Politique d'enregistrement BNP Paribas Fortis

Autorité d'enregistrement

de l'autorité de certification Mediacert

itg

Revue		
Nom	Fonction	Date

Validation		
Nom	Fonction	Date
PMA	Instance de gouvernance	18/10/23

Suivi des versions			
Version	Date	Auteur	Nature des modifications
0.4.1	23/09/2020	Sealweb	Initialisation du document
0.4.2	21/10/2020	Sealweb	Finalisation du document pour validation
0.4.3	07/11/2020	Sealweb	Prise en compte des dernières remarques de Worldline
0.4.4	19/11/2020	Sealweb	Prise en compte des retours de Fortis
1.0.0	13/10/2021	ITA	Revue interne, Prise en compte des remarques du juridique BNP Paribas Fortis • Modification du I.A, 1.E.4, V.E.3, V.D.3
1.1	28/10/2021	ITA	Prise en compte de la remarque du juridique BNP Paribas Fortis suite à la PMA : • Modification du V.E.3
1.2	15/12/2021	MBA	Prise en compte de la remarque de l'audit interne de SealWeb • Modification du chapitre IV.C.2 [Validée par la PMA du 21 décembre 2021]
1.3	09/09/2022	GFE	Modification suite à : • nouveau canaux : EBA, EBBM • nouveau token : Easy PIN (Gemalto) in EBA, EBBM • itsme moyen d'autorisation • modification dans le champ OU du certificat • distinction écran layout Web & Mobile [Validée par la PMA du 19 septembre 2022]
1.4	01/04/2023	RZE	Prise en compte du transfert de l'activité de Worldline vers Worldline France sur la migration de la PKI "Mediacert Root CA 2018" (et AC filles 2019) vers "Mediacert Root CA 2021" Prise en compte des remarques de Worldline et du changement des OID des OTU CA 2021 de Mediacert (entrée en vigueur le 17 février 2022 pour Worldline France/Mediacert) : passage de 1.2.250.1.111.20.5.5 à 1.2.250.1.111.20.5.6

Sommaire

I. Introduction

I.A. Présentation générale

Ce document définit la Politique d'enregistrement applicable aux certificats des clients de l'entité Fortis de BNP Paribas.

- ***émis par les autorités de certifications « Mediacert OTU CA 2021 » et « Mediacert OTU CA S2 2021 » de Worldline France («OTU CA » dans la suite de ce document) agissant en tant que fournisseur de services de Certification,***
- ***pour répondre aux besoins de confiance d'applications métiers (en particulier, dans le cas d'applications bancaires dématérialisées).***

Cette politique d'enregistrement (nommée PE dans la suite de ce document) concerne l'émission de certificats de signatures électroniques de documents au format PDF, XML (XAdES, XML-DSig) ou CMS.

L'autorité « OTU CA » répond, entre autres, aux besoins de signature des clients de BNP Paribas Fortis, utilisateurs de certificats personnels, et fait partie de l'infrastructure de gestion des clés (IGC) utilisée par le groupe BNP Paribas.

La présente politique d'enregistrement est inscrite dans un processus de certification de conformité des exigences et pratiques d'enregistrement à la norme Européenne ETSI EN 319 411-1 niveau LCP a pour objet de décrire :

- ***Les engagements de l'autorité d'enregistrement « FORTIS RA » relatifs à la définition des règles d'émission et à la gestion des certificats émis par l'AC « OTU CA », ainsi qu'à leur mise en œuvre***
- ***Les conditions d'utilisation des certificats émis par l'AC « OTU CA » émis pour le compte de BNP Paribas Fortis enregistrés et demandés par la « FORTIS RA ».***

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

Elle vise également :

- ***A être conforme aux exigences d'enregistrement imposées aux AC OTU (OID 1.2.250.1.111.20.5.6.1 et 1.2.250.1.111.20.5.6.5) telles que décrites dans la PC Mediacert[1]***
- ***A être conforme aux exigences d'enregistrement du programme Adobe AATL***

I.B. Identification du document

Cette politique d'enregistrement 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.

OID de la présente politique d'enregistrement
1.2.250.1.62.10.202.6.5.1

[1] Disponible à l'adresse : **Autorité de Certification - Mediacert**

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 des AC « OTU CA », cette dernière s'organise autour des entités suivantes :

- ***Autorité de Certification (AC)***
- ***Autorité d'Enregistrement (AE)***
- ***Porteurs de certificats***
- ***Application utilisatrice (application de signature de documents mise à disposition de ses clients par BNP Paribas Fortis)***
- ***PMA (Policy Management Authority) : instance de gouvernance du service de signature de BNP Paribas et de l'AE Fortis.***

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

« OTU 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 « OTU CA » qu'elle assume directement, « OTU CA » est un service externe à BNP Paribas. Cependant, dans le cadre des usages, elle délègue à BNP Paribas Fortis un certain nombre de responsabilités. En particulier, BNP Paribas Fortis, entité légale au sens de la loi belge s'engage à respecter les exigences suivantes :

- ***Être en relation par voie contractuelle ou être en cours d'entrée en relation avec les clients 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 « OTU CA ».***
  - ***La définition, pour le périmètre des certificats émis pour BNP Paris, des règles d'enregistrement des porteurs en vue de l'émission des certificats émis par l'AC « OTU CA » et leur bonne application,***
  - ***La définition des conditions d'utilisation des certificats émis par l'AC « OTU CA » pour le compte de BNP Paribas Fortis***
- ***La remise des certificats à l'application utilisatrice, pour le compte du porteur des certificats émis par l'AC « OTU CA » et pour lesquels, à l'intermédiaire de BNP Paribas Fortis, Mediacert a la charge de la gestion des certificats des porteurs, clients de BNP Paribas Fortis.***

I.C.1. Autorité de Certification

L'autorité de certification « OTU 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 à l'application utilisatrice, pour le compte du 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. Dans le cadre de la présente PE et du contexte d'utilisation de l'AC par le Service de Signature de BNP Paribas, des demandes de révocations techniques sont initiées à l'attention de l'AC par le service de signature de BNP Paribas sur certains événements intervenant dans le processus de signature (refus de signer du futur porteur…) décrits dans la présente PE.***
- ***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 sont décrites dans la PC de l'AC « OTU CA ».

I.C.2. Autorité d'enregistrement (AE)

L'AE FORTIS RA 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 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces .

La procédure d'enregistrement pour les certificats émis par les AC « OTU CA » pour BNP Paribas Fortis se déroule en deux étapes telles que décrites ci-dessous. La 1ère étape est réalisée une seule fois et est un prérequis à la suivante.

1) Etape 1 : Enregistrement

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

- ***Etape REG 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*

- ***Etape REG 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 avec l'un des moyens décrit en III.B.3: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.*
- ***Etape REG 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 PE 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 BNP Paribas Fortis 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)*
  - *le système Easy PIN (Gemalto), qui permet de s'authentifier au travers d'un canal sécurisé entre le client et la banque (EBA, EBBM)*
  -

  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)*
  - *la carte Isabel (fournie par BNP Paribas Fortis 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)*
  - *le système itsme, qui permet de signer au travers d'un canal sécurisé entre le client et la banque (EBW, EBB)*
  - *le système Easy PIN (Gemalto), qui permet de signer au travers d'un canal sécurisé entre le client et la banque (EBA, EBBM)*

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 PE (Chapitre XI). 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 et utilisation 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 :

- *l'initialisation du processus permettant de contractualiser en ligne, qui requière l'authentification préalable du client via un des moyens d'authentification acceptés par BNP Paribas Fortis (listés ci-dessus).*
- *l'initialisation du processus permettant de signer électroniquement, suivant l'étape précédente.*

Le client donne son accord sur un ou plusieurs documents spécifiques 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 BNP Paribas Fortis (listés ci-dessus).

Au préalable, le client accepte :

- ***les CGU du service de signature Fortis et donne son consentement sur l'utilisation de ses données personnelles pour l'émission d'un certificat en son nom.***
- ***Les CGS du TSP Mediacert, au travers de l'acceptation des CGU du service de signature Fortis.***

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 si le client abandonne l'étape, le processus de signature est annulé. 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.

Ensuite il y a une distinction dépendant les écrans layout style :
1) Layout Mobile :
Il n'y a pas d'étape supplémentaire puisque le client déclare déjà dans cette écran avec une case « avoir pris connaissance des « Conditions d'utilisation des certificats de signature électronique », que toutes les données sont correctes et qu'un certificat portant son nom pourra être créé dans le cadre de ces conditions ».
2) Layout Web :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 PE à cette étape, ainsi que la PC et les CGS Mediacert.

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

Cette étape permet également de confirmer l'acceptation du certificat et de valider son contenu, en particulier les données à caractère personnel qu'il contient.

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.

Pour révocation voir chapitre IV.J.

I.C.3. Décomposition fonctionnelle de l'AE

L'IGC de BNP Paribas Fortis 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 (.***
  - ***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 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.4. Porteur de certificat

Dans la présente politique d'enregistrement un porteur de certificat est un client de BNP Paribas Fortis.

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 des AE de BNP Paribas, qui a pour principales missions de :

- ***Définir, revoir, approuver et faire appliquer les Politiques d'Enregistrement et les Déclaration des Pratiques d'enregistrement,***
- ***Gérer l'ensemble des risques liés à l'AE,***
- ***Définir et gérer les personnels ou entité de confiance opérant l'AE***
- ***Gérer les relations avec les entités extérieures, en particulier avec l'AC OTU***
- ***Prendre toutes les actions nécessaires pour assurer l'exécution de l'ensemble des tâches listées précédemment.***

I.D. Usage des certificats

Les certificats éphémères émis dans le cadre de cette présente politique d'enregistrement sont utilisés uniquement dans le cadre de l'utilisation de solutions pour la 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', comme défini dans la PC de l'AC « OTU CA ».

I.E. Gestion de la politique de la présente politique d'enregistrement

I.E.1. Entité gérant la politique d'enregistrement

L'entité en charge de l'administration et de la gestion de la présente politique d'enregistrement est ITG. Elle est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PE.

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

La présente PE fait l'objet d'une relecture par l'entité gérant la Politique de Certification de l'AC « OTU CA » afin de s'assurer que les engagements de la présente PE soient bien alignés avec celle décrite dans la PC des AC « OTU CA ». La validation de la présente PE est réalisée au travers de l'audit de l'AE (voir VIII).

I.E.2. Point de contact

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

Hello Bank peut être contacté pour toutes questions relatives à cette PE via Hello bank ! au 02/433 41 42 (FR) ou au 02/433 41 41 (NL).

Easy Banking Business Helpdesk peut être contacté pour toutes questions relatives à cette PE 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 DPE avec cette politique d'enregistrement

La PMA (Policy Management Authority), instance de gouvernance de l'AE, désigne les personnes (ou Services) déterminant la conformité de la Déclaration des Pratiques d'enregistrement (DPE) avec la présente Politique d'enregistrement

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

La présente Politique d'enregistrement sera revue chaque changement majeur et a minima annuellement par la PMA (Policy Management Authority), instance de gouvernance de cette AE, pour assurer

- ***sa conformité aux normes de sécurité attendues par l'organisme de contrôle national (cf. Règlement européen eIDAS 910/2014).***
- ***aux exigences énoncées dans la PC des AC « OTU CA »***

La présente PE fait l'objet d'une relecture par l'entité gérant la Politique de Certification de l'AC « OTU CA » afin de s'assurer que les engagements de la présente PE soient bien alignés avec celle décrite dans la PC des AC « OTU CA ». La validation de la présente PE pour l'entité gérant la Politique de Certification de l'AC « OTU CA » se repose sur l'audit de l'AE (voir VIII).

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

I.F. Définitions et acronymes

Les acronymes utilisés dans la présente PE sont les suivants :

- ***AA : Autorité d'Archivage***
- ***AC : Autorité de Certification***
- ***AE : Autorité d'Enregistrement***
- ***ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information***
- ***CGS: Conditions Générales de Service du TSP Mediacert, dans le cadre de la signature électronique et émission de Certificats Electroniques***
- ***CGU : Conditions Général d'Utilisateur du Service de Signature***
- ***CGA : Condition Générales d'adhésion***
- ***CRL : Liste de Certificats Révoqués***
- ***DN : Distinguished Name***
- ***DPC : Déclaration des Pratiques de Certification***
- ***DPE : Déclaration des Pratiques d'enregistrement***
- ***ETSI : European Telecommunications Standards Institute***
- ***IGC : Infrastructure de Gestion de Clés***
- ***OID : Object Identifier***
- ***OCSP : Online Certificate Status Protocol***
- ***PMA : Policy Management Authority***
- ***PC : Politique de Certification***
- ***PE : Politique d'enregistrement***
- ***RGS : Référentiel Général de Sécurité***
- ***RSA : Rivest Shamir Adleman***
- ***SSI : Sécurité des Systèmes d'Information***
- ***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.
Politique d'enregistrement (PE)	Ensemble de règles et d'exigences auxquelles est soumise une autorité d'enregistrement dans la mise en place et la fourniture de ses prestations.
Déclaration des pratiques de certification (DPC)	Description des pratiques de certification (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.
Déclaration des pratiques d'enregistrement (DPE)	Description des pratiques d'enregistrement (organisation, procédures opérationnelles, moyens techniques et humains) que l'autorité d'enregistrement applique dans le cadre de la fourniture de ses services d'enregistrement en vue de la certification électronique, en conformité avec la ou les politiques d'enregistrement et 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 LAR ou ARL)
Répondeur OCSP	Service de statut en ligne des certificats
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 telle 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 d'enregistrement « FORTIS RA » s'appuie sur la fonction de publication de l'AC « OTU CA » qui est en charge de sa publication[2].

La politique de certification de l'AC précise les méthodes de mise à disposition et les URL correspondantes (serveurs Web de publication) pour les documents de l'AC (PC, certificats d'AC, CRL…).

Les documents complémentaires relatifs à la présente AE (la présente PE, les CGUs) suivent les mêmes

[2] FORTIS s'autorise également à mettre à disposition la présente PE et les CGUs, le cas échéant, sur d'autres sites de publication pour des raisons opérationnelles.

méthodes de publication[3].

II.B. Informations devant être publiées

En plus des informations décrites dans la PC des AC « OTU CA », les informations suivantes sont publiées :

La présente politique d'enregistrement	https://www.mediacert.com/
Les CGS des certificats éphémères.	https://www.mediacert.com/certification/fr/wls-otu-f022

II.C. Délais et fréquences de publication

Les délais et les fréquences de publication pour les informations liées à l'AE (nouvelle version de la PE, 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.

II.D. Contrôle d'accès aux informations publiées

Voir PC des AC « OTU CA »

III. Identification et authentification

Les règles de l'AC « OTU CA » s'appliquent ici. Nous précisons uniquement les règles complémentaires imposées par l'AE.

III.A. Nommage

III.A.1. Types de noms

Voir PC des AC « OTU CA »

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

[3] FORTIS s'autorise à changer le lieu de publication de ces documents. Dans un tel cas de figure, la présente PE sera alors mise à jour.

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 de normalisation concernant le nom et les prénoms du porteur. Ces transformations sont limitées aux cas suivants :

- ***le nom ne peut contenir que 32 caractères, qui sont obligatoirement des lettres, des blancs ou des tirets, à l'exclusion de tout autre.***
- ***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 DPE.***

III.A.5. Unicité de Noms

BNP Paribas Fortis est responsable de l'unicité des noms de ses porteurs et de la résolution des litiges portant 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 « OTU 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.

A ce titre, en plus des règles définies dans la PC de l'AC OTU, le champ SN (serialNumber) contient un numéro (UUID)

L'unicité est garantie par via l'ajout d'un numéro unique (UUID – cf. RFC 4122 –) dans l'attribut SN du sujet (DN) du certificat. Ce numéro de série unique est géré par l'AC « OTU CA »

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=***

1) Moyen de signature pour autorisation

Position 1:

- F: UCR
- I: Isabel/intellisign
- G: Gemalto
- B: ITSME

2) Identification du sujet / personne physique

Position 2-11

- SMID

3) Canal de signature

Position 12-13

- 12 : EBB
- 49 : EBA
- 52 : EBW
- 56 : EBBM

- ***C=BE***

Dans le cas d'un certificat de test, conformément à la PC§1.4.4 des AC « OTU CA », 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 préfixe, soit « TEST-MONITORING »***
- ***SN (surName) = soit le nom du sujet / personne physique avec l'ajout de «TEST» en suffixe, soit « TEST-MONITORING »***
- ***givenName = soit le prénom du sujet / personne physique, soit « TEST-MONITORING »***
- ***SN (serialNumber) = N° unique (UUID)***
- ***OU= F-1***
- ***C = BE***

Dans le cas d'un certificat de test, le champ CN contiendra en préfixe « TEST », conformément à la PC de l'AC « OTU CA ».

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

- ***La marque BNP Paribas est une marque déposée par BNP Paribas dont, entre autres:***BNP PARIBAS, marque de l'Union européenne déposée à l'EUIPO le 8 octobre 1999 dans les classes 35, 36 et 38 et enregistrée le 19 janvier 2001 sous le numéro 1338888.
- BNP PARIBAS, marque de l'Union européenne déposée à l'EUIPO le 25 novembre 2005 dans les classes 9, 35, 36 et 38 et enregistrée le 24 janvier 2007 sous le numéro 004743639

La marque **BNP Paribas Fortis** est une marque déposée par BNP Paribas Fortis NV auprès de l'Office Benelux de la propriété intellectuelle le 3 janvier 2013 dans les classes 35, 36 et 42 et enregistrée le 07 janvier 2013 sous le numéro 931084

La marque **Fintro** est une marque déposée par BNP Paribas Fortis NV dont, entre autres :

- FINTRO, marque Benelux, déposée auprès de l'Office Benelux de la propriété intellectuelle le 27 septembre 2004 dans la classe 36 et enregistrée le 10 mars 2005 sous le numéro 764125.
- FINTRO, marque de l'Union européenne déposée à l'EUIPO le 27 septembre 2004 dans la classe 36 et enregistrée 10 mai 2007 le sous le numéro 004046173.

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

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

Non applicable.

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

L'enregistrement d'un porteur 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. Cependant, ces règles de vérifications :

- ***Sont documentées dans la DPE de BNP Paribas***
- ***Sont conformes, a minima, aux exigences de la norme ETSI EN 319411-1 pour le niveau LCP***
- ***Sont conformes aux exigences du programme AATL***
- ***Sont conformes aux exigences de la PC des AC « OTU CA ».***

Ces règles sont en conformité avec les exigences du chapitre §3.2.2.2 de la PC des AC OTU, en particulier :

- ***La demande de certificat est signée électroniquement.***
- ***La vérification de l'identité est réalisée dans le cadre de la règlementation KYC à l'aide de l'une des pièces d'identité suivante :***
  - ***La carte d'identité électronique Belge dans le cas d'un résident Belge***
  - ***La carte d'identité nationale ou le passeport émis par le Pays de résidence est utilisé dans les cas de non-résident.***
- ***La date de validité de la pièce d'identité fait l'objet d'une vérification***

BNP Paribas Fortis pourra, dans le cadre d'une future version de la présente PE, étendre les moyens de vérification d'identité sous réserve que ces moyens présentent un niveau de fiabilité démontré équivalent ou supérieur aux moyens actuels, qu'ils soient conformes à la norme ETSI 319411-1 pour le niveau LCP et aux exigences AATL[4].

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.C. Validation de l'autorité du demandeur

Cf. chapitre III.B.4

[4] Les moyens de vérifications feront l'objet d'une acceptation explicite par l'AC, dans le cadre du processus de mise à jour de la présente PE.

III.C.1. Certification croisée d'AC

Sans objet pour une politique d'enregistrement. Se référer à la PC « OTU CA ».

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

III.D.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 PE.

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

Sans objet.

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

La demande de révocation du certificat final ne peut être initiée que par le porteur dans le cadre de ses opérations dématérialisées. 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.A.

IV. Exigences opérationnelles sur le cycle de vie des certificats

IV.A. Origine d'une demande de certificat

Dans le cadre de la présente PE, 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 par certificat pour toute demande de certificat porteur

IV.B. 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.C. Traitement d'une demande de certificat

IV.C.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.***
- ***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 aux AC « OTU CA » pour signature***

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

L'Autorité d'Enregistrement accepte automatiquement d'effectuer la demande de certificat à l'Autorité de Certification suite à l'authentification du porteur avec un des moyens d'autorisation acceptés par BNP Paribas Fortis et listés en clause I.C.2.

Le document est présenté au porteur par l'application métier de BNP Paribas Fortis et le porteur donne son consentement avant signature.

En cas de rejet, le porteur est informé par l'application métier de BNP Paribas Fortis.

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

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

IV.D. Délivrance du certificat

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

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

- ***Le respect de la syntaxe des attributs du sujet (DN), cf. §III.A.5.***
- ***Les attributs cryptographiques de la requête (taille de clé),***

IV.D.2. Notification de la délivrance du certificat au porteur

Il s'agit d'une opération automatique lors d'un processus de signature électronique.

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

IV.E. Acceptation du certificat

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

Le porteur donne son consentement en:

1) Ecrans layout Web : 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.

2) Ecrans layout Mobile : cochant la case indiquant que le client déclare « avoir pris connaissance des « Conditions d'utilisation des certificats de signature électronique », que toutes les données sont correctes et qu'un certificat portant son nom pourra être créé dans le cadre de ces conditions »,

IV.E.2. Publication du certificat

Le certificat ne fait pas l'objet de publication.

IV.E.3. Notification de la délivrance du certificat

Conformément à la PC de l'AC « OTU CA », L'AC transmet le Certificat produit au à l'AE en réponse du traitement de la demande de création de Certificat. L'A.E. le transmet à son tour au dispositif de signature de BNP Paribas. Cette transmission vaut notification

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

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

S'agissant du certificat éphémère du signataire, l'utilisation de la clé privée du porteur générée par le service de signature de BNP Paribas et du certificat associé, émis dans le cadre de la présente PE est strictement limité au service de signature offert par BNP Paribas. Par design, l'application métier de BNP Paribas Fortis ne permet pas d'autre utilisation de la clé privée[5].

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

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

L'AE technique génère un fichier de preuve (trace d'audit, optionnellement des données métier de l'application BNP Paribas Fortis, fichiers de preuve de validation de signature) lors de chaque signature par le porteur.

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

IV.G. Renouvellement d'un certificat

Non applicable dans le cadre de la présente PE

IV.H. 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 de délivrance est la même que pour un certificat initial.

[5] Il est à noter que les AC « OTU CA » peuvent émettre des certificats en dehors du périmètre de la présente PE, pour d'autres clients par exemple.

IV.I. 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 le cadre de la présente PE.

IV.J. Révocation et suspension des certificats

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

Dans la suite du paragraphe, seules seront décrites les informations relatives à la révocation des certificats finaux.

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

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'un porteur et s'ajoutent à celle décrite dans la PC :

- ***Les informations du porteur figurant dans son certificat ne sont pas en conformité avec son identité ;***
- ***Le porteur a abandonné son opération de signature électronique[6].***

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

. Dans les écrans

1) layout Web 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.

2) layout Mobile : l'identité du porteur, utilisé pour le CN de son certificat, est présentée au porteur. Si cette identité est erronée, le porteur doit refuser la continuation de l'étape. Si le client abandonne l'étape, le processus de signature est annulé. Aucun certificat n'est généré.

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

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

IV.J.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 « OTU CA », et que cette liste est accessible au téléchargement.

De part la nature des certificats émis (durée de vie limité au maximum à la durée de vie de la session de signature), comme indiqué dans la PC Mediacert, la révocation est « un instrument permettant avant tout de fournir une LCR pour des composants techniques qui ont obligation d'en disposer ». La fonction est cependant opérée par l'AC et utilisée par le service de signature de BNP Paribas. La demande de révocation devant, être formulée durant la période de validité du certificat, la formulation de la demande doit

[6] Dans ce cas de figure, la RA envoie automatique une demande de révocation à l'AC.

être traitée durant le temps de session d'une signature électronique d'une application de BNP Paribas.

A cette fin, le service de Signature de BNP Paribas crée de façon automatique une demande de révocation à destination de l'AC « OTU CA » lorsque les événements décrits en IV.J.1 se produisent.

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

Voir PC « OTU CA »

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

En complément des exigences de la PC « OTU CA », l'AE technique est tenue de vérifier que le certificat de l'autorité de certification « OTU CA » ayant émis le certificat du porteur est valide.

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

Voir PC « OTU CA »

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

Voir PC « OTU CA »

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

Voir PC « OTU CA »

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

Voir PC « OTU CA »

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

Sans objet.

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

Voir PC « OTU CA »

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

Sans objet.

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

Voir PC « OTU CA »

V. Mesures de sécurité non techniques

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que les autorités d'enregistrement BNP PARIBAS doivent respecter.

La partie confidentielle de la déclaration des pratiques d'enregistrement (DPE) décrit les moyens mis en

œuvre pour respecter ces exigences

V.A. Mesures de sécurité physique

BNPP Paribas et BNP Paribas Fortis contrôlent les accès physiques aux composants de l'AE dont la sécurité est critique quant à la fourniture du service d'enregistrement, afin de minimiser le risque lié à la sécurité physique. En particulier :

- ***L'accès physique aux composants critiques est limité aux seules personnes autorisées***
- ***Des contrôles sont mis en place afin d'éviter les pertes, les altérations et les compromissions des biens, ainsi que l'interruption du service.***
- ***Des contrôles sont mis en œuvre pour éviter la compromission ou le vol d'information, en particulier dans les espaces de traitement des informations***
- ***Les composants critiques pour la sécurité des opérations d'enregistrement sont localisés au sein de périmètre de sécurité avec des moyens de protection physique contre les intrusions, tel que le contrôle d'accès physique au périmètre et la mise en place d'alarme en cas d'intrusion.***

V.B. Mesures de sécurité procédurales

V.B.1. Rôles de confiance

On distingue les rôles suivants sur le périmètre de l'AE :

- *L'officier de sécurité de l'AE* ***: il est en charge de l'application de la présente politique d'enregistrement.***
- *Opérateurs techniques de l'AE* ***: 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 nommé par l'organisation BNP Paribas ou l'AC « OTU CA » 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 et d'enregistrement, aux déclarations des pratiques de certification de l'IGC et de l'AE, ainsi aux politiques de sécurité de la composante.***

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 PE requière un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques du service de signature BNP PARIBAS, celles-ci sont décrites dans la DPE.

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

ITG fait vérifier l'identité et les autorisations de tout personnel avant de lui attribuer un rôle et les droits correspondants. Se référer à la DPE 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. Le rôle d'auditeur ne peut être cumulé avec aucun autre rôle ;

- ***les personnes qui mettent en œuvre une composante ne peuvent être les mêmes que les personnes qui en réalise le contrôle***

Les attributions associées à chaque rôle sont décrites dans la DPE de l'AE et sont 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'AE est soumis contractuellement à une clause de sécurité et confidentialité.

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

L'AE informe toute personne intervenant dans des rôles de confiance de l'AE :

- ***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 V.C.8

V.C.2. Procédures de vérification des antécédents

Les personnels de l'AE 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 d'enregistrement 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

Concernant les personnels contractants travaillant pour BNP Paribas et BNP Paribas Fortis, 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 d'enregistrement propre au domaine de certification ;***
- ***Documents constructeurs des matériels et logiciels utilisés ;***
- ***Politiques d'enregistrement supportées par la composante à laquelle il appartient ;***
- ***Politique de certification des AC « OTU CA » ;***
- ***Procédures internes de fonctionnement.***

L'autorité d'enregistrement veille à ce que son personnel (comme défini dans la DPE) possède bien les documents identifiés ci-dessus en fonction de leur besoin comme le précise la DPE.

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'AE du groupe BNP Paribas Fortis 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'AE :

- ***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.***
- ***Réception d'une demande de certificat (initiale et renouvellement),***
- ***-Validation / rejet d'une demande de certificat,***
- ***-Réception d'une demande de révocation,***
- ***-Validation / rejet d'une demande de révocation.***

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 de l'AE sont conservés 7 ans au travers de la conservation du fichier de preuve.

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

L'AE du groupe BNP Paribas Fortis 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'AE 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 de signature du groupe BNP Paribas.

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

L'AE 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 de BNP Paribas Fortis sur son AE.

Des tests d'intrusion complémentaires sont réalisés périodiquement, a minima de façon annuelle.

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'AE.***
- ***Conserver les pièces papier liées aux opérations, 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 mis en œuvre par l'AE***
- ***La présente PE et la DPE associée***
- ***Les données d'audit***
- ***Les journaux d'évènements des différentes entités de l'AE***
- ***Les pièces papier liées à l'AE.***

V.E.2. Procédure de constitution des archives

Se référer au chapitre correspondant de la DPE.

V.E.3. Période de conservation des archives

La durée de conservation des archives électroniques est la suivante :

- ***Durée de rétention des archives de journaux d'évènements : 1 an***
- ***Les dossiers d'enregistrement et les données liées à l'identité du Signataire seront conservés pour une durée de 10 ans à compter de la fin de la relation entre le Client et BNP PARIBAS FORTIS.***
- ***Le document signé sera conservé en fonction du type de document pour une durée de minimum 10 et maximum 30 ans à compter :***
  - ***(i) de la fin du contrat***
  - ***(ii) l'expiration du document si une période de validité s'applique***
  - ***(iii) de la date du document si (i) et (ii) ne s'appliquent pas.***
- ***Les traces techniques assurant l'imputabilité des actions seront conservées en fonction du type de document pour une durée de minimum 10 et maximum 30 ans à compter :***
  - ***(i) de la fin du contrat***
  - ***(ii) de l'expiration du document si une période de validité s'applique***
  - ***(iii) de la date du document si (i) et (ii) ne s'appliquent pas.***
- ***La durée de conservation des éléments spécifiques à l'AC (CRL, traces techniques de l'AC…) est précisée dans la PC « OTU CA »***

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 DPE 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 DPE.

V.E.7. Système de collecte des archives

Les traces du processus d'enregistrement sont conservées dans le fichier de preuve associé à la transaction. Celui-ci est conservé dans conditions assurant sa disponibilité, son intégrité et sa confidentialité.

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

Les archives sont sous la gestion de l'AE du groupe BNP Paribas. Le processus de récupération fait l'objet d'une procédure interne de fonctionnement mentionnée dans la DPE. La récupération peut être effectuée

sous un délai maximal égal à 5 jours ouvrés.

V.F. Changement de clé de l'autorité

Sans objet pour une AE.

V.G. Reprise suite à compromission et sinistre

L'AE « FORTIS RA » s'engage à respecter l'ensemble des mesures de reprise suite à compromission et sinistre énoncée dans la Politique de Certification des AC OTU du TSP Mediacert, en particulier :

- ***L'AE « FORTIS RA » a défini et tient à jour un plan de continuité d'activité en cas de sinistre.***
- ***En cas de sinistre, y compris en cas de compromission d'une clé de signature ou de compromission de moyen d'authentification, l'AE « FORTIS RA » s'engage à mettre en œuvre l'ensemble des mesures du plan de son plan de continuité d'activité en particulier :***
    - ***La notification immédiate, le cas échéant, de la compromission au TSP Mediacert,***
    - ***La mise en œuvre de mesures de remédiation appropriées permettant de rétablir la sécurité des opérations.***
-

V.H. Fin de vie de l'AE

En cas fin de vie de l'AE, l'ensemble des archives ainsi que les traces de l'AE seront archivés par BNP Paribas. L'AC « OTU CA » ne sera donc pas impactée par l'arrêt de l'AE. Les moyens d'authentification de l'AE technique BNP Paribas seront révoqués.

VI. Mesures de sécurité techniques

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'autorité d'enregistrement « FORTIS RA » doit respecter concernant les bi-clés des porteurs.

Pour les mesures de sécurité technique applicable aux clés d'AC, hors du périmètre du présent document, se référer à la PC « OTU CA ».

La DPE 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

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

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 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 un logiciel de signature dans un format qui permet de prouver la possession de clés, 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

Voir PC « OTU CA »

VI.A.5. Taille des clés

Les porteurs utilisent des clés de 2048 bits minimum.

Concernant la taille des clés, l'application de signature BNP PARIBAS suit les recommandations de l'ANSSI en matière de dimensionnement cryptographique.

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. §VI.C.2.

VI.A.8. Objectifs d'usage de la clé

Pour les certificats des porteurs, cf. I.C.4

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

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

Les clés privées des porteurs ne sont pas contrôlées par plusieurs personnes. Elles sont sous le contrôle du porteur.

VI.B.3. Séquestre de la clé privée

Sans objet

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

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

VI.B.5. Archivage de la clé privée

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

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

Sans objet pour les clés privées des porteurs

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

Les clés privées des porteurs sont stockées dans un module cryptographique répondant au minimum aux exigences ci-dessous :

- ***Critères communs EAL4+ , ou***
- ***FIPS 140-2 level 2***

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

Les clés sont activées une fois générées. Leur utilisation nécessite une authentification du porteur à l'aide de deux facteurs.

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

Non applicable.

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

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

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

Voir VI.B.1

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

VI.C.1. Archivage des clés publiques

Les clés publiques des porteurs ne sont pas archivées par l'AE. Elles sont archivées par l'AC au travers de l'archivage des certificats émis.

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

La durée de vie des certificats est paramétrée à 50 min.

La durée de vie des bi-clés est limitée à son association à un certificat.

VI.D. Données d'activation

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

La génération et l'installation des données d'activation d'un module cryptographique de la plate-forme de signature de BNP Paribas 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 DPE.

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

Se référer au chapitre correspondant de la DPE

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 DPE.

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

Voir VI.B.1

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'infrastructure de signature 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 la solution de signature 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'infrastructure utilisent l'heure système en assurant une synchronisation des horloges des systèmes 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

Voir PC « OTU CA »

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, sur le périmètre des AE 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 BNP Paribas à une équipe d'acteurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée. En particulier, les auditeurs doivent avoir une maîtrise des référentiels d'exigences applicables au périmètre de l'AE, en particulier la norme ETSI EN 319 411-1, la PC Mediacert et le référentiel d'exigence AATL. Ils doivent prendre en compte les exigences de ces référentiels dans leur plan d'audit et dans les contrôles mis en œuvre.

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 DPE associée.

VIII.D. Sujets couverts par les évaluations

Les contrôles de conformité ou des contrôles internes menés par BNP Paribas portent sur l'ensemble des AE du groupe BNP Paribas et vise à vérifier le respect des engagements et pratiques définies dans la présente politique de certification et dans la DPE 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 et à l'AC « OTU CA ».

IX. Autres problématiques métiers et légales

IX.A. Tarifs

Sans objet.

IX.B. Responsabilité financière

En cas d'inadéquations défavorables pour le prestataire entre licences achetées / utilisées, nous pouvons indiquer qu'effectivement et conformément au contrat signé avec le prestataire, BNP PARIBAS demeurera responsable financièrement et devra régulariser la situation dans les meilleurs délais, des dommages et intérêts pouvant toutefois être exigés par le prestataire.

IX.C. Confidentialité des données professionnelles

IX.C.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- ***La partie confidentielle de la DPE correspondante à la présente PE,***
- ***Les clés privées des composantes et des porteurs de certificats du service de signature du groupe BNP Paribas***
- ***Tous les secrets du HSM du service de signature du groupe BNP Paribas***
- ***Les journaux d'évènements des composantes techniques du groupe BNP Paribas***
- ***Le dossier d'enregistrement des porteurs***

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 d'enregistrement, 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 (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) et les autres lois et règlementations applicables (nationales ou autres) relatives à la protection des données).

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

Toutes les données concernant le dossier d'enregistrement des porteurs sont considérées comme personnelles, a minima.

IX.D.3. Données à caractères non personnel

Aucune exigence spécifique n'est formulée à ce sujet.

Responsabilité en termes de protection des données personnelles

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

IX.D.4. Notification et consentement d'utilisation des données personnelles

Conformément à la législation et réglementation en vigueur sur le territoire belge, les informations personnelles remises par les porteurs à l'AE ne doivent ni être divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

IX.D.5. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

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

IX.D.6. 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

IX.F.1. Obligation de l'AC

Voir PC « OTU CA »

IX.F.2. Obligation de l'AE

Les obligations de l'AE sont les suivantes :

- ***protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,***
- ***n'utiliser les 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, la présente PE, et les documents qui en découlent,***
- ***respecter et appliquer la DPE,***
- ***se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC ou l'AE (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***

En plus des obligations ci-dessus, les obligations exprimées dans la PC « OTU CA » sont applicables.

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 du client par exemple)

En plus de l'obligation ci-dessus, les obligations exprimées dans la PC « OTU CA » sont applicables.

IX.G. Utilisateurs de certificats

Aucune exigence spécifique n'est formulée dans le cadre de la présente PE.
Les obligations de la PC « OTU CA » sont applicables.

IX.H. Autres participants

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

Les obligations de la PC « OTU CA » sont applicables.

IX.I. 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. Les clauses de la PC « OTU CA » sont applicables.

IX.J. 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.
Les clauses de la PC « OTU CA » sont applicables.

IX.K. 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.
Les clauses de la PC « OTU CA » sont applicables.

IX.L. Durée et fin anticipée de validité de la PE

IX.L.1. Durée de validité

La PE de l'AE doit rester en application au moins jusqu'à la fin de vie du dernier certificat émis dans le cadre de cette PE.

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

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

Les clauses de la PC « OTU CA » sont applicables.

IX.L.3. Notifications individuelles et communications entre les participants

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

Les clauses de la PC « OTU CA » sont applicables.

IX.M. Amendements à la PE

IX.M.1. Procédures d'amendements

Les amendements majeurs apportés à la présente PE 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 PE. Pour le processus de validation de la PE cf. chapitre I.E.4.

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 PE.

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

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

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

Le changement d'OID de la PE est déclenché dès lors que les amendements apportés par la PE 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.N. 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.O. Juridictions compétentes

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

IX.P. Conformités aux législations et réglementations

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

La conception et la mise en œuvre des services, logiciels et procédures de BNP Paribas prennent en compte, dans la mesure du possible, l'accessibilité à tous les utilisateurs, « quel que soit leur matériel ou logiciel, leur infrastructure réseau, leur langue maternelle, leur culture, leur localisation géographique, ou leurs aptitudes physiques ou mentales » (**https://www.w3.org/Translations/WCAG20-fr/**).

IX.Q. Dispositions diverses

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

IX.R. Autres dispositions

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

X. Annexe – 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 PE sont décrites dans les annexes de la DPE qui est consultable à la demande par les personnes autorisées

XI. Annexe : Procédures enregistrement – authentification et autorisation acceptées sous la présente PE

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

XI.A.1. Etape 1 : enregistrement (REG).

La banque procède aux étapes d'enregistrement REG 1.1 et REG 1.2 (cf. I.D.1) telles que décrites dans la présente PE.

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

- ***la carte bancaire (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

XI.A.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).

XI.A.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).

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

XI.B.1. Etape 1 : enregistrement (REG).

La banque procède aux étapes d'enregistrement REG 1.1 et REG 1.2 (cf. I.D.1) telles que décrites dans la présente PE.

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

XI.B.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 BNP Paribas Fortis***
- ***Une carte Isabel fournie par BNP Paribas Fortis***
- ***Une carte Isabel fournie par une autre banque***

XI.B.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).

XI.C. Procédure basée sur itsme pour client retail

XI.C.1. Etape 1 : enregistrement (REG).

La banque procède aux étapes d'enregistrement REG 1.1 et REG 1.2 (cf. I.D.1) telles que décrites dans la présente PE.

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

- ***la carte bancaire (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 Web (EBW) 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).

XI.C.2. Etape 2 : authentification (AUTH)

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

XI.C.3. Etape 3 : autorisation (AUT)

La personne physique choisit itsme dans son canal électronique bancaire et ensuite utilise l'app itsme et son itsme pincode pour autoriser 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).

XI.D. Procédure basée sur itsme pour client professionnel

XI.D.1. Etape 1 : enregistrement (REG).

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

L'activation itsme pour le canal électronique bancaire Easy Banking Business (EBB) se fait d'une façon sécurisée par l'utilisateur, via l'utilisation d'une session sécurisée itsme où il s'est préalablement identifié de manière unique (reférence client unique + numéro mobile) en tant que personne physique dans son canal électronique bancaire Easy Banking Business (EBB. La session itsme prend en charge l'activation du token itsme pour EBB.

XI.D.2. Etape 2 : authentification (AUTH)

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

XI.D.3. Etape 3 : autorisation (AUT)

La personne physique choisit itsme dans son canal électronique bancaire et ensuite utilise l'app itsme et son itsme pincode pour autoriser 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).

XI.E. Procédure basée sur Easy PIN (Gemalto) pour client retail

XI.E.1. Etape 1 : enregistrement (REG).

La banque procède aux étapes d'enregistrement REG 1.1 et REG 1.2 (cf. I.D.1) telles que décrites dans la présente PE.

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

- ***la carte bancaire (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 Easy PIN (Gemalto) pour le canal électronique bancaire Easy Banking App (EBA) se fait d'une façon sécurisée par l'utilisateur, via l'utilisation d'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 App (EBA) avec sa carte bancaire (procédure M1).

XI.E.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 App (EBA) avec son Easy PIN (Gemalto), enregistrée à l'étape 1 ci-dessus.

XI.E.3. Etape 3 : autorisation (AUT)

La personne physique utilise son Easy PIN (Gemalto) pincode 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).

XI.A. Procédure basée sur Easy PIN (Gemalto) pour client professionnel

XI.A.1. Etape 1 : enregistrement (REG).

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

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.

L'activation Easy PIN (Gemalto) pour le canal électronique bancaire Easy Banking Business Mobile (EBBM) se fait au moment de l'installation de l'app EBBM. Au moment de l'installation l'utilisateur est redirigé vers le canal électronique bancaire Easy Banking Business (EBB) ou il entre dans une session sécurisée où il s'est préalablement authentifié de manière unique (en introduisant ses références client unique) en tant que personne physique (avec sa carte bancaire intelligente ou itsme). Dans la session sécurisée EBB un code QR personnel est disponible qui permet au client de continuer l'installation EBBM sur son mobile. L'activation de Easy PIN (Gemalto) et le choix du PIN se fait dans le courant de l'installation.

XI.A.2. Etape 2 : authentification (AUTH)

Lors cette étape, le client s'authentifie de manière unique (références client unique) en tant que personne physique dans son canal électronique bancaire Easy Banking Business Mobile (EBBM) avec son application Easy PIN (Gemalto), enregistrée à l'étape 1 ci-dessus.

XI.A.3. Etape 3 : autorisation (AUT)

La personne physique utilise son Easy PIN (Gemalto) pincode pour autoriser 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).