Politique et déclarations des pratiques d'enregistrement BNP Paribas Fortis

Autorité d'enregistrement

de l'autorité de certification LuxTrust Corporate CA

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 CA2021 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
Suivi des versions à partir de migration LuxTrust			
2.0	20/03/2024	SEALED	Mise à jour du document dans le cadre de la migration vers l'autorité LuxTrust Corporate CA
2.1	10/04/2024	YNU & GFE	Review
2.3	15/04/2024	SEALED	Last review for integration of feedback from YNU & GFE
2.4	30/04/2024	SEALED	Update V.B.1 roles

Sommaire

I. Introduction

I.A. Présentation générale

Ce document définit la Politique (PE) et les Déclarations de Pratiques d'Enregistrement (DPE) applicables aux certificats des clients de l'entité Fortis de BNP Paribas.

- ***émis par l'autorité de certification « LuxTrust Corporate CA » (« 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).***

Ces Politique et Déclarations de Pratiques d'Enregistrement (nommées PE / DPE dans la suite de ce document) concernent l'émission de certificats de signatures électroniques de documents au format PDF, XML (XAdES, XML-DSig) ou CMS.

La « CA » émet les certificats de signature des clients de BNP Paribas Fortis, utilisateurs de certificats personnels (ci-après nommés « porteurs »).

Les présentes Politique et Déclarations de Pratiques d'Enregistrement sont inscrites dans un processus de certification de conformité des exigences et procédures d'enregistrement à la norme Européenne ETSI EN 319 411-1 niveau NCP+, et ont 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 la « CA » et la manière d'atteindre ces engagements ;***
- ***Les conditions d'utilisation des certificats émis par la « CA » émis pour le compte de BNP Paribas Fortis enregistrés et demandés par la « FORTIS RA », dénommée RA par la suite.***

Les présentes Politique et Déclarations de Pratiques d'Enregistrement répondent aux exigences « Extended Normalized Certificate Policy » (NCP+) définies dans la norme ETSI EN 319 411-1.

L'OID NCP+ est le suivant: **0.4.0.2042.1.2**.

Elles visent également :

- ***A être conforme aux exigences d'enregistrement imposées aux RA LuxTrust (OID 1.3.171.1.1.10) telles que décrites dans la PC LuxTrust Corporate CA[1] identifiée sous l'OID 1.3.171.1.1.1.10.4.5 et conformément à la norme EN 319 411-1/NCP.***
- ***A être conforme aux exigences d'enregistrement du programme Adobe AATL***

I.B. Identification du document

Les présentes Politique et Déclarations de Pratiques d'Enregistrement sont identifiées par leur 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] Disponibles à l'adresse : https://www.luxtrust.com/fr/repository

1.3.171.1.1.10

I.C. Entités intervenant dans l'IGC (infrastructure à clés publiques)

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

- ***Autorité de Certification (CA)***
- ***Autorité d'Enregistrement (RA)***
- ***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 présente PE ne demandent pas de fonctions de séquestre.

Dans le cadre des fonctions de fourniture de service de certification « CA » qu'elle assume directement, « 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 avec les clients finaux pour laquelle elle est chargée d'assurer:

- ***La demande d'émission et de gestion des certificats en s'appuyant pour cela sur l'infrastructure à clés publiques (IGC) de « 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 « CA » et leur bonne application,***
- ***La définition des conditions d'utilisation des certificats émis par l'AC « CA » pour le compte de BNP Paribas Fortis***

I.C.1. Autorité de Certification

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

L'ensemble des fonctions assurées par l'IGC sont décrites dans la PC de la « CA».

I.C.2. Autorité d'enregistrement (RA

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) 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) ;***
- ***aux exigences d'enregistrement imposées aux RA LuxTrust;***
- ***aux exigences d'enregistrement du programme Adobe AATL.***

La procédure d'enregistrement pour les certificats émis par la « 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 (exigence **REG1** telle qu'identifiée dans le document [1]). 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 (exigence **REG2** telle qu'identifiée dans le document [1]). 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 (**AUTH**) et/ou donner son accord (**SAS**) lors de ses contacts subséquents avec l'application utilisatrice (exigence **ENR** telle qu'identifiée dans le document [1]).*
  *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.*

  Le document [4] définit les exigences à remplir pour s'authentifier **(AUTH)** et/ou donner son accord (**SAS**), identifie et analyse la conformité des moyens utilisés par la banque par rapport à ces exigences.

  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 d'autoriser une signature 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 d'autoriser une signature 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 d'autoriser une signature au travers d'un canal sécurisé entre le client et la banque (EBW, EBB)*
- *le système Easy PIN (Gemalto), qui permet d'autoriser une signature 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 dans le document [4] et résumés 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) Étape 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 a besoin d'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 s'articule sur deux processus:

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

Cette étape exige que le client comprenne les conditions générales liées à l'utilisation du service de signature électronique, en particulier le fait qu'un certificat de signature est délivré à son nom (exigences « certificate acceptance and subscriber agreement» (**CAA**), telles qu'elles sont présentées dans [2]). A cet effet une série d'écrans est présentée au client, requérant des actions de sa part, tel que présentées dans le document [3], qui montre comment ces écrans et les étapes générées suite aux actions du client permettent d'être conforme aux exigence de la norme ETSI 319 411-1.

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 [6] et donne son consentement sur l'utilisation de ses données personnelles pour l'émission d'un certificat en son nom.***
- ***Les CGV de la « CA » LuxTrust [5], au travers de l'acceptation des CGU du service de signature Fortis [6].***

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 peut y avoir une distinction selon le business process :

3) 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 ».

4) 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 [6] et les présentes PE / DPE à cette étape, ainsi que la PC et les CGV Luxtrust [5].

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

Cette dernière 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.

I.C.3. Décomposition fonctionnelle de la RA

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 et des autres normes applicables à la présente PE.*
- *Conserver en confidentialité et en intégrité des données personnelles d'authentification du porteur en adéquation avec la réglementation bancaire et applicables à la présente PE.*

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 (« evidence book »).*

I.C.4. Porteur de certificat

Dans la présente politique d'enregistrement un porteur de certificat est un client personne physique 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 et 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 « CA »,***
- ***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 la « CA».

I.E. Gestion de la présente politique d'enregistrement et des déclarations des pratiques d'enregistrement

I.E.1. Entité gérant la politique d'enregistrement et les déclarations des pratiques d'enregistrement

L'entité en charge de l'administration et de la gestion des présentes politique et déclaration des pratiques d'enregistrement est la PMA (Policy Management Authority), instance de gouvernance de l'AE au sein de

BNPP Fortis. Elle est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PE.

Les présentes PE / DPE font l'objet d'une relecture par l'entité gérant la Politique de Certification de l'AC « CA » afin de s'assurer que les engagements des présentes PE / DPE soient bien alignés avec celle décrite dans la PC des AC « CA». La validation des présente PE / DPE est réalisée conjointement par la PMA et par l'entité dédiée de l'AC « CA ». Cette PE est revue dans le cadre de l'audit régulier (voir VIII).

I.E.2. Point de contact

Toute personne (porteur, relying parties) qui a des questions peut trouver les points de contacts pertinents dans les conditions générales d'utilisation qui sont présentées au porteur lors de la demande de certificat, ou dans la PC de la CA.

I.E.3. Entité déterminant la conformité des DPE avec les politiques applicables

La PMA (Policy Management Authority), instance de gouvernance de l'AE, désigne les personnes (ou Services) déterminant la conformité des présentes Politiques et Déclarations des Pratiques d'enregistrement (DPE) avec les Politiques applicables càd;

- *les exigences d'enregistrement imposées aux RA LuxTrust (OID 1.3.171.1.1.10) telles que décrites dans la PC LuxTrust Corporate CA[2]identifiée par l'OID 1.3.171.1.1.1.10.4.5.*
- *la norme EN 319 411-1/NCP+.*
- *les exigences d'enregistrement du programme Adobe AATL*

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

Les présentes Politique et Déclarations des Pratiques d'enregistrement seront revues à 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 « CA »***
- ***aux exigences Adobe AATL applicables***

I.F. Définitions et acronymes

Les acronymes utilisés dans les présentes PE / DPE sont les suivants :

- ***AA : Autorité d'Archivage***
- ***AC : Autorité de Certification***
- ***AE : Autorité d'Enregistrement***
- ***CGV : Conditions Générales de Vente LuxTrust [5]***
- ***CGU : Conditions Général d'Utilisateur du Service de Signature [6]***
- ***CGA : Condition Générales d'adhésion***
- ***DN : Distinguished Name***

[2] Disponibles à l'adresse https://www.luxtrust.com/fr/repository

- ***CPS : Certificate Practice Statement***
- ***DPC : Déclaration des Pratiques de Certification***
- ***DPE : Déclaration des Pratiques d'Enregistrement***
- ***ETSI : European Telecommunications Standards Institute***
- ***IGC : Infrastructure de Gestion de Clés***
- ***ILNAS: Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services***
- ***OID : Object Identifier***
- ***PMA : Policy Management Authority***
- ***PC : Politique de Certification***
- ***PE : Politique d'enregistrement***
- ***RSA : Rivest Shamir Adleman***
- ***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.
Porteur	« Subject » au sens ETSI. Dans le contexte de ce document, le « subject » est le client de BNPP FORTIS, c'est toujours une personnes physique.
Organisation	« Subscriber » au sens ETSI. Dans le contexte de ce document, le « subscriber » est toujours BNPP FORTIS

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 « CA » qui est en charge de sa publication[3].

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 l'AE (les présentes PE / DPE, les CGUs [6]) suivent les mêmes méthodes de publication[4].

II.B. Informations devant être publiées

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

Les présentes Politique et Déclaration des	https://www.luxtrust.com/fr/repository

[3] FORTIS s'autorise également à mettre à disposition les présentes PE / DPE et les CGUs [6], le cas échéant, sur d'autres sites de publication pour des raisons opérationnelles.

[4] FORTIS s'autorise à changer le lieu de publication de ces documents. Dans un tel cas de figure, les présentes PE / DPE seront alors mises à jour.

pratiques d'enregistrement	
Les CGU [6] et CGV [5] des certificats éphémères.	https://www.luxtrust.com/fr/repository

II.C. Délais et fréquences de publication

Les délais et les fréquences de publication pour les informations liées à l'AE (nouvelle version des PE / DPE, 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 « CA»

III. Identification et authentification

Les règles de l'AC « 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 « 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 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 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'***

III.A.5. Unicité de Noms

BNP Paribas Fortis est responsable de l'unicité des noms de ses porteurs.

Afin d'assurer une continuité d'une identification unique du porteur au sein du domaine de l'AC « 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 « CA », 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 « 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), as constructed by LRAO***
- ***O (organizationName) = BNPPF Customer***
- ***OU= identifiant du titulaire du certificat au sein de l'organisation et (éventuellement) du type de demande de certificat comme suit :***
    1) Identification du sujet / personne physique
        Position 1-10
        - SMID
    2) Canal de signature
        Position 11-12
        - 12 : EBB
        - 49 : EBA
        - 52 : EBW
        - 56 : EBBM
- ***C=BE***

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 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 (généré par l'AC "CA")***
- ***OU= F-1***
- ***C = BE***

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

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

Section non applicable car les certificats ne sont émis que pour des personnes physiques clients de BNPPF.

III.B. Validation initiale de l'identité

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

Non applicable; la paire de clé est générée par l'AC « CA ».

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 et décrites dans le document [1] (*SEALED - AdES Requirements Part 2 identification*) dans le cadre de son activité et dans son rôle d'AE fonctionnelle. Cependant, ces règles de vérifications :

- ***Sont conformes, a minima, aux exigences de la norme ETSI EN 319411-1 pour le niveau NCP+ ;***
- ***Sont conformes aux exigences du programme AATL ;***
- ***Sont conformes aux exigences de la PC des AC « CA».***

Ces règles sont en conformité avec les exigences de la PC de l'AC « CA ».

Les méthodes de vérifications d'identité acceptées dans le cadre du présent document, conformes aux exigences listées ci-dessus, sont détaillés dans le document [1] 2024-03-07 - SEALED - AdES Requirements Part 2 identification v1.0 qui analyse leur conformité aux standards et normes applicables (identifiés dans le document [1]) et sont les suivants :

Méthode 1: istme
Méthode 2: Face-to-face registration by BNPPF
Méthode 3: Registration by face-to-face of a representant
Méthode 4: Delegated registration

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 NCP+ et aux exigences AATL[5].

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 » et l'association d'un numéro de client unique, SMID, 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

III.C.1. Certification croisée d'AC

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

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

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

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

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

Ne s'applique pas dans le cadre de cette PE.

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

Ne s'applique pas dans le cadre de cette PE.

IV. Exigences opérationnelles sur le cycle de vie des certificats

IV.A. Origine d'une demande de certificat

Dans le cadre des présentes PE / DPE, la demande de certificat ne peut être émise que par une application

[5] Les moyens de vérification feront l'objet d'une acceptation explicite par l'AC, dans le cadre du processus de mise à jour des présentes PE / DPE.

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.***

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 à signer 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 un délai le plus court possible 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 « CA», la demande de certification transmise par l'AE technique est automatiquement signée par l'AC « CA»,***

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

Au travers des différents écrans qui lui sont présentés (voir document [3]), le porteur donne son consentement sur le fait qu'un certificat généré en son nom pourra être utilisé à des fin de signature selon les « Conditions d'utilisation des certificats de signature électronique ».

IV.E.2. Publication du certificat

Le certificat ne fait pas l'objet de publication.

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

Le certificat émis est joint au données signées par le porteur.

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 et du certificat associé, émis dans le cadre de la présente PE est strictement limité 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[6].

Les conditions générales d'utilisation du service de signature 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.

L'AC « CA » génère par ailleurs un fichier de preuve lors de chaque transaction effectuée par l'utilisateur du certificat au nom du porteur.

Ces deux fichiers de preuves, ensemble, constituent le cahier de preuve lié à la signature.

IV.G. Renouvellement d'un certificat

Le renouvellement ne s'applique pas dans le cadre de cette PE, voir III.D.1.

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.

[6] Il est à noter que l'AC « CA » peut émettre des certificats en dehors du périmètre des présentes PE / DPE, pour d'autres clients par exemple.

IV.I. Modification du certificat

La modification de certificat n'est pas autorisée dans le cadre de la présente PE.

IV.J. Révocation et suspension des certificats

Non applicable dans le cadre des présentes Politique et Déclarations des Pratique d'Enregistrement.

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

Non applicable dans le cadre des présentes Politique et Déclarations des Pratique d'Enregistrement.

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

Non applicable dans le cadre des présentes Politique et Déclarations des Pratique d'Enregistrement.

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

Non applicable dans le cadre des présentes Politique et Déclarations des Pratique d'Enregistrement.

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

Non applicable dans le cadre des présentes Politique et Déclarations des Pratique d'Enregistrement.

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

Non applicable dans le cadre des présentes Politique et Déclarations des Pratique d'Enregistrement.

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

Voir PC « CA »

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

Voir PC « CA »

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

Voir PC « CA »

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

Voir PC « CA »

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

Voir PC « 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 « CA »

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

Sans objet.

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

Voir PC « 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 FORTIS 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 d'enregistrement*** *: personne nommée par la PMA, et qui accepte ce rôle, en charge de vérifier que les informations requises pour toute demande de certificat sont correctes et suffisantes pour être conformes aux différentes exigences du présent document, notamment et en particulier en validant les différents processus utilisés pour collecter ces informations.*
- ***Opérateurs techniques*** *de l'AE : personnes chargées de l'utilisation, de la configuration et de la maintenance technique des équipements en charge de la création et de la soumission des requêtes de certificats à l'autorité de certification et en charge de la création du fichier de preuve de validation de signature lors de chaque signature par le porteur (« evidence book »).*

Note : le rôle d'officier de révocation n'est pas attribué, sachant que les certificats éphémères ne donnent pas lieu à des révocations.

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.

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

La PMA fait vérifier l'identité et les autorisations de tout personnel avant de lui attribuer un rôle et les droits correspondants.

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***

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'elle met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle elle 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 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 :

- ***Les présentes Politiques et Déclaration des Pratiques d'enregistrement;***
- ***Documents constructeurs des matériels et logiciels utilisés ;***
- ***Politique de certification des AC « CA » ;***
- ***Procédures internes de fonctionnement.***

L'autorité d'enregistrement veille à ce que son personnel possède bien les documents identifiés ci-dessus

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 (),***
- ***Validation / rejet d'une demande de certificat,***

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.

En outre :

- ***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.***
- ***l'AC « CA » génère par ailleurs un fichier de preuve lors de chaque transaction effectuée par l'utilisateur du certificat au nom du porteur.***

Ces deux fichiers de preuves, ensemble, constituent le cahier de preuve lié à la signature.

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 et 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.

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 des présentes politique et déclarations des pratiques d'enregistrement.

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 des présentes politique et déclarations des pratiques d'enregistrement .

Une copie de sauvegarde des journaux d'événements est réalisée après chaque cérémonie sur les plates-formes de de signature de BNP Paribas Fortis.

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

L'AE de BNP Paribas Fortis 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 présente PE et DPE***
- ***Les données d'audit***
- ***Les journaux d'évènements des différentes entités de l'AE***
- ***Les pièces papier liées à l'AE.***
- ***Les éléments qui lui incombent dans la constitution du cahier de preuve lié à la signature***

V.E.2. Procédure de constitution des archives

Se référer au chapitre correspondant de CARINA.

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 (en particulier les éléments qui incombent à l'AE dans la constitution du cahier de preuve lié à la signature) 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 « 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.***

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

Se référer au chapitre correspondant de Carina.

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 de BNP Paribas Fortis. Le processus de récupération fait l'objet d'une procédure interne de fonctionnement décrite dans la documentation du système Carina. 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 de l'AC « CA » de LuxTrust, 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 de son moyen d'authentification vis-à-vis de l'AC « CA », l'AE « FORTIS RA » s'engage à mettre en œuvre l'ensemble des mesures de son plan de continuité d'activité en particulier :***
    - ***La notification immédiate, le cas échéant, de la compromission à LuxTrust,***
    - ***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 Fortis. L'AC « CA » ne sera donc pas impactée par l'arrêt de l'AE. Les moyens d'authentification de l'AE technique BNP Paribas Fortis vis-à-vis de l'AC « CA » 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 « CA».

VI.A. Génération et installation de bi clés

Se référer au chapitre correspondant de la CPS de la « CA».

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

Se référer au chapitre correspondant de la CPS de la « CA».

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

VI.C.1. Archivage des clés publiques

Se référer au chapitre correspondant de la CPS de la « CA».

VI.D. Données d'activation

Se référer au chapitre correspondant de la CPS de la « CA».

VI.E. Mesures de sécurité des systèmes informatiques

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

Se référer aux documents internes de BNPP Fortis.

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 FORTIS 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 « 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 NCP+, sur le périmètre des AE du groupe BNP Paribas FORTIS est réalisé tous les deux ans. Un audit interne sera mené par BNP Paribas FORTIS au moins une fois tous les deux ans.

VIII.B. Identités / qualifications des évaluateurs

Le contrôle d'une composante doit être assigné par la direction de BNP Paribas FORTIS 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 LuxTrust 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 CPS LuxTrust.

VIII.D. Sujets couverts par les évaluations

Les contrôles de conformité ou des contrôles internes menés par BNP Paribas Fortis vise à vérifier le respect des engagements et procédures définies dans la présente politique et déclaration de pratiques de certification 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 la PMA et de LuTrust un rapport de conformité assorti de recommandations. A charge des acteurs identifiés dans les présentes politique et déclarations des pratiques d'enregistrement e, de résoudre les points de non-conformité ainsi que de choisir les mesures 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 « CA » LuxTrust.

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 Fortis 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 des documents référencés par le présent document,***
- ***Les journaux d'évènements des composantes techniques du groupe BNP Paribas Fortis***
- ***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 et luxembourgeois si applicable.

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 d'enregistrement 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 et luxembourgeois si applicable

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 et luxembourgeois.

IX.D.6. Autres circonstances de divulgation de données à caractère personnel

Cf. législation et réglementation en vigueur sur le territoire belge et luxembourgeois si applicable.

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 « 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,***
- ***,***
- ***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 « 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 les conditions générales d'utilisation du service de signature de BNPPF et de la PC « CA » qui y est référencée, 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 « CA » sont applicables.

IX.H. Autres participants

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

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 des conditions générales d'utilisation du service de signature de BNPPF et de la PC « CA » qui y est référencée 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 des conditions générales d'utilisation du service de signature de BNPPF et de la PC « CA » qui y est référencée 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 des conditions générales d'utilisation du service de signature de BNPPF et de la PC « CA » qui y est référencée 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 des conditions générales d'utilisation du service de signature de BNPPF et de la PC « CA » qui y est référencée 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 des conditions générales d'utilisation du service de signature de BNPPF et de la PC « CA » qui y est référencée» sont applicables.

IX.M. Amendements aux PE / DPE

IX.M.1. Procédures d'amendements

Les amendements majeurs apportés aux présentes PE / DPE 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 des PE / DPE. Pour le processus de validation des PE / DPE 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 des PE / DPE.

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

Toute mise à jour est mentionnée dans le suivi des versions et le document correspondant est publié sur le site de LuxTrust dès que la validation finale de ce document est obtenue de la part des entités désignées (PMA et LuxTrust)

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

Le changement d'OID des PE / DPE est déclenché dès lors que les amendements apportés par les PE / DPE 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 indiqués dans le chapitre I.E.2.

IX.O. Juridictions compétentes

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

IX.P. Conformités aux législations et réglementations

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

La conception et la mise en œuvre des services, logiciels et procédures de BNP Paribas Fortis 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
[1] 2024-03-07 - SEALED - AdES Requirements Part 2 identification v1.0	Presents and assesses the various identification methods used to enroll signatories toward the BNPPF eNotary signature platform according to applicable Regulations and Standards presented in [2].
[2] 2023-12-19 - SEALED - AdES Requirements Part 1 applicable requirements v0.4	Identifies and lists the rules and standards that are applicable to the BNPPF eNotary signature platform and derives the applicable requirements.
[3] 2022-05-09 - SEALED - AdES Requirements Part 4 screens - v0.1	Analyses the wording displayed to the customer and the actions (s)he takes in the eSignature screens (with and without eNotary). It indicates if/under which conditions this information complies with the requirements derived from the applicable Regulations and Standards presented in [2] requiring to ensure that the customer understands the general terms and conditions linked to the use of the eNotary signature service, in particular the fact that a signing certificate is issued on his/her name (CAA requirements, as introduced in [2]).
[4] 2022-08-25 - SEALED - AdES Requirements Part 3 tokens - v0.2	Assesses the various tokens used to authenticate the registered customers toward the BNPPF eNotary signature platform and / or used by the customer to trigger a signature. It indicates if/under which conditions these tokens comply with the requirements derived from the applicable Regulations and Standards as introduced in [2].
[5] CGV Luxtrust	**https://www.luxtrust.com/fr/conditions-generales-de-vente**
[6] CGU signature services (FORTIS)	**https://easybankingbusiness.bnpparibasfortis.be/pics/BE/commonB/fr/lib_download/Docserver/eSignature_CGU_Cosi_BNPPF_FR.pdf**

Toutes les procédures détaillées relatives aux présentes PE / DPE sont décrites dans les documents référencés ci-dessus sont consultables à la demande par les personnes autorisées.

XI. Annexe : Procédures enregistrement – authentification et autorisation acceptées sous les présentes PE / DPE

XI.A.1. Étape 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 les présentes PE / DPE.

Les méthodes d'enregistrements décrites en [1] conformes aux présentes PE / DPE sont les suivantes :

Méthode 1: istme : applicable à tous les utilisateurs
Méthode 2: Face-to-face registration by BNPPF: applicable à tous les utilisateurs
Méthode 3: Registration by face-to-face of a representant: applicable à tous les utilisateurs
Méthode 4: Delegated registration: en support de l'enregistrement des utilisateurs liés à une organization et vivant à étranger

A cette occasion la banque associe à l'utilisateur et de façon non ambiguë un moyen d'authentification et d'autorisation (AUTH/AUT).

Les différentes manières d'associer le moyen d'authentification et d'autorisation à un utilisateurs dûment enregistré sont décrites en [4].

Elles peuvent varier selon le canal électronique bancaire (EBW pour personnes privées, ou EBB pour personnes associées à une organisation) et selon le type d'application (mobile ou web) mais offrent le même niveau de sécurité dans l'association non-ambigüe avec la personne dans tous les cas.

XI.A.1. Étape 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 EBW ou personne associée à une organisation dans son canal électronique EBB, selon qu'il est un client « retail » ou associé à une organisation.

Les moyens d'authentification décrits en [4] conformes aux présentes PE / DPE sont les suivants :

Token1: The BNPPF app based on Gemalto (for both EBW and EBB channels) - applicable à tous les utilisateurs
Token2: Itsme (for both EBW and EBB channels) - applicable à tous les utilisateurs
Token3: The EMV card (M1 – M2 signature with an UCR token, for both EBW and EBB channels) - applicable à tous les utilisateurs
Token4: Isabel card (for EBB channel) - applicable aux utilisateurs liés à une organisation

Token5: Isabel IntelliSign (for EBB channel) - applicable aux utilisateurs liés à une organisation

Ces moyens peuvent être utilisés quelle que soit la méthode d'enregistrement. Ils sont soit liés à la personne lors de son enregistrement, soit liés à la personne par la suite, au travers d'un canal sécurités (EBW ou EBB) sur base d'une demande authentifiée de la personne en question (sur base du moyen d'authentification et d'autorisation fourni lors de l'enregistrement).

XI.A.2. Étape 3 : autorisation (AUT)

La personne physique signe un challenge à l'aide de son moyen d'authentification / autorisation (sous son contrôle) dans son canal électronique bancaire afin d'autoriser la signature de(s) documents) présenté(s).

Les moyens d'autoriser une signature décrits en [4] conformes aux présentes PE / DPE sont les suivants :

Token1: The BNPPF app based on Gemalto (for both EBW and EBB channels)
Token2: Itsme (for both EBW and EBB channels)
Token3: The EMV card (M1 – M2 signature with an UCR token, for both EBW and EBB channels)
Token4: Isabel card (for EBB channel)
Token5: Isabel IntelliSign (for EBB channel)

Le moyen utilisé pour autoriser la signature est celui qui a été utilisé pour l'authentification. Cependant, pour un même moyen le protocole d'autorisation est généralement différent du protocole d'authentification (par exemple pour les cartes EMV, l'authentification repose sur l'utilisation du mode M1 alors que l'autorisation repose sur une signature de type M2. Il en va de même avec itsme qui offre plusieurs protocoles selon les usages).

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-SMID).