPF Certificate.

Le Souscripteur signe un accord avec une PKI@BNPPF RA avant ou au moment de la délivrance du certificat. La PKI@BNPPF RA conserve un exemplaire de cet accord. Les Souscripteurs sont liés par les droits et obligations qu'ils ont envers BNP Paribas Fortis au titre de leur accord contractuel avec PKI@BNPPF RA.

Les Souscripteurs et Sujets du PKI@BNPPF Certificate ont les obligations suivantes :

#### 2.1.3.1. OBTENIR LES INFORMATIONS NÉCESSAIRES À L'UTILISATION CORRECTE ET SÛRE DES SERVICES DE L'INFRASTRUCTURE PKI

Le Sujet du PKI@BNPPF Certificate est tenu d'obtenir auprès du RA PKI@BNPPF RA ayant délivré sonPKI@BNPPF Certificate:

1. la notification de ses obligations ;
2. la notification des exigences relatives à la protection de sa vie privée ;
3. la notification des garanties exactes offertes par les services de l'infrastructure PKI.

La communication de la présente PKI@BNPPF CP aux Sujets du PKI@BNPPF Certificate et aux Parties Utilisatrices du PKI@BNPPF Certificate doit être considérée comme une notification. L'utilisation du PKI@BNPPF Certificate par le Sujet suppose l'acceptation des déclarations figurant dans les notifications susmentionnées.

#### 2.1.3.2. GARANTIR LA CONFIDENTIALITÉ DE LA CLÉ PRIVÉE

Le Sujet du PKI@BNPPF Certificate est tenu de conserver pour lui seul sa Clé privée et d'en garantir la confidentialité et la sécurité, de même que la confidentialité des Données d'activation.

De manière générale, le Sujet prend les précautions nécessaires pour éviter la perte, la divulgation à une quelconque partie, la modification ou l'usage non autorisé des éléments clés et de la PKI@BNPPF Secure Signing Card, ainsi que les Données d'activation qui lui sont associées.

Toute utilisation faite de la Clé privée du Sujet est réputée être une utilisation faite par le Sujet lui-même jusqu'à ce que le contraire ait été dûment prouvé.

#### 2.1.3.3. LIMITATION DE L'UTILISATION DE LA CLÉ PRIVÉE ET DU PKI@BNPPF CERTIFICATE

Le Sujet du PKI@BNPPF Certificate ne peut utiliser sa Clé privé et son PKI@BNPPF Certificate qu'aux fins autorisées, conformément aux dispositions figurant :

1. à la section « 1.3.6 – Champ d'application » de la présente PKI@BNPPF CP.
2. tout accord déjà conclu ou conclu ultérieurement entreBNP Paribas Fortis et le BNP Paribas Fortis Client.

Lorsque le Sujet pense que la sécurité de sa Clé privée pourrait être compromise, il doit demander la révocation de son PKI@BNPPF Certificate et arrêter de générer des signatures numériques avec cette Clé privée.

Lorsque tous les certificats liés à une même Clé publique ont été révoqués ou ont expiré, la Clé publique devient invalide et le Sujet n'est plus en droit d'utiliser la Clé privée y correspondant, pour générer une signature numérique comme pour effectuer un décryptage.

#### 2.1.3.4. NOTIFICATION DE LA MISE EN PÉRIL DE LA CLÉ PRIVÉ/DU CODE PIN AU PKI@BNPPF REVOCATION SERVICE – PERTE DE PKI@BNPPF SECURE SIGNING CARD

Le PKI@BNPPF Certificate Sujet ou le PKI@BNPPF Certificate Souscripteur doit immédiatement prévenir la PKI@BNPPF Registration Authority en cas de :

1. mise en péril, crainte ou avérée, de perte ou de divulgation de la Clé Privée du Sujet ;
2. perte, crainte ou avérée, de la PKI@BNPPF Secure Signing Card du Sujet ;
3. mise en péril, crainte ou avérée, de perte ou de divulgation du code PIN du Sujet.

À titre subsidiaire, s'il est impossible de contacter la PKI@BNPPF Registration Authority le service de révocation Card Stop peut être notifié, conformément à la section « 3.4 – Demande de révocation ».

#### 2.1.3.5. NOTIFICATION D'UN CHANGEMENT DE STATUT À LA PKI@BNPPF RA

Le Sujet du PKI@BNPPF Certificate ou le Souscripteur du PKI@BNPPF Certificate doit prévenir immédiatement sa PKI@BNPPF RA de tout changement des informations fournies dans la demande de PKI@BNPPF Certificate du Sujet.

#### 2.1.3.6. UTILISER UN DISPOSITIF INFORMATIQUE DE CRÉATION SÉCURISÉE DE SIGNATURES

Le Sujet du PKI@BNPPF Certificate doit utiliser un dispositif informatique de création sécurisée de signatures pour conserver et utiliser sa Clé privée : la PKI@BNPPF Secure Signing Card.

#### 2.1.3.7. RESTRICTION DE L'UTILISATION DE LA CLÉ PUBLIQUE

Le Sujet ou Souscripteur du PKI@BNPPF Certificate ne peut soumettre de demande de certificat contenant la Clé publique dans un PKI@BNPPF Certificate à une CA tierce, même si le PKI@BNPPF Certificate a expiré ou a été révoqué.

Le Sujet ou Souscripteur du PKI@BNPPF Certificate ne peut soumettre de demande de certificat contenant la Clé publique dans un certificat tiers à un CA Isabel, même si le certificat tiers en question a expiré ou a été révoqué.

## 2.1.4. OBLIGATIONS DES PARTIES UTILISATRICES

Les Parties Utilisatrices possèdent les obligations spécifiques suivantes :

### 2.1.4.1. OBTENIR LES INFORMATIONS NÉCESSAIRES À L'UTILISATION CORRECTE ET SÛRE DES SERVICES DE L'INFRASTRUCTURE PKI

Les Parties Utilisatrices sont tenues d'obtenir, de la part du CA Isabel ayant délivré le PKI@BNPPF Certificate qu'elles entendent utiliser, une notification au sujet des garanties, responsabilités et obligations précises offertes par les services de l'infrastructure PKI conformément à la section « 2.2 – Responsabilité » de la présente PKI@BNPPF CP.

Les Parties Utilisatrices sont tenues de lire et d'accepter les déclarations notifiées. En général, les Parties Utilisatrices acceptent la présente CP avant d'utiliser un PKI@BNPPF Certificate délivré par un CA Isabel, y compris l'ensemble des limitations de responsabilité et des garanties applicables. Par ailleurs, les Parties Utilisatrices sont tenues de prendre connaissance et de respecter l'ensemble des règles, règlementations et dispositions législatives applicables aux informations contenues dans un PKI@BNPPF Certificate.

### 2.1.4.2. OBTENIR ET VÉRIFIER LE CERTIFICAT AUTO-SIGNÉ DU CA ISABEL

Les Parties Utilisatrices sont tenues d'obtenir et de contrôler la validité du certificat auto-signé du CA Isabel au sommet de la chaîne des certificats nécessaires au contrôle de la validité d'un certificat PKI@BNPPF.

Les Parties Utilisatrices sont tenues de contrôler et d'accepter le contenu et la validité du certificat auto-signé par le CA Isabel avant d'utiliser le certificat.

Les Parties Utilisatrices sont tenues de contrôler les attributs suivants du certificat auto-signé par le CA Isabel :

1. l'émetteur (CA Isabel) ;
2. la période de validité ;
3. les utilisations et limitations de la clé et du certificat ;
4. la signature du CA.

Les Parties Utilisatrices sont tenues d'accepter le certificat auto-signé par le CA Isabel, conformément à ce qui est indiqué au point 4.3 – Acceptation du certificat.

### 2.1.4.3. LIMITATION DE L'UTILISATION DU PKI@BNPPF CERTIFICATE

Les Parties Utilisatrices ne peuvent faire usage d'un PKI@BNPPF Certificate qu'aux fins autorisées et dans les limites d'utilisation fonctionnelle et de valeur établies, conformément aux dispositions de la section « 1.3.6 – Champ d'application » de la présente CP.

Chaque Partie Utilisatrice est tenue de contrôler et d'accepter le contenu et la validité du PKI@BNPPF Certificate avant d'en faire usage.

Les Parties Utilisatrices doivent contrôler les attributs suivants du PKI@BNPPF Certificate :

1. l'émetteur (CA Isabel) ;
2. la période de validité ;
3. le statut de révocation ;
4. l'utilisation et les limitations de la clé et du certificate, comme indiqué dans le PKI@BNPPF Certificate conformément à la section « 7.1.2 – Extensions de certificats » ;
5. la signature du CA.

Les attributs d'un PKI@BNPPF Certificate se trouvent à la section « 7.1 – Profil du certificat » de la présente PKI@BNPPF CP.

Les Parties Utilisatrices ne peuvent faire usage d'un PKI@BNPPF Certificate :

1. en cas d'échec de la vérification de la signature numérique du PKI@BNPPF Certificate ou du PKI@BNPPF Certificate lui-même ;
2. en cas d'expiration du PKI@BNPPF Certificate ;
3. en cas de révocation du PKI@BNPPF Certificate ;

4. en cas d'utilisation du PKI@BNPPF Certificate à des fins non autorisées ou ne respectant pas les limitations d'utilisation.

#### 2.1.4.4. VÉRIFIER LES SIGNATURES

Les Parties Utilisatrices sont tenues de vérifier les signatures numériques à l'aide du PKI@BNPPF Certificate certifiant la Clé publique associée à la Clé publique utilisée pour générer la signature numérique.

#### 2.1.4.5. MANQUEMENT AUX OBLIGATIONS DES PARTIES UTILISATRICES

Les Parties Utilisatrices sont tenues de connaître les dispositions énoncées à la section « 2.3.1 – Indemnisation par les Clients, Parties Utilisatrices et Sujets de BNP Paribas Fortis » et à la section « 2.2 – Responsabilité » de la présente PKI@BNPPF CP.

### 2.1.5. OBLIGATIONS EN MATIÈRE DE REGISTRE

Isabel conserve et met à la disposition des intéressés un registre électronique des informations sur les PKI@BNPPF Certificate et les révocations de PKI@BNPPF Certificate.

Isabel protège au mieux possible ce registre électronique contre les modifications non autorisées.

Ce registre électronique contiendra au minimum :

1. les PKI@BNPPF Certificates ayant été délivrés par l'Autorité de Certification Isabel conformément à la présente PKI@BNPPF CP ;
2. la liste des révocations de certificats publiée conformément à la présente PKI@BNPPF CP ;
3. le certificat auto-signé de l'Autorité de Certification Isabel ;
4. la version actuelle du présent PKI@BNPPF Certificate Policy.

Le registre électronique est disponible à la consultation électronique directe en permanence (24h/24).

Le registre électronique ne peut être consulté que par les Clients de BNP Paribas Fortis ou leurs représentants.

## 2.2. RESPONSABILITÉ

### 2.2.1. RESPONSABILITÉ DU CA

#### 2.2.1.1. GARANTIES ET LIMITATIONS DES GARANTIES

Isabel garantit uniquement que toute délivrance de PKI@BNPPF Certificate a été effectuée conformément aux dispositions de la présente PKI@BNPPF CP pour le niveau d'assurance pertinent. D'autres garanties peuvent également avoir été établies par la loi.

Sauf disposition contraire et dans les limites du droit applicable, Isabel décline toute garantie ou responsabilité, quelle qu'elle soit, y compris les garanties relatives à la commercialisation, les garanties d'adéquation à un but particulier et les garanties relatives à l'exactitude des informations fournies. Elle décline également toute responsabilité en cas de négligence ou de manque de prudence raisonnable de la part des Souscripteurs, des Sujets, des Clients et des Parties Utilisatrices de BNP Paribas Fortis. Les garanties s'appliquent aux Souscripteurs, Sujets, Clients et Parties Utilisatrices de BNP Paribas Fortis.

#### 2.2.1.2. EXCLUSION DE LA RESPONSABILITÉ D'ISABEL À L'ÉGARD DES SOUSCRIPTEURS, SUJETS, CLIENTS ET PARTIES UTILISATRICES DE BNP PARIBAS FORTIS

Les limitations de responsabilité incluent l'exclusion des préjudices indirects, particuliers, conséquents ou incidents.

Sauf disposition contraire ci-dessous, Isabel décline toute responsabilité en cas de perte ou de préjudice subi, de plainte portée à l'encontre ou de coûts exposés par les Souscripteurs, Sujets, Clients et/ou Parties Utilisatrices de BNP Paribas Fortis dans la mesure où ces pertes, préjudices, plaintes ou coûts découlent :

1. d'une perte ou d'une mise en péril d'une Clé privée d'Isabel, pour autant qu'Isabel n'ait pas manqué à ses devoirs au titre de la présente PKI@BNPPF CP, auquel cas la responsabilité de BNP Paribas Fortis sera engagée (sans préjudice des restrictions ou exclusions énoncées ci-après) vis-à-vis de la Partie Utilisatrice concernée, à condition que celle-ci soit en mesure de prouver avoir subi une perte ou un préjudice en raison d'un manquement d'Isabel ;
2. d'une information inexacte ou incorrecte figurant dans un PKI@BNPPF Certificate délivré par Isabel, à moins qu'Isabel n'ait pas mis tout en œuvre pour assurer l'exactitude et la correction de ces informations ou qu'Isabel n'ait pas contrôlé l'authenticité de toutes les preuves documentaires relatives à ces informations conformément à la présente PKI@BNPPF CP, auquel cas la responsabilité d'Isabel sera engagée (sans préjudice des restrictions ou exclusions énoncées ci-dessous) vis-à-vis de la Partie Utilisatrice concernée pour autant que celle-ci soit en mesure de prouver avoir subi une perte ou un préjudice suite à un manquement d'Isabel ;
3. de l'utilisation, par une Partie Utilisatrice, d'un PKI@BNPPF Certificate délivré par Isabel et révoqué, dans le cas où cette Partie Utilisatrice n'aurait pas vérifié auprès de la Validation Authority que le PKI@BNPPF Certificate pertinent n'avait pas été révoqué ;
4. de l'utilisation, par une Partie Utilisatrice, d'un PKI@BNPPF Certificate délivré par Isabel alors que la Partie Utilisatrice savait ou aurait raisonnablement dû savoir que ce PKI@BNPPF Certificate avait été révoqué, mais a tout de même accepté et fait usage de ce PKI@BNPPF Certificate ;
5. d'une indisponibilité de la Validation Authority ou du registre, pour quelque raison que ce soit ;
6. d'une information incorrecte ou inexacte contenue dans la CRL d'Isabel, utilisé par la Validation Authority, à moins qu'Isabel n'ait pas mis à jour son CRL conformément aux procédures établies dans la présente PKI@BNPPF CP, auquel cas la responsabilité d'Isabel sera engagée (sans préjudice des restrictions ou exclusions ci-dessous) vis-à-vis de la Partie Utilisatrice concernée pour autant que celle-ci soit en mesure de prouver avoir subi une perte ou un préjudice suite à un manquement d'Isabel ;
7. de tout manquement d'une PKI@BNPPF Registration Authority à ses obligations aux termes de la présente PKI@BNPPF CP ou d'un (éventuel) accord entre une Partie Utilisatrice et la PKI@BNPPF Registration Authority en question, le cas échéant ;
8. de la perte ou de la mise en péril de la Clé privée d'une PKI@BNPPF Registration Authority ;
9. de tout manquement d'un service de révocation à ses obligations au titre de la PKI@BNPPF CP applicable ;
10. d'une perte ou d'une mise en péril de la Clé privée d'un service de révocation ;
11. de tout manquement d'une autre partie, y compris une PKI@BNPPF Registration Authority, à l'une de ses obligations explicites vis-à-vis d'une Partie Utilisatrice ;
12. de toute utilisation du PKI@BNPPF Certificate, de la Clé privée et/ou du logiciel autre que celle autorisée par la présente PKI@BNPPF CP ;
13. de toute modification ou de tout changement de situation non notifié à Isabel ;
14. de toute utilisation indue ou de tout abus par les Souscripteurs, Sujets, Clients et/ou Parties Utilisatrices de BNP Paribas Fortis ;

#### 2.2.1.3. D'UNE PERTE INDIRECTE ET CONSÉCUTIVE DES SOUSCRIPTEURS, SUJETS, CLIENTS ET/OU PARTIES UTILISATRICES DE BNP PARIBAS FORTIS

Même si Isabel a été informé de la possibilité de ces préjudices, Isabel ne saurait être tenu responsable :

1. de toute perte ou de tout préjudice indirect ou consécutif ;
2. de toute perte de profits ;
3. de dommages-intérêts punitifs ;

4. des conséquences des actions et plaintes introduites à l'encontre des Souscripteurs, Sujets, Clients et Parties Utilisatrices de BNP Paribas Fortis ;
5. de toute détérioration de l'image de marque ;
6. de toute perte d'économies escomptées ;
7. de toute perte de recettes ;
8. de toute perte commerciale ;
9. de toute interruption de l'activité commerciale ; ou
10. de toute perte d'informations ou de données.

#### 2.2.1.4. LIMITATIONS DE LA RESPONSABILITÉ D'ISABEL VIS-À-VIS DES SOUSCRIPTEURS, SUJETS, CLIENTS ET/OU PARTIES UTILISATRICES DE BNP PARIBAS FORTIS

Dans le cas où la responsabilité d'Isabel serait engagée, la responsabilité totale d'Isabel vis-à-vis des parties, notamment, mais pas exclusivement, les Souscripteurs, Sujets, Clients et/ou Parties Utilisatrices de BNP Paribas Fortis, à l'égard de toute plainte isolée ou série de plaintes liées, ne peut en aucun cas dépasser le plafond de responsabilité établi ci-après pour ce PKI@BNPPF Certificate. La responsabilité totale d'Isabel vis-à-vis de toutes les personnes concernées sera limitée, pour la totalité des signatures et des transactions liées à ce PKI@BNPPF Certificate, à 2 500 EUR. Ce plafond de responsabilité de 2 500 EUR est applicable entre, d'une part, Isabel, et, d'autre part, les Souscripteurs, Sujets, Clients et/ou Parties Utilisatrices de BNP Paribas Fortis.

Cette limitation des dommages-intérêts s'applique aux pertes et préjudices de tous types, subis par toute personne, notamment, mais pas exclusivement, un Souscripteur, un Sujet, un Client ou une Partie Utilisatrice de BNP Paribas Fortis, causés par l'utilisation d'un PKI@BNPPF Certificate délivré, géré, utilisé ou révoqué par Isabel ou d'un certificat expirant. Cette limitation des dommages-intérêts s'applique également à la responsabilité contractuelle, à la responsabilité civile et à toute autre forme de poursuite en responsabilité. Le plafond de responsabilité établi pour chaque PKI@BNPPF Certificate est le même quel que soit le nombre de signatures numériques, de transactions ou de plaintes liées au certificat en question. En cas de dépassement du plafond de responsabilité, ce dernier est distribué, dans un premier temps, en faveur des plaintes les plus anciennes, afin d'assurer la résolution définitive des litiges, sauf ordonnance contraire d'un tribunal ou d'une juridiction. Isabel n'est en aucun cas tenu de payer davantage que le montant maximal total établi pour chaque certificat.

#### 2.2.1.5. CAS DE FORCE MAJEURE

Dans le cas où Isabel serait empêché, gêné ou retardé dans l'exécution de l'une ou l'autre de ses obligations, au titre de la présente CP ou de tout autre document pertinent, en raison d'un cas de force majeure, p.ex. une guerre, un acte de terrorisme, une insurrection, des grèves, un conflit social, un accident, un incendie, une inondation ou des incidents liés à des tierces parties (comme des retards de transport ou de livraison, une panne d'équipement ou des problèmes de connexion pour la communication des données), Isabel ne saurait être tenu responsable :

1. d'un manquement à ses obligations ou d'un retard dans l'exécution de celles-ci pour autant que ce manquement soit dû au cas de force majeure en question ; et
2. de toute perte ou de tout préjudice, de quelque nature que ce soit, de toute plainte, de quelque nature que ce soit, ou de tout coût, de quelque nature que ce soit, subi par une Partie Utilisatrice des suites de ce manquement ou retard d'exécution des obligations d'Isabel dû au cas de force majeure.

#### 2.2.1.6. LIMITATIONS DE L'EXCLUSION OU DE LA LIMITATION DE RESPONSABILITÉ D'ISABEL

Aucune disposition du présent règlement ne limite ou n'exclut la responsabilité d'Isabel :

1. en cas de décès ou de blessure corporelle des suites d'une négligence d'Isabel ; ou
2. en cas de fraude commise par Isabel.

## 2.2.2. PKI@BNPPF RA RESPONSABILITÉ

### 2.2.2.1. GARANTIES ET LIMITATIONS DES GARANTIES

BNP Paribas Fortis garantit uniquement que toute délivrance d'un PKI@BNPPF Certificate est effectuée conformément aux dispositions de la présente PKI@BNPPF CP pour le niveau d'assurance pertinent. D'autres garanties peuvent également avoir été établies par la loi.

Sauf accord contraire et dans les limites du droit applicable, BNP Paribas Fortis décline toute garantie ou responsabilité, quelle qu'elle soit, y compris les garanties relatives à la commercialisation, les garanties d'adéquation à un but particulier et les garanties relatives à l'exactitude des informations fournies. Elle décline également toute responsabilité en cas de négligence ou de manque de prudence raisonnable de la part des Souscripteurs, des Sujets, des Clients et des Parties Utilisatrices de BNP Paribas Fortis.

### 2.2.2.2. EXCLUSION DE LA RESPONSABILITÉ DE BNP PARIBAS FORTIS VIS-À-VIS DES SOUSCRIPTEURS, SUJETS, CLIENTS ET PARTIES UTILISATRICES DE BNP PARIBAS FORTIS

Sauf disposition contraire ci-dessous, BNP Paribas Fortis ne saurait être tenu responsable en cas de perte, de préjudice, de plainte ou de coût subi par les Souscripteurs, Sujets, Clients et/ou Parties Utilisatrices de BNP Paribas Fortis pour autant que ces pertes, préjudices, plaintes ou coûts découlent :

1. de la perte ou de la mise en péril de la Clé privée de Sujets de BNP Paribas Fortis, à moins d'un manquement de BNP Paribas Fortis à ses obligations au titre de la présente CP, auquel cas la responsabilité de BNP Paribas Fortis sera engagée (sans préjudice des restrictions ou exclusions ci-après) vis-à-vis de la Partie Utilisatrice concernée, pour autant que celle-ci soit en mesure de prouver avoir subi une perte ou un préjudice suite au manquement en question de BNP Paribas Fortis ;
2. d'une information inexacte ou incorrecte figurant dans un PKI@BNPPF Certificate délivré par le CA Isabel, à moins que BNP Paribas Fortis n'ait pas mis tout en œuvre pour assurer l'exactitude et la correction de ces informations ou que BNP Paribas Fortis n'ait pas contrôlé l'authenticité de toutes les preuves documentaires relatives à ces informations conformément à la présente PKI@BNPPF CP, auquel cas la responsabilité de BNP Paribas Fortis sera engagée (sans préjudice des restrictions ou exclusions énoncées ci-dessous) vis-à-vis de la Partie Utilisatrice concernée pour autant que celle-ci soit en mesure de prouver avoir subi une perte ou un préjudice suite à un manquement de BNP Paribas Fortis ;
3. de l'utilisation, par une Partie Utilisatrice, d'un PKI@BNPPF Certificate délivré par le CA Isabel et révoqué, dans le cas où cette Partie Utilisatrice n'aurait pas vérifié que le PKI@BNPPF Certificate pertinent n'avait pas été révoqué ;
4. de l'utilisation, par une Partie Utilisatrice, d'un PKI@BNPPF Certificate délivré par le CA Isabel alors que la Partie Utilisatrice savait ou aurait raisonnablement dû savoir que ce PKI@BNPPF Certificate avait été révoqué, mais a tout de même accepté et fait usage de ce PKI@BNPPF Certificate ;
5. d'une indisponibilité de la CRL ou du registre d'Isabel, pour quelque raison que ce soit ;
6. de toute information incorrecte ou inexacte figurant dans la CRL d'Isabel ;
7. de toute utilisation faite du PKI@BNPPF Certificate, de la Clé privée et/ou du logiciel autre que celle autorisée par la présente PKI@BNPPF CP;
8. de toute modification ou changement de situation non notifié à la PKI@BNPPF RA ;
9. de toute utilisation indue ou abus par les Souscripteurs, Sujets, Clients et/ou Parties Utilisatrices.

### 2.2.2.3. D'UNE PERTE INDIRECTE ET CONSÉCUTIVE DES SOUSCRIPTEURS, SUJETS, CLIENTS ET/OU PARTIES UTILISATRICES DE BNP PARIBAS FORTIS

Même si BNP Paribas Fortis a été informé de l'éventualité de ces préjudices, BNP Paribas Fortis ne saurait être tenu responsable d'une perte ou d'un préjudice indirect ou consécutif, notamment, mais pas exclusivement :

1. de toute perte de profits ;

2. de dommages-intérêts punitifs ;
3. des conséquences des actions et plaintes introduites à l'encontre des Souscripteurs, Sujets, Clients et/ou Parties Utilisatrices de BNP Paribas Fortis par de tierces parties ;
4. de toute détérioration de l'image de marque ;
5. de toute perte d'économies escomptées ;
6. de toute perte de recettes ;
7. de toute perte commerciale ;
8. de toute interruption de l'activité commerciale ; ou
9. de toute perte d'informations ou de données.

#### 2.2.2.4. LIMITATIONS DE LA RESPONSABILITÉ DE BNP PARIBAS FORTIS VIS-À-VIS DES SOUSCRIPTEURS, SUJETS, CLIENTS ET/OU PARTIES UTILISATRICES DE BNP PARIBAS FORTIS

Pour autant que la responsabilité de BNP Paribas Fortis soit engagée, la responsabilité globale de BNP Paribas Fortis vis-à-vis de toutes les parties, notamment, mais pas exclusivement, les Souscripteurs, Sujets, Clients et/ou Parties Utilisatrices de BNP Paribas Fortis, à l'égard d'une plainte isolée ou d'une série de plaintes liées, ne peut en aucun cas dépasser le plafond de responsabilité applicable pour le PKI@BNPPF Certificate concerné, établi ci-dessous. La responsabilité globale de BNP Paribas Fortis vis-à-vis de toutes les personnes concernées par un PKI@BNPPF Certificate donné se limite, pour l'ensemble des signatures et transactions relevant de ce PKI@BNPPF Certificate, au plus élevé des deux montants suivants: 2 500 EUR ou un montant équivalent à un an de redevances dues pour les services du PKI@BNPPF Certificate.

Cette limitation des dommages-intérêts s'applique aux pertes et préjudices de tous types, subis par toute personne, notamment, mais pas exclusivement, un Souscripteur, un Sujet, un Client ou une Partie Utilisatrice de BNP Paribas Fortis, causés par l'utilisation d'un PKI@BNPPF Certificate délivré, géré, utilisé ou révoqué par un CA Isabel ou d'un PKI@BNPPF Certificate expirant. Cette limitation des dommages-intérêts s'applique également à la responsabilité contractuelle, à la responsabilité civile et à toute autre forme de poursuite en responsabilité. Le plafond de responsabilité établi pour chaque PKI@BNPPF Certificate est le même quel que soit le nombre de signatures numériques, de transactions ou de plaintes liées au PKI@BNPPF Certificate en question. En cas de dépassement du plafond de responsabilité, ce dernier est distribué, dans un premier temps, en faveur des plaintes les plus anciennes, afin d'assurer la résolution définitive des litiges, sauf ordonnance contraire d'un tribunal ou d'une juridiction. BNP Paribas Fortis n'est en aucun cas tenu de payer davantage que le montant maximal total établi pour chaque PKI@BNPPF Certificate.

#### 2.2.2.5. CAS DE FORCE MAJEURE

Dans le cas où BNP Paribas Fortis serait empêché, gêné ou retardé dans l'exécution de l'une ou l'autre de ses obligations, au titre de la présente CP ou de tout autre document pertinent, en raison d'un cas de force majeure, p.ex. une guerre, un acte de terrorisme, une insurrection, des grèves, un conflit social, un accident, un incendie, une inondation ou des incidents liés à de tierces parties (comme des retards de transport ou de livraison, une panne d'équipement ou des problèmes de connexion pour la communication des données), BNP Paribas Fortis ne saurait être tenu responsable :

1. d'un manquement à ses obligations ou d'un retard dans l'exécution de celles-ci pour autant que ce manquement soit dû au cas de force majeure en question ; et
2. de toute perte ou de tout préjudice, de quelque nature que ce soit, de toute plainte, de quelque nature que ce soit, ou de tout coût, de quelque nature que ce soit, subi par une Partie Utilisatrice des suites de ce manquement ou retard d'exécution des obligations de BNP Paribas Fortis dû au cas de force majeure.

#### 2.2.2.6. LIMITATIONS DE L'EXCLUSION OU DE LA LIMITATION DE RESPONSABILITÉ DE BNP PARIBAS FORTIS

Aucune disposition du présent règlement ne limite ou n'exclut la responsabilité de BNP Paribas Fortis :

1. en cas de décès ou de blessure corporelle des suites d'une négligence de BNP Paribas Fortis ou d'Isabel ; ou

2. en cas de fraude commise par BNP Paribas Fortis ou Isabel.

### 2.2.3. RESPONSABILITÉ DES SOUSCRIPTEURS, SUJETS, CLIENTS ET/OU PARTIES UTILISATRICES DE BNP PARIBAS FORTIS

En acceptant ou en utilisant un PKI@BNPPF Certificate, le client BNP Paribas Fortis, le Souscripteur, le Sujet et/ou la Partie Utilisatrice déclarent accepter d'indemniser et de dégager BNP Paribas Fortis, Isabel et ses agents et sous-traitants de toute responsabilité en cas d'acte ou d'omission entraînant une perte, un dommage, un procès ou un dépens de nature quelconque susceptible d'être subi par BNP Paribas Fortis, Isabel et ses agents et sous-traitants et causés par l'utilisation ou la publication d'un PKI@BNPPF Certificate et découlant :

1. d'un manquement à ses obligations aux termes de la présente PKI@BNPPF CP ;
2. d'un mensonge ou d'une représentation erronée des faits par le Client, le Souscripteur ou le Sujet de BNP Paribas Fortis ;
3. la non-divulgation, par le Client, Souscripteur ou Sujet de BNP Paribas Fortis d'un fait matériel, si l'omission ou la représentation erronée a été commise par négligence ou dans l'intention de tromper BNP Paribas Fortis, une PKI@BNPPF RA ou toute personne recevant ou utilisant le PKI@BNPPF Certificate ;
4. du non-respect de l'obligation de protéger la Clé privée des Souscripteurs ou Sujets de BNP Paribas Fortis, d'utiliser un système fiable ou de prendre les précautions nécessaires pour empêcher la mise en péril, la perte, la divulgation, la modification ou l'utilisation non autorisée de cette Clé privée ;
5. de toute utilisation du PKI@BNPPF Certificate, de la Clé privée et/ou du logiciel autre que celui autorisé par BNP Paribas Fortis.

Tous les Souscripteurs, Sujets, Clients et/ou Parties Utilisatrices de BNP Paribas Fortis acceptent que l'utilisation d'un PKI@BNPPF Certificate en dehors de la Communauté de BNP Paribas Fortis (voir section « 1.3 – Communauté et applicabilité ») sans l'autorisation explicite de BNP Paribas Fortis, ou l'utilisation d'un PKI@BNPPF Certificate après l'interdiction, par BNP Paribas Fortis, d'une utilisation donnée au moyen d'une lettre de mise en demeure entraîne la responsabilité décrite ci-dessus et que cette utilisation interdite sera considérée ipso facto comme une violation de la présente PKI@BNPPF CP.

## 2.3. RESPONSABILITÉ FINANCIÈRE

BNP Paribas Fortis assure les risques de responsabilité professionnelle financière liés à ses activités et responsabilités découlant de sa fourniture de services liés aux PKI@BNPPF Certificates auprès d'une compagnie d'assurance réputée. Isabel N.V. / S.A. doit avoir une assurance adéquate contre la responsabilité civile et professionnelle dans le cadre de l'exécution de ses obligations en tant que CA.

### 2.3.1. INDEMNISATION PAR LES CLIENTS, PARTIES UTILISATRICES ET SUJETS DE BNP PARIBAS FORTIS ET PAR BNP PARIBAS FORTIS

Les Clients de BNP Paribas Fortis et/ou Parties Utilisatrices et/ou Sujets d'un PKI@BNPPF Certificate sont tenus d'indemniser toutes les parties (y compris l'Autorité de Certification Isabel et les PKI@BNPPF RA) et/ou BNP Paribas Fortis pour tout préjudice résultant d'un manquement à leur obligations.

En cas de manquement établi d'une Partie Utilisatrice à ses obligations au titre de la présente PKI@BNPPF CP, cette partie ne pourra en aucun cas tenir Isabel responsable d'un quelconque préjudice.

BNP Paribas Fortis BNP Paribas Fortis n'est pas responsable de toute conséquence d'une violation de ses obligations par une Partie Utilisatrice.

### 2.3.2. RELATIONS FIDUCIAIRES

La relation entre BNP Paribas Fortis et les Sujets de PKI@BNPPF Certificate, ainsi que celle entre BNP Paribas Fortis et les Parties utilisatrices de PKI@BNPPF Certificate, n'est pas celle d'un agent et de son commettant. Ni les Sujets du PKI@BNPPF Certificate, ni les Parties Utilisatrices ne sont habilités à contraindre BNP Paribas Fortis, par voie contractuelle ou autre, à respecter une quelconque obligation.

### 2.3.3. PROCÉDURE ADMINISTRATIVE

Les comptes et rapports annuels de BNP Paribas Fortis sont publiés et audités chaque année conformément à la législation belge.

## 2.4. INTERPRÉTATION ET APPLICATION

En cas de conflit ou d'incohérence entre la présente PKI@BNPPF CP et les accords contractuels liant les Clients de BNP Paribas Fortis les Souscripteurs et Sujets d'un PKI@BNPPF Certificate à BNP Paribas Fortis, les dispositions de la présentePKI@BNPPF CP prévalent sur l'accord contractuel ainsi que sur tout accord spécifique nouvellement conclu, sauf disposition contraire et dans la mesure où ils sont applicables aux PKI@BNPPF Certificates.

### 2.4.1. DROIT APPLICABLE

La législation belge régit l'applicabilité, la construction, l'interprétation et la validité de la présente PKI@BNPPF CP.

### 2.4.2. DIVISIBILITÉ, SURVIE, FUSION, PRÉAVIS

Dans le cas où le tribunal d'une juridiction compétente ou organe similaire jugerait invalide, inapplicable ou illégale l'une ou l'autre clause du présent document, celle-ci serait retirée du présent document, qui demeurerait applicable. Les clauses supprimées seraient alors remplacées par une clause se rapprochant le plus près possible de l'intention de la clause invalide.

Dans le cas exceptionnel où les lois d'un territoire applicables à un Souscripteur ou à un Sujet d'un PKI@BNPPF Certificate étranger ne permettraient pas l'inclusion de certaines dispositions de la présente PKI@BNPPF CP, ces dispositions seraient alors réputées nulles et non avenues, comme si elles n'avaient pas été incluses, et le premier paragraphe de la présente section s'appliquerait alors, uniquement pour le Souscripteur ou le Sujet de PKI@BNPPF Certificate concerné.

Les dispositions qui, de par leur nature, doivent continuer à exister une fois expirée la validité de la présente CP, continueront donc à exister.

Toutes les notifications officielles exigées aux termes de la présente CP se font par écrit et sont envoyées par courrier recommandé ou par télécopie, ou encore par courrier électronique avec signature électronique avancée.

### 2.4.3. PROCÉDURES DE RÉSOLUTION DES LITIGES

Toutes les parties impliquées, le CA Isabel, les Clients, Souscripteurs, Sujets et Parties Utilisatrices de PKI@BNPPF RA, BNP Paribas Fortis, tenteront, en faisant preuve de bonne foi et en déployant leurs meilleurs efforts, de trouver une solution à l'amiable aux plaintes, litiges ou différends qui pourraient les opposer.

Lorsqu'aucune solution à l'amiable ne peut être trouvée dans des délais raisonnables, les litiges sont soumis à la compétence exclusive des tribunaux de Bruxelles.

## 2.5. FRAIS

Les redevances payables pour les PKI@BNPPF Certificates et les services y afférents, ainsi que leurs modalités, sont établies dans les accords contractuels conclus entre les Clients/Souscripteurs/Sujets des PKI@BNPPF Certificate et BNP Paribas Fortis.

Le remboursement est applicable uniquement s'il a été explicitement convenu entre les parties.

## 2.6. PUBLICATION ET REGISTRE

### 2.6.1. PUBLICATION DES INFORMATIONS

Les informations devant être publiées sont les suivantes :

1. la présente PKI@BNPPF CP ;
2. les PKI@BNPPF Certificates acceptés par le Sujet, déclarant ce faisant que les informations y figurant sont correctes ;
3. les listes de révocation des PKI@BNPPF Certificates ;
4. le certificat auto-signé et les certificats croisés du CA Isabel ;
5. BNP Paribas Fortis les conditions générales des services de certification de BNP Paribas Fortis ;
6. les contrats types pour les services de certification BNP Paribas Fortis ;

Ces informations sont publiées en ligne et éventuellement sous d'autres formes.

### 2.6.2. FRÉQUENCE DE PUBLICATION

La publication des PKI@BNPPF Certificates est garantie dans les 24 heures suivant leur acceptation par leur Sujet. Les PKI@BNPPF Certificates sont généralement publiés dans la demi-heure suivant leur acceptation.

Les Certificate Revocation Lists (CRL) sont habituellement mises à jour dans la demi-heure suivant une modification. Elles sont republiées au moins une fois toutes les 24 heures.

La PKI@BNPPF CP est soumise à un contrôle de version, comme indiqué dans le présent document.

La délivrance des PKI@BNPPF CP est abordée à la section « 8 – ADMINISTRATION DES SPÉCIFICATIONS » de la présente PKI@BNPPF CP.

### 2.6.3. CONTRÔLE DES ACCÈS

Le CA Isabel veille à ce que les contrôles d'accès adéquats soient mis en place afin d'éviter l'écriture, la modification ou la suppression non autorisée de certificats, de documents de politique, de CRL et d'autres éléments contenus dans le registre.

La présente PKI@BNPPF CP est accessible en **mode lecture** par :

1. l'Autorité de Certification Isabel ;
2. Les PKI@BNPPF RA ;
3. Les Souscripteurs et Sujets d'un PKI@BNPPF Certificate ;
4. les Parties Utilisatrices d'un PKI@BNPPF Certificate ;

La présente PKI@BNPPF CP est accessible en mode écriture/modification par la Policy Authority, voir la section « 8 – ADMINISTRATION DES SPÉCIFICATIONS ».

Les PKI@BNPPF Certificates sont accessibles en **mode lecture** par :

1. les PKI@BNPPF RA ;
2. les Souscripteurs et Sujets d'un PKI@BNPPF Certificate ;
3. la Policy Authority de BNP Paribas Fortis ;

Les PKI@BNPPF Certificates et la liste de révocation des certificats pour les PKI@BNPPF Certificates sont accessibles en mode **écriture/modification** par l'Autorité de Certification Isabel.

Le service de validation n'est accessible que par les Clients de la PKI@BNPPF CP

### 2.6.4. REGISTRES

Les PKI@BNPPF Certificates et les listes de révocation des certificats pour les PKI@BNPPF Certificates sont publiés dans un registre d'Isabel.

La gestion du registre d'Isabel relève de la responsabilité d'Isabel S.A./N.V., mais pas de l'Autorité de Certification Isabel.

## 2.7. AUDIT DE CONFORMITÉ

BNP Paribas Fortis effectue des audits de toutes ses procédures et de leur respect de la présente PKI@BNPPF CP. Un audit peut être effectué pour vérifier que Isabel NV / SA est en conformité avec l'exécution de ses obligations en tant que CA.

### 2.7.1. FRÉQUENCE DES AUDITS DE CONFORMITÉ DES ENTITÉS

La fréquence de ces audits est déterminée par

1. Les politiques internes de BNP Paribas Fortis;
2. le cadre législatif belge en vigueur ;
3. les autres parties chargées d'exécuter un audit en raison de leur relation avec BNP Paribas Fortis.

### 2.7.2. IDENTITÉ/QUALIFICATIONS DES AUDITEURS

Le ou les auditeurs choisis sont des parties indépendantes disposant d'une expertise dans le domaine des infrastructures PKI.

Le ou les auditeurs présenteront les qualifications correspondant aux pratiques professionnelles et aux dispositions de la loi, le cas échéant. La mission principale du ou des auditeurs est d'exécuter des audits sur le CA ou la sécurité des systèmes d'information. Ils doivent disposer d'une solide connaissance des politiques des infrastructures PKI (CPS et CP).

### 2.7.3. RELATION DE L'AUDITEUR AVEC LA PARTIE AUDITÉE

Les auditeurs doivent être indépendants de BNP Paribas Fortis et d'Isabel S.A./N.V.

Les auditeurs nouent une relation contractuelle avec BNP Paribas Fortis aux fins de l'exécution de l'audit. Ils sont suffisamment séparés, d'un point de vue organisationnel, du CA Isabel audité, de la PKI@BNPPF RA ou de tout autre BNP Paribas Fortis ou composant de l'infrastructure PKI pour fournir une évaluation impartiale et indépendante.

### 2.7.4. THÈMES COUVERTS PAR LES AUDITS

Des audits seront réalisés sur les thèmes suivants :

1. l'infrastructure du CA Isabel ;
2. la gestion du CA Isabel ;
3. Les principales politiques et procédures de gestion du CA Isabel ;
4. les activités du CA Isabel ;

5. les opérations des PKI@BNPPF RA ;
6. le respect de la PKI@BNPPF CP ;
7. le respect des règlementations belges ;

### 2.7.5. LES MESURES PRISES SUITE À LA DÉTECTION D'UNE LACUNE.

Les rapports d'audit sont évalués par BNP Paribas Fortis. La priorité est accordée à la détection d'incohérences par rapport à la PKI@BNPPF CP ou d'autres irrégularités. Des mesures correctives sont planifiées en tenant compte du risque résiduel. Un nouvel audit peut être réalisé par la suite pour réexaminer les corrections demandées.

### 2.7.6. COMMUNICATION DES RÉSULTATS

Les conclusions de l'audit sont reprises dans un rapport uniquement adressé au Security Manager de BNP Paribas Fortis.

Les informations contenues dans les rapports d'audit ne sont pas rendues publiques, sauf disposition contraire du droit national. Les informations fournies par les audits doivent être considérées comme des informations strictement confidentielles dans le cadre de la présente CP.

## 2.8. CONFIDENTIALITÉ

### 2.8.1. TYPES D'INFORMATIONS À GARDER CONFIDENTIELLES

toutes les informations relatives à la demande, à la délivrance, à l'acceptation et à la révocation d'un PKI@BNPPF Certificate sont réputées confidentielles et sont soumises à un accès limité, à l'exception de celles reprises à la section « 2.8.2 – Types d'informations non considérées comme confidentielles ».

Ces informations peuvent faire partie d'un accord bilatéral entre BNP Paribas Fortis et une tierce partie et communiquées dans le cadre d'un accord de confidentialité.

Les informations suivantes sont réservées aux Souscripteurs, aux Sujets et aux Parties Utilisatrices d'un PKI@BNPPF Certificate :

1. PKI@BNPPF Certificateles PKI@BNPPF Certificates et les informations y figurant ;
2. les certificats auto-signés des Certification Authorities d'Isabel ;

### 2.8.2. TYPES D'INFORMATIONS NON CONSIDÉRÉES COMME CONFIDENTIELLES

La présente PKI@BNPPF CP est publiquement disponible et ne relève donc pas des obligations de confidentialité visées à la présente section.

La présente PKI@BNPPF CP n'étant pas un document confidentiel, elle ne contient aucune information confidentielle.

### 2.8.3. DIVULGATION D'INFORMATIONS RELATIVES À LA RÉVOCATION DES CERTIFICATS

Les motifs de révocation d'un certificat sont formalisés par la norme ITU-T X.509 avec le champ Extension « Code Motif ».

Le Sujet d'un PKI@BNPPF Certificate ou le Souscripteur d'un PKI@BNPPF Certificate ayant demandé la révocation du certificat du Sujet sera notifié de la révocation du PKI@BNPPF Certificate.

Le motif de révocation n'est pas communiqué aux Parties Utilisatrices.

### 2.8.4. COMMUNICATION AUX POUVOIRS RÉPRESSIFS

Le CA Isabel et les PKI@BNPPF RA sont en droit de communiquer des informations confidentielles sur ordonnance dûment signée par un juge ou un agent dans le cadre d'une enquête pénale ou au titre de toute autre disposition de la loi.

### 2.8.5. DIVULGATION EN VERTU DU PRINCIPE DE COMMUNICATION PRÉALABLE AU CIVIL

Aucune disposition.

### 2.8.6. DIVULGATION SUR DEMANDE D'UN SOUSCRIPTEUR/SUJET

Le CA et les PKI@BNPPF RA d'Isabel sont autorisés à communiquer des informations confidentielles au sujet d'un Souscripteur/Sujet de PKI@BNPPF Certificate sur demande ou avec l'approbation du Souscripteur/Sujet de PKI@BNPPF Certificate en question.

### 2.8.7. AUTRES CIRCONSTANCES PERMETTANT LA COMMUNICATION D'INFORMATIONS

Aucune disposition.

## 2.9. DROITS DE PROPRIÉTÉ INTELLECTUELLE

Toutes les informations fournies dans le présent document font partie des droits de propriété intellectuelle de BNP Paribas Fortis ou d'Isabel. Cela vaut pour l'ensemble des informations publiées par BNP Paribas Fortis et Isabel, dans le cadre d'une relation publique ou privée.

Ces droits dépassent toute relation contractuelle pouvant exister avec BNP Paribas Fortis. Le PKI@BNPPF Certificate, les moyens d'accès à celui-ci et la signature, y compris la Clé publique, sont la propriété exclusive d'Isabel. Toute utilisation des PKI@BNPPF Certificates, des moyens d'accès à ceux-ci et de la signature en dehors des fonctionnalités convenues du système de BNP Paribas Fortis doit faire l'objet d'un contrat signé avec BNP Paribas Fortis. Lorsque les certificats relatifs à une même Clé publique ont expiré ou ont été révoqués, il est interdit au Sujet, au Souscripteur ou au Client d'utiliser, après ladite expiration ou révocation, les données afférentes à la création de signature correspondante afin de signer ou de faire certifier ces données par un autre fournisseur de services de certification.

# 3. IDENTIFICATION ET AUTHENTICATION

Le présent chapitre décrit les procédures utilisées pour authentifier un Souscripteur de PKI@BNPPF Certificate préalablement à la délivrance d'un certificat. Il décrit également la manière dont les parties demandant une nouvelle clé ou une révocation sont authentifiées et abordera les pratiques de dénomination, notamment la reconnaissance de la titularité d'un nom et de résolution des litiges relatifs aux noms.

## 3.1. ENREGISTREMENT INITIAL

La présente section décrit les dispositions relatives à l'identification et à l'authentification dans le cadre de l'enregistrement initial d'un Sujet de PKI@BNPPF Certificate.

On distingue deux types de Sujets d'un PKI@BNPPF Certificate :

- Sujet personne physique : le Sujet est représenté par la personne physique identifiée dans le certificat.
- Sujet fonction : le Sujet est représenté par une personne physique habilitée à représenter la fonction identifiée dans le certificat (représentant de fonction).

### 3.1.1. TYPES DE NOMS

Le CA Isabel doit utiliser le format du nom distingué de la norme X.500 pour les champs de nom du Sujet et de l'Émetteur dans un PKI@BNPPF Certificate.

### 3.1.2. LES NOMS DOIVENT AVOIR UN SENS

Le PKI@BNPPF RA doit veiller à ce que les informations relatives au nom distingué indiquées dans le champ « Sujet » d'un PKI@BNPPF Certificate dans l'espace réservé au nom X.500, pour lequel Isabel a reçu une autorisation, aient un sens.

Le CA Isabel ne délivre aucun certificat anonyme ou sous un pseudonyme.

### 3.1.3. RÈGLES D'INTERPRÉTATION DES DIFFÉRENTES FORMES DE NOMS

Les Noms Distingués figurant dans les certificats sont interprétés sur la base des normes X.500 et de la syntaxe ASN.1. Voir RFC 2253 et RFC 2616 pour plus d'informations sur la manière dont les noms distingués X.500 dans les certificats sont interprétés en tant que qu'identificateurs de ressources uniformes et références HTTP.

### 3.1.4. CARACTÈRE UNIQUE DES NOMS

Le CA Isabel doit garantir le caractère unique du Nom Distingué inscrit dans le champ « Sujet » du PKI@BNPPF Certificate dans l'espace réservé au nom X.500 pour lequel Isabel a reçu une autorisation et qui a été réservé pour BNP Paribas Fortis.

Voir « 7 – Profils du certificat, de la CRL et de l'OCSP ».

### 3.1.5. PROCÉDURE DE RÉSOLUTION DES LITIGES RELATIFS AUX NOMS

Le CA Isabel est habilité à résoudre les litiges relatifs aux Noms Distingués utilisés dans le champ « Sujet » des PKI@BNPPF Certificates dans le ou les espaces X.500 pour lesquels Isabel a reçu une autorisation.

### 3.1.6. RECONNAISSANCE, AUTHENTIFICATION ET RÔLE DES MARQUES COMMERCIALES

Les PKI@BNPPF RA ne peuvent ni contrôler ni garantir que les marques commerciales, marques de service et autres signes protégés mentionnés dans les PKI@BNPPF Certificates peuvent être légitimement utilisés sans enfreindre un droit de propriété intellectuelle. Ni les RA, ni les CA de l'infrastructure PKI ne sont tenus de réaliser une telle enquête sur une infraction potentielle.

### 3.1.7. MÉTHODE UTILISÉE POUR DÉMONTRER LA POSSESSION D'UNE CLÉ PRIVÉE

Aucune disposition.

### 3.1.8. AUTHENTIFICATION DE L'IDENTITÉ DE L'ORGANISATION

Les PKI@BNPPF RA sont tenus d'authentifier l'identité d'un Client BNP Paribas Fortis candidat avant que les Souscripteurs de ce Client de BNP Paribas Fortis ne soient autorisés à demander des PKI@BNPPF Certificates.

L'authentification de l'identité d'un Client de BNP Paribas Fortis candidat est effectuée dans le cadre du processus de souscription déterminant la signature d'un contrat de service/produit BNP Paribas Fortis entre le Client BNP Paribas Fortis en question et BNP Paribas Fortis. Le contrat décrit également plus en détail la procédure d'authentification et les éléments devant être fournis au PKI@BNPPF RA par le Client BNP Paribas Fortis candidat dans le cadre de ce processus de souscription.

### 3.1.9. AUTHENTIFICATION D'UNE IDENTITÉ DONNÉE

L'identification du Client BNP Paribas Fortis candidat est effectuée conformément à une procédure documentée appliquée par les PKI@BNPPF RA.

## 3.2. CRÉATION ROUTINIÈRE D'UNE NOUVELLE CLÉ

Un PKI@BNPPF Certificate non révoqué est automatiquement renouvelé par le CA Isabel à l'approche de la fin de sa période de validité.

## 3.3. CRÉATION D'UNE NOUVELLE CLÉ APRÈS RÉVOCATION

Le Sujet d'un PKI@BNPPF Certificate dont le PKI@BNPPF Certificate a été révoqué et qui souhaite demander un nouveau PKI@BNPPF Certificate doit recommencer à nouveau le processus de PKI@BNPPF Certificate entier et se faire authentifier.

Une nouvelle PKI@BNPPF Secure Signing Card est alors émise et délivrée au Souscripteur.

## 3.4. DEMANDE DE RÉVOCATION

Pour demander la révocation de leur PKI@BNPPF Certificate, les Clients BNP Paribas Fortis doivent faire appel au PKI@BNPPF RA. Si celui-ci est indisponible, ils peuvent contacter le service de révocation Card Stop.

### 3.4.1. AUTHENTIFICATION PAR LE PKI@BNPPF REVOCATION SERVICE PKI@BNPPF REVOCATION SERVICE

Pour générer une demande de révocation, le PKI@BNPPF revocation service doit identifier et authentifier le Sujet. Un formulaire complété à la main devra être utilisé pour l'authentification.

PKI@BNPPF revocation service La PKI@BNPPF Registration Authority génère une demande de révocation basée sur les informations fournies sur papier par le Sujet.

### 3.4.2. AUTHENTIFICATION PAR LE PKI@BNPPF REVOCATION SERVICE PKI@BNPPF REGISTRATION AUTHORITY

La fonction de PKI@BNPPF Registration Authority est assurée par les Operations Teams de BNP Paribas Fortis.

La PKI@BNPPF Registration Authority génère une demande de révocation basée sur les informations fournies sur papier par le Sujet.

### 3.4.3. AUTHENTIFICATION PAR LE SERVICE DE RÉVOCATION CARD STOP

Le service de révocation Card Stop ne doit être utilisé qu'en cas d'indisponibilité de la PKI@BNPPF Registration Authority. Le service de révocation Card Stop est dirigé par :

**Card Stop**

**Tél. : +32 (0)70/344.344**

**Fax: +32 (0)70/344.355**

Le service de révocation Card Stop génère une demande de révocation basée sur les informations que le Sujet transmet par téléphone.

Une confirmation écrite doit ensuite être effectuée à titre d'authentification et de confirmation. Cela n'empêche pas la publication de la CRL mise à jour.

### 3.4.4. AUTHENTIFICATION PAR LE CA ISABEL

Le CA Isabel authentifie les demandes de révocation sur la base d'une signature numérique générée à partir de la Clé privée du PKI@BNPPF RA et vérifiée grâce au certificat du PKI@BNPPF RA.

# 4. EXIGENCES OPÉRATIONNELLES

## 4.1. DEMANDE DE CERTIFICAT

Les PKI@BNPPF RA agissent lors d'une demande de certificat, pour valider l'identité du demandeur. Ensuite, le PKI@BNPPF RA approuve ou rejette la demande de certificat. Cette approbation ou ce rejet ne doit pas nécessairement être justifié auprès du demandeur ou d'une autre partie.

Le PKI@BNPPF RA utilise des procédures documentées et adopte ses propres pratiques.

Le CA Isabel traite de manière sécurisée les demandes de PKI@BNPPF Certificate émises par les PKI@BNPPF RA sous son contrôle et les publie conformément à la section « 2.6.2 – Fréquence de publication ». Le CA Isabel n'accepte que les demandes de PKI@BNPPF Certificate émanant de PKI@BNPPF RA formellement approuvés.

Le CA Isabel rejette toute demande de certificat ne respectant visiblement pas l'ensemble des dispositions de la présente PKI@BNPPF CP.

## 4.2. DÉLIVRANCE DES CERTIFICATS

Une fois la demande de certificat validée et approuvée, le PKI@BNPPF RA envoie au CA Isabel une demande de délivrance de certificat.

Les demandes émanant des PKI@BNPPF RA sont approuvées pour autant qu'elles soient valides et qu'elles contiennent des données valides sur le Souscripteur, formatées conformément aux spécifications du CA Isabel.

Les PKI@BNPPF Certificates émis sont délivrés au Sujet. Le Sujet reçoit sa PKI@BNPPF Secure Signing Card et est invité à télécharger son propres PKI@BNPPF Certificate à partir du registre d'Isabel.

## 4.3. ACCEPTATION DU CERTIFICAT

Le CA Isabel doit obtenir l'acceptation du PKI@BNPPF Certificate par le Sujet du PKI@BNPPF Certificate.

L'acceptation du PKI@BNPPF Certificate se fait (1) par notification d'acceptation explicite, (2) en utilisant le PKI@BNPPF Certificate, ou (3) automatiquement après le 10e jour suivant la publication au registre, sans notification de remarques par le Sujet.

En téléchargeant son PKI@BNPPF Certificate, le Sujet installe et accepte également le certificat auto-signé du CA Isabel.

## 4.4. SUSPENSION ET RÉVOCATION DU CERTIFICAT

### 4.4.1. CIRCONSTANCES DE RÉVOCATION

La révocation d'un PKI@BNPPF Certificate consiste à mettre fin, de manière permanente, à la période d'activité de ce certificat avant la fin de sa période de validité établie. Le CA Isabel révoque un certificat numérique :

- en cas de perte, de vol, de modification, de divulgation non autorisée ou d'autre mise en péril de la Clé privée associée au certificat numérique ;
- en cas de manquement du Souscripteur, du Sujet, d'Isabel ou de BNP Paribas Fortis à une de ses obligations matérielles au titre de la présente PKI@BNPPF CP ;
- en cas de retard ou d'empêchement d'exécution des obligations du Souscripteur, d'Isabel ou de BNP Paribas Fortis au titre de la présente PKI@BNPPF CP en raison d'une catastrophe naturelle, d'une panne informatique ou de communication ou de toute autre cause échappant au contrôle raisonnable de la personne menaçant ou mettant matériellement en péril les informations d'une autre personne ;
- lorsqu'Isabel ou BNP Paribas Fortis reçoit une ordonnance légale et contraignante d'une instance gouvernementale ou réglementaire l'invitant à révoquer le PKI@BNPPF Certificate ;
- en cas de modification des informations relatives au Souscripteur figurant dans le PKI@BNPPF Certificate.

### 4.4.2. QUI PEUT DEMANDER UNE RÉVOCATION ?

La révocation du PKI@BNPPF Certificate d'un Sujet personne physique ou d'un Sujet fonction peut être demandée par :

- la personne physique identifiée dans le PKI@BNPPF Certificate d'un Sujet personne physique ;
- la personne physique représentant un certificat PKI@BNPPF Certificate de fonction ;
- toute personne physique habilitée par un Client demander BNP Paribas Fortis à demander la révocation des PKI@BNPPF Certificates de son Sujet.
- le PKI@BNPPF RA ;
- le CA Isabel ayant délivré le certificat.

### 4.4.3. PROCÉDURE DE DEMANDE DE RÉVOCATION

Le CA Isabel traite de manière sécurisée les demandes de révocation d'un PKI@BNPPF Certificate émises par les PKI@BNPPF RA sous son contrôle et publie la révocation conformément à la section « 2.6.2 – Fréquence de publication ».

### 4.4.4. PÉRIODE DE GRÂCE POUR LES DEMANDES DE RÉVOCATION

Aucune période de grâce n'est accordée.

### 4.4.5. MOTIFS DE SUSPENSION

Aucune disposition

### 4.4.6. QUI PEUT DEMANDER UNE SUSPENSION ?

Aucune disposition

### 4.4.7. PROCÉDURE DE DEMANDE DE SUSPENSION

Aucune disposition

### 4.4.8. LIMITES DE LA PÉRIODE DE SUSPENSION

Aucune disposition

### 4.4.9. FRÉQUENCE DES PUBLICATIONS DES CRL

La Liste des révocations de certificats est publiée conformément à la section « 2.6.2 – Fréquence de publication » après la révocation d'un PKI@BNPPF Certificate.

### 4.4.10. OBLIGATIONS DE CONTRÔLE DES CRL

Aucune disposition

### 4.4.11. DISPONIBILITÉ D'UNE FONCTION DE SUIVI EN LIGNE DU STATUT/DE LA RÉVOCATION

Le CA Isabel propose un service de suivi en ligne du statut/de la révocation.

### 4.4.12. EXIGENCES CONCERNANT LE SUIVI EN LIGNE DE LA RÉVOCATION

Le service de suivi en ligne de la révocation fourni des informations sur le statut de la révocation sur la base de la dernière CRL publiée.

### 4.4.13. AUTRES FORMES D'ANNONCES DE RÉVOCATION DISPONIBLES

Aucune disposition.

### 4.4.14. VÉRIFICATION DES EXIGENCES RELATIVES AUX AUTRES FORMES D'ANNONCES DE RÉVOCATION

Aucune disposition.

### 4.4.15. EXIGENCES SPÉCIALES CONCERNANT LA MISE EN PÉRIL DE LA CLÉ

Aucune disposition.

## 4.5. PROCÉDURES D'AUDIT SUR LA SÉCURITÉ

La procédure d'audit sur la sécurité doit se conformer aux dispositions de la section « 2.7 – Audit de conformité ».

### 4.5.1. TYPES DE DONNÉES ENREGISTRÉES

Le CA Isabel et les PKI@BNPPF RA enregistrent dans des journaux d'audit l'ensemble des évènements se rapportant à un PKI@BNPPF Certificate donné. Ces évènements sont enregistrés pendant une période de dix ans, notamment afin de fournir des preuves de la certification ou de la révocation dans le cadre de procédures judiciaires. Voir également réf. [2] à la section 9.2 – Annexe B – Références de la présente CP, pour les exigences des règlementations nationales belges en matière d'enregistrement des évènements.

Les évènements relatifs aux principales activités de gestion des certificats, des clés et de l'environnement du CA sont enregistrés, notamment :

- l'ensemble des évènements relatifs au cycle de vie des clés du CA ;
- l'ensemble des évènements relatifs au cycle de vie desPKI@BNPPF Certificates ;
- l'ensemble des évènements relatifs à la préparation d'une PKI@BNPPF Secure Signing Card ;
- l'ensemble des demandes et rapports relatifs à une révocation, ainsi qu'aux actions prises en conséquence ;

Le CA Isabel garantit que l'ensemble des évènements d'enregistrement, y compris les demandes de PKI@BNPPF Certificates, de renouvellement des clés de ces certificats ou de renouvellement des certificats sont enregistrés, et notamment :

- les documents présentés par le Souscripteur du PKI@BNPPF Certificate au PKI@BNPPF RA afin d'appuyer l'enregistrement conformément à l'accord conclu entre le PKI@BNPPF RA et le Client de BNP Paribas Fortis ;
- l'endroit où sont conservées les copies des documents d'identification, y compris la demande de PKI@BNPPF Certificate signée ;
- tout choix spécifique figurant dans la demande du Souscripteur ;
- l'identité du Client de BNP Paribas Fortisacceptant la demande de PKI@BNPPF Certificate ;
- le cas échéant, la méthode utilisée pour valider les documents d'identification ;
- le nom du CA récepteur et/ou du RA émetteur, le cas échéant.

les détails des événements et les données à enregistrer sont documentés en tant que procédures internes d'Isabel.

### 4.5.2. FRÉQUENCE DES JOURNAUX

Le CA Isabel permet d'effectuer des journaux d'audit sur la revue du personnel régulièrement, au moins chaque semaine.

### 4.5.3. PÉRIODE DE CONSERVATION DES JOURNAUX D'AUDIT

Toutes les informations relatives aux PKI@BNPPF Certificates sont archivées pendant au moins 10 ans.

### 4.5.4. PROTECTION DES JOURNAUX D'AUDIT

La confidentialité et l'intégrité des évènements archivés et actuels concernant les PKI@BNPPF Certificates doivent être garanties.

### 4.5.5. PROCÉDURES DE SAUVEGARDE DES JOURNAUX D'AUDIT

Isabel veille à ce que les journaux d'audit soient régulièrement sauvegardés.

### 4.5.6. SYSTÈME DE COLLECTE D'AUDITS (INTERNE/EXTERNE)

Le système de collecte d'audits est interne au système du CA Isabel et à BNP Paribas Fortis.

### 4.5.7. NOTIFICATION AU SUJET AYANT DÉCLENCHÉ L'ÉVÈNEMENT

Aucune disposition.

### 4.5.8. ÉVALUATIONS DE LA VULNÉRABILITÉ

Des audits de sécurité des systèmes et procédures du CA Isabel et de BNP Paribas Fortis sont régulièrement effectués conformément aux politiques internes du système du CA Isabel.

## 4.6. ARCHIVAGE DES DOSSIERS

### 4.6.1. TYPES D'ÉVÈNEMENTS ENREGISTRÉS

Les éléments suivants sont archivés :

- PKI@BNPPF Certificates
- la liste des révocations de certificats d'Isabel ;
- PKI@BNPPF Certificate Policy
- l'ensemble des évènements et demandes entraînant des modifications aux PKI@BNPPF Certificates et à la liste des révocations de certificats.

### 4.6.2. PÉRIODE DE CONSERVATION DES ARCHIVES

Toutes les informations relatives aux PKI@BNPPF Certificates sont archivées pendant au moins 10 ans.

### 4.6.3. PROTECTION DES ARCHIVES

Les archives papier et électroniques sont protégées par des mécanismes de contrôle physique et logique des accès afin d'empêcher les accès non autorisés. Les archives sont protégées contre les menaces environnementales comme la température, le feu, les dégâts des eaux, l'humidité et le magnétisme.

### 4.6.4. PROCÉDURES DE SAUVEGARDE DES ARCHIVES

Afin de garantir leur disponibilité, il existe de multiples copies des archives.

Les archives sont régulièrement réinscrites sur des médias à la pointe de la technologie afin d'assurer la période de conservation et d'éviter les infrastructures de médias obsolètes.

### 4.6.5. EXIGENCES EN MATIÈRE D'HORODATAGE DES ARCHIVES

Les informations archivées sont signées numériquement et horodatées.

### 4.6.6. SYSTÈME DE COLLECTE DES ARCHIVES (INTERNE OU EXTERNE)

Le système de collecte des archives est interne au système du CA Isabel.

### 4.6.7. PROCÉDURES D'OBTENTION ET DE VÉRIFICATION DES INFORMATIONS DES ARCHIVES

Le PKI@BNPPF Certificate Sujet dispose d'un accès aux informations archivées le concernant, sans mettre en péril les obligations générales de confidentialité du CA Isabel et des PKI@BNPPF RA. Toute demande visant à obtenir des informations archivées doit être adressée par écrit au Security Manager de BNP Paribas Fortis.

Les informations des archives doivent être régulièrement contrôlées pour assurer la disponibilité des informations archivées pendant la période de conservation.

## 4.7. CHANGEMENT DE CLÉ

Le CA Isabel veille à ce que ses clés de signature privées ne soient pas utilisées au-delà de leur cycle de vie. Lorsqu'une clé privée du CA Isabel arrive en fin de vie, son certificat est révoqué.

## 4.8. PLAN DE REPRISE APRÈS MISE EN PÉRIL OU SINISTRE

Le CA Isabel a mis en place des politiques et des procédures permettant aux activités de reprendre le plus tôt possible en cas de sinistre, et notamment de mise en péril d'une clé de signature privée du CA.

Pas d'autre disposition.

## 4.9. DISSOLUTION DU CA/RA

En cas de cessation des activités du CA pour quelque raison que ce soit, Isabel avertit en temps opportun les entités prenant la suite et leur transfère les responsabilités, assure la maintenance des registres et les réparations en accord avec BNP Paribas Fortis pour l'ensemble des activités liées au PKI@BNPPF Certificate.

En cas de cessation des activités d'un CA Isabel, Isabel agit conformément à la législation nationale belge ; voir réf. [2] à la section 9.2 – Annexe B – Références de la présente CP.

En cas de cessation des activités d'un PKI@BNPPF RA, BNP Paribas Fortis avertit en temps utile le CA Isabel.

# 5. CONTRÔLES DE SÉCURITÉ PHYSIQUES, PROCÉDURAUX ET PERSONNELS

## 5.1. CONTRÔLES PHYSIQUES

Aucune disposition.

## 5.2. CONTRÔLES PROCÉDURAUX

### 5.2.1. RÔLES DE CONFIANCE

Le CA Isabel exige que les rôles définis aux sections ci-après soient assurés par du personnel de confiance.

#### 5.2.1.1. OPÉRATEURS CA

Ces personnes assumeront le rôle d'opérateurs du système du CA Isabel en utilisant le poste de travail CA sous double contrôle. Il y aura deux groupes d'opérateurs CA.

#### 5.2.1.2. ADMINISTRATEURS DU SYSTÈME DU CA

Ces personnes gèrent le système du CA Isabel en utilisant la console.

#### 5.2.1.3. AGENTS DE SÉCURITÉ CA

Ces personnes mettent en œuvre les politiques du CA, assurent le respect de la PKI@BNPPF CP et vérifient les journaux d'audit.

### 5.2.2. NOMBRE DE PERSONNES REQUISES PAR TÂCHE

Aucune disposition.

### 5.2.3. IDENTIFICATION ET AUTHENTIFICATION POUR CHAQUE RÔLE

Les représentants de chaque rôle de confiance sont authentifiés au moyen d'une signature numérique générée à l'aide de leur Clé privée insérée dans une carte à puce.

## 5.3. CONTRÔLES DU PERSONNEL

Les contrôles du personnel sont effectués conformément aux politiques internes d'Isabel et de BNP Paribas Fortis.

# 6. CONTRÔLES DE SÉCURITÉ TECHNIQUES

## 6.1. GÉNÉRATION ET INSTALLATION DE PAIRS DE CLÉS

Le CA Isabel utilise pour l'exécution des tâches de gestion des clés du CA des dispositifs cryptographiques adéquats. Ces dispositifs cryptographiques sont appelés « Hardware Security Modules » (HSM).

Ces dispositifs répondent aux exigences formelles, ce qui garantit notamment la détection immédiate des falsifications du dispositif ; en outre, les clés privées ne peuvent quitter le dispositif avant d'avoir été cryptées. Les mécanismes matériels et logiciels protégeant les clés privées du CA sont documentés.

### 6.1.1. GÉNÉRATION DE PAIRES DE CLÉS

Le CA Isabel génère de manière sécurisée et protège lui-même ses clés privées à l'aide d'un système fiable. Il prend les précautions nécessaires pour empêcher la mise en péril ou l'utilisation non autorisée de ce système.

La génération de la paire de clés du Sujet de BNP Paribas Fortis est effectuée au niveau central par le CA Isabel à l'aide d'un système fiable et sur la base d'une procédure documentée.

Le CA Isabel doit garantir le caractère unique des paires de clés au sein de l'infrastructure PKI.

### 6.1.2. DÉLIVRANCE DES CLÉS PRIVÉS AUX ENTITÉS

Le CA Isabel délivre au Sujet de BNP Paribas Fortis sa clé privée sur une PKI@BNPPF Secure Signing Card reliée à laPKI@BNPPF RA branche locale du PKI@BNPPF Certificate Souscripteur.

Le CA Isabel livre de manière sécurisée les données d'activation de la PKI@BNPPF Secure Signing Card directement au Sujet s'il s'agit d'une personne physique et au Souscripteur si le Sujet est une fonction.

La PKI@BNPPF Secure Signing Cardet le code PIN correspondant ne peuvent *jamais* se trouver au même endroit en même temps, sauf lorsque le Souscripteur de BNP Paribas Fortis vient d'aller chercher la PKI@BNPPF Secure Signing Card.

### 6.1.3. DÉLIVRANCE DE LA CLÉ PUBLIQUE À L'ÉMETTEUR DU CERTIFICAT

Les paires de clés du Sujet de BNP Paribas Fortis sont générées au niveau central à l'aide d'un « Générateur de clé » basé sur un système fiable. La clé publique est délivrée au CA via un message électronique, garantissant ainsi son intégrité et sa provenance (générée au niveau interne chez le CA Isabel)

### 6.1.4. DÉLIVRANCE DE LA CLÉ PUBLIQUE DU CA AUX UTILISATEURS

La clé publique du CA Isabel est publiée dans le référentiel Isabel. Ce référentiel est accessible aux entités en mode lecture 24h/24 et 7j/7.

### 6.1.5. TAILLES DES CLÉS

La taille de la clé publique (modulus n), certifiée par un PKI@BNPPF Certificate et associée à une PKI@BNPPF Secure Signing Card, doit être d'au moins 1 024 octets.

La taille des clés du CA Isabel doit être d'au moins 2 048 octets.

### 6.1.6. GÉNÉRATION DES PARAMÈTRES DES CLÉS PUBLIQUES

Le processus de génération de clés d'Isabel constitue une information propre à Isabel.

Le processus de génération a été soumis à un audit qualité.

La qualité des paramètres des processus de génération est contrôlée en permanence.

### 6.1.7. CONTRÔLE DE LA QUALITÉ DES PARAMÈTRES

Le CA d'Isabel utilise un système informatique de contrôle des composants de la génération des clés.

### 6.1.8. GÉNÉRATION DE CLÉS MATÉRIELLE/LOGICIELLE

Le CA Isabel utilise un composant de génération matérielle des clés afin d'assurer un niveau de sécurité au moins aussi élevé que la PKI@BNPPF Secure Signing Card qui abritera la clé privée une fois celle-ci générée.

### 6.1.9. FINALITÉS DE L'UTILISATION DES CLÉS (D'APRÈS LE CHAMP «UTILISATION DE LA CLÉ» X.509 V3)

L'utilisation des certificats par les entités finales est limité grâce à l'utilisation d'extensions de certificats sur l'utilisation et l'utilisation prolongée des clés. Toute utilisation du certificat qui serait incohérente avec ces extensions est interdite.

## 6.2. PROTECTION DE LA CLÉ PRIVÉE

Isabel supporte l'utilisation de dispositifs sécurisés et de matériel anti-falsification afin de délivrer, gérer et conserver les certificats en toute sécurité. Isabel utilise du matériel informatique fiable et accrédité afin d'éviter la mise en péril de sa clé privée.

### 6.2.1. NORMES POUR LE MODULE CRYPTOGRAPHIQUE

La Clé privée du Sujet PKI@BNPPF Certificate est insérée dans une PKI@BNPPF Secure Signing Card, évaluée EAL 4+.

### 6.2.2. CLÉ PRIVÉE (N SUR M) CONTRÔLE MULTI-PERSONNES

Les clés privées du CA sont soumises à un triple contrôle.

BNP Paribas FortisLes clés privées du Souscripteur doivent être sous le contrôle exclusif du Souscripteur de BNP Paribas Fortis.

### 6.2.3. BLOCAGE DES CLÉS PRIVÉES

Les Clés privées du CA Isabel ne sont pas bloquées.

La Clé privée des Souscripteurs BNP Paribas Fortis n'est pas bloquée.

### 6.2.4. SAUVEGARDE DES CLÉS PRIVÉES

Les Clés privées du CA Isabel sont sauvegardées.

La Clé privée des Souscripteurs BNP Paribas Fortis ne doit pas être sauvegardée.

### 6.2.5. ARCHIVAGE DES CLÉS PRIVÉES

Les Clés privées des Souscripteurs BNP Paribas Fortis ne sont pas archivées.

### 6.2.6. INSERTION DE LA CLÉ PRIVÉE DANS UN MODULE CRYPTOGRAPHIQUE

Les Clés privées du CA Isabel sont chargées dans le module cryptographique de manière sécurisée.

### 6.2.7. MÉTHODE D'ACTIVATION DE LA CLÉ PRIVÉE

Les Clés privées du CA Isabel sont protégées par un code PIN ou un mot de passe.

### 6.2.8. MÉTHODE DE DÉSACTIVATION DE LA CLÉ PRIVÉE

Les Clés privées du CA Isabelle sont désactivées en débranchant le matériel.

Les Clés privées BNP Paribas Fortis sont désactivées en retirant la PKI@BNPPF Secure Signing Card du lecteur de cartes.

### 6.2.9. MÉTHODE DE DESTRUCTION DE LA CLÉ PRIVÉE

Les Clés privées du CA Isabel sont détruites de manière sécurisée lorsque la clé n'est plus utilisée par le CA Isabel.

Les Clés privées des Souscripteurs BNP Paribas Fortis sont détruites en même temps que la PKI@BNPPF Secure Signing Card.

## 6.3. AUTRES ASPECTS DE LA GESTION DES PAIRES DE CLÉS

### 6.3.1. ARCHIVAGE DES CLÉS PUBLIQUES

Les PKI@BNPPF Certificates et, par conséquent, la Clé publique qu'ils certifient, doivent être archivés pendant au moins 10 ans.

### 6.3.2. PÉRIODES D'UTILISATION DES CLÉS PUBLIQUES ET PRIVÉES

Aucune disposition.

## 6.4. DONNÉES D'ACTIVATION

La génération des données d'activation du Sujet de BNP Paribas Fortis consistant en un code PIN initial pour la PKI@BNPPF Secure Signing Card, est effectuée au niveau central par le CA Isabel. Le CA Isabel garantit la transmission sécurisée du code PIn initial au Souscripteur de BNP Paribas Fortis. Une fois la délivrance effectuée, le Sujet est tenu de garantir la confidentialité de son code PIN. Isabel ne sauvegarde pas, ne bloque pas et n'archive pas les codes PIN initiaux des Sujets.

### 6.4.1. GÉNÉRATION ET INSTALLATION DES DONNÉES D'ACTIVATION

La génération du code PIN initial du Sujet BNP Paribas Fortis et la transmission de ce code au Sujet se font de manière sécurisée. À aucun moment la Clé privée, c.-à-d. la PKI@BNPPF Secure Signing Card, et son code PIN initial ne peuvent se trouver au même endroit, excepté immédiatement après avoir été retirés par le Client de BNP Paribas Fortis.

Pendant l'installation, le Souscripteur de BNP Paribas Fortis est invité à modifier son code PIN initial assigné par le CA Isabel en le remplaçant par le code PIN de son choix.

### 6.4.2. PROTECTION DES DONNÉES D'ACTIVATION

Le code PIN est protégé, au niveau de sa confidentialité et de son intégrité, jusqu'à sa délivrance et son acceptation par le Souscripteur du PKI@BNPPF Certificate.

### 6.4.3. AUTRES ASPECTS RELATIFS AUX DONNÉES D'ACTIVATION

Aucune disposition

## 6.5. CONTRÔLES DE SÉCURITÉ INFORMATIQUES

Les contrôles techniques de sécurité informatique sont mis en œuvre conformément aux politiques internes d'Isabel pour le CA Isabel et de BNP Paribas Fortis pour les PKI@BNPPF RA.

## 6.6. CONTRÔLES TECHNIQUES DU CYCLE DE VIE

Les contrôles techniques du cycle de vie sont mis en œuvre conformément aux politiques internes d'Isabel pour le CA Isabel et deBNP Paribas Fortis pour lesPKI@BNPPF RA.

## 6.7. CONTRÔLES DE SÉCURITÉ DU RÉSEAU

Les contrôles de sécurité du réseau sont mis en œuvre conformément aux politiques internes d'Isabel pour le CA Isabel et de BNP Paribas Fortis pour les PKI@BNPPF RA.

## 6.8. CONTRÔLES TECHNIQUES DU MODULE CRYPTOGRAPHIQUE

Aucune disposition.

# 7. Profils du certificat, de la CRL et de l'OCSP

## 7.1. PROFIL DU CERTIFICAT

Le profil d'un PKI@BNPPF Certificate délivré à une personne physique ou à une fonction est le suivant :

| champ de certificat | valeur ou format de la valeur |
|---|---|
| Version | INTEGER {V3(2)}<br>(Note : integer value 2 correspond aux certificats v3) |
| SerialNumber | INTEGER {0..MAX}<br>le format du nombre est yyyydddnnnnn, avec<br>• yyyy = l'année de production du certificat<br>• ddd= le jour de l'année<br>• nnnnn = le nombre séquentiel correspondant à ce jour |
| Signature | *AlgorithIdentifier sha-1WithRSAEncryption*<br>*OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}* |
| Émetteur | *CN = Isabel Certification Authority ; O=CA ; L=ISABEL ; C=BE ;* |
| Validité | *notBefore*=UTCTime<br>*notAfter*=UTCTime |
| subject (Normal) | • champ obligatoire : CN=<br><Nom>+<Prénom>, pour les personnes physiques<br><Nomdefonction>, pour les fonctions<br>• champ obligatoire OU= <User ID><br>• champ obligatoire : OU= <ID technique de l'entité souscriptrice><br>• champ obligatoire : OU= <Code pays ISO de l'entité souscriptrice>+<Numéro d'entreprise de l'entité souscriptrice><br>• champ obligatoire : O= <Nom de l'entité souscriptrice><br>• L= Isabel<br>• C=BE ; |
| subjectPublicKeyInfo | *AlgorithmIdentifier rsaEncryption*<br>*OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1}* |

### 7.1.1. NUMÉRO DE VERSION

Tous les PKI@BNPPF Certificates délivrés par les Autorités de Certification Isabel doivent être conformes à la norme ITU-T X.509 v3. voir réf. [3] à la section «9.2 – Annexe B - Références » de la présente PKI@BNPPF CP.

### 7.1.2. EXTENSIONS DE CERTIFICATS

Ls extensions définies pour les certificats X.509v3 fournissent des méthodes permettant d'associer d'autres attributs aux Utilisateurs ou Clés publiques ainsi que de gérer la hiérarchie des certificats. Ce champ ne peut apparaître qu'avec la version 3. Ce champ est une séquence d'une ou plusieurs extensions de certificat.

Une application DOIT rejeter le certificat si elle rencontre une extension critique qu'elle ne reconnaît pas ; toutefois, une extension non-critique peut être ignorée si elle n'est pas reconnue.

Voici la liste des extensions de certificats standard (tels que définies dans la norme ITU-T X.509) utilisées dans les certificats Isabel délivrés par les Autorités de Certification Isabel, ainsi qu'une description de leur utilisation, en indiquant notamment si ces extensions sont critiques (C) ou non-critiques (NC).

Pour une description plus complète de ces extensions de certificats; voir la norme ITU-T X.509v3.

Le tableau ci-après reprend les extensions OBLIGATOIRES ainsi que leur valeur pour un PKI@BNPPF Certificate délivré à une personne physique ou à une fonction :

| Champ d'extension du certificat | Criticité | valeur ou format de la valeur |
|---|---|---|
| authorityKeyIdentifier | NC | Ce champ identifie la clé publique du CA à utiliser pour vérifier la signature appliquée sur les certificats.<br>OCTET STRING ::= {4341 3032} (“CA02”) |
| subjectPublicKeyInfo OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) allocation per country (16) Belgium(56) Isabel(1) 8.1} | NC | Ce champ est une extension propre à Isabel.<br>*Pour usage interne uniquement.* |
| subjectContractInfo OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) allocation per country (16) Belgium(56) Isabel(1) 8.2} | NC | Ce champ représente le type de contrat d'Isabel-BNP Paribas Fortis : « PKI@BNPPF »<br>*Pour usage interne uniquement.* |
| SerialNumber (OID 2.5.4.5) | NC | Ce champ représente l'identifiant de la PKI@BNPPF Secure Signing Card (CardID). |
| KeyUsage | NC | Ce champ donne une liste des utilisations autorisées pour la clé.<br>BIT STRING ::= {digitalSignature(0), nonRepudiation(1), keyEncipherment(2), dataEncipherment(3)} |

| Champ d'extension du certificat | Criticité | valeur ou format de la valeur |
|---|---|---|
| CertificatePolicies | NC | Ce champ contient une séquence d'un ou plusieurs termes d'informations sur la politique, consistant chacun en un identificateur d'objet (OID) et en qualificateurs optionnels. Ces termes d'information sur la politique indiquent la politique aux termes de laquelle le certificat a été délivré et les fins auxquelles il peut être utilisé.<br>Il possède la valeur {joint-iso-ccitt(2) allocation per country (16) Belgium (56) Isabel (1) certification-policies(9) policy-specification(…)}, qui correspond à la présente PKI@BNPPF CP: 2.16.56.1.9.48.1.1<br>Ce champ contient également un attribut représentant un URI de la version complète de la PKI@BNPPF CP renvoyant au site web Easy Banking Business de BNP Paribas Fortis |
| ExtKeyUsage | NC | Ce champ propose d'autres utilisations acceptables de la clé. Il s'agit d'une liste d'OID.<br>KeyPurposeID ::= {id-kp-clientAuth, id-kp-emailProtection} |
| AuthorityInfoAccess | NC | Ce champ redirige vers un service de suivi en ligne du statut de révocation d'un certificat.<br>Sa valeur est : https://pki.isabel.be/ocsp |

### 7.1.3. IDENTIFICATEURS D'OBJETS D'ALGORITHMES

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

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

### 7.1.4. FORMES DE NOM

| Entité | Forme de nom |
|---|---|
| PKI@BNPPF Certificate du Sujet ; | *Voir plus haut.* |
| Autorité de Certification Isabel | *CN = Isabel Certification Authority ; O=CA ; L=ISABEL ; C=BE ;* |

Aucune adresse e-mail, ni les noms qu'elle contient, figurant dans le PKI@BNPPF Certificate ne peut être considérée comme un élément d'identification sur la base duquel lePKI@BNPPF Certificate est délivré.

### 7.1.5. NAME CONSTRAINTS

L'extension Name Constraint n'est pas utilisée dans un PKI@BNPPF Certificate.

### 7.1.6. IDENTIFICATEUR D'OBJET DES POLITIQUES DE CERTIFICATION

Voir Section 1.2 – Identification de la présentePKI@BNPPF Certificate Policy.

### 7.1.7. UTILISATION DE L'EXTENSION POLICY CONSTRAINTS

L'extension Policy Constraint n'est pas utilisée dans un PKI@BNPPF Certificate.

### 7.1.8. SYNTAXE ET SÉMANTIQUE DES QUALIFICATEURS DE POLITIQUE

Un qualificateur de police est défini pour la politique de certification définie dans l'extension des politiques de certification.

Ce qualificateur est un URI de la version complète de la PKI@BNPPF Certificate Policy renvoyant au site web Easy Banking Business de BNP Paribas Fortis.

### 7.1.9. TRAITEMENT DE LA SÉMANTIQUE POUR LES EXTENSIONS CRITIQUE DE POLITIQUES DE CERTIFICATION

L'extension de politiques de certification est indiquée comme étant non-critique, voir 7.1.2.

## 7.2. PROFIL DES CRL

Pour les besoins de BNP Paribas Fortis, la CRL est conservée au niveau interne ; l'OCSP est le moyen privilégié à disposition des Clients de BNP Paribas Fortis pour les informations sur la validation.

## 7.3. PROFIL OCSP

Le CA Isabel maintient un registre du profil OCSP qu'elle utilise en tant que document technique interne. Ce document sera disponible à la discrétion du CA Isabel.

# 8. ADMINISTRATION DES SPÉCIFICATIONS

## 8.1. PROCÉDURES DE CHANGEMENT DES SPÉCIFICATIONS

Les commentaires, questions et demandes de changements visant la présente PKI@BNPPF CP doivent être adressés à la Policy Authority indiquée à la section « 1.3.7 – Coordonnées » de la présente PKI@BNPPF CP.

BNP Paribas FortisBNP Paribas Fortis peut modifier à tout moment la présente PKI@BNPPF CP.

## 8.2. POLITIQUES EN MATIÈRE DE PUBLICATION ET DE NOTIFICATION

La présente PKI@BNPPF Certificate Policy est placée sous le contrôle direct de la Policy Authority, voir « 1.3.5 – Policy Authorities ». La haute direction de BNP Paribas Fortis s'engage à veiller à ce que les pratiques décrites dans la présente PKI@BNPPF CP soient correctement mises en œuvre.

Afin de tenir compte de l'évolution des circonstances, de la législation, des technologies et des risques de sécurité, la Policy Authority réexamine régulièrement la présente PKI@BNPPF Certificate Policy .

Elle formule des recommandations de modifications de la présente PKI@BNPPF Certificate Policy, qui seront soumises à un processus de consultation au sein de BNP Paribas Fortis ainsi qu'à l'autorisation du Directeur général « Multichannel Banking » avant que toute modification ne soit apportée.

La présente PKI@BNPPF Certificate Policy et ses versions ultérieures sont publiées sur site web Easy Banking Business de BNP Paribas Fortis. La date de publication et la date d'entrée en vigueur de la présente PKI@BNPPF Certificate Policy, ainsi que son numéro de version, seront indiqués sur sa page de garde. La version publiée sur cette adresse URL est la seule version valide pendant toute la durée de la publication.

Les notifications ayant trait à la présente PKI@BNPPF Certificate Policy seront également publiées à l'adresse URL susmentionnée.

L'utilisation prolongée d'un PKI@BNPPF Certificate après la publication d'une nouvelle version de la PKI@BNPPF Certificate Policy suppose l'acceptation de cette nouvelle version par le Sujet.

La dernière version de la présente PKI@BNPPF CP sera disponible en ligne. Les versions antérieures sont archivées par BNP Paribas Fortis.

## 8.3. PKI@BNPPF CERTIFICATE POLICY PROCÉDURES D'APPROBATION DE LA PKI@BNPPF CERTIFICATE POLICY

La Policy Authority pour la présente PKI@BNPPF Certificate Policy et le Directeur Général « Multichannel Banking » doivent approuver les modifications apportées au présent document.

# 9. Annexes

## 9.1. ANNEXE A – DÉFINITIONS

### 9.1.1. ACRONYMES

| Acronyme | Description |
|---|---|
| CA | Autorité de Certification |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Liste des révocations de certificats |
| HSM | Module informatique « Security » |
| OCSP | Online Certificate Status Protocol |
| OID | Identificateur d'objet |
| PIN | Numéro d'identification personnel |
| PKI | Public Key Infrastructure |
| RA | Registration Authority |
| URI | Identificateur de ressources uniformes |
| URL | Localisateur de ressources uniformes |

## 9.1.2. LEXIQUE

| Terme | Description |
|---|---|
| Données d'activation | Toute donnée utilisée pour protéger la Clé privée : p.ex. mot de passe, code PIN, etc.<br>Dans le cadre des PKI@BNPPF Certificates, les données d'activation consistent en un code PIN initial envoyé au Souscripteur au moment de la création de sa PKI@BNPPF Secure Signing Card et qu'il doit modifier lors de sa première utilisation. |
| Authentification | Processus consistant à établir l'identité d'une personne sur la base d'une preuve fiable. |
| BNP Paribas Fortis | Fortis Bank SA/NV, Montagne du Parc 3, 1000 Bruxelles – Belgique, ayant son siège social à Bruxelles, RPM/RPR no BE0403.199.702. |
| PKI@BNPPF Certificate | Certificat numérique délivré par un CA Isabel à un Souscripteur du PKI@BNPPF Certificate. |
| PKI@BNPPF Certificate de la Partie Utilisatrice ; | Une Partie Utilisatrice du PKI@BNPPF Certificate est une personne physique ou une fonction étant, le Client de BNP Paribas Fortis, ou appartenant à celui-ci, et faisant usage des informations contenues dans un PKI@BNPPF Certificate, et/ou des signatures numériques vérifiées au moyen de ce certificat et/ou de toute autre information publiée par un CA Isabel délivrant desPKI@BNPPF Certificates. |
| PKI@BNPPF Certificate Demande | Soumission d'une demande de PKI@BNPPF Certificate validée par un PKI@BNPPF RA à un CA Isabel afin que celui-ci délivre un PKI@BNPPF Certificate. PKI@BNPPF Certificate |
| PKI@BNPPF Certificate du Sujet ; | Une personne physique ou une fonction (p.ex. « comptable ») identifiée dans un certificat comme étant le détenteur de la Clé privée associée à la Clé publique donnée dans le certificat.<br>Le Sujet du PKI@BNPPF Certificate s'est vu délivrer un PKI@BNPPF Certificate dans le cadre de ses activités et décrypte et/ou signe au moyen de la Clé privée associée à ce PKI@BNPPF Certificate au nom du Client de BNP Paribas Fortis auquel il appartient.<br>Le Sujet d'un PKI@BNPPF Certificate est représenté par :<br>- s'il s'agit d'un Sujet-personne physique : le Sujet est représenté par la personne physique identifiée dans le certificat.<br>- s'il s'agit d'un Sujet-fonction : le Sujet est représenté par une personne physique habilitée à représenter la fonction identifiée dans le certificat (représentant de fonction). |
| PKI@BNPPF Certificate du souscripteur ; | Une personne physique habilitée par un Client de BNP Paribas Fortis en vue d'introduire une demande de PKI@BNPPF Certificate au nom d'un ou plusieurs Sujets personnes physiques ou fonctions. |
| BNP Paribas Fortis Client | Entité ayant signé un contrat BNP Paribas Fortis avec BNP Paribas Fortis dans l'intention de recevoir des services et/ou des produits de BNP Paribas Fortis. |
| PKI@BNPPF RA | Voir PKI@BNPPF Registration Authority. |
| PKI@BNPPF Registration Authority | RA, nommé par BNP Paribas Fortis, agissant sous l'autorité et le contrôle d'un CA Isabel pour des PKI@BNPPF Certificates. |
| PKI@BNPPF Secure Signing Card | Carte à puce renfermant la Clé privée d'un Sujet et utilisée par ce Sujet pour créer une signature numérique. La signature numérique est créée à l'intérieur de la PKI@BNPPF Secure Signing Card. |

| Terme | Description |
|---|---|
| Certificate Policy | Un ensemble défini de règles indiquant l'applicabilité d'un certificat à une communauté donnée et/ou à une classe d'applications présentant des exigences de sécurité communes. |
| Liste des révocations de certificats | Liste de nombres de certificats révoqués numériquement signés par le CA émetteur. |
| Autorité de Certification | Autorité habilitée par les utilisateurs à délivrer et gérer des certificats. Le CA peut éventuellement créer les paires de clés des utilisateurs. |
| Certification Practice Statement | Déclaration des pratiques employées par un CA pour délivrer des certificats. |
| Certificat numérique | Clé publique d'un Sujet, accompagnée de l'identité du Sujet et d'autres informations, rendue infalsifiable par chiffrage avec la clé privée du CA ayant délivré le certificat. |
| Autorité de Certification Isabel | CA dirigé par Isabel.<br>Le CA Isabel désigne également l'organisation technique entourant l'Autorité de Certification, dirigée par la société Isabel NV/SA. |
| Isabel | Isabel NV/SA, Boulevard de l'Impératrice 13-15, 1000 Bruxelles – Belgique, ayant son siège social à Bruxelles, RPR/RPM no BE0455.530.509. |
| Registre Isabel | Entité entourant le CA Isabel et assurant la publication des certificats et de la liste des révocations de certificats. |
| Numéro d'identification personnel | Code secret (PIN) utilisé pour empêcher les accès non autorisés à une Clé privée. |
| Policy Authority | Entité responsable de la spécification et de la validation des CP. |
| Clé privée | Élément d'une paire de clés publique/privée devant être gardée secrète et connue uniquement du Sujet. |
| Clé publique | Élément d'une paire de clés publique/privée pouvant être publiquement divulguée ou distribuée sans nuire à la sécurité du système cryptographique. |
| Public Key Infrastructure | Structure constituée de matériel informatique, de logiciels, de personnes, de processus et de politiques employant une technologie de signatures numériques afin de faciliter une association vérifiable entre le composant public d'une Clé publique asymétrique avec un Sujet donné possédant la Clé privée correspondante. |
| Registration Authority | Entité responsable de l'identification et de l'authentification de Sujets d'un certificat, mais qui ne signe ni ne délivre de certificats. Le RA peut participer au processus de demande de certificat, au processus de révocation, ou aux deux, comme indiqués dans la CP applicable. |
| de la Partie Utilisatrice ; | Voir Partie Utilisatrice d'un PKI@BNPPF Certificate. |
| Certificat auto-signé | Certificat signé au moyen de la Clé privée pour laquelle la Clé publique se trouve dans le certificat. Généralement utilisée pour les certificats racines des CA, pour lesquels la clé racine se trouve dans un certificat signé au moyen de la clé privée correspondante. |
| Sujet ; | Voir Sujet d'un PKI@BNPPF Certificate. |
| souscripteur ; | Voir Souscripteur d'un PKI@BNPPF Certificate. |
| Validation Authority | Autorité permettant aux Parties Utilisatrices d'un PKI@BNPPF Certificate d'obtenir des informations sur le statut de la révocation d'un PKI@BNPPF Certificate. |

## 9.2. ANNEXE B - RÉFÉRENCES

| | Titre | Propriétaire | Date |
|---|---|---|---|
| [1] | « Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques » | Parlement européen et Conseil européen | 13 décembre 1999 |
| [2] | « Wet houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische hantekeningen en certificatiediensten » | Parlement belge | 9 juillet 2001 |
| [3] | Recommandation X.509 de l'ITU-T | ITU-T | Juin 1997 |
| [4] | RFC 2527: « Internet X.509 Public Key Infrastructure – CP and Certification Practices Framework » | Internet Engineering Task Force (IETF) | Mars 1999 |
| [5] | Banking – Public Key Infrastructure Policy and Practices framework – ISO/TC68/SC2/WG8 N 001 | Organisation internationale de normalisation | 22 octobre 2002 |