Politique de certification BNP Paribas Fortis

Autorité de certification

BNP Paribas Fortis Customer Ephemeral Certification Authority

itg

Revue		
Nom	Fonction	Date

Validation		
Nom	Fonction	Date
PMA	Instance de gouvernance	13/02/2018
PMA	Instance de gouvernance	12/09/2019

Suivi des versions			
Version	Date	Auteur	Nature des modifications
0.5	17/10/2016	Cédric SZANIEC	Première version d'initialisation
0.6	28/10/2016	Gert FEYT	Modifications suite à la réunion avec Fortis et Signel (21/10) et suite au retour des juristes Fortis.
1.0	09/11/216	Cédric SZANIEC	Version validée par la PMA
1.1	18/2/2017	Cédric SZANIEC	Prise en compte des différentes remarques de Fortis et des consultants
2.0	23/06/2017	Cédric SZANIEC	Changement de Safran I&S vers OT Morpho Adaptation de la PC pour eIDAS EN 319 411 - 1
2.1	25/06/2017	Cédric SZANIEC	Ajout des éléments pour le nouveau canal : Easy Banking Business
2.2	16/01/2018	Cédric SZANIEC	Changement d'OT Morpho vers IDEMIA et d'ITP ITG vers ITG. Correction des écarts de l'audit ETSI EN 319 411-1 : • Ajout du I.C.6 • Modification et clarification du III.A.4, III.A.5 • Précisions du IV.J.1
2.3	03/05/2019	Cédric SZANIEC	Adaptation du III.A.4
3.0	04/07/2019	Ibrahima TAMBOURA	Revue annuelle avec IDEMIA Prise en compte des modifications BNP Paribas Fortis : Intégration de multiméthodes d'enregistrement et multiméthodes d'authentification et autorisation : • Modification du I.C.1, I.C.2, V.E.3, VI.A.2
3.1	16/03/2020	Ibrahima TAMBOURA	Correction des écarts de l'audit ETSI EN 319 411-1 • Modification du I.A, III.B.3 III.B.4, III.B.5, III.D, IV.A.1, IV.A.2, IV.B.1, IV.B.2, IV.B.3, IV.C.1, IV.C.2, IV.D.1, IV.G, IV.I.1, IV.I.2, IV.I.3, IV.I.4, IV.I.5, IV.L, V.E.3, VI.A.2, VI.A.3, VI.B.1, VI.B.2, VI.B.3, VI.B.4, VI.B.5, VI.B.7, VI.B.8, VI.B.9, VI.B.10, VI.B.11, VI.C.1, VI.D.1, VII.A.6
3.2	3/6/2020	Ibrahima TAMBOURA	Modification chapitre XII.D : Ajout ITSME comme authorisarion token pour le canal Easy Banking Business

Sommaire

I. Introduction

I.A. Présentation générale

Ce document définit la Politique de Certification applicable aux certificats,

- émis par les autorités de certifications « BNP Paribas Fortis Customer Ephemeral Certification Authority <N> » (« BNPPF Instant CA » dans la suite de ce document), agissant en tant que fournisseur de services de Certification (CSP),
- pour répondre aux besoins de confiance d'applications métiers (en particulier, dans le cas d'applications de contractualisation en ligne).

Cette politique de certification (nommée PC dans la suite de ce document) concerne l'émission de certificats de signature électronique de documents aux formats PDF, XML (XAdES, XML-DSig) ou CMS.

Ces certificats sont exclusivement créés et utilisés dans le cadre du service de création signature que BNP Paribas Fortis (BNPPF) met à disposition de ses clients pour signer des documents au nom du client. Ce service est référencé ci-après comme « application utilisatrice ».L'autorité « BNPPF Instant Fortis CA » répond aux besoins de personnes physiques, clients de BNP Paribas Fortis et utilisateurs de certificats personnels de BNP Paribas Fortis (ci-après appelés porteurs), et fait partie de l'infrastructure de gestion des clés (IGC) du groupe BNP Paribas comme indiqué à la Figure 1.

La présente politique de certification inscrite dans un processus de qualification ETSI EN 319 411-1 a pour objet de décrire :

- Les engagements de l'autorité « BNPPF Instant CA » relatifs à la définition des règles d'émission et à la gestion des certificats émis par BNP Paribas Fortis, ainsi qu'à leur mise en œuvre
- Les conditions d'utilisation des certificats émis par l'AC « BNPPF Instant CA »

La présente Politique de Certification répond aux exigences « Lightweight Certificate Policy » (LCP) définie dans la norme ETSI EN 319 411-1. L'OID LCP est le suivant : 0.4.0.2042.1.3.

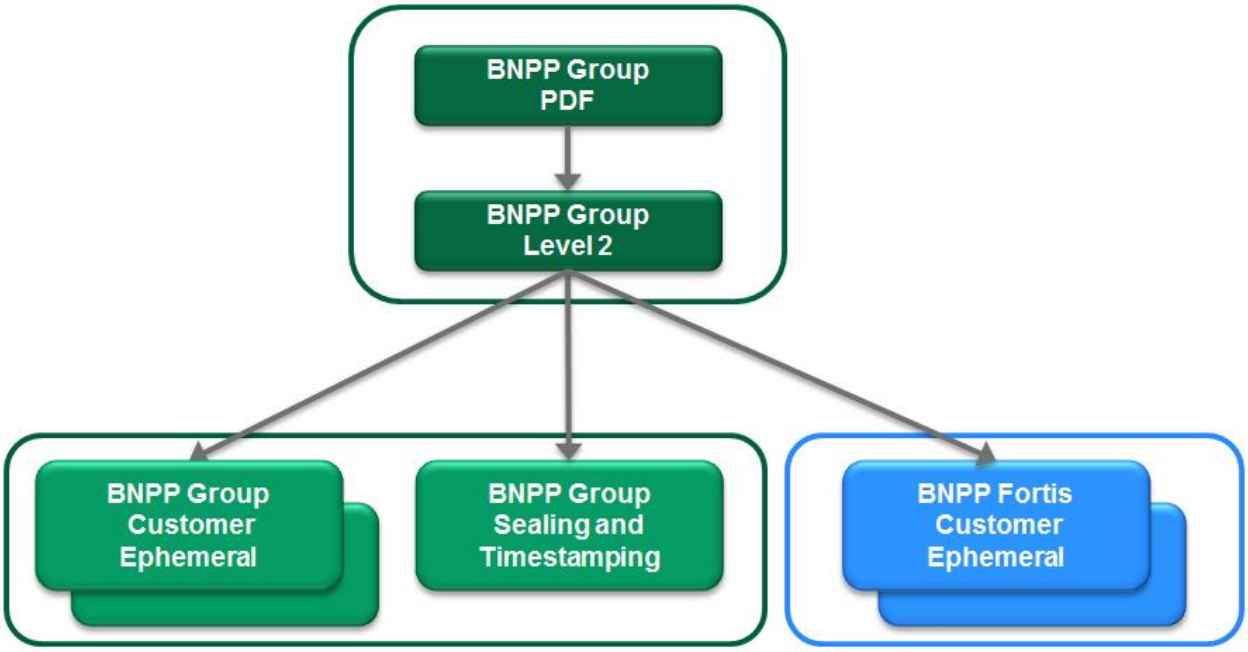


Figure 1 : IGC du groupe BNP Paribas

L'émission de certificats par les autorités de certifications « BNP Paribas Fortis Customer Ephemeral Certification Authority <N> », est exclusivement limitée en interne au groupe BNP Paribas.

I.B. Identification du document

Cette politique de certification est identifiée par son numéro d'identifiant d'objet (OID, pied de page de chaque page de ce document). D'autres éléments, plus explicites, comme par exemple le nom, numéro de version, date de mise à jour permettent également de l'identifier.

Les numéros d'OID correspondant à la présente politique de certification indiqué dans les certificats dépendent de l'instance technique de l'AC émettrice soit :

- Pour les certificats de signature électronique :
  - AC BNPPF Instant n° 1 : 1.2.250.1.62.10.7.1.1.2
  - AC BNPPF Instant n° 2 : 1.2.250.1.62.10.8.1.1.2
- Pour les certificats OCSP :
  - AC BNPPF Instant n° 1 : 1.2.250.1.62.10.7.1.2.1
  - AC BNPPF Instant n° 2 : 1.2.250.1.62.10.8.1.2.1

La branche OID de BNP Paribas est déposée : {iso(1) member-body(2) fr(250) type-org(1) BNP Paribas(62)} Signel (10) Autorités BNPPF Instant CA (7 ou 8) Politique de Certification(1) Gabarit de Certificat(1 ou 2) Version(1 ou 2)

Elle correspond aux certificats émis à partir du 24 juillet 2017.

I.C. Entités intervenant dans l'IGC

Afin de clarifier et faciliter l'identification des exigences, et en cohérence avec les documents de l'ETSI dans le domaine de la décomposition fonctionnelle de la PC de « BNPPF Instant CA », cette dernière s'organise autour des entités suivantes :

- Autorité de Certification (AC)
- Autorité d'Enregistrement (AE)
- Porteurs
- Opérateur
- Application utilisatrice (application de signature de documents mise à disposition par BNP Paribas Fortis)
- PMA (Policy Management Authority) : instance de gouvernance de l'IGC

Les cas d'usage couverts par la PC ne demandent pas de fonctions de séquestre.

« BNPPF Instant CA » désigne un Gestionnaire de certificats pour la gestion de son IGC, notamment comme interface avec l'Opérateur.

Dans le cadre des fonctions de fourniture de service de certification « BNPPF Instant CA » qu'elle assume directement, « BNPPF Instant CA » est un service de BNP Paribas Fortis. BNP Paribas Fortis une entité légale au sens de la loi belge qui s'engage à respecter les exigences suivantes :

- Être en relation par voie contractuelle avec les utilisateurs finaux pour laquelle elle est chargée d'assurer :
  - L'émission et la gestion des certificats en s'appuyant pour cela sur l'infrastructure à clés publiques (IGC) de BNP Paribas.
  - La définition des règles d'émission des certificats émis par l'AC « BNPPF Instant CA » et leur bonne application,
  - La définition des conditions d'utilisation des certificats émis par l'AC « BNPPF Instant CA »
- La remise au porteur des certificats émis par l'AC « BNPPF Instant CA » et pour lesquels, à l'intermédiaire de BNP Paribas, IDEMIA a la charge de la gestion des certificats des porteurs.

I.C.1.Autorité de Certification

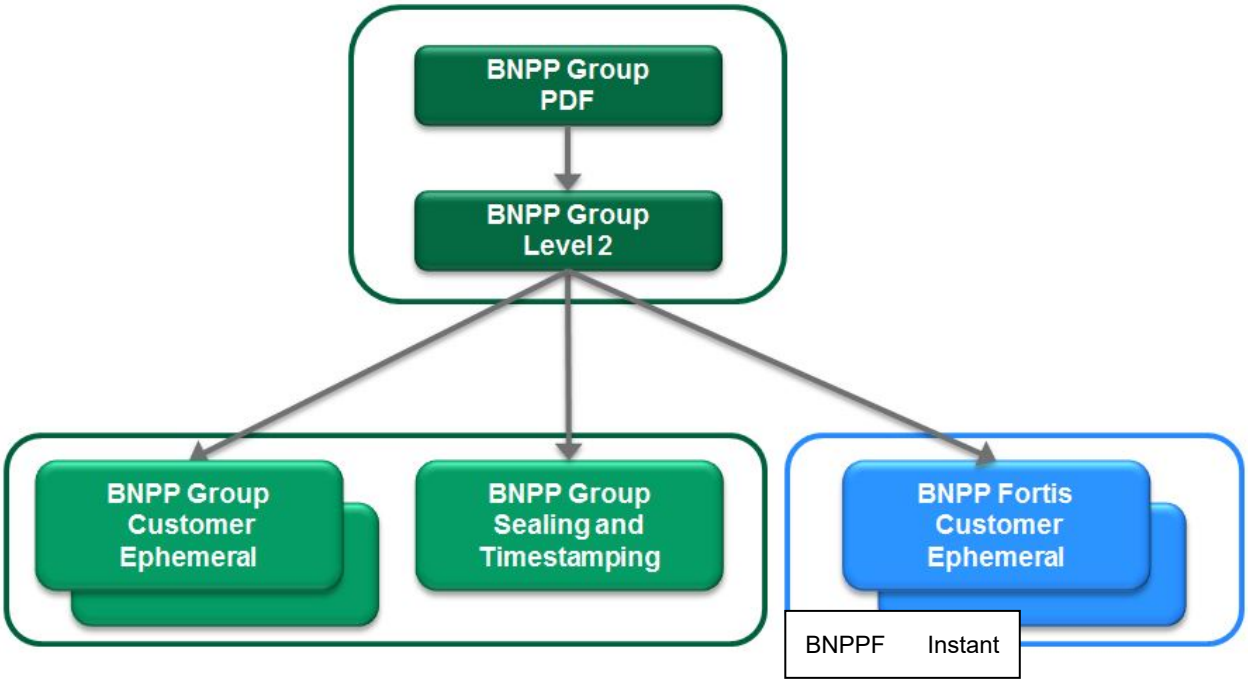
L'autorité de certification « BNPPF Instant CA » est en charge de la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation …) et s'appuie pour cela sur une infrastructure à clés publiques (IGC).

Afin de clarifier et faciliter l'identification des exigences, et en cohérence avec les documents de l'ETSI (European Telecommunications Standards Institute) dans le domaine, la décomposition fonctionnelle de cette IGC est la suivante :

- **Fonction de génération des certificats** - Cette fonction génère (création du format, signature électronique avec la clé privée associée) les certificats :
    - Soit en s'appuyant sur les outils propres aux composants techniques ou aux futurs porteurs de certificat
    - Soit en s'appuyant sur les outils de son IGC
- **Fonction de remise au porteur** - Cette fonction remet au porteur au minimum son certificat ou la chaîne de certification.
- **Fonction de publication** - Cette fonction met à disposition des différentes parties concernées : les politiques publiées, les certificats d'autorité et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats.
- **Fonction de gestion des révocations** - Cette fonction traite les demandes de révocation et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.
- **Fonction d'information sur l'état des certificats** - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (statut révoqué en particulier). Cette fonction est mise en œuvre selon un mode de publication d'informations qui se matérialise par une Liste de Certificats Révoqués (CRL).
- **Fonction d'administration de l'IGC**- Cette fonction est associée au rôle qui définit le comportement fonctionnel et le paramétrage technique de l'IGC.

L'ensemble des fonctions assurées par l'IGC de BNP Paribas (en tant que service technique) est opérée par le service informatique de IDEMIA. qui agit en tant que fournisseur de BNP Paribas. BNP Paribas agit en tant que fournisseur de l'IGC pour l'autorité de certification « BNPPF Instant CA », service de BNP Paribas Fortis. BNP Paribas Fortis est liée à BNP Paribas via un Master Service Agreement (MSA).

La Déclaration des Pratiques de Certification (DPC) associées aux autorités identifiées dans le présent document décrit l'organisation opérationnelle de l'IGC et la répartition des rôles entre les différentes composantes en fonction de l'organisation fonctionnelle et de la définition des rôles décrites dans la présente politique :



Techniquement, l'autorité de certification « BNPPF Instant CA » se compose de deux services d'IGC distincts. Ils sont identifiés par un CN commun suffixé par un incrément :

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

  Avec <N> valant 1 ou 2

I.C.2.Autorité d'enregistrement (AE)

L'AE a pour rôle de vérifier l'identité du demandeur de certificat afin de valider la demande d'émission du certificat.

Cette fonction vérifie les informations d'identification du futur porteur d'un certificat, ainsi qu'éventuellement, d'autres attributs spécifiques, avant de transmettre la demande correspondante (génération, révocation) à la fonction adéquate de l'IGC.

Elle se doit d'appliquer des procédures d'identification des personnes physiques permettant d'émettre des certificats selon une procédure en conformité avec la réglementation bancaire belge, et notamment avec la réglementation relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme (loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme).

La procédure d'enregistrement pour les certificats émis par BNPPF Instant CA se déroule en deux étapes telles que décrites ci-dessous. La 1ière étape est réalisée une seule fois et est un prérequis à la suivante.

1) Etape 1 : enregistrement (REG).

Cette 1ière étape est réalisée une seule fois, lorsque la personne physique entre en relation avec la banque. Elle est constituée de 3 éléments:

1.1 la constitution d'un dossier d'identité de la personne physique et la conservation des justificatifs d'identité fournis par celle-ci (REG1) ;

Ces documents sont archivés électroniquement. Leur validité est maintenue au cours du temps en accord avec la réglementation bancaire belge. Toutes les preuves de document d'identité sont conservées dans le système bancaire d'archivage, et cela est mis à disposition de toutes les agences bancaires BNP Paribas Fortis.

1.2 la vérification que les données d'identité récoltées en 1.1. appartiennent bien à la personne qui se présente comme client de la banque ou mandataire (REG2) ;

La vérification des données d'identité sur base de documents probants conformément à la réglementation applicable aux établissements de crédit. Elle est réalisée lors d'un face à face ou équivalent.

- Dans le cas d'un résident belge, la carte d'identité électronique (ou le cas échéant un autre document) émise par les autorités belges est utilisée
- Dans le cas d'un non-résident, la carte d'identité ou le cas échéant le passeport émis par le pays de résidence est utilisée. A défaut de pièce d'identité, des processus ad-hoc ont été mises en place

Lorsque les données d'identification sont vérifiées, pendant le face à face avec le client, un processus d'acceptation est entamé pour devenir client de la banque ou mandataire.

1.3 l'attribution ou l'identification d'un moyen d'authentification fort que la personne utilisera pour s'authentifier et/ou donner son accord (autorisation) lors de ses contacts subséquents avec l'application utilisatrice (ENR.AUTH).

Il doit s'agir d'un système d'authentification (AUTH) qui utilise les méthodes d'authentification reconnues par la Banque et d'un niveau d'assurance élevé sur l'identité de la personne.

Les moyens d'authentification acceptés dans le cadre de la présente PC sont :

- la carte bancaire intelligente (standard EMV) qui permet de s'authentifier grâce au protocole M1 au moyen d'un lecteur UCR, au travers d'un canal sécurisé entre le client et la banque (EBW, EBB)
- la carte Isabel (fournie par BNPPF ou une autre banque) qui permet de s'authentifier grâce à un certificat et au moyen d'un lecteur de carte, au travers d'un canal sécurisé entre le client et la banque (EBB)
- le système itsme, qui permet de s'authentifier au travers d'un canal sécurisé entre le client et la banque (EBW, EBB)

Les moyens d'autorisation acceptés sont :

- la carte bancaire intelligente (standard EMV) qui permet de signer grâce au protocole M2 au moyen d'un lecteur UCR, au travers d'un canal sécurisé entre le client et la banque (EBW, EBB)
- la carte Isabel (fournie par BNPPF ou une autre banque) qui permet de signer grâce à un certificat et au moyen d'un lecteur de carte, au travers d'un canal sécurisé entre le client et la banque (EBB)

Les processus d'activation et d'utilisation des moyens d'authentification et d'autorisation et les détails techniques de ces moyens d'authentification et d'autorisation sont détaillés en annexe de la présente PC (Annexe IV). Seules les combinaisons de moyens d'authentification et d'autorisation décrites dans ce document annexe sont permises. Il est à noter que certains moyens peuvent être utilisés pour l'authentification et l'autorisation.

2) Etape 2 : requête de certificat.

Cette seconde étape, qui repose sur les éléments enregistrés lors de la 1ière étape, est réalisée à chaque fois que la personne physique demande un certificat éphémère, c'est-à-dire à chaque fois qu'une transaction nécessitant une signature est nécessaire. Elle requière une authentification forte de la personne, au moyen d'une des méthodes d'authentification enregistrées pour cette personne en 1.3.

Cette étape se produit lors du processus de contractualisation en ligne qui repose sur 2 étapes :

2.1 l'initialisation du processus permettant de contractualiser en ligne, qui requière l'authentification préalable du client via un des moyens d'authentification acceptés par BNPPF (listés ci-dessus).

2.2 l'initialisation du processus permettant de signer électroniquement, suivant l'étape 2.1.

Le client donne son accord sur un document contractuel spécifique à signer. Si le client coche la case de confirmation, il peut ensuite officialiser la demande de signature via un des moyens d'autorisation acceptés par BNPPF (listés ci-dessus)

Si cette demande est **valable, une requête de certificat est envoyée à l'AE technique** qui fait générer un certificat au nom de la personne physique.

Note 1: à ce stade, en cliquant sur « annuler » au lieu de signer avec son moyen d'autorisation, le processus de signature est annulé et l'utilisateur revient sur l'écran du produit/service sélectionné. Aucun certificat n'est généré.

Note 2 : c'est également cette étape qui lie la demande aux données à signer.

Cette étape officialise la demande de création d'un certificat de signature.

2.3 l'autorisation de signer électroniquement et d'utiliser le certificat

Un second écran d'autorisation permet à la personne physique de donner son consentement sur la création d'une signature électronique à son nom sur base des données d'identification le concernant reprises du certificat (prénom & nom tels que présentés à l'écran), sur le document contractuel spécifique.

Note 1: le client peut consulter les CGU et la PC à cette étape.

Note 2 : les données d'identification concernant le client et reprises du certificat généré sont à nouveau présentées.

Soit la personne accepte, et ce processus officialise la demande de signature électronique. En conséquence le certificat généré est utilisé pour signer le document liant le client ou mandataire avec la Banque d'une façon légale. Cette étape permet également de confirmer l'acceptation du certificat.

Soit la personne physique met fin au processus de signature électronique en cliquant sur « annuler » au lieu de donner son consentement (écran d'autorisation). En conséquence, le certificat généré est révoqué. L'utilisateur revient sur l'écran de signature et aucune signature n'est générée.

L'AC « BNPPF Instant CA » met en œuvre 2 composantes d'AE :

- **Une AE fonctionnelle** : responsable de la vérification initiale de l'identité de la personne physique et de la conservation des justificatifs d'identité fournis par celle-ci (REG1 et REG2) et de la vérification subséquente de l'identité de la personne physique à chaque transaction susceptible de donner lieu à l'émission d'un certificat (AUTH). L'AE fonctionnelle est responsable de :
    - Conserver les éléments de vérification du porteur de certificat en application de la réglementation applicable aux établissements de crédit (*loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme*).
    - Conserver en confidentialité et en intégrité des données personnelles d'authentification du porteur en adéquation avec la réglementation bancaire.

  Toutes les informations relatives aux données confidentielles se trouvent stockées dans le système - d'archivage bancaire.

- **Une AE technique** : responsable de la création des clés et de la soumission des requêtes de certificats à l'autorité de certification.

  Elle génère également un fichier de preuve de validation de signature lors de chaque signature par le porteur.

I.C.3.Opérateur de certification

L'Opérateur de Certification assure des prestations techniques, en particulier, cryptographiques et d'hébergement permettant d'atteindre les exigences de la présente politique.

Le rôle d'opérateur de certification est assuré par IDEMIA.

I.C.4.Porteur de certificat

Dans la présente politique de certification un porteur de certificat est une personne physique identifiée par BNP Paribas Fortis selon l'étape 1 du processus d'enregistrement décrit ci-dessus (client titulaire ou mandataire).

I.C.5.Applications utilisatrices de certificats

Les applications utilisatrices des certificats sont :

- Une application de création de signature électronique mise à disposition du porteur de certificat par BNP Paribas Fortis,
- Tous les logiciels de visualisation et de validation de signature électronique.

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

La PMA est l'instance de gouvernance de l'IGC de BNP Paribas, qui a pour principales missions de :

- Définir, revoir, approuver et faire appliquer les Politiques de Certifications et les Déclaration des Pratiques de Certifications,
- Gérer l'ensemble des risques liés à l'IGC,
- D'assurer la gestion des évènements spécifiques de l'IGC (cérémonie des clés ou fin de vie par exemple),
- Définir et gérer les personnels ou entité de confiance opérant l'IGC
- Gérer les relations avec les entités extérieures,
- Prendre toutes les actions nécessaires pour assurer l'exécution de l'ensemble des tâches listées précédemment.

I.D. Usage des certificats

I.D.1.Bi-clés et certificats des porteurs

Les certificats éphémères émis dans le cadre de cette présente politique de certification sont utilisés uniquement dans le cadre de l'utilisation de solutions de signature électronique et la validation de documents dans un format défini par BNP Paribas Fortis.

Le seul usage permis est la signature personnelle à travers la valeur 'Non Repudiation' (2.5.29.15.(1)) de l'extension 'Key Usage'.

I.D.2.Bi-clés et certificats de l'autorité « BNPPF Instant CA »

Les certificats de l'autorité « BNPPF Instant CA » définis par la présente PC sont utilisés pour signer les certificats personnels de signature éphémère et les CRL.

I.D.3.Bi-clés et certificats OCSP

Les clés de signature du service OCSP de l'AC (OID : 1.2.250.1.62.10.7.1.2.1 & 1.2.250.1.62.10.8.1.2.1) sont uniquement utilisées pour signer les jetons OCSP produits par la fonction d'information sur le statut des certificats.

I.E. Gestion de la politique de certification

I.E.1.Entité gérant la politique de certification

L'entité en charge de l'administration et de la gestion de la présente politique de certification est ITG en accord avec BNP Paribas Fortis. Elle est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PC.

ITP ITG est la fonction Informatique et Technologie Groupe (ITG).

I.E.2. Point de contact

BNP Paribas Fortis peut être contacté pour toutes questions relatives à cette PC via l'Easy Banking Center (Ebc) au numéro 02 762 20 00 (FR) ou 02 762 60 00 (NL).

Fintro peut être contacté pour toutes questions relatives à cette PC via l'Easy Banking Fintro (Web & App) au numéro 02 433 45 20 (FR) ou 02 433 45 10 (NL).

Easy Banking Business Helpdesk peut être contacté pour toutes questions relatives à cette PC via l'EBB Helpdesk au 02 565 05 00.

Si la réponse ou le traitement ne sont toujours pas satisfaisants, l'intervention du service Gestion des plaintes peut être demandée.

I.E.3. Entité déterminant la conformité d'une DPC avec cette politique de certification

La PMA (Policy Management Authority), instance de gouvernance de l'IGC, désigne les personnes (ou Services) déterminant la conformité de la Déclaration des Pratiques de Certification avec cette Politique de Certification.

I.E.4. Procédures d'approbation de la conformité de la PC

La présente Politique de Certification sera revue périodiquement par la PMA (Policy Management Authority), instance de gouvernance de cette IGC, pour assurer sa conformité aux normes de sécurité attendues par l'organisme de contrôle national (cf. Règlement européen eIDAS 910/2014).

De plus, l'approbation de cette Politique de Certification sera effectuée durant une instance de la PMA.

I.F. Définitions et acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

- **AA** : Autorité d'Archivage
- **AC** : Autorité de Certification
- **ACR** : Autorité de Certification Racine
- **AE** : Autorité d'Enregistrement
- **ANSSI** : Agence Nationale de la Sécurité des Systèmes d'Information
- **CAP**: Client Acceptance Procedure
- **CFU**: Customer Follow-up
- **CGU** : Conditions générales d'utilisation
- **CRL** : Liste de Certificats Révoqués
- **DN** : Distinguished Name
- **DPC** : Déclaration des Pratiques de Certification
- **EMV**: Europay/Mastercard/Visa
- **IGC** : Infrastructure de Gestion de Clés
- **OID** : Object Identifier
- **OCSP** : Online Certificate Status Protocol
- **PMA** : Policy Management Authority
- **PC** : Politique de Certification
- **RGS** : Référentiel Général de Sécurité
- **RSA** : Rivest Shamir Adleman
- **SMID**: Single Multichannel Identifier
- **UCR**: Unconnected card reader
- **URL** : Uniform Resource Locator

Public Key Infrastructure (PKI ou IGC)	Ensemble de composants physiques, procédures et logiciels permettant de gérer le cycle de vie des certificats et d'offrir des services d'authentification, de chiffrement et de signature.
Certificat	Fichier électronique délivré par une Autorité de Certification attestant l'identité d'un porteur (personne physique, machine…). Le certificat est valide pendant une durée donnée précisée dans celui-ci.
Autorité de Certification (AC ou CA)	Service chargé de signer, émettre et maintenir les certificats d'une infrastructure à clés publiques, conformément à une politique de certification. Services applicatifs exploitant les certificats émis par l'Autorité de Certification du porteur du certificat.
Politique de certification (PC)	Ensemble de règles et d'exigences auxquelles est soumise une autorité de certification dans la mise en place et la fourniture de ses prestations.
Déclaration des pratiques de certification (PC)	Description des pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'autorité de certification applique dans le cadre de la fourniture de ses services de certification électronique, en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.
Liste de révocation des Certificats (CRL ou LCR)	Liste publiée par l'autorité de certification présentant les certificats n'étant plus dignes de confiance (révoqués, invalides…). Par simplicité on y associe également les listes de révocation d'autorités (appelées ARL)
Répondeur OCSP	Service de statut en ligne des certificats
Bi-clé	Couple de clés composé d'une clé privée et d'une clé publique.
X 509	Norme de l'Union internationale des télécommunications (UIT) relative aux infrastructures à clés publiques (PKI), entre autres les formats standards de ses composants : certificats électroniques, listes de révocation, algorithme de validation…
UTF-8	Codage des caractères définis par Unicode où chaque caractère est codé sur une suite de un à six mots de 8 bits (il n'existe pas actuellement de caractères codés avec plus de 4 mots).
Distinguished Name (DN)	Elément permettant d'identifier un porteur ou une autorité de certification de façon unique.
Object Identifier (OID)	identifiant universel, représenté sous la forme d'une suite d'entiers associé dans le cadre d'une PKI à un élément de référence tel que la politique de certification ou la déclaration de pratiques de certification.
Isabel Card	Un type de carte de la société Isabel avec une technologie très sécurisée qui permet une authentification forte techniquement et une identification élevée juridiquement.
EBB Card	Un type de carte de la société Isabel pour la plateforme EBB avec une technologie très sécurisée qui permet une authentification forte techniquement et une identification élevée juridiquement.
eID Belgium	Un type de carte d'identification du gouvernement belge avec une technologie très sécurisée qui permet une authentification forte techniquement et une identification élevée juridiquement.

II. Responsabilités concernant la mise à disposition des informations devant être publiées

II.A. Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des porteurs et des utilisateurs de certificats, l'autorité « BNPPF Instant CA » met en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats.

La présente politique précise les méthodes de mise à disposition et les URL correspondantes (serveurs Web de publication).

II.B. Informations devant être publiées

L'autorité « BNPPF Instant CA » publie les informations suivantes à destination des porteurs et des utilisateurs de certificat :

- La présente politique de certification : **https://bnpp.digitaltrust.morpho.com/cp** ,
  Les listes des certificats révoqués : **http://bnpp.digitaltrust.morpho.com/crl/bnpp-fortis-customer-ephemeral1-ca.crl** et **http://bnpp.digitaltrust.morpho.com/crl/bnpp-fortis-customer-ephemeral2-ca.crl**,
- Les certificats des autorités « BNPPF Instant CA », en cours de validité : **https://bnpp.digitaltrust.morpho.com/ca/bnpp-fortis-customer-ephemeral1-ca.cer** et **https://bnpp.digitaltrust.morpho.com/ca/bnpp-fortis-customer-ephemeral2-ca.cer**.
- Les conditions générales d'utilisation des certificats éphémères.

II.C. Délais et fréquences de publication

Les délais et les fréquences de publication dépendent des informations concernées :

- Pour les informations liées à l'IGC (nouvelle version de la PC, conditions générales d'utilisation), l'information est publiée dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements effectifs de l'AC. Ce délai n'excède pas 7 jours ouvrés.
- Pour les informations d'état des certificats, se reporter au IV.I.
- Pour les systèmes publiant ces informations, BNP Paribas et IDEMIA s'engagent sur les exigences de disponibilité suivantes :
  - Pour les informations liées à l'IGC (nouvelle version de la PC, conditions générales d'utilisation.), les systèmes ont une disponibilité pendant les jours ouvrés avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 8h (jours ouvrés) et une durée totale maximale d'indisponibilité tolérée 2h10 par mois hors maintenance planifiée et hors cas de force majeure (incident grave de sécurité avéré).
  - Pour les certificats d'AC et les listes de certificats révoqués, les systèmes ont une disponibilité de 24h/24 7j/7 avec une durée maximale d'indisponibilité tolérée de 2h10 par mois hors maintenance planifiée et hors cas de force majeure (incident grave de sécurité avéré).

II.D. Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture. L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC.

III. Identification et authentification

III.A. Nommage

III.A.1. Types de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500.

Dans chaque certificat X509 v3 l'autorité émettrice (*issuer*) et le porteur (*subject*) sont identifiés par un « *Distinguished Name* » DN de type X.501 dont le format exact est précisé dans le chapitre VII décrivant le profil des certificats, conformément à la norme ETSI EN 319 412-1.

III.A.2. Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les porteurs de certificats doivent être explicites. Le DN respecte la structure de l'identité utilisée dans les référentiels de BNP Paribas Fortis et que la banque communique dans sa fonction d'AE technique à l'opérateur pour signature du certificat correspondant.

Le nom commun (CN) du sujet doit impérativement représenter l'identité de la personne destinatrice dont l'identité aura été vérifiée (cf. §III.B) et ne peut en aucun cas représenter autre chose que son identité en lien avec son état civil (pas de nom de machine, ou l'identité d'une autre personne).

III.A.3. Pseudonymisation des porteurs

Les certificats des porteurs ne sont pas pseudonymisés.

III.A.4. Règles d'interprétation des différentes formes de nom

L'AE fonctionnelle est responsable de l'unicité des noms de ses porteurs et de la résolution des litiges portants sur la revendication d'utilisation d'un nom par ceux-ci.

L'AE fonctionnelle, dans le cadre de l'entrée en relation, procède à des transformations concernant le nom et les prénoms du porteur. Ainsi, le nom ne peut contenir que 40 caractères, qui sont obligatoirement des lettres, des blancs, des tirets, des points ou des virgules, à l'exclusion de tout autre.

Concernant les prénoms,seul le premier prénom est retenu et la longueur du prénom ne peut pas dépasser 16 caractères et ne peut contenir que des lettres, des blancs, des tirets, des points ou des virgules, à l'exclusion de tout autre.

De plus, les transformations suivantes sont appliquées :

- pour les minuscules, 'abcdefghijklmnopqrstuvwxyzâäàáãåçñéêëèíîïìôöòóõûüùúý' sont transformés en 'ABCDEFGHIJKLMNOPQRSTUVWXYZAAAAAACNEEEEIIIIOOOOOUUUUY'
- pour les majuscules, 'ÂÄÀÁÃÅÇÑÉÊËÈÍÎÏÌÔÖÒÓÕÛÜÙÚÝ' sont transformés en 'AAAAAACNEEEEIIIIOOOOOUUUUY'

Les règles détaillées sont indiquées dans la DPC.

III.A.5. Unicité de Noms

a) S'agissant d'un certificat éphémère

BNP Paribas Fortis est responsable de l'unicité des noms de ses porteurs et de la résolution des litiges portants sur la revendication d'utilisation d'un nom par ceux-ci.

Afin d'assurer une continuité d'une identification unique du porteur au sein du domaine de l'AC « BNPPF Instant CA », le DN du champ « subject » de chaque certificat de porteur permet d'identifier de façon unique le porteur correspondant au sein du domaine de l'AC.

Ce DN doit pour cela respecter les exigences suivantes pour les porteurs :

- CN = Identité du sujet / personne physique, sous la forme « Prénom Nom »
- SN (surName) = nom du sujet / personne physique
- givenName = prénom du sujet / personne physique
- SN (serialNumber) = N° unique (UUID)
- OU= F+ (SMID du client) ou I+(Isabel ID + SMID)
- C=BE

L'unicité est garantie par BNP Paribas Fortis via l'ajout d'un numéro unique (UUID – cf. RFC 4122 –) dans l'attribut SN du sujet (DN) du certificat.

Dans le cas d'un certificat de test, le gabarit utilisé est le même que le gabarit d'un certificat éphémère. Cependant, le DN respectera les exigences suivantes :

- CN (commonName) = soit l'Identité du sujet / personne physique, sous la forme « Prénom Nom » avec l'ajout d'un « – Test » en suffixe, soit « MONITORING – TEST »
- SN (surName) = soit le nom du sujet / personne physique avec l'ajout de « - Test » en suffixe, soit « MONITORING –TEST »
- givenName = soit le prénom du sujet / personne physique soit « MONITORING –TEST »
- SN (serialNumber) = N° unique (UUID)
- OU = F-1
- C = BE

b) S'agissant d'un certificat OCSP

Le numéro de série intégré au sujet du certificat OCSP permet d'en garantir l'unicité.

- CN (commonName) = OCSP Responder <N>

Dans le cas d'un certificat de test, le champ CN contiendra en suffixe « TEST ».

c) S'agissant d'un certificat de l'autorité de certification « Instant CA »

Le numéro de série intégré au sujet de l'autorité de certification permet d'identifier l'AC ayant émis le certificat éphémère.

III.A.6. Identification, authentification et rôle de marques déposées

La marque BNP Paribas est déposée par BNP Paribas :

- BNP PARIBAS, marque française déposée le 3 septembre 1999 dans les classes 35, 36 et 38 sous le numéro 99810625.
- BNP PARIBAS, marque communautaire déposée le 8 octobre 1999 dans les classes 35, 36 et 38 sous le numéro 1338888.

La marque BNP Paribas Fortis est une marque déposée dans l'Union européenne par BNP Paribas le 17 février 2010 dans les classes dans les classes 9, 35, 36 et 41 sous le numéro 008373185

- Cette marque a été déposée auprès du Bureau Benelux des Marques le 3 janvier 2013 dans les classes 35, 36 et 42 sous le numéro 0931084

La marque Fintro est une marque déposée dans l'Union européenne par BNP Paribas Fortis le 10 mai 2007 dans la classe 36 sous le numéro 004046173.

- Cette marque a été déposée auprès du Bureau Benelux des Marques par BNP Paribas Fortis le 27 septembre 2004 dans la classe 36 sous le numéro 0764125.

III.B. Validation initiale de l'identité

III.B.1. Méthode pour prouver la possession de la clé privée

La demande de certificat générée par l'AE technique BNP Paribas est signée à partir de la clé privée associée, la bi-clé étant générée par un module cryptographique de l'AE technique BNP Paribas.

La demande d'un certificat OCSP générée par un opérateur de l'IGC est signée à partir de la clé privée associée, la bi-clé étant générée par un module cryptographique de l'AC de BNP Paribas.

III.B.2. Validation de l'identité de l'organisme client de BNP Paribas

Non applicable.

III.B.3. Validation de l'identité d'un individu

L'enregistrement d'un porteur (cf. chapitre I.C.2 pour plus de détails) pour l'émission d'un certificat est réalisé par BNP Paribas Fortis dans sa fonction d'AE fonctionnelle.

Les règles de vérification d'identité du porteur sont laissées à la discrétion de BNP Paribas Fortis dans le cadre de son activité et dans son rôle d'AE fonctionnelle

La procédure d'émission d'un certificat repose sur les spécifications de l'AE technique qui utilise les informations du porteur en se basant sur les données transmises par l'application métier de BNP Paribas Fortis à l'AE technique.

La procédure de vérification de l'identité du porteur sous la forme « Prénom Nom » est uniquement de la responsabilité de BNP Paribas Fortis dans le cadre de son activité bancaire.

Le nom commun (CN) du certificat ne peut être associé qu'à une personne physique et aucunement à un nom de service, application ou assimilé.

III.B.4. Information non vérifiée du porteur

Toutes les informations certifiées sont vérifiées.

III.B.5. Validation de l'autorité du demandeur

Cf. chapitre III.B.4.

III.B.6. Certification croisée d'AC

Sans objet.

III.C. Identification et validation d'une demande de renouvellement des clés

III.C.1. Identification et validation pour un renouvellement courant

Conformément au document [RFC 3647], la notion de "renouvellement de certificat" correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique du porteur).

Le renouvellement ne s'applique pas dans le cadre de cette PC.

III.C.2. Identification et validation pour un renouvellement après révocation

Sans objet.

III.D. Identification et validation d'une demande de révocation

a) S'agissant d'un certificat éphémère

La demande de révocation du certificat final ne peut être initiée que par le porteur dans le cadre de son opération de souscription en ligne. L'acceptation de la demande de révocation est automatique. Le porteur demande la révocation en annulant la requête de signature notamment si les informations du CN contenues dans le certificat éphémère (Prénom - Nom) qui lui sont présentées sont erronées.

Les conditions de cette demande sont précisées au chapitre IV.I.

b) S'agissant d'un certificat de l'autorité de certification « BNPPF Instant CA »

La validation d'une demande de révocation d'une autorité de certification est un phénomène exceptionnel.
Les conditions de cette demande sont précisées au chapitre IV.I

IV. Exigences opérationnelles sur le cycle de vie des certificats

IV.A. Demande de certificat

IV.A.1. Origine d'une demande de certificat

La demande de certificat ne peut être émise que par une application métier de BNP Paribas Fortis dans sa fonction d'AE fonctionnelle. L'application métier de BNP Paribas Fortis et l'AE technique sont authentifiées fortement pour toute demande de certificat porteur.

IV.A.2. Processus et responsabilités pour l'établissement d'une demande de certificat

La demande de certificat nécessite une authentification forte des composantes techniques de l'AE fonctionnelle de BNP Paribas Fortis et l'AE technique en utilisant des protocoles sécurisés qui utilisent des certificats d'authentification.

- L'AE fonctionnelle vérifie les statuts de ces certificats avant de traiter la demande.
- L'AE fonctionnelle de BNP Paribas Fortis est responsable de la vérification de l'intégrité des données qu'elle transmet à l'AE technique
- Le processus de demande d'établissement d'un certificat porteur est décrit dans le chapitre I.C.2.

IV.B. Traitement d'une demande de certificat

IV.B.1. Exécution des processus d'identification et de validation de la demande

La procédure d'identification et de validation de la demande d'un certificat porteur est la suivante :

- La demande est établie automatiquement par l'AE fonctionnelle de BNP Paribas Fortis sous forme électronique et transmise à l'AE technique de BNP Paribas
- Une preuve de possession de la clé est générée et est formatée par l'AE technique, avec les informations à certifier, sous forme d'une requête de certificat
- Cette preuve est envoyée à l'opérateur de certification pour signature du certificat

IV.B.2. Acceptation ou rejet de la demande

Le porteur manifeste l'acceptation de la demande de certificat en autorisant sa demande initiale avec un des moyens d'autorisation acceptés par BNPPF et listés en clause I.C.2. Le document lui est présenté par l'application métier de BNP Paribas Fortis et le porteur donne son consentement avant signature.

IV.B.3. Durée d'établissement du certificat

L'établissement du certificat est réalisé par l'AC dès réception de la demande par l'AE technique et dans la limite de de trente (30) secondes suivant la réception de la demande.

IV.C. Délivrance du certificat

IV.C.1. Actions de l'AC concernant la délivrance du certificat au porteur

Après authentification de l'AE technique vis-à-vis de l'AC « BNPPF Instant CA », la demande de certification transmise par l'AE technique est automatiquement signée par l'AC « BNPPF Instant CA », après contrôle de la conformité de son contenu, à savoir :

- Le respect de la syntaxe des attributs du sujet (DN), cf. le chapitre III.A.5.

- Les attributs cryptographiques de la requête (taille de clé).

Il s'agit d'une opération automatique lors d'un processus de contractualisation en ligne.

Le certificat est transmis au porteur au travers du document signé remis à la fin d'une transaction métier BNP Paribas Fortis.

IV.D. Acceptation du certificat

IV.D.1. Démarche d'acceptation du certificat

Le porteur donne son consentement en acceptant explicitement le CN du certificat généré en son nom, cf. chapitre I.C.2. Il accepte de signer les données qui lui sont présentées par l'AE fonctionnelle de BNP Paribas Fortis.

IV.D.2. Publication du certificat

Les certificats ne sont pas publiés dans le cadre de cette PC. L'AC « BNPPF Instant CA » conserve les certificats émis en base selon les spécifications techniques de son IGC.

IV.D.1. Notification de la délivrance du certificat

Se référer au chapitre correspondant de la DPC.

IV.E. Usages de la bi-clé et du certificat

IV.E.1. Utilisation de la clé privée et du certificat par le porteur

a) S'agissant d'un certificat éphémère

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service de signature offert par BNP Paribas Fortis. Par design, l'application métier de BNP Paribas Fortis ne permet pas d'autre utilisation de la clé privée.

Les conditions générales d'utilisation du certificat précisent les rôles et responsabilités des parties.

b) S'agissant d'un certificat OCSP

Les certificats OCSP sont des certificats d'AC, voir §I.D.3.

IV.E.2. Utilisation de la clé privée et du certificat par l'utilisateur du certificat

Voir le chapitre I.C.2 pour la description de l'AE technique.

La clé privée d'un certificat de signature électronique éphémère est détruite à la fin de la transaction utilisateur.

IV.F. Renouvellement d'un certificat

Non applicable dans le cadre de la présente PC.

IV.G. Délivrance d'un nouveau certificat suite à changement de la bi-clé

Le changement de bi-clé pour un certificat éphémère est considéré comme une demande de nouveau certificat. Cela peut être effectué pour un porteur donné sous la responsabilité de l'AE fonctionnelle lors de la fin de vie d'un certificat précèdent.

La procédure délivrance est la même que pour un certificat initial.

IV.H. Modification du certificat

La modification d'un certificat correspond à la délivrance d'un nouveau certificat pour la même clé publique, consécutif à des modifications d'informations autres que les dates de validité et le numéro de série (dans le cas contraire il s'agit d'un renouvellement de certificat).

La modification de certificat n'est pas autorisée dans la présente politique.

IV.I. Révocation et suspension des certificats

La suspension ne s'applique pas dans le cadre de cette PC.

Les procédures relatives à la révocation d'une AC sont décrites dans la PC des AC hors lignes « BNPP PDF CA » et « BNPP LEVEL2 CA » dont les OID sont respectivement 1.2.250.1.62.10.1.1.1.1 & 1.2.250.1.62.10.2.1.1.1. Dans la suite du paragraphe, seuls seront décrites les informations relatives à la révocation des certificats finaux.

IV.I.1. Causes possibles d'une révocation

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'un porteur :

- Les informations du porteur figurant dans son certificat ne sont pas en conformité avec son identité ;
- Le porteur a abandonné son opération de souscription en ligne.

IV.I.2. Origine d'une demande de révocation

L'acceptation du certificat est obligatoire avant toute signature électronique. L'identité du porteur est présentée au porteur à partir du CN issu de son certificat. Si cette identité est erronée, le porteur se doit de refuser ce certificat à partir d'une fonctionnalité « Annuler » de la souscription en ligne.

IV.I.3. Procédure de traitement d'une demande de révocation

La demande de révocation d'un porteur est traitée automatiquement par l'AE technique.

IV.I.4. Délai accordé au porteur pour formuler la demande de révocation

Par nature une demande de révocation doit être traitée en urgence. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC « BNPPF Instant CA », et que cette liste est accessible au téléchargement.

La formulation de la demande doit être traitée durant le temps de session d'une souscription en ligne d'une application de BNP Paribas Fortis.

IV.I.5. Délai de traitement d'une demande de révocation

La durée de traitement de la révocation n'excédera pas quelques minutes en cohérence avec la durée de vie du certificat éphémère.

IV.I.6. Exigences de vérification de la révocation par les utilisateurs de certificats

L'AE technique est tenue de vérifier que le certificat de l'autorité de certification « BNPPF Instant CA » ayant émis le certificat du porteur est valide.

Il n'est pas précisé d'exigence sur les certificats révoqués des porteurs.

IV.I.7. Fréquence d'établissement des CRL

Une CRL est générée régulièrement toutes les 24 heures.

IV.I.8. Délai maximum de publication d'une CRL

Une CRL doit être publiée dans un délai maximum de 30 minutes suivant sa génération.

IV.I.9. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

L'AC met en œuvre un système de vérification en ligne de la révocation et de l'état des certificats conforme à la RFC 6960. Ce service est disponible 7 jours sur 7, 24 heures sur 24.

IV.I.10. Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Cf. IV.I.6.

IV.I.11. Autres moyens disponibles d'information sur les révocations

Sans objet.

IV.I.12. Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats d'AC ou d'OCSP, en cas de révocation suite à une compromission de la clé privée, une information sera clairement diffusée.

En cas de révocation pour compromission ou suspicion de compromission de clé, la mise à jour de la CRL doit être réalisée selon la politique exprimée au chapitre IV.J.2. En cas de révocation pour cause de compromission de clé, il sera indiqué aux personnes autorisées la date à laquelle l'on suppose que la compromission a eu lieu.

L'information consistant à savoir si un certificat a un statut révoqué ou non doit être disponibles 24h/24 7j/7 à l'ensemble de la communauté ayant le besoin d'en connaître. Le statut d'un certificat doit pouvoir être authentifié et être protégé en intégrité.

IV.I.13. Causes possibles d'une suspension

Sans objet.

IV.J. Fonction d'information sur l'état des certificats

IV.J.1. Caractéristiques opérationnelles

La fonction d'information sur l'état des certificats met à disposition plusieurs mécanismes : soit un mécanisme de consultation libre de CRL soit un répondeur OCSP.

Plusieurs adresses sont mises en œuvre par l'AC « BNPPF Instant CA » pour vérifier Plusieurs adresses sont mises en œuvre par l'AC « BNPPF Instant CA » pour vérifier le statut d'un certificat :

- Pour les certificats de porteurs :
  - CRL
    - **http://bnpp.digitaltrust.morpho.com/crl/bnpp-fortis-customer-ephemeral1-ca.crl**
    - **http://bnpp.digitaltrust.morpho.com/crl/bnpp-fortis-customer-ephemeral2-ca.crl**
  - OCSP
    - **http://bnpp.digitaltrust.morpho.com/ocsp/bnpp-fortis-customer-ephemeral1-ca**

- **http://bnpp.digitaltrust.morpho.com/ocsp/bnpp-fortis-customer-ephemeral2-ca**

- Pour les certificats de l'autorité de certification « BNPPF Instant CA » elle-même :
  - **http://bnpp.digitaltrust.morpho.com/crl/bnpp-level2-ca.crl**

De par leur nature, les deux services de statut des certificats n'ont pas une information immédiatement synchrone à l'issue d'une révocation. En effet, le service OCSP répond en temps réel alors que la mise à jour d'une CRL est un processus nativement asynchrone (cf. Erreur ! Source du renvoi introuvable. et Erreur ! Source du renvoi introuvable.) avec par conséquent un temps de latence entre les deux services.

Concernant le statut des certificats éphémères, l'écart maximum entre les deux services tient compte de la périodicité d'émission de la CRL plus celle du délai de publication, soit 24h30.

IV.J.2. Disponibilité de la fonction

Une CRL est publiée dans un délai maximum de 30 min suivant sa génération. Le taux de disponibilité est a minima de 99,7%, 24/7.

Le temps de réponse du serveur de vérification du statut d'un certificat (OCSP) à la requête reçue est inférieur à 10 secondes.

IV.K. Fin de la relation avec le porteur

Lorsque la relation entre le porteur et BNP Paribas Fortis prend fin, le porteur ne dispose plus de l'accès à l'AE fonctionnelle, et donc ne peut plus demander de certificat.

IV.L. Séquestre de clé et recouvrement

Le séquestre des clés privées des porteurs et de répondeurs OCSP est interdit.

V. Mesures de sécurité non techniques

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que les autorités « BNPPF Instant CA » doivent respecter.

La DPC décrit les moyens mis en œuvre pour respecter ces exigences dans le cadre de l'hébergement de l'IGC BNP Paribas chez IDEMIA et le cas échéant, dans le cadre des autres activités liées à la certification

V.A. Mesures de sécurité physique

V.A.1. Situation géographique et construction des sites

Les sites d'hébergement de l'IGC BNP Paribas sont décrits dans le contrat liant IDEMIA à son prestataire.

Les sites contenant les informations devant être publiées sont ceux de l'hébergeur de IDEMIA.

V.A.2. Accès physique

L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

L'accès aux machines (serveurs, boîtiers cryptographiques, poste d'administration de l'AC, éléments actifs du réseau) est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines (contrôle d'accès par biométrie, droits associés)

V.A.3. Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'IGC telles que fixées par leurs fournisseurs.

Elles permettent également de respecter les exigences de la présente PC, ainsi que les engagements de l'AC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

V.A.4. Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences de la présente PC, ainsi que les engagements pris par l'AC, en tant qu'autorité, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

V.A.5. Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences de la présente PC, ainsi que les engagements pris par l'AC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

V.A.6. Conservation des supports

Les supports (papier, disque dur, CD, etc.) correspondant aux informations relatives à l'activité de l'IGC (fonctions d'exploitation, de sauvegarde, etc.) sont traités et conservés dans une enceinte sécurisée accessibles aux seules personnes autorisées.

V.A.7. Mise hors service des supports

Les supports papier et magnétiques en fin de vie sont systématiquement détruits par des moyens appropriés, permettant d'éviter toute perte de confidentialité.

Les supports de stockage (disque dur de serveurs) de l'IGC ne sont pas réutilisés à d'autres fins avant destruction complète des informations liées à l'IGC qu'ils sont susceptibles de contenir.

V.A.8. Sauvegardes hors site

Les sauvegardes sont stockées sur les différents sites de production de l'hébergeur de l'IGC : en local sur le site primaire et à distance via des mécanismes de synchronisation automatique.

V.B. Mesures de sécurité procédurales

V.B.1. Rôles de confiance

On distingue les rôles suivants :

- **L'officier de sécurité de l'IGC** : il est en charge de l'application de la politique de certification de « BNPPF Instant CA ».
- **Responsable de sécurité physique** : Il est chargé des contrôles d'accès physiques aux équipements des systèmes de la composante d'AC hors AE. Ce responsable est nommé par le partenaire hébergeur de IDEMIA.
- **Opérateurs techniques de l'IGC :** ils sont chargés de l'utilisation, de la configuration et de la maintenance technique des équipements, boîtiers cryptographiques et serveurs. En particulier, ils développent techniquement le déroulement de la cérémonie de clé.
- **Auditeur :**Personne désignée par une autorité compétente (conforme par exemple à « Instruction relative à la procédure d'habilitation des organismes qui procèdent à la qualification des prestataires de services de confiance ») et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante. L'auditeur est nommé par l'organisation BNP Paribas ou IDEMIA.

V.B.2. Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

Pour des raisons de sécurité, les fonctions sensibles seront réparties sur plusieurs personnes. La présente PC requière un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'IGC, celles-ci sont décrites en DPC

V.B.3. Identification et authentification pour chaque rôle

ITG et l'hébergeur de l'IGC font vérifier l'identité et les autorisations de tout personnel avant de lui attribuer un rôle et les droits correspondants. Voir DPC pour plus d'informations.

V.B.4. Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul doivent être respectées.

Les attributions associées à chaque rôle doivent être décrites dans la DPC de l'AC et être conformes à la politique de sécurité de la composante concernée.

V.C. Mesures de sécurité vis-à-vis du personnel

V.C.1. Qualifications, compétences et habilitations requises

Tout le personnel amené à travailler au sein des composantes de l'IGC est soumis contractuellement à une clause de sécurité.

Chaque Service opérant une composante de l'IGC doit s'assurer que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

L'AC et l'opérateur de certification informent toute personne intervenant dans des rôles de confiance de l'IGC :

- De ses responsabilités relatives aux services de l'IGC,
- Des procédures liées à la sécurité du système et au contrôle du personnel.

Chaque personne dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille.

La documentation adéquate est décrite au chapitre V.C.8.

V.C.2. Procédures de vérification des antécédents

Les personnels de l'IGC sont identifiés et ne doivent pas avoir de condamnation en contradiction avec leurs attributions.

V.C.3. Exigences en matière de formation initiale

Le personnel exécutant doit être formé aux logiciels, matériels et procédures internes de fonctionnement de la composante pour laquelle il opère.

V.C.4. Exigences et fréquence en matière de formation continue

Le personnel concerné doit recevoir une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

V.C.5. Fréquence et séquence de rotation entre différentes attributions

En termes de gestion de carrière pour un exploitant donné, les règles à appliquer sont celles pratiquées par l'organisme employeur.

V.C.6. Sanctions en cas d'actions non autorisées

L'autorité de certification décide des sanctions à appliquer lorsqu'un agent abuse de ses droits ou effectue une opération non conforme à ses attributions.

V.C.7. Exigences vis-à-vis du personnel des prestataires externes

Pour les personnels contractants travaillant pour IDEMIA, ils doivent respecter les mêmes conditions que celles énoncées dans les chapitres V.C.1 à V.C.4.

Concernant les personnels contractants travaillant pour BNP Paribas, ils doivent se conformer aux politiques Ressources Humaines et vérifications imposées par leur société.

V.C.8. Documentation fournie au personnel

Les documents dont doit disposer le personnel sont les suivants :

- Déclaration des Pratiques de Certification propre au domaine de certification ;
- Documents constructeurs des matériels et logiciels utilisés ;
- Politiques de Certification supportées par la composante à laquelle il appartient ;
- Procédures internes de fonctionnement.

L'autorité de certification et l'opérateur de certification doivent veiller à ce que leur personnel respectif (comme défini dans la DPC) possède bien les documents identifiés ci-dessus en fonction de leur besoin comme le précise la DPC.

V.D. Procédures de constitution des données d'audit

La journalisation consiste à enregistrer des événements sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

V.D.1. Type d'évènements à enregistrer

L'IGC du groupe BNP Paribas hébergée chez IDEMIA journalise les évènements suivants, automatiquement dès le démarrage d'un système et sous forme électronique, concernant les systèmes liés aux fonctions qu'elle met en œuvre dans le cadre de l'IGC :

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.),
- Démarrage et arrêt des systèmes informatiques et des applications,
- Évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation,
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres évènements doivent pouvoir aussi être recueillis par l''officier de sécurité de IDEMIA, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- Les accès physiques,
- Les actions de maintenance et de changements de la configuration des systèmes,
- Les changements apportés au personnel,
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs,...),

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'IGC doivent également être journalisés, notamment :

- Réception d'une demande de certificat (initiale et renouvellement),
- Validation / rejet d'une demande de certificat,
- Évènements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...),
- Génération des certificats des porteurs,
- Publication et mise à jour des informations liées à l'AC (PC,certificats d'AC, conditions générales d'utilisation, etc.),
- Réception d'une demande de révocation,
- Validation / rejet d'une demande de révocation,
- Génération puis publication des CRL

Chaque enregistrement d'un évènement dans un journal doit contenir au minimum les champs suivants :

- Type de l'évènement,
- Nom de l'exécutant ou référence du système déclenchant l'évènement,
- Date et heure de l'évènement,
- Résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer explicitement dans l'un des champs du journal d'évènements.

V.D.2. Fréquence de traitement des journaux d'évènements

L'analyse du contenu des journaux d'événements doit être effectuée de manière régulière au minimum une fois par trimestre.

V.D.3. Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés 7 ans.

V.D.4. Protection des journaux d'évènements

L'IGC du groupe BNP Paribas met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente politique.

V.D.5. Procédure de sauvegarde des journaux d'évènements

L'IGC du groupe BNP Paribas met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente politique.

Une copie de sauvegarde des journaux d'événements est réalisée après chaque cérémonie sur les plates-formes de l'IGC du groupe BNP Paribas.

V.D.6. Système de collecte des journaux d'évènements

L'IGC du groupe BNP Paribas s'appuie sur les systèmes de collecte internes à chacune de ses composantes.

V.D.7. Notification de l'enregistrement d'un évènement au responsable de l'évènement

Sans objet.

V.D.8. Évaluation des vulnérabilités

Le processus d'évaluation des vulnérabilités est référencé dans l'analyse de risque menée par IDEMIA et BNP Paribas sur son IGC.

Des tests d'intrusion complémentaires sont réalisés périodiquement.

V.E. Archivage des données

V.E.1. Types de données à archiver

L'archivage permet de :

- Assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.
- Conserver les pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver concernent aussi bien le format papier que le format électronique.

Les données à archiver sont les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques
- La PC
- Les certificats et CRLs tels qu'émis ou publiés
- Les données d'audit
- Les journaux d'évènements des différentes entités de l'IGC
- Les pièces papiers liées à l'IGC

V.E.2. Procédure de constitution des archives

Pour tout ce qui concerne les archives liées aux certificats clients il faut se référer aux informations relatives aux données stockées dans le dossier de preuve qui se trouvent dans les annexes de la DPC.

Se référer au chapitre correspondant de la DPC.

V.E.3. Période de conservation des archives

La durée de conservation des archives électronique est la suivante :

- Durée de rétention des archives de journaux d'évènements : 1 ans
- Durée de rétention des archives de certificats, CRL après leur expiration : 7 ans
- Les dossiers d'enregistrement contenant les éléments relatifs à l'exécution du Service et les traces techniques assurant l'imputabilité des actions sont conservés à minima 10 ans à compter de la fin du Document concerné, signé avec le Certificat

V.E.4. Durée de restitution des archives

Les archives peuvent être récupérées dans un délai inférieur à 5 jours ouvrés.

V.E.5. Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, sont :

- Protégées en intégrité,
- Accessibles aux personnes autorisées,
- Accessibles pour relecture et exploitation.

La DPC précise les moyens mis en œuvre pour archiver les pièces en toute sécurité.

V.E.6. Exigences d'horodatage des données

Se référer au chapitre correspondant de la DPC.

V.E.7. Système de collecte des archives

Le système de collecte des archives est celui du système d'informations de IDEMIA et de son hébergeur.

V.E.8. Procédures de récupération et de vérification des archives

Les archives sont sous la gestion de l'IGC du groupe BNP Paribas. Le processus de récupération doit faire l'objet d'une procédure interne de fonctionnement mentionnée dans la DPC des AC en lignes. La récupération doit être effectuée sous un délai maximal égal à 5 jours ouvrés.

V.F. Changement de clé de l'autorité

L'autorité « BNPPF Instant CA » ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant à la sienne. Pour cela, la période de validité de son certificat est supérieure à celle des certificats qu'elle signe.

Aussi lorsqu'elle accède à une demande de certification, l'autorité « BNPPF Instant CA » fixe la durée de vie du certificat demandé de telle sorte qu'il ne soit jamais valable au-delà de la date de fin de validité du certificat de sa bi-clé utilisée pour la signature.

V.G. Reprise suite à compromission et sinistre

V.G.1. Procédures de remontée et de traitement des incidents et des compromissions

Les équipes d'exploitation de IDEMIA mettent en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels

L'analyse des différents journaux d'évènements est contrôlée par l'officier de sécurité de IDEMIA.

V.G.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

La sauvegarde des composants de l'IGC permet d'assurer une reprise d'activité en cas de sinistre sous 48 heures. Ceci ne s'applique que lorsque des CRL doivent être générées en urgence.

V.G.3. Procédures de reprise en cas de compromission de la clé privée d'une composante

Dans le cas de compromission d'une clé d'autorité, le certificat correspondant est immédiatement révoqué (en fonction des délais de réalisation de la cérémonie de clés).

V.G.4. Procédures de reprise en cas de compromission d'un algorithme d'une composante

Dans le cas de compromission d'un algorithme employé dans un certificat d'autorité, le certificat correspondant est révoqué par le biais d'une réalisation de la cérémonie de clés.

V.G.5. Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC du groupe BNP Paribas disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente politique.

S'agissant de l'autorité en ligne, la continuité d'activité consiste à restaurer l'IGC à partir des sauvegarde et secrets.

V.H. Fin de vie de l'IGC du groupe BNP Paribas

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

En cas de cessation d'activité, BNP Paribas et IDEMIA s'engagent à mettre en œuvre les moyens humains permettant de révoquer tous les certificats d'AC de l'IGC.

Enfin, dans les cas où IDEMIA ne pourrait assurer la prise en charge des coûts nécessaires à la poursuite des opérations de l'AC, par exemple en cas de cessation d'activité, BNP Paribas s'engage à couvrir les coûts nécessaires.

V.H.1. Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC doit entre autres obligations :

- mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats) ;
- assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des CRL), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC.
- communiquer au préalable son intention de transfert d'activité à une date donnée ;
- mettre en œuvre tous les moyens dont elle dispose pour informer ses partenaires (utilisateurs finaux, autres composantes, autres IGC, etc.) de ses intentions de fin d'activité ;

- l'AC doit préciser dans sa DPC qui elle doit prévenir, comment se déroule le transfert des obligations (archives et logs à une autre entité), et comment seront traités les certificats encore valides qui seraient amenés à être révoqués.

V.H.2. Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées aux trois premiers items ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des ARL conformément aux engagements pris dans sa PC.

Lors de l'arrêt du service, l'AC doit :

- S'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
- Prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- Révoquer son certificat ;
- Révoquer les certificats valides qu'elle a signé (uniquement pour une fin de vie due à une compromission ou suspicion de compromission de clé, une perte ou un vol) ;
- Révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- Informer (par exemple par récépissé) tous les porteurs des certificats révoqués ou à révoquer ;
- Les clés privées de l'AC doivent être détruites ou ne doivent plus être utilisées ;
- Communiquer en amont son intention de cessation d'activité.

En fin de vie l'IGC, l'autorité « BNPP Service CA » :

- Révoque tous les certificats encore valides qu'elle a signée, y compris les siens ;
- Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante.

VI. Mesures de sécurité techniques

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que les autorités « BNPPF Instant CA » doivent respecter.

La DPC décrit les moyens mis en œuvre pour respecter ces exigences.

VI.A. Génération et installation de bi clés

VI.A.1. Génération des bi-clés

a) Clés d'autorité

La génération des clés de signature de l'autorité « BNPPF Instant CA » est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance, dans le cadre de « cérémonies des clés ». Ces cérémonies se déroulent suivant des scripts préalablement définis.

Les clés de signature de l'autorité « BNPPF Instant CA » sont générées et mises en œuvre dans un boitier cryptographique dont les caractéristiques sont décrites dans la DPC.

La confidentialité des clés est notamment assurée par des mesures techniques détaillées dans la DPC.

b) Clés des porteurs

La génération de la bi-clé d'un porteur est assurée par un module cryptographique matériel (HSM) dont les exigences sont décrites au §VI.B.1.

VI.A.2. Transmission de la clé privée à son propriétaire

a) Clés d'autorité

Se référer au chapitre correspondant de la DPC.

b) Clés des porteurs

La clé privée du porteur est maintenue sous le seul contrôle de l'individu via un logiciel de signature et n'est utilisable que par ce logiciel lors d'une signature d'un document mis à disposition par BNP Paribas Fortis ou de révocation lors d'un refus de signature. Elle est détruite immédiatement après son utilisation.

VI.A.3. Transmission de la clé publique à l'AC

Les clés publiques des porteurs sont remises à l'AC à partir de demandes générées par le logiciel de signature dans un format qui permet de prouver la possession de la clé, en signant la requête.. La signature est vérifiée par l'AC. Celle-ci émet un certificat si cette vérification est correcte. La délivrance est ainsi protégée en intégrité de bout en bout lors de la demande de génération du certificat.

VI.A.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats

L'IGC du groupe BNP Paribas met à disposition tous les certificats d'autorité via son service de publication.

L'AC peut remettre également son certificat sur un support amovible directement aux participants d'une cérémonie de clés.

VI.A.5. Taille des clés

Les autorités utilisent des clés de 4096 bits.

Les porteurs utilisent des clés de 2048 bits minimum.

Les certificats des répondeurs OCSP utilisent des clés de 2048 bits minimum.

L'AC suit les recommandations cryptographiques de l'ANSSI dans le cadre du RGS.

VI.A.6. Vérification de la génération des paramètres des bi-clés et de leur qualité

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé (cf. chapitre VII).

VI.A.7. Durée de vie des clés

Cf. chapitre VI.C.2.

VI.A.8. Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats et de CRL.

Pour les certificats des porteurs, cf. I.D.1.

Pour les certificats OCSP, cf.I.D.3.

VI.B. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

VI.B.1. Standards et mesures de sécurité pour les modules cryptographiques

a) Clés d'autorité

Se référer au chapitre correspondant de la DPC.

b) Clés des porteurs

La clé privée du porteur est protégée par un boitier cryptographique dont le niveau de résistance est a minima FIPS 140-2 level 2.

VI.B.2. Contrôle de la clé privée par plusieurs personnes

a) Clés d'autorité

Se référer au chapitre correspondant de la DPC.

b) Clés des porteurs

La clé privée des porteurs n'est pas contrôlée par plusieurs personnes.

VI.B.3. Séquestre de la clé privée

Sans objet

VI.B.4. Copie de secours de la clé privée

a) Clés d'autorité

Se référer au chapitre correspondant de la DPC.

b) Clés des porteurs

Les clés privées des porteurs ne font l'objet d'aucune copie de secours par l'AC.

VI.B.5. Archivage de la clé privée

a) Clés d'autorité

Se référer au chapitre correspondant de la DPC.

b) Clés des porteurs

Les clés privées des porteurs ne sont en aucun cas archivées.

VI.B.6. Transfert de la clé privée vers / depuis le module cryptographique

Cf. chapitre VI.B.4.

VI.B.7. Stockage de la clé privée dans un module cryptographique

a) Clés d'autorité

Se référer au chapitre correspondant de la DPC.

b) Clés des porteurs

Les clés privées des porteurs sont stockées dans un module cryptographique répondant au minimum aux exigences du chapitre XI ci-dessous.

VI.B.8. Méthode d'activation de la clé privée

a) Clés d'autorité

Se référer au chapitre correspondant de la DPC.

b) Clés des porteurs

Les clés sont activées une fois générées.

VI.B.9. Méthode de désactivation de la clé privée

a) Clés d'autorité

Se référer au chapitre correspondant de la DPC.

b) Clés des porteurs

Non applicable.

VI.B.10. Méthode de destruction des clés privées

a) Clés d'autorité

Se référer au chapitre correspondant de la DPC.

b) Clés des porteurs

La destruction des clés est déclenchée au terme de l'opération de signature.

VI.B.11. Niveau d'évaluation sécurité du module cryptographique

a) Clés d'autorité

Les modules cryptographiques d'une AC de l'IGC du groupe BNP Paribas sont évalués au niveau correspondant à l'usage visé, tel que précisé au chapitre XI ci-dessous.

b) Clés des porteurs

Voir le paragraphe précédent.

VI.C. Autres aspects de la gestion des bi-clés

VI.C.1. Archivage des clés publiques

a) Clés d'autorité

Les clés publiques des AC de l'IGC du groupe BNP Paribas sont archivées dans le cadre de l'archivage des certificats correspondants.

b) Clés des porteurs

Elles ne sont pas archivées.

VI.C.2. Durées de vie des bi-clés et des certificats

S'agissant d'un certificat d'AC,

- La durée de vie des clés est de 23 ans.

S'agissant d'un certificat éphémère,

- La durée de vie des certificats est paramétrable et est de 1 heure au maximum.
- La durée de vie des bi-clés est limitée à son association à un certificat

S'agissant d'un certificat OCSP,

- La durée de vie des clés est de 1 an.

La fin de validité d'un certificat d'AC est postérieure à la fin de vie des certificats qu'elle émet.

VI.D. Données d'activation

VI.D.1. Génération et installation des données d'activation du HSM

a) S'agissant des clés d'autorité

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC se font lors de la phase d'initialisation et de personnalisation du boîtier cryptographique. Les données d'activation sont choisies et saisies par les responsables de ces données eux-mêmes.

b) S'agissant des clés de porteurs

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC se font lors de la phase d'initialisation et de personnalisation du boîtier cryptographique. Les données d'activation sont choisies et saisies par les responsables de ces données eux-mêmes.

Elles ne sont connues que par les membres d'ITG dans le cadre des rôles qui leurs sont attribués.

VI.D.2. Protection des données d'activation du HSM

Les données d'activation générées pour les modules cryptographiques de l'IGC du groupe BNP Paribas sont protégées en intégrité et en confidentialité.

VI.D.3. Protection des données d'activation correspondant aux clés privées des porteurs

Se référer au chapitre correspondant de la DPC.

VI.D.4. Autres aspects liés aux données d'activation

Se référer au chapitre correspondant de la DPC.

VI.E. Mesures de sécurité des systèmes informatiques

VI.E.1. Exigences de sécurité techniques spécifiques aux systèmes informatiques

Se référer au chapitre correspondant de la DPC.

VI.E.2. Niveau de qualification des systèmes informatiques

Le module cryptographique utilisé par l'IGC du groupe BNP Paribas fait l'objet d'une certification critère commun EAL4+.

VI.F. Mesures de sécurité liées au développement des systèmes

Les environnements de développement sont distincts de l'environnement de production.

VI.F.1. Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'IGC du groupe BNP Paribas doit être documentée et doit apparaître dans les procédures de fonctionnement interne de la composante concernée et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

VI.F.2. Niveau d'évaluation sécurité du cycle de vie des systèmes

La présente politique ne formule pas d'exigence spécifique sur le sujet.

VI.G. Mesures de sécurité réseau

Les interconnexions et accès aux ressources de l'IGC sont contrôlés par des équipements et logiciels permettant une segmentation des données, services et utilisateurs par rôle et fonction. Ces solutions assurent le contrôle des flux entrants et sortants. Les modifications des ports ouverts, droits d'accès et des modifications doivent être tracées systématiquement dans un espace de suivi de modifications des accès logiques.

VI.H. Horodatage / Système de datation

Pour dater ces évènements, les différentes composantes de l'IGC utilisent l'heure système de l'IGC en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près.

VII. Profils des certificats, OCSP et des CRL

VII.A. Profil des certificats

VII.A.1. Numéro de version

Les certificats émis dans le cadre de l'IGC du groupe BNP Paribas respectent la norme X.509 v3.

VII.A.2. Champs de base

Les certificats respectent le format de base des certificats définis dans la recommandation x.509v3 et incluent au minimum les champs de base suivants :

Nom du champ	Description	Contenu
Version	Version du certificat X.509	Contient la valeur 2 pour indiquer que le certificat est un certificat x.509v3
SerialNumber	Numéro de série du certificat	Contient une valeur entière pour indiquer le numéro de série du certificat, cette valeur doit être unique pour chaque certificat émis par l'autorité racine.
Signature	Signature de l'autorité pour l'authentifier	Sha2WithRSAEncryption
Issuer	Nom de l'autorité	Contient le DN (X.500) de l'autorité. L'émetteur est l'une des valeurs suivantes : - CN=BNP Paribas Fortis Customer Ephemeral Certification Authority 1, OU=VATBE-0403199702, O=BNP Paribas Fortis, C=BE - CN=BNP Paribas Fortis Customer Ephemeral Certification Authority 2, OU=VATBE-0403199702, O=BNP Paribas Fortis, C=BE
Validity	Période de validité du certificat	Contient les dates/ heures d'activation et d'expiration du certificat.
Subject	Nom du porteur	Contient le DN du porteur (voir le paragraphe III.A.5)
Subject Public Key Info	Informations sur la clé publique de l'abonné	Contient l'OID de l'algorithme et la clé publique de l'abonné
Extensions	Liste des extensions	Voir chapitre suivant

VII.A.3. Extensions du certificat

Les certificats émis par l'autorité de certification « BNPPF Instant CA » comportent les extensions X.509v3 suivantes. La DPC précise les valeurs utilisées.

a) S'agissant des certificats de porteurs

Extension	Extension critique	Description
Authority Key Identifier	N	Elément d'identification de la clé publique de l'autorité signant le certificat
Basic Constraint	O	Indique que le certificat est une entité finale.
Certificate Policies	N	OID de la PC régissant le certificat et Intitulé de la PC. Les OID possibles sont les suivants : - 1.2.250.1.62.10.7.1.1.2 - 1.2.250.1.62.10.8.1.1.2
Subject Key Identifier	N	Elément d'identification de la clé publique du porteur
KeyUsage	O	Description des utilisations autorisées de la clé privée : Non repudiation
CRL Distribution Point	N	Contient l'URL de la CRL (voir le paragraphe IV.J.1).
Authority Information Access	N	Informations d'accès au certificat de l'autorité.

b) S'agissant des certificats OCSP

Extension	Extension critique	Description
Authority Key Identifier	N	Elément d'identification de la clé publique de l'autorité signant le certificat
Basic Constraint	O	Indique que le certificat est une entité finale.
Key Usage	O	Description des utilisations autorisées de la clé privée : digitalSignature
Extended Key Usage	N	Indique que le certificat signe les réponses OCSP (ocspSigning)
Certificate Policies	N	OID de la PC régissant le certificat et Intitulé de la PC. Les OID possibles sont les suivants : - 1.2.250.1.62.10.7.1.2.1 - 1.2.250.1.62.10.8.1.2.1
OCSP no Check	N	Indique au client OCSP de faire confiance au

Extension	Extension critique	Description
		répondeur OCSP pour la durée de vie du certificat.
Subject Key Identifier	N	Elément d'identification de la clé publique du porteur

VII.A.4. OID des algorithmes

Les identificateurs d'algorithmes doivent être inscrits auprès d'un registre (par exemple, un registre international tel que celui de l'ISO).

L'algorithme de condensat utilisé dans le cadre de l'IGC du groupe BNP Paribas est SHA-2 (OID 2.16.840.1.101.3.4.2.1). L'algorithme de chiffrement utilisé dans le cadre de l'IGC du groupe BNP Paribas est RSA.

La signature est effectuée en RSA-SHA256 dont l'OID est 1.2.840.113549.1.1.11.

VII.A.5. Forme des noms

Dans le cadre de l'IGC du groupe BNP Paribas, les noms attribués aux porteurs et aux certificats OCSP respectent la norme X.500, comme détaillé au chapitre III.A de ce document.

VII.A.6. OID des politiques de certification

a) Certificats d'autorité

Les acteurs présents lors de la cérémonie de clés s'assurent que les certificats émis contiennent l'OID « Any Policy » (2.5.29.32.0).

b) Certificats des porteurs

Les certificats des porteurs référencent l'OID de la présente politique de certification.

VII.A.7. Utilisation de l'extension « contraintes de politique »

La présente politique n'émet pas d'exigence particulière sur ce sujet.

VII.A.8. Sémantique et syntaxe des qualifiants de politique

La présente politique n'émet pas d'exigence particulière sur ce sujet.

VII.A.9. Sémantiques de traitement des extensions critiques de la politique de certification

La présente politique n'émet pas d'exigence particulière sur ce sujet.

VII.B. Profil des CRL

VII.B.1. Numéro de version

Les CRL émises utilisent la version 2 du format défini dans la norme ISO [9594-8].

VII.B.2. Champs de base

Les champs de base des CRL émise par l'autorité racine sont les suivants :

Champ	Description
Version	Version de la CRL X.509
Signature	Identifiant de l'algorithme utilisé pour produire le sceau d'intégrité de la liste Sha2WithRSAEncryption retenu pour la présente PC.
Issuer	Nom de l'autorité de l'IGC du groupe BNP Paribas. L'émetteur est l'une des valeurs suivantes : - CN=BNP Paribas Fortis Customer Ephemeral Certification Authority 1, OU=VATBE-0403199702, O=BNP Paribas Fortis, C=BE - CN=BNP Paribas Fortis Customer Ephemeral Certification Authority 2, OU=VATBE-0403199702, O=BNP Paribas Fortis, C=BE
This Update	Date d'émission de la CRL
Next Update	Date limite d'émission de cette CRL
Revoked Certificates	Liste d'enregistrement de révocation. On spécifiera pour chaque révocation les valeurs associées aux champs suivants : - User Certificate (numéro de série du certificat révoqué) - Revocation Date (date de révocation du certificat).
CRL Extensions	Extensions générales de la CRL

La CRL dans sa forme finale est l'ensemble des éléments suivants :

Champ	Description
tbsCertlist	L'ensemble des champs décrits ci-dessus
signatureAlgorithm	L'identifiant de l'algorithme utilisé pour produire le sceau d'intégrité de la liste Sha2WithRSAEncryption retenu pour la présente PC.
signatureValue	Le résultat de cet algorithme sur l'ensemble des champs de tbsCertList

VII.C. Extensions de CRL et d'entrées de CRL

Les CRL incluent les champs de base présentés au paragraphe précédent, ainsi que les extensions d'entrée suivantes :

Extension d'entrée	Description
Authority Key Identifier	Identifie la clé publique de l'autorité ayant signé la CRL

CRL Number	Donne un nombre croissant séquentiel pour chaque CRL émise
MS "CA Version"	Extension Microsoft AD CS liée à la version des clés d'AC
MS "CRL Next Publish"	Extension Microsoft AD CS liée à la date de prochaine publication
Reason Code	Identifie la cause de révocation du certificat.

VIII. Audit de conformité et autres évaluations

VIII.A. Fréquences et / ou circonstances des évaluations

Un contrôle de conformité, par rapport au référentiel de l'ETSI EN 319 411-1 LCP, de l'ensemble de l'IGC du groupe BNP Paribas est réalisé tous les deux ans. Un audit interne sera mené par BNP Paribas tous les ans.

VIII.B. Identités / qualifications des évaluateurs

Le contrôle d'une composante doit être assigné par la direction de IDEMIA ou BNP Paribas à une équipe d'acteurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée

De la même façon, les acteurs menant les audits internes devront respecter les conditions stipulées dans le paragraphe précédent.

VIII.C. Relations entre évaluateurs et entités évaluées

L'organisation des audits internes est écrite dans la DPC associée.

VIII.D. Sujets couverts par les évaluations

Les contrôles de conformité ou des contrôles internes menés par BNP Paribas portent sur l'ensemble de l'IGC du groupe BNP Paribas et vise à vérifier le respect des engagements et pratiques définies dans la présente politique de certification et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

VIII.E. Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité ou d'un audit interne, l'évaluateur émet auprès de ITG un rapport de conformité assorti de recommandations.

ITG, par délégation aux acteurs identifiés dans la présente politique, a en charge la résolution des points de non-conformité ainsi que le choix de la mesure à appliquer.

VIII.F. Communication des résultats

Les résultats des audits de conformité sont confidentiels et ne peuvent être communiqué à des tiers qu'en cas de demande explicite.

De plus, les résultats des audits de conformité et des audits menés en interne seront communiqués à la PMA.

IX. Annexe 1 - Autres problématiques métiers et légales

IX.A. Tarifs

La tarification appliquée par BNP Paribas Fortis à l'utilisateur du certificat est spécifiée dans les conditions générales applicables au canal de BNP Paribas Fortis dans lequel le certificat est utilisé.

IX.B. Responsabilité financière

La responsabilité financière de BNP Paribas Fortis à l'égard de l'utilisateur du certificat est spécifiée et limitée dans les conditions générales applicables au canal de BNP Paribas Fortis dans lequel le certificat est utilisé.

IX.C. Confidentialité des données professionnelles

IX.C.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- La DPC correspondante à la présente PC
- Les clés privées des composantes et des porteurs de certificats de l'IGC du groupe BNP Paribas
- Les données d'activation associées aux clés privées des autorités de l'IGC du groupe BNP Paribas
- Tous les secrets de l'IGC du groupe BNP Paribas
- Les journaux d'évènements des composantes de l'IGC du groupe BNP Paribas
- Le dossier d'enregistrement des porteurs
- Les procès-verbaux des cérémonies de clés.

IX.C.2. Informations hors du périmètre des informations confidentielles

Sans objet.

IX.C.3. Responsabilités en termes de protection des informations confidentielles

BNP Paribas Fortis, en tant qu'autorité de certification, est tenue de respecter la législation et la réglementation en vigueur sur le territoire belge.

IX.D. Protection des données personnelles

BNP Paribas Fortis applique la législation et la réglementation applicables relatives à la protection des données personnelles, tant en matière de collecte que d'usage des données à caractère personnel (loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel ; Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) à partir du 25 mai 2018).

IX.D.1. Politique de protection des données à caractère personnel

Il est entendu que toute collecte et tout usage de données à caractère personnel par l'ensemble de ses composantes de l'IGC du groupe BNP Paribas sont réalisés dans le strict respect de la législation et de la réglementation en vigueur.

IX.D.2. Données à caractères personnel

Les données considérées comme personnelles sont au moins les suivantes :

- toutes les données concernant le dossier d'enregistrement des porteurs

IX.D.3. Données à caractères non personnel

Aucune exigence spécifique n'est formulée à ce sujet.

IX.D.4. Responsabilité en termes de protection des données personnelles

BNP Paribas Fortis est le responsable du traitement des données à caractère personnel des utilisateurs de certificats.

IX.D.5. Notification et consentement d'utilisation des données personnelles

Le traitement des données à caractère personnel des utilisateurs de certificats fait l'objet des informations, notifications et collectes de consentement spécifiées dans les conditions générales applicables au canal de BNP Paribas Fortis dans lequel le certificat est utilisé.

IX.D.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Cf. législation et réglementation en vigueur sur le territoire belge.

IX.D.7. Autres circonstances de divulgation de données à caractère personnel

Cf. législation et réglementation en vigueur sur le territoire belge.

IX.E. Droits sur la propriété intellectuelle et industrielle

Application de la législation et de la réglementation en vigueur sur le territoire belge.

IX.F. Interprétations contractuelles et garanties

Les obligations communes aux composantes de l'IGC sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent,
- respecter et appliquer la partie de la DPC leur incombant,
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre VIII),
- respecter les accords ou contrats qui les lient entre elles ou aux porteurs,
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

IX.F.1. Autorité de Certification

L'AC a pour obligation de :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un porteur donné et que ce porteur a accepté le certificat, conformément aux exigences du chapitre IV.4 ci-dessus.
- Garantir et maintenir la cohérence de sa DPC avec sa PC.

- Prendre toutes les mesures raisonnables pour s'assurer que ses porteurs sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC. La relation entre un porteur et l'AC est formalisée par un lien contractuel précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

IX.F.2. Service d'enregistrement

Voir le paragraphe IX.F.1.

IX.F.3. Porteurs de certificats

Le porteur a le devoir de vérifier et communiquer des informations exactes et à jour lors du processus d'identification (identité de la personne physique par exemple) ;

IX.F.4. Utilisateurs de certificats

L'utilisateur de certificat ne peut faire usage du certificat que dans le canal de BNP Paribas Fortis dans lequel sa création est proposée, et dans le cadre des seules relations entre l'utilisateur du certificat et BNP Paribas Fortis.

IX.F.5. Autres participants

Aucune exigence spécifique n'est formulée dans le cadre de la présente PC

IX.G. Limite de garantie

La responsabilité de BNP Paribas Fortis à l'égard de l'utilisateur du certificat est spécifiée et limitée dans les conditions générales applicables au canal de BNP Paribas Fortis dans lequel le certificat est utilisé

IX.H. Limite de responsabilité

La responsabilité de BNP Paribas Fortis à l'égard de l'utilisateur du certificat est spécifiée et limitée dans les conditions générales applicables au canal de BNP Paribas Fortis dans lequel le certificat est utilisé

IX.I. Indemnités

La responsabilité financière de BNP Paribas Fortis à l'égard de l'utilisateur du certificat est spécifiée et limitée dans les conditions générales applicables au canal de BNP Paribas Fortis dans lequel le certificat est utilisé

IX.J. Durée et fin anticipée de validité de la PC

IX.J.1. Durée de validité

La PC de l'AC doit rester en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

IX.J.2. Effets de la fin de validité et clauses restants applicables

Aucune exigence spécifique n'est formulée dans le cadre de la présente PC.

IX.K. Notifications individuelles et communications entre les participants

Aucune exigence spécifique n'est formulée dans le cadre de la présente PC.

IX.L. Amendements à la PC

IX.L.1. Procédures d'amendements

Les amendements majeurs apportés à la présente PC doivent être présentés lors d'une Policy Management Authority (PMA) afin de valider les modifications apportées et ce, en préalable de la publication de la nouvelle version de PC.

Dans le cas d'amendements mineurs (coquilles, fautes de frappe, etc.), ces amendements ne requièrent pas de validation formelle de la PMA pour déclencher la publication de la nouvelle version de la PC.

IX.L.2. Mécanisme et période d'informations sur les amendements

Aucun mécanisme n'est prévu pour donner de l'information sur les amendements effectués.

IX.L.3. Circonstances selon lesquelles l'OID doit être changé

Le changement d'OID de la PC est déclenché dès lors que les amendements apportés par la PC sont majeurs et approuvés par la PMA.

Dans ce cas, le dernier chiffre de l'OID sera modifié afin de refléter les amendements majeurs.

IX.M. Dispositions concernant la résolution de conflits

En cas de litige, le porteur doit contacter les points de contact indiqué dans le chapitre I.E.2.

IX.N. Juridictions compétentes

Application de la législation et de la réglementation en vigueur sur le territoire belge.

IX.O. Conformités aux législations et réglementations

Application de la législation et de la réglementation en vigueur sur le territoire belge.

IX.P. Dispositions diverses

Aucune exigence spécifique n'est formulée dans le cadre de la présente PC.

IX.Q. Autres dispositions

Aucune exigence spécifique n'est formulée dans le cadre de la présente PC.

X. Annexe 2 – Documents cités en référence

X.A. Réglementation

Non applicable.

X.B. Documents techniques

Référence	Objet du document
FIPS140-2_LEVEL3_CERT	Certificat de qualification FIPS 140-2 level 3 du boitier cryptographique nShield (firmware 2.50.16)

Toutes les procédures détaillées relatives à cette PC sont décrites dans les annexes de la DPC qui est consultable à la demande par les personnes autorisées (cf. chapitre I.E.2)

XI. Annexe 3 - Exigences de sécurité du module cryptographique des AC

XI.A. Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'IGC du groupe BNP Paribas pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des CRL), ainsi que générer les bi-clés des porteurs, doit répondre aux exigences de sécurité suivantes :

- Assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- Etre capable d'identifier et d'authentifier ses utilisateurs ;
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- Etre capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- Permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- Garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

XI.B. Exigence sur la qualification

Le module cryptographique utilisé par l'IGC du groupe BNP Paribas n'est pas qualifié selon le processus décrit dans le Référentiel Général de Sécurité de l'administration française.

XII. ANNEXE 4 : Procédures enregistrement – authentification et autorisation acceptées sous la présente PC.

XII.A. Procédure basée sur carte EMV pour client retail

1) Etape 1 : enregistrement (REG).

La banque procède aux étapes d'enregistrement 1.1 et 1.2 telles que décrites dans la présente PC.

La Banque est en charge de remettre à l'utilisateur qu'elle enregistre:

- la carte bancaire intelligente (standard EMV) qui permet de s'authentifier grâce au protocole M1 et de signer grâce au protocole M2.
- son code PIN
- l'UCR brandé au nom de BNP Paribas Fortis

La banque associe la carte à l'utilisateur de façon non ambiguë.

2) Etape 2 : authentification (AUTH)

Lors cette étape, le client s'authentifie de manière unique (SMID : numéro client) en tant que personne physique dans son canal électronique bancaire Easy Banking Web (EBW) avec sa carte bancaire (procédure M1).

3) Etape 3 : autorisation (AUT)

La personne physique encode le challenge M2 de sa carte bancaire en tant que personne physique (SMID) dans son canal électronique bancaire. Cette étape officialise la demande de création d'un certificat de signature.

Si cette demande est **valable, une requête de certificat est envoyée à l'AE technique** qui fait générer un certificat au nom de la personne physique (prénom - nom).

XII.B. Procédure basée sur carte PRO pour client professionnel

1) Etape 1 : enregistrement (REG).

La banque procède aux étapes d'enregistrement 1.1 et 1.2 telles que décrites dans la présente PC.

La Banque est en charge de remettre à l'utilisateur qu'elle enregistre, ou d'associer à cet utilisateur, la carte bancaire intelligente (standard Isabel) qui permet de s'authentifier et signer et optionnellement remettre son code PIN ; l'activation de la carte pour le canal électronique bancaire Easy Banking Business (EBB) se fait d'une façon sécurisée : soit en face à face à la Banque soit en ligne par l'utilisateur, via sa carte d'identité belge (Belgium eID) avec l'utilisation de son code PIN.

La banque peut également remettre à l'utilisateur qu'elle enregistre une carte bancaire intelligente (EBB) qui permet de s'authentifier et signer.

2) Etape 2 : authentification (AUTH)

Lors de cette étape, la personne physique s'authentifie de manière unique dans canal électronique bancaire avec sa carte et son code PIN. La carte peut-être :

- Une carte EBB fournie par BNPP Fortis
- Une carte Isabel fournie par BNPP Fortis
- Une carte Isabel fournie par une autre banque

3) Etape 3 : autorisation (AUT)

La personne physique utilise sa carte EBB ou Isabel dans son canal électronique bancaire et encode son code PIN. Cette étape officialise la demande de création d'un certificat de signature.

Si cette demande est **valable, une requête de certificat est envoyée à l'AE technique** qui fait générer un certificat au nom de la personne physique (prénom - nom).

XII.C. Procédure basée sur EMV & itsme pour client retail

1) Etape 1 : enregistrement (REG).

La banque procède aux étapes d'enregistrement 1.1 et 1.2 telles que décrites dans la présente PC.

La Banque est en charge de remettre à l'utilisateur qu'elle enregistre :

- la carte bancaire intelligente (standard EMV) qui permet de s'authentifier grâce au protocole M1 et de signer grâce au protocole M2.
- son code PIN
- l'UCR brandé au nom de BNP Paribas Fortis

La banque associe la carte à l'utilisateur de façon non ambiguë.

L'activation itsme pour le canal électronique bancaire Easy Banking Business (EBB) se fait d'une façon sécurisée par l'utilisateur, via l'utilisation une session sécurisée où il s'est préalablement authentifié de manière unique (SMID : numéro client) en tant que personne physique dans son canal électronique bancaire Easy Banking Web (EBW) avec sa carte bancaire (procédure M1).

2) Etape 2 : authentification (AUTH)

Lors cette étape, le client s'authentifie de manière unique (SMID : numéro client) en tant que personne physique dans son canal électronique bancaire Easy Banking Web (EBW) avec son application itsme, enregistrée à l'étape 1 ci-dessus.

3) Etape 3 : autorisation (AUT)

La personne physique encode le challenge M2 de sa carte bancaire en tant que personne physique (SMID) dans son canal électronique bancaire. Cette étape officialise la demande de création d'un certificat de signature.

Si cette demande est **valable, une requête de certificat est envoyée à l'AE technique** qui fait générer un certificat au nom de la personne physique (prénom - nom).

XII.D. Procédure basée sur carte PRO & ITSME pour client professionnel

1) Etape 1 : enregistrement (REG).

La banque procède aux étapes d'enregistrement 1.1 et 1.2 telles que décrites dans la présente PC.

La Banque est en charge de remettre à l'utilisateur qu'elle enregistre, ou d'associer à cet utilisateur, la carte bancaire intelligente (standard Isabel) qui permet de s'authentifier et signer et optionnellement remettre son code PIN ; l'activation de la carte pour le canal électronique bancaire Easy Banking Business (EBB) se fait d'une façon sécurisée : soit en face à face à la Banque soit en ligne par l'utilisateur, via sa carte d'identité belge (Belgium eID) avec l'utilisation de son code PIN.

La banque peut également remettre à l'utilisateur qu'elle enregistre une carte bancaire intelligente (EBB) qui permet de s'authentifier et signer.

L'activation itsme pour le canal électronique bancaire Easy Banking Business (EBB) se fait d'une façon sécurisée par l'utilisateur, via l'utilisation une session sécurisée où il s'est préalablement authentifié de manière unique (SMID : numéro client) en tant que personne physique dans son canal électronique bancaire Easy Banking Web (EBW) avec sa carte bancaire (procédure M1).

2) Etape 2 : authentification (AUTH)

Lors cette étape, le client s'authentifie de manière unique (SMID : numéro client) en tant que personne physique dans son canal électronique bancaire Easy Banking Business (EBB) avec son application itsme, enregistrée à l'étape 1 ci-dessus.

3) Etape 3 : autorisation (AUT)

La personne physique choisit ITSME dans son canal électronique bancaire et ensuite utilise ITSME et son ITSME pincode pour authoriser la demande de création d'un certificat de signature. Cette étape officialise la demande de création d'un certificat de signature.

Si cette demande est **valable, une requête de certificat est envoyée à l'AE technique** qui fait générer un certificat au nom de la personne physique (prénom - nom).