Politique de certification BNP Paribas

Autorités de certification

BNP Paribas Group PDF Certification Authority

BNP Paribas Group Level 2 Certification Authority

itg

Revue		
Nom	Fonction	Date

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

Suivi des versions			
Version	Date	Auteur	Nature des modifications
0.1	18/11/2014	Morpho DSA	Initialisation du document
0.2	29/06/2015	Morpho DSA	Mise à jour
0.3	13/07/2015	Morpho DSA	Mise à jour
0.5	19/01/2016	Cédric SZANIEC	Finalisation de la relecture globale des documents : version avant complétion par les différents contributeurs
0.6	06/04/2016	Cédric SZANIEC	Fusion des différents retours des différents contributeurs
0.7	03/05/2016	Cédric SZANIEC	Intégration des derniers retours suite au pré audit
1.0	09/05/2016	Cédric SZANIEC	Version validée par la PMA
1.1	21/06/2016	Cédric SZANIEC	Intégration des remarques de la phase 1 de l'audit ETSI TS 102 042 : • Ajout du V.G.4, IX • Modification du I.A, I.E.4, IV.D.3, IV.I.7, IV.I.8, V.H • Correction de coquille du III.A.3, IV.J.2, IV.L, VI.B.3
2.0	14/09/2016	Cédric SZANIEC	Correction d'une partie des écarts de l'audit ETSI TS 102 042 : • Changement d'OID • Modification du I.B, IX.C.1
2.1	27/02/2017	Cédric SZANIEC	Ajout de Fortis : • Correction du I.A, IV.E.1
2.2	26/06/2017	Cédric SZANIEC	Changement de Safran I&S vers OT Morpho Adaptation de la PC pour eIDAS EN 319 411-1
2.3	01/07/2019	Ibrahima TAMBOURA	Revue annuelle avec IDEMIA : • Changement d'OT Morpho vers IDEMIA et D'ITP ITG en ITG • Modification du I.E.1

Sommaire

I. Introduction

I.A. Présentation générale

Ce document constitue la Politique de Certification (PC) de l'autorité racine de BNP Paribas dénommée BNP Paribas Group PDF Certification Authority (« BNPP PDF CA » dans la suite du document) et de l'autorité de certification intermédiaire dénommée BNP Paribas Group Level 2 Certification Authority (« BNPP LEVEL2 CA » dans la suite de ce document) dans le cadre de l'émission de certificats électroniques destinés aux autorités de certification de plus bas niveau de l'infrastructure de gestion des clés.

Ce document expose le niveau d'exigence que s'engage à respecter et maintenir des autorités « BNPP PDF CA » et « BNPP LEVEL2 CA », lors de l'émission, de la gestion du cycle de vie et de la publication de ces certificats.

Il s'appuie, en tant que cadre de référence documentaire uniquement, sur les préconisations de la norme ETSI EN 319 411-1.

La présente Politique de Certification répond aux exigences « Normalized Certificate Policy » (NCP) définies dans la norme ETSI EN 319 411-1. L'OID NCP est le suivant : 0.4.0.2042.1.1.

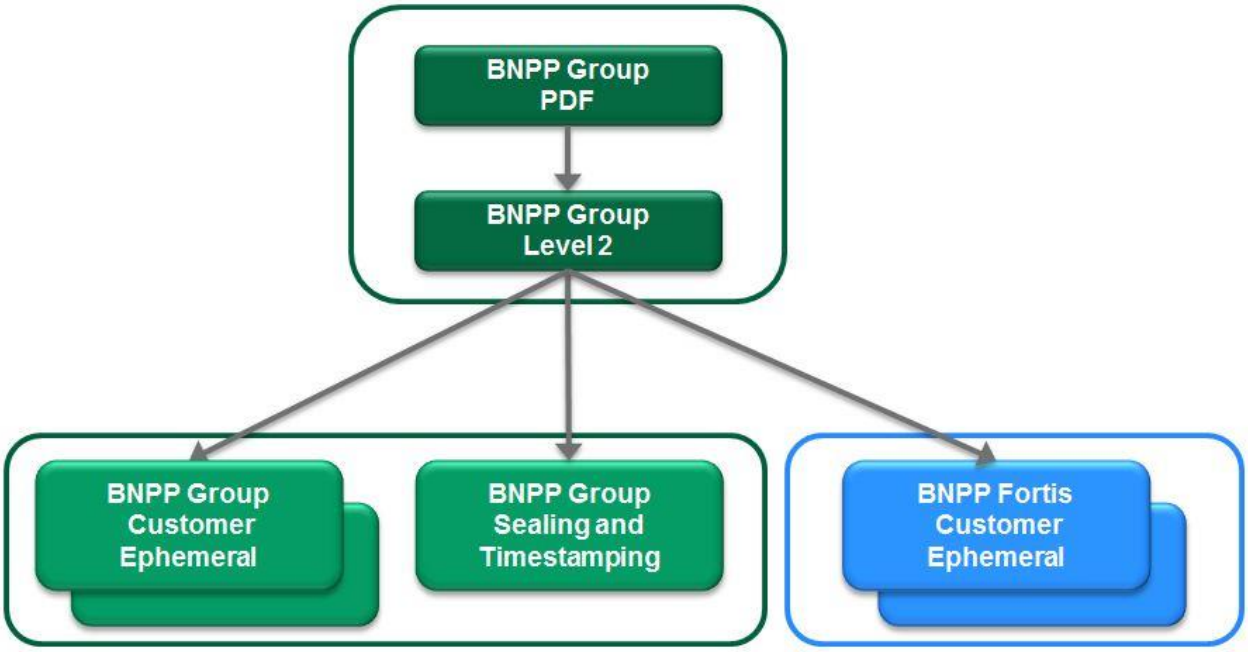

Figure 1 : IGC du groupe BNP Paribas

I.B. Identification du document

Le présent document est dénommé « Politique de Certification – Autorité Racine et Intermédiaire de l'IGC BNP Paribas ».

Les numéros d'OID correspondant à la présente politique de certification sont :

- BNPP PDF CA : 1.2.250.1.62.10.1.1.1.1
- BNPP LEVEL2 CA : 1.2.250.1.62.10.2.1.1.1

La branche OID de BNP Paribas est déposée : {iso(1) member-body(2) fr(250) type-org(1) BNP Paribas(62)} Signel (10) Autorités BNPP PDF & LEVEL2 CA (1 ou 2) Politique de Certification(1) Gabarit de Certificat(1) Version(1)

Elle correspond aux certificats émis à partir du 23 septembre 2016.

I.C. Entités intervenant dans la PKI

I.C.1. Autorités de certifications

Les autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » sont 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).

Les prestations des autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » sont le résultat de fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats (cf. ci-dessous).

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

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

L'ensemble des fonctions assurées par l'IGC de BNP Paribas (en tant que service technique) est opéré par le service informatique de IDEMIA Identity & Security France, dénommé IDEMIA par la suite.

La Déclaration des Pratiques de Certification (DPC) associées aux autorités identifiées dans le présent document décrit l'organisation opérationnelle de l'IGC et la répartition des rôles entre les différentes composantes en fonction de l'organisation fonctionnelle et de la définition des rôles décrites dans la présente politique. (cf. chapitre V.B.2).

a) Autorités de certification hors ligne

Les autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » sont une composante de la PKI qui dispose d'une plate-forme lui permettant d'émettre et de gérer les certificats d'autorité de plus bas niveau.

b) Autorités de certification en ligne

Il s'agit des autorités de certification de plus bas niveau des métiers, rattachées à l'autorité « BNPP LEVEL2 CA ».

I.C.2. Porteurs de certificats

a) S'agissant de l'autorité de certification « BNPP PDF CA »

Dans le cadre de la présente politique, un porteur de certificat est l'autorité de certification « BNPP LEVEL2 CA ».

b) S'agissant de l'autorité de certification « BNPP LEVEL2 CA »

Dans le cadre de la présente politique, un porteur de certificat est une des autorités de certification de plus bas niveau de l'IGC de BNP Paribas, également appelées « **autorités en ligne** ».

I.C.3. Opérateur de certification

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

Le rôle d'opérateur de certification est assuré par IDEMIA qui s'appuie sur son partenaire Colt, en position d'hébergeur. Toutes les fonctions qui ne sont pas directement assurées par IDEMIA, sont prises en charge par Colt via Getronics dont les responsabilités vis-à-vis de IDEMIA sont décrites contractuellement. Toutes les fonctions sous la responsabilité de Getronics sont documentées par cette entreprise. Certaines informations sont confidentielles et leur diffusion nécessite une validation préalable des parties prenantes.

I.C.4. Utilisateurs de certificats

La présente politique traitant de certificats d'autorités de certification, un utilisateur de certificats peut être :

- Un service applicatif qui reconnaît les certificats des autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » et vérifie, en s'appuyant sur un dispositif de vérification, le certificat fourni et la chaîne de certification d'un certificat de porteur émis par l'autorité émettrice.
- Tout client de BNPP qui souhaite vérifier la chaîne de certification de l'autorité (des autorités) émettrice de son certificat

I.D. Usage des certificats

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

La présente politique traite des bi-clés et des certificats à destination des catégories de porteurs identifiés au chapitre I.C.2, afin que ces porteurs puissent :

- Signer les certificats avec leur certificat d'Autorité de Certification pour le compte de leurs propres porteurs
- Signer les listes de révocation

I.D.2. Bi-clés et certificats des autorités « BNPP PDF CA » et « BNPP LEVEL2 CA »

Les autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » génèrent et signent différents types d'objets : certificats et listes de révocation.

Pour signer ces objets, elles disposent d'une bi-clé unique chacune. Cette bi-clé et le certificat associé ne sont utilisés ni à des fins de chiffrement, ni à des fins d'authentification.

I.E. Gestion de la politique de certification

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

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

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

I.E.2. Point de contact

Pour toute demande concernant la présente Politique de Certification, le client doit contacter son conseiller habituel ou le Directeur d'agence (niveau 1) : l'adresse postale est donc celle de son agence, qui peut se retrouver facilement sur internet, notamment à partir de son espace sécurisé.

En cas d'indisponibilité de son conseiller, le client peut également joindre le Centre de Relation Client (CRC) au 0 820 820 001 (0,12 €/min + prix d'un appel).

Si le conseiller (agence ou CRC) et / ou le Directeur de l'agence ne peuvent pas répondre, ou si le client n'obtient pas satisfaction, la réclamation est transmise au Pôle Réclamations de la Direction Régionale concernée qui la traitera (niveau 2).

Si le client estime que la réponse / traitement ne sont toujours pas satisfaisants, il peut alors demander l'intervention de la Médiation Bancaire (niveau 3).

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

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

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

L'approbation de cette Politique de Certification sera effectuée durant une instance de la PMA (Policy Management Authority), instance de gouvernance de cette IGC.

I.F. Définitions et acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

- **AA** : Autorité d'Archivage
- **AC** : Autorité de Certification
- **ACR** : Autorité de Certification Racine
- **AE** : Autorité d'Enregistrement
- **CRL** : Liste de Certificats Révoqués
- **DN** : Distinguished Name
- **DPC** : Déclaration des Pratiques de Certification
- **IGC** : Infrastructure de Gestion de Clés
- **OID** : Object Identifier
- **PC** : Politique de Certification
- **RGS** : Référentiel Général de Sécurité
- **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	Service chargé de signer, émettre et maintenir les certificats d'une

(AC ou CA)	infrastructure à clés publiques, conformément à une politique de certification. Services applicatifs exploitant les certificats émis par l'Autorité de Certification du porteur du certificat.
Politique de certification (PC)	Ensemble de règles et d'exigences auxquelles est soumise une autorité de certification dans la mise en place et la fourniture de ses prestations.
Déclaration des pratiques de certification (PC)	Description des pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'autorité de certification applique dans le cadre de la fourniture de ses services de certification électronique, en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.
Liste de révocation des Certificats (CRL ou LCR)	Liste publiée par l'autorité de certification présentant les certificats n'étant plus dignes de confiance (révoqués, invalides…). Par simplicité on y associe également les listes de révocation d'autorités (appelées ARL)
Bi-clé	Couple de clés composé d'une clé privée et d'une clé publique.
X 509	Norme de l'Union internationale des télécommunications (UIT) relative aux infrastructures à clés publiques (PKI), entre autres les formats standards de ses composants : certificats électroniques, listes de révocation, algorithme de validation…
UTF-8	Codage des caractères définis par Unicode où chaque caractère est codé sur une suite de un à six mots de 8 bits (il n'existe pas actuellement de caractères codés avec plus de 4 mots).
Distinguished Name (DN)	Elément permettant d'identifier un porteur ou une autorité de certification de façon unique.
Object Identifier (OID)	Identifiant universel, représenté sous la forme d'une suite d'entiers associé dans le cadre d'une PKI à un élément de référence tel que la politique de certification ou la déclaration de pratiques de certification.

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, les autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » mettent en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats (cf. § I.C.1).

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

II.B. Informations devant être publiées

Les autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » publient les informations suivantes à destination des porteurs et des utilisateurs de certificat :

- La présente politique de certification,
- Les listes des certificats révoqués,
- Les certificats des autorités « BNPP PDF CA » et « BNPP LEVEL2 CA », en cours de validité.

II.C. Délais et fréquences de publication

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

- Pour les informations liées à l'IGC (nouvelle version de la PC, etc.), l'information doit être publiée dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'autorité racine.
- Pour les informations d'état des certificats, cf. § IV.J.2.
- Pour les systèmes publiant ces informations, BNP Paribas et IDEMIA s'engagent sur les exigences de disponibilité suivantes :
    - Pour les informations liées à l'IGC (nouvelle version de la PC), les systèmes ont une disponibilité pendant les jours ouvrés avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 8h (jours ouvrés) et une durée totale maximale d'indisponibilité tolérée 2h10 par mois hors maintenance planifiée et hors cas de force majeure (incident grave de sécurité avéré).
    - Pour les certificats d'AC et les listes de certificats révoqués, les systèmes ont une disponibilité de 24h/24 7j/7 avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2h et une durée totale maximale d'indisponibilité tolérée de 2h10 par mois hors maintenance planifiée et hors cas de force majeure (incident grave de sécurité avéré).

A noter que la perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une indisponibilité de cette information ; les exigences ci-dessus s'appliquent donc de la même façon.

II.D. Contrôle d'accès aux informations publiées

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

III. Identification et authentification

III.A. Nommage

III.A.1. Types de noms

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

Dans chaque certificat X509 v3 l'autorité émettrice (*issuer*) et le porteur (*subject*) sont identifiés par un « *Distinguished Name* » DN de type X.501 dont le format exact est précisé dans le chapitre VII décrivant le profil des certificats.

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

Le DN comprend dans sa structure le nom d'usage du certificat au sein de l'IGC de BNP Paribas. Le contrôle des informations est assuré lors de la cérémonie de clés par les opérateurs techniques de l'IGC.

III.A.3. Pseudonymisation des AC

Les certificats des porteurs ne sont pas pseudonymisés.

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

Aucune exigence n'est stipulée en plus des règles spécifiées au §III.A.1.

III.A.5. Unicité de Noms

Afin d'assurer la continuité d'une identification unique du porteur au sein de l'IGC de BNP Paribas dans ses certificats successifs (renouvellement) et pour éviter toute ambigüité, le DN du champ « *subject* » de chaque certificat de porteur doit permettre d'identifier de façon unique son usage au sein de l'IGC de BNP Paribas.

L'unicité d'un certificat est basée sur l'unicité de son numéro de série définie par l'AC. Cependant, il convient d'éviter les ambiguïtés sur la propriété d'un certificat en respectant l'unicité d'un même nom au sein de la même AC. Cette unicité est garantie par l'exigence décrite au paragraphe III.A.2.

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

La marque BNP Paribas est déposée par BNP Paribas :

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

III.B. Validation initiale de l'identité

L'identification des autorités de certification en ligne est décrite dans la DPC associée.

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

a) Pour l'autorité de certification « BNPP PDF CA »

Lorsqu'elle génère sa bi-clé, elle génère également un certificat auto signé.

b) Pour l'autorité de certification « BNPP LEVEL2 CA »

Lorsqu'elle génère sa bi-clé, elle doit fournir à l'autorité racine une preuve de possession de sa clé privée correspondant à la clé publique contenue dans la demande de certificat.

Cette preuve est fournie techniquement par la transmission à l'autorité racine d'une requête de certificat, ou CSR (Certificate Signing Request), au format PKCS#10.

c) Pour les autorités de certification en ligne

Lorsqu'elles génèrent leur bi-clé, elles doivent fournir à l'autorité « BNPP LEVEL2 CA » une preuve de possession de leur clé privée correspondant à la clé publique contenue dans la demande de certificat.

Cette preuve est fournie techniquement par la transmission à l'autorité « BNPP LEVEL2 CA » d'une requête de certificat, ou CSR (Certificate Signing Request), au format PKCS#10.

III.B.2. Validation de l'identité d'un organisme

Cf. §III.B.3.

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

La validation est interne à BNP Paribas et provient de la direction d'ITG.

III.B.4. Informations non vérifiées de l'AC

Sans objet.

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

Cette étape est effectuée lors d'une cérémonie de clés constatée par l'officier de sécurité de BNP Paribas.

III.B.6. Certification croisée d'AC

Sans objet.

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

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

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

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

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

Si une autorité de certification a sa clé privée compromise, il faut avoir l'accord de la direction de ITG pour générer une nouvelle bi-clé.

Si le certificat d'une des AC est révoqué alors il ne peut y avoir de renouvellement de certificat. Il faut que l'AC génère de nouvelles clés.

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

La validation d'une demande de révocation d'une autorité de certification est un phénomène exceptionnel.

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

La méthode de validation d'une demande de révocation issue d'une autorité de certification est identique à la validation initiale du porteur.

IV. Exigences opérationnelles sur le cycle de vie des certificats

IV.A. Demande de certificat

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

Un certificat peut être demandé uniquement par une personne habilitée d'ITG.

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

Les informations suivantes doivent au moins faire partie de la demande de certificat (cf. chapitre III.B) :

- Les données à certifier, y compris le DN ;
- La clé publique ;
- La preuve de possession de la clé privée ;
- Les éléments d'identification de l'autorité de certification concernée

IV.B. Traitement d'une demande de certificat

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

L'identité du demandeur est vérifiée conformément aux exigences du chapitre III.B.

Un témoin, a minima, atteste de la conformité de la demande de création de tout certificat d'autorité de l'IGC de BNP Paribas.

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

Celle-ci se matérialise par la signature d'un procès-verbal de Cérémonie des clés

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

Le délai de traitement est variable car il dépend essentiellement du travail à réaliser pour vérifier la recevabilité de la demande.

La durée d'établissement du certificat est conditionnée par le déroulement de la cérémonie de clé.

IV.C. Délivrance du certificat

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

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande, les autorités « BNPP PDF CA » et « BNPP LEVEL2 CA », en qualité de service technique, déclenchent les processus de génération du certificat.

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

A l'issue de la cérémonie, si aucune anomalie n'a été signalée sur le certificat, celui-ci est officiellement remis à ITG, sous la forme d'un fichier, sur un media amovible.

IV.D. Acceptation du certificat

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

ITG accepte formellement le certificat délivré lors de la cérémonie de clés en émargeant le registre de cérémonie. Aucune objection postérieure à la cérémonie ne pourra être reçue pour annuler l'acceptation du certificat.

IV.D.2. Publication du certificat

Cette information doit être accessible à partir d'internet.

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

La notification de la délivrance du certificat s'effectue durant la cérémonie des clés.

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

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

L'utilisation des clés privées des autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » et de leurs certificats associés est strictement limitée à la signature de certificats d'autorités de certification et à la signature de listes de certificats d'autorités révoqués.

L'usage autorisé de la bi-clé et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des clés.

Dans la suite du document, l'autorité de certification BNPP Group Customer Epheremal sera nommée « BNPP Instant CA », l'autorité de certification certifications BNP Paribas Fortis Customer Ephemeral sera nommée « BNPPF Instant CA » et l'autorité de certification BNPP Group Sealing and Timestamping sera nommée « BNPP Service CA ».

L'utilisation de la clé privée est limitée à :

a) Pour l'autorité de certification « BNPP Instant CA » :

- La signature de certificats de signature pour les clients de BNP Paribas
- La signature de certificats OCSP,
- La signature de listes de certificats révoqués.

b) Pour l'autorité de certification « BNPPF Instant CA » :

- La signature de certificats de signature pour les clients de BNP Paribas Fortis
- La signature de certificats OCSP,
- La signature de listes de certificats révoqués.

c) Pour l'autorité de certification « BNPP Service CA » :

- La signature de certificats de signature cachet au nom de BNP Paribas ou de ses filiales.
- La signature de certificats d'horodatage au nom de BNP Paribas
- La signature de certificats OCSP,
- La signature de listes de certificats révoqués.

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

Les certificats délivrés par les autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » ne peuvent être utilisés par un utilisateur qu'à des fins de validation d'une chaîne de confiance comprenant le certificat de celle-ci.

IV.F. Renouvellement d'un certificat

Non applicable dans le cadre de la présente PC.

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

IV.G.1. Causes possibles de changement d'une bi-clé

Les bi-clés doivent être changées :

- Pour suivre l'évolution de l'état de l'art en cryptographie, et en particulier les recommandations émises par l'Agence Nationale de Sécurité des Système d'Information afin de minimiser les possibilités d'attaques cryptographiques ;
- En cas de fin de vie du certificat associée à une des autorités de certification ;
- En cas de compromission, suspicion de compromission, vol ou perte des moyens de reconstitution de la clé privée d'une des autorités de certification.

Dans tous ces cas la délivrance d'un nouveau certificat d'autorité est possible pour toute l'IGC de BNP Paribas.

Enfin, dans le cas d'un changement de bi-clé, il est nécessaire de procéder à la révocation du certificat correspondant à l'ancienne bi-clé (cf. §IV.I).

IV.G.2. Origine d'une demande d'un nouveau certificat

La demande d'un nouveau certificat suit les mêmes conditions que celles portées au paragraphe IV.A.

IV.G.3. Procédure de traitement d'une demande d'un nouveau certificat

Le traitement d'une demande de certificat suite au changement d'une bi-clé est identique à celui décrit au paragraphe IV.B.

IV.G.4. Notification au porteur de l'établissement du nouveau certificat

Cf. chapitre IV.C.2.

IV.G.5. Démarche d'acceptation du nouveau certificat

Cf. chapitre IV.D.1.

IV.G.6. Publication du nouveau certificat

Cf. chapitre IV.D.2.

IV.G.7. Notification par les autorités hors ligne aux métiers de la délivrance d'un nouveau certificat

Cf. chapitre IV.D.3.

IV.H. Modification du certificat

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

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

IV.I. Révocation et suspension des certificats

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

Pour une autorité de certification en ligne et hors ligne, les causes de révocation sont les suivantes :

- Cessation d'activité commerciale associée à l'autorité de certification
- Compromission, suspicion de compromission, vol ou perte des moyens de reconstitution de la clé privée de l'autorité métier
- Non-conformité révélée lors d'un contrôle de conformité.

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

Seul ITG est habilité à effectuer une demande de révocation.

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

La révocation d'un certificat nécessite une cérémonie de clés.

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

Dans le cas d'une compromission ou d'une suspicion de compromission de clé privée d'une autorité hors ligne ou en ligne la direction de ITG demande immédiatement à révoquer le certificat de celle-ci.

IV.I.5. Délai de traitement par les autorités hors ligne d'une demande de révocation

La révocation est traitée dans les 24 heures suivant la réception de la demande. Les demandes de révocation devront être traitées à réception par l'Autorité correspondante durant la cérémonie des clés.

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

Sans objet.

IV.I.7. Fréquence d'établissement des CRL des autorités hors ligne

La fréquence de publication des CRL des autorités hors ligne est de 1 an. Les CRL des autorités hors ligne se recouvrent sur une période d'un mois : la CRL suivante a une date de validité qui est inférieure d'un mois à la date d'expiration de la CRL en cours.

Dans le cas exceptionnel d'une révocation, cette CRL sera mis à jour tel qu'indiqué au § IV.I.8 ci-après.

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

Une CRL doit être publiée dans un délai maximum de 8 heures suivant sa génération.

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

Les autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » ne mettent en œuvre aucun système de vérification en ligne de la révocation et de l'état des certificats, indépendamment de la publication sur Internet d'ARL et de certificats (pas d'OCSP par exemple).

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

Sans objet.

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

Si d'autres moyens sont mis en œuvre, la DPC les précisera.

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

La révocation suite à une compromission de la clé privée doit faire l'objet d'une information clairement diffusée au moins sur le site Internet de BNP Paribas.

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

La suspension de certificats n'est pas autorisée dans la présente PC.

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

IV.J.1. Caractéristiques opérationnelles

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de CRL.

Les ARL de l'autorité racine sont au format V2, accessibles en http aux adresses suivantes :

- S'agissant de l'autorité « BNPP PDF CA » :
  http://bnpp.digitaltrust.morpho.com/crl/bnpp-pdf-ca.crl
- S'agissant de l'autorité « BNPP LEVEL2 CA » :
  http://bnpp.digitaltrust.morpho.com/crl/bnpp-level2-ca.crl

Ces informations sont accessibles depuis internet.

IV.J.2. Disponibilité de la fonction

La fonction d'information sur l'état des certificats est rendue disponible par les autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » avec une durée maximale d'indisponibilité référencée au §II.C.

Le taux de disponibilité est a minima de 99,7%, 24/7.

IV.K. Fin de la relation avec le porteur

Cf. chapitre IV.I.1, les causes possibles d'une révocation.

IV.L. Séquestre de clé et recouvrement

Le séquestre des clés privées est interdit.

V. Mesures de sécurité non techniques

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que les autorités de certification hors ligne (BNPP PDF CA & BNPP Level 2 CA) doivent respecter. La DPC décrit les moyens mis en œuvre pour respecter ces exigences.

V.A. Mesures de sécurité physique

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

Les sites d'hébergement sont décrits dans le contrat liant IDEMIA à son prestataire.

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

V.A.2. Accès physique

Sans objet puisque les AC sont hors-ligne

V.A.3. Alimentation électrique et climatisation

Sans objet puisque les AC sont hors-ligne

V.A.4. Vulnérabilité aux dégâts des eaux

Sans objet puisque les AC sont hors-ligne

V.A.5. Prévention et protection incendie

Sans objet puisque les AC sont hors-ligne

V.A.6. Conservation des supports

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

V.A.7. Mise hors service des supports

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

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

V.A.8. Sauvegardes hors site

Les sauvegardes hors site sur support amovible sont stockées dans des coffres. La DPC précise les modalités de stockage.

V.B. Mesures de sécurité procédurales

V.B.1. Rôles de confiance

On distingue les rôles suivants :

- **L'officier de sécurité de L'IGC** : il est en charge de la bonne application de la politique de certification.
- **Responsable de sécurité physique** : Il est chargé des contrôles d'accès physiques aux équipements des systèmes de la composante d'AC hors AE. Ce responsable est nommé par le partenaire hébergeur de IDEMIA.

- **Opérateurs techniques de l'IGC** : ils sont chargés de l'utilisation, de la configuration et de la maintenance technique des équipements, boîtier cryptographique et serveur. En particulier, ils développent techniquement le déroulement de la cérémonie de clé.
- **Auditeurs :** Personne désignée par une autorité compétente (conforme par exemple à « Instruction relative à la procédure d'habilitation des organismes qui procèdent à la qualification des prestataires de services de confiance ») et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante. L'auditeur est nommé par l'organisation BNP Paribas ou IDEMIA.
- **Porteurs de secrets :**
    - L'administrateur porteur de secret permet de créer le contexte de sécurité d'accès au boîtier et de le restaurer ;
    - L'opérateur porteur de secret participe à créer et activer la bi-clé des autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » dans le contexte de sécurité détenu par les administrateurs porteur de secret.

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 peuvent être différents.

Pour des raisons de sécurité, les fonctions sensibles seront réparties sur plusieurs personnes. La présente politique définit les exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'IGC.

La DPC de l'autorité racine précise quelles sont les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter (positions dans l'organisation, liens hiérarchiques, etc.).

Il est admis qu'une même personne puisse assurer plusieurs rôles. La répartition est définie dans le cadre de la DPC.

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

La Direction de IDEMIA et ITG fait vérifier l'identité et les autorisations de tout membre de son 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.

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

Les porteurs de secret ne détiennent jamais le quorum minimum d'un même secret.

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

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

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

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

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

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

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

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

V.C.2. Procédures de vérification des antécédents

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

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

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

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

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

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

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

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

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

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

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

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

V.C.8. Documentation fournie au personnel

Les documents dont doit disposer le personnel sont les suivants :

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

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

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

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

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

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

L'IGC de BNP Paribas permet de journaliser les évènements suivants pour les autorités de certification hors ligne :

- Journaux applicatifs de la PKI
  - Réception d'une demande de certificat (initiale et renouvellement),
  - Validation / rejet d'une demande de certificat,
  - Evènements liés aux clés de signature et aux certificats d'autorités (génération, sauvegarde / récupération, révocation, renouvellement, destruction,...),
  - Génération des certificats des porteurs,
  - Réception d'une demande de révocation,
  - Validation / rejet d'une demande de révocation,
  - Génération puis publication des CRL,
- Autre journaux :
  - Les accès physiques,
  - Les actions de maintenance et de changements de la configuration des systèmes,
  - Les changements apportés au personnel,
  - Publication et mise à jour des informations liées à l'autorité (PC, certificats d'autorité, conditions générales d'utilisation, etc.).

De plus, en fonction du type de l'évènement, chaque enregistrement devra également contenir les champs suivants lorsqu'applicable :

- Destinataire de l'opération,
- Nom du demandeur de l'opération ou référence du système effectuant la demande,
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes),
- Cause de l'évènement,
- Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat),

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

L'analyse du contenu des journaux d'événements doit être effectuée de manière régulière par les autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » lors de chaque signature de certificat ou de CRL.

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

Les journaux d'évènements sont conservés jusqu'à la fin de vie des autorités « BNPP PDF CA » et « BNPP LEVEL2 CA ».

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

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements.

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

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

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

L'IGC de 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

Se référer au chapitre correspondant de la DPC.

V.D.8. Evaluation des vulnérabilités

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

Des tests d'intrusion complémentaires sont réalisés périodiquement.

V.E. Archivage des données

V.E.1. Types de données à archiver

Les procédures et les outils permettent d'archiver les données suivantes :

- Certificats des autorités hors ligne
- Certificat des autorités en lignes, valides comme révoqués
- Journaux d'événements Cf. §V.D
- Logiciels et fichiers de configuration des différentes composantes
- Ensembles des éléments utiles à l'enregistrement ou à la révocation :
    - Récépissés
    - Demandes de révocation et leurs résultats
- Registres de cérémonie de clés
- Scripts des cérémonies
- Listes de révocations

V.E.2. Procédure de constitution des archives

Se référer au chapitre correspondant dans la DPC.

V.E.3. Période de conservation des archives

Les archives sont conservées jusqu'à la fin de vie de l'IGC de BNP Paribas.
De la même façon, les données papier sont conservées jusqu'à la fin de vie de l'IGC.

V.E.4. Durée de restitution des archives

Les archives (papier ou électroniques) peuvent être récupérées dans un délai inférieur à 5 jours ouvrés.

V.E.5. Protection des archives

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

- Protégées en intégrité,
- Accessibles aux personnes autorisées,

- Accessibles pour relecture et exploitation.

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

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

Se référer au chapitre correspondant de la DPC.

V.E.7. Système de collecte des archives

Se référer au chapitre correspondant de la DPC.

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

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

V.F. Changement de clé de l'autorité

L'AC change sa bi-clé lorsqu'elle n'est plus conforme au référentiel cryptographique de niveau standard émis par l'ANSSI. La durée de vie maximale d'un certificat d'AC doit être en cohérence avec le référentiel cryptographique de l'ANSSI.

Les autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » ne peuvent pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant à la sienne. Pour cela, la période de validité de son certificat est supérieure à celle des certificats qu'elle signe.

Aussi lorsqu'elle accède à une demande de certification, l'autorité « BNPP PDF CA » et « BNPP LEVEL2 CA » fixe la durée de vie du certificat demandé de telle sorte qu'il ne soit jamais valable au-delà de la date de fin de validité du certificat de sa bi-clé utilisée pour la signature.

V.G. Reprise suite à compromission et sinistre

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

Les officiers de sécurité de BNP Paribas et IDEMIA mettent en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels.

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

En cas de corruptions des ressources informatiques durant la cérémonie des clés, celle-ci est interrompue et reprogrammée dans les plus brefs délais.

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

Dans le cas de compromission d'une clé d'autorité, le certificat correspondant est immédiatement révoqué (voir § IV.I.5, en fonction des délais de réalisation de la cérémonie de clés).

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

Dans le cas de compromission d'un algorithme, le certificat correspondant est révoqué (voir § IV.I.5, en fonction des délais de réalisation de la cérémonie de clés) et un nouveau certificat est généré n'employant pas l'algorithme compromis (voir §IV.A).

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

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

S'agissant des autorités « BNPP PDF CA » et « BNPP LEVEL2 CA », hors ligne, la continuité d'activité consiste à restaurer l'IGC à partir des sauvegardes et secrets.

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

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

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

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

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

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

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

Le transfert d'activité est sans objet dans le cadre de la présente Politique de Certification.

La cessation d'activité dans ce paragraphe ne concerne qu'une composante autre que l'ACR « BNPP PDF CA ». Si l'ACR cesse son activité, voir § V.H.2.

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

- mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, l'archivage des certificats des porteurs et des informations relatives aux certificats) ;
- assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des CRL), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC.
- communiquer au préalable son intention de transfert d'activité à une date donnée ;
- mettre en œuvre tous les moyens dont elle dispose pour informer ses partenaires (utilisateurs finaux, autres composantes, autres IGC, etc.) de ses intentions de fin d'activité ;
- remettre ses archives à l'AA ;
- l'ACR doit préciser dans sa DPC qui elle doit prévenir, comment se déroule le transfert des obligations (archives et logs à une autre entité), et comment seront traités les certificats encore valides qui seraient amenés à être révoqués.

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

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées aux trois premiers items ci-dessous soient à exécuter par l'ACR, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.
Dans l'hypothèse d'une cessation d'activité totale, l'ACR ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des ARL conformément aux engagements pris dans sa PC.

VI. Mesures de sécurité techniques

VI.A. Génération et installation de bi clés

VI.A.1. Génération des bi-clés

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

Les clés de signature des autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » sont générées et mises en œuvre dans un boîtier cryptographique dont les caractéristiques sont décrites dans la DPC.

La génération des clés de signature des autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. chapitre V.B.1), dans le cadre de « cérémonies de clés ». Ces cérémonies se déroulent suivant des scripts préalablement définis.

L'initialisation de l'IGC et/ou la génération des clés de signature des autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » s'accompagne de la génération de parties de secrets (principe de protection n sur m). Ces parties de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature des autorités « BNPP PDF CA » et « BNPP LEVEL2 CA », notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures de l'autorité racine.

Le boîtier cryptographique, utilisé par toutes les autorités de l'IGC de BNP Paribas pour générer et mettre en œuvre les clés de signature (pour la génération des certificats électroniques, des listes de révocation) a pour objectif :

- D'assurer la confidentialité et l'intégrité des clés privées de signature durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- D'être capable d'identifier et d'authentifier ses utilisateurs, porteurs de secrets d'activation du boîtier ;
- De permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'autorité, qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- De créer des enregistrements d'audit pour chaque action réalisée à partir d'une clé d'autorité.

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

Les clés privées des autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » sont transmises à BNPP sous la forme de secrets partagés entre plusieurs porteurs BNPP.

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

a) S'agissant de l'autorité racine « BNPP PDF CA »

Les modes de transmission de la clé publique de l'autorité (**certificat auto-signé**, PKCS#10, …), sont définis dans la procédure de demande de certificat indiquée au paragraphe IV.B.

b) S'agissant de l'autorité « BNPP LEVEL2 CA »

Les modes de transmission de la clé publique de l'autorité (**certificat signé par l'AC « BNPP PDF CA »**, PKCS#10, …), sont définis dans la procédure de demande de certificat indiquée au paragraphe IV.B.

c) S'agissant des autorités en ligne

Les modes de transmission de la clé publique de l'autorité (**certificat signé par l'AC « BNPP LEVEL2 CA »**, PKCS#10, …), sont définis dans la procédure de demande de certificat indiquée au paragraphe IV.B.

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

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

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

VI.A.5. Taille des clés

Les autorités utilisent des clés de 4096 bits.

L'AC suit les recommandations cryptographiques de l'ANSSI sur la base de la TS 119 312 de l'ETSI.

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

La durée de vie des clés est de 23 ans.

VI.A.8. Objectifs d'usage de la clé

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

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

Les clés privées des autorités de certification de l'IGC de BNP Paribas (hors ligne ou en ligne) sont protégées par un boitier cryptographique dont le niveau de résistance est évalué certifié FIPS 140-2 level 3.

Le boîtier utilisé par les AC « BNPP PDF CA » et « BNPP LEVEL2 CA » n'est pas qualifié par l'ANSSI.

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

Le contrôle des clés privées de signature de l'AC doit être assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets (systèmes où n exploitants parmi m doivent s'authentifier, avec n au moins égal à 2).

Le management de ITG désigne ces porteurs de secrets.

VI.B.3. Séquestre de la clé privée

Les clés privées de toutes les autorités de l'IGC de BNP Paribas ne sont pas séquestrées.

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

La copie de secours des clés des autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » est réalisée en utilisant les spécifications du boîtier cryptographique qui est décrit dans la DPC.

VI.B.5. Archivage de la clé privée

Les clés privées de toutes les autorités de l'IGC de BNP Paribas ne sont en aucun cas archivées.

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

Cf. VI.B.4.

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

Les clés privées d'une autorité de l'IGC de BNP Paribas (racine ou subordonnée) sont stockées, durant leur activation, dans un module cryptographique répondant au minimum aux exigences du chapitre XI ci-dessous.

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

L'activation de la clé privée de toutes les AC de l'IGC de BNP Paribas dans un module cryptographique doit être contrôlée via des données d'activation et doit faire intervenir au moins n parmi m personnes identifiées dans les rôles de confiance correspondants.

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

La désactivation des clés privées des AC de l'IGC de BNP Paribas dans un module cryptographique doit être automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur technique de la PKI, etc.

La désactivation de la clé privée d'une AC de l'IGC de BNP Paribas utilisée lors d'une cérémonie de clés ou de génération de bi-clé et de certificat, est réalisée immédiatement après l'utilisation de la clé.

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

La méthode de destruction de la clé privée d'une AC de l'IGC de BNP Paribas doit permettre de répondre aux exigences définies dans le chapitre XI.

En fin de vie d'une AC de l'IGC de BNP Paribas, normale ou anticipée (révocation), cette clé est systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

Elle n'est réalisée que sur demande du management de ITG.

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

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

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

VI.C.1. Archivage des clés publiques

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

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

La fin de validité du certificat des AC de l'IGC de BNP Paribas doit être postérieure à la fin de vie des certificats porteurs qu'elle émet.

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 l'IGC sont effectuées lors de la phase d'initialisation et de personnalisation de ce module.

Ces données d'activation ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (cf. chapitre V.B.1).

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

Les données d'activation générées pour les modules cryptographiques de l'IGC de BNP Paribas sont protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire.

Ce destinataire de la donnée d'action transmet au gestionnaire de coffre celle-ci, qui en a ensuite la responsabilité afin d'en assurer la confidentialité, l'intégrité et la disponibilité.

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

Se référer au chapitre correspondant de la DPC.

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

Sans objet.

VI.E. Mesures de sécurité des systèmes informatiques

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

Se référer au chapitre correspondant de la DPC.

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

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

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

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

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

Toute évolution significative d'un système d'une composante de l'IGC de 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 autorités « BNPP PDF CA » et « BNPP LEVEL2 CA » sont hors ligne.

VI.H. Horodatage / Système de datation

Il n'y a pas d'horodatage au sein de l'IGC, mais un système de datation dont la description est donnée dans la DPC.

VII. Profils des certificats, OCSP et des CRL

VII.A. Profil des certificats

VII.A.1. Numéro de version

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

VII.A.2. Champs de base

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

Nom du champ	Description	Contenu
Version	Version du certificat X.509	Contient la valeur 2 pour indiquer que le certificat est un certificat x.509v3
SerialNumber	Numéro de série du certificat	Contient une valeur entière pour indiquer le numéro de série du certificat, cette valeur doit être unique pour chaque certificat émis par l'autorité racine.
Signature	Signature de l'autorité pour l'authentifier	Sha2WithRSAEncryption
Issuer	Nom de l'autorité	Contient le DN (X.500) de l'autorité
Validity	Période de validité du certificat	Contient les dates d'activation et d'expiration du certificat.
Subject	Nom du porteur	Contient le DN de l'autorité
Subject Public Key Info	Informations sur la clé publique de l'abonné	Contient l'OID de l'algorithme et la clé publique de l'abonné.
Extensions	Liste des extensions	Voir chapitre suivant

VII.A.3. Extensions du certificat

Les certificats émis par les autorités hors ligne de l'IGC de BNP Paribas comportent les extensions X.509v3 suivantes. La DPC précise les valeurs utilisées.

Extension	Extension critique	Description
Authority Key Identifier	N	Elément d'identification de la clé publique de l'autorité signant le certificat
KeyUsage	O	Description des utilisations autorisées de la clé privée
Certificate Policies	N	OID de la PC régissant le certificat et Intitulé de la PC
Authority Information Access	N	Informations d'accès au certificat de l'autorité.
Subject Key Identifier	N	Elément d'identification de la clé publique du porteur
Certificate Policy	N	Indique l'adresse ou sont publiées toutes les politiques de certification
CRL Distribution Points	O	Indique les adresses auxquelles est publiée la CRL de l'autorité ayant émis le certificat, sauf pour « BNPP PDF CA »

VII.A.4. OID des algorithmes

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

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

VII.A.5. Forme des noms

Les noms attribués aux porteurs dans le cadre de l'IGC de BNP Paribas respectent la norme X.500, comme détaillé au chapitre III.A de ce document.

VII.A.6. OID des politiques de certification

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

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

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

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

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

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

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

VII.B. Profil des CRL

VII.B.1. Numéro de version

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

VII.B.2. Champs de base

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

Champ	Description
Version	Version de la CRL X.509
Signature	Identifiant de l'algorithme utilisé pour produire le sceau d'intégrité de la liste Sha2WithRSAEncryption retenu pour la présente PC.
Issuer	Nom de l'autorité de l'IGC de BNP Paribas
This Update	Date d'émission de la CRL
Next Update	Date limite d'émission de cette CRL
Revoked Certificates	Liste d'enregistrement de révocation. On spécifiera pour chaque révocation les valeurs associées aux champs suivants : - User Certificate (numéro de série du certificat révoqué) - Revocation Date (date de révocation du certificat).
CRL Extensions	Extensions générales de la CRL

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

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

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

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

Extension d'entrée	Description
Authority Key Identifier	Identifie la clé publique de l'autorité ayant signé la CRL
CRL Number	Donne un nombre croissant séquentiel pour chaque CRL émise
Reason Code	Identifie la cause de révocation du certificat. Sauf spécification particulière, la valeur pour chaque révocation sera « unspecified ».

VIII. Audit de conformité et autres évaluations

VIII.A. Fréquences et / ou circonstances des évaluations

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

VIII.B. Identités / qualifications des évaluateurs

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

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

VIII.C. Relations entre évaluateurs et entités évaluées

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

VIII.D. Sujets couverts par les évaluations

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

VIII.E. Actions prises suite aux conclusions des évaluations

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

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

VIII.F. Communication des résultats

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

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

IX. Annexe 1 - Autres problématiques métiers et légales

IX.A. Tarifs

Sans objet.

IX.B. Responsabilité financière

Non applicable pour les autorités de certification hors ligne.

IX.C. Confidentialité des données professionnelles

IX.C.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

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

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

Sans objet.

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

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

IX.D. Protection des données personnelles

BNP Paribas respecte la réglementation sur les données personnelles, tant en matière de collecte que d'usage des données à caractère personnel.

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 de BNP Paribas sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi [CNIL].

IX.D.2. Données à caractère personnel

Les données considérées comme personnelles sont a minima les données suivantes :

- Les dossiers de la cérémonie des clés
- Les dossiers d'enregistrement des différents rôles (Référents, Gestionnaire de Certificats, etc.)

IX.D.3. Données à caractère non personnel

Aucune exigence spécifique n'a été formulée à ce sujet.

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

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

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

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

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

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

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

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

IX.E. Droits sur la propriété intellectuelle et industrielle

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

IX.F. Interprétations contractuelles et garanties

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

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

IX.F.1. Autorité de Certification

L'AC a pour obligation de garantir et maintenir la cohérence de sa DPC avec sa PC.

IX.F.2. Service d'enregistrement

Voir le paragraphe IX.F.1.

IX.F.3. Porteurs de certificats

Dans le cas des certificats d'autorités, les porteurs de ces certificats ont le devoir de :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- protéger la clé privée du certificat dont il a la responsabilité par des moyens appropriés à son environnement ;
- protéger les données d'activation de cette clé privée et, le cas échéant, les mettre en œuvre ;
- respecter les conditions d'utilisation de la clé privée et du certificat correspondant ;
- informer l'AC de toute modification concernant les informations contenues dans le certificat électronique ;
- faire, sans délai, une demande de révocation du certificat électronique dont il est responsable auprès de l'AE ou de l'AC en cas de compromission ou de suspicion de compromission de la clé privée correspondante (ou de ses données d'activation).

IX.F.4. Utilisateurs de certificats

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

IX.F.5. Autres participants

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

IX.G. Limite de garantie

Sans objet.

IX.H. Limite de responsabilité

Sans objet.

IX.I. Indemnités

Sans objet.

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

IX.J.1. Durée de validité

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

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

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

IX.K. Notifications individuelles et communications entre les participants

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

IX.L. Amendements à la PC

IX.L.1. Procédures d'amendements

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

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

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

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

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

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

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

IX.M. Juridictions compétentes

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

IX.N. Conformités aux législations et réglementations

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

IX.O. Dispositions diverses

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

IX.P. Autres dispositions

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

X. Annexe 2 – Documents cités en référence

X.A. Réglementation

Non applicable.

X.B. Documents techniques

Référence	Objet du document
FIPS140-2_LEVEL3_CERT	Certificat de qualification FIP 140-2 level 3 du boitier cryptographique nShield (firmware 2.59.6)

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

XI.A. Exigences sur les objectifs de sécurité

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

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

XI.B. Exigence sur la qualification

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