Politique de certification BNP Paribas

Autorité de certification

BNP Paribas Group Sealing and Timestamping CA

itg

Revue		
Nom	Fonction	Date

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

Suivi des versions			
Version	Date	Auteur	Nature des modifications
0.1	06/07/2015	Morpho DSA	Initialisation du document
0.2	17//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.B.3, V.H • Distinction entre porteurs et autorités au VI.B • Correction de coquille du III.A.3, IV.J.2 • Correction du IV.C.2, IV.D.2, IV.D.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, IX.J, VI.B.8 et VI.B.9
2.1	21/02/2017	Cédric SZANIEC	Correction des reliquats des écarts de l'audit et corrections diverses: • Clarification du IV.A.1, • Précisions du III.B.2, III.B.5, IV.E.1 • Ajout du IX.M
3.0	23/06/2017	Cédric SZANIEC	Changement de Safran I&S vers OT Morpho Adaptation de la PC pour eIDAS EN 319 411-1
3.1	16/01/2018	Cédric SZANIEC	Changement d'IDEMIA en IDEMIA et d'ITP ITG en ITG. Correction des écarts de l'audit ETSI EN 319 411-1 : • Ajout du I.C.6 • Modification et clarification du III.A.5 • Précisions du IV.J.1
3.2	01/07/2019	Ibrahima TAMBOURA	Revue annuelle avec IDEMIA : • Modification : V.E.3, V.D.8

Sommaire

I. Introduction

I.A. Présentation générale

Ce document constitue la Politique de Certification (PC) de l'autorité de certification « BNP Paribas Group Sealing and Timestamping CA » (« BNPP Service CA » dans la suite de ce document) dans le cadre de l'émission de certificats électroniques destinés aux clients de BNP Paribas pour un usage de signature d'entité (aussi dénommé signature cachet) et à BNP Paribas pour un usage de signature d'horodatage.

Ce document expose le niveau d'exigence que s'engage à respecter et maintenir l'autorité de certification 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, émises par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et la Direction Générale de la Modernisation de l'Etat (DGME) et de l'European Telecommunications Standards Institute (ETSI).

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.

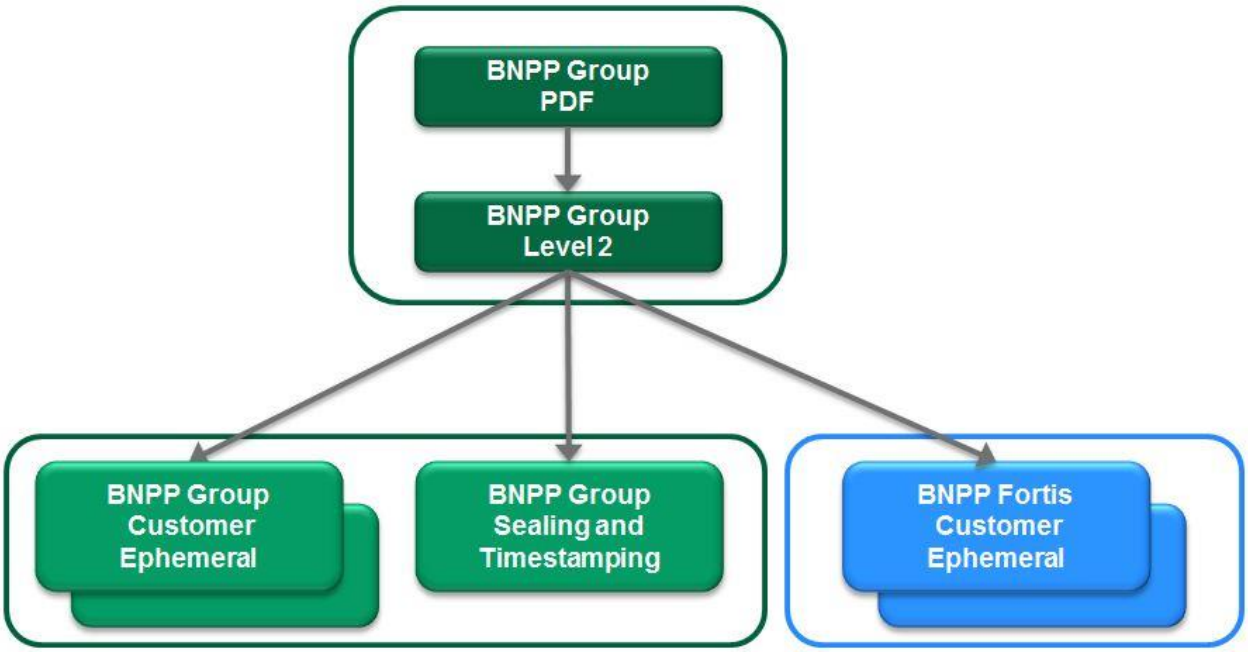

Figure 1 : IGC du groupe BNP Paribas

I.B. Identification du document

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

- Les numéros d'OID correspondant à la présente politique de certification indiqué dans les certificats sont les suivants : Certificat d'entité ou cachet serveur : 1.2.250.1.62.10.5.1.1.2
- Horodatage : 1.2.250.1.62.10.5.1.2.2
- Certificats OCSP : 1.2.250.1.62.10.5.1.3.1

La branche OID de BNP Paribas est déposée : {iso(1) member-body(2) fr(250) type-org(1) BNP Paribas(62)} Signel (10) « BNPP Service CA » (5) Politique de Certification(1) Gabarit de Certificat(1, 2 ou 3) Version(1 ou 2).

Elle correspond aux certificats émis à partir du 20 juillet 2017.

I.C. Entités intervenant dans l'IGC

I.C.1. Autorité de Certification

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

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

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

L'ensemble des fonctions assurées par l'IGC de BNP Paribas (en tant que service technique) est opéré par le service informatique de IDEMIA.

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.

I.C.2. Autorité d'enregistrement (AE)

L'AE a pour rôle de vérifier l'identité du futur porteur de certificat ainsi que des contraintes liées à l'usage du certificat qui lui est délivré, conformément à la politique de certification. L'AE doit être reconnue par l'AC de l'IGC pour laquelle elle édite des demandes de certificats et les demandes de révocation.

I.C.3. Porteurs de certificats

Un porteur de certificat est soit :

- Une application du client de BNP Paribas dont l'usage exclusif est la signature de document au nom de ce client.
- Une unité d'horodatage opérée par BNP Paribas. Une unité d'horodatage est un ensemble de matériel et de logiciel en charge de la création de contremarques de temps caractérisées par un identifiant de l'unité d'horodatage accordé par l'autorité d'horodatage de BNP Paribas, et une clé unique de signature de contremarques de temps.

I.C.4. Opérateur de certification

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

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

I.C.5. Utilisateurs de certificats

Les Utilisateurs sont les entités de BNP Paribas qui émettent des documents signés en leur qualité de personne morale.

De plus, l'autre utilisation des certificats est l'émission de contremarques de temps.

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

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

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

I.C.7. Autres participants

a) S'agissant d'un certificat entité de BNP Paribas

Le gestionnaire de certificat est en relation directe avec l'entité demandeuse. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des porteurs de cette entité.

Pour chaque Entité, celle-ci devra nommer un ou deux référent(s) seul(s) habilité(s) à contacter le gestionnaire de certificat afin de pouvoir obtenir un certificat de signature entité.

b) S'agissant d'un certificat d'horodatage de BNP Paribas

Le gestionnaire de certificat de BNP Paribas assure le contrôle de la cohérence des demandes de certificats des Unités d'Horodatage.

c) S'agissant d'un certificat OCSP

Le gestionnaire de certificat de BNP Paribas assure le contrôle de la cohérence des demandes de certificats OCSP

I.D. Usage des certificats

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

a) S'agissant d'un certificat entité de BNP Paribas

Les porteurs ne génèrent que des signatures électroniques dans un usage défini contractuellement entre les parties et mettant en œuvre des produits de IDEMIA.

La politique de signature et de vérification de signatures est consultable à cette adresse :

http://bnpp.digitaltrust.morpho.com/psv.html

b) S'agissant d'un certificat d'horodatage de BNP Paribas

Les porteurs ne génèrent que des contremarques de temps conforme à la RFC 3161.

La politique d'horodatage de ces certificats est consultable à cette adresse :

http://bnpp.digitaltrust.morpho.com/ph.html

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

L'autorité « BNPP Service CA » émet uniquement des certificats dits de signature entité (aussi dénommé cachet) pour les clients de BNP Paribas ou d'horodatage pour BNP Paribas et des CRL.

I.D.3. Bi-clés et certificats OCSP

Les clés de signature du service OCSP de l'AC (OID : 1.2.250.1.62.10.5.1.3.1), sont uniquement utilisées pour signer les jetons OCSP produits par la fonction d'information sur le statut des certificats.

I.E. Gestion de la politique de certification

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

L'entité en charge de l'administration et de la gestion de la présente politique de certification est ITG. 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

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

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

I.F. Définitions et acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

- **AA** : Autorité d'Archivage
- **AC** : Autorité de Certification
- **ACR** : Autorité de Certification Racine
- **AE** : Autorité d'Enregistrement
- **ANSSI** : Agence nationale de la sécurité des systèmes d'information
- **CRL** : Liste de Certificats Révoqués
- **DN** : Distinguished Name
- **DPC** : Déclaration des Pratiques de Certification
- **IGC** : Infrastructure de Gestion de Clés
- **OID** : Object Identifier
- **OCSP** : Online Certificate Status Protocol
- **PMA** : Policy Management Authority
- **PC** : Politique de Certification
- **RGS** : Référentiel Général de Sécurité
- **RSA** : Rivest Shamir Adleman
- **SSI** : Sécurité des Systèmes d'Information
- **URL** : Uniform Resource Locator

Public Key Infrastructure (PKI ou IGC)	Ensemble de composants physiques, procédures et logiciels permettant de gérer le cycle de vie des certificats et d'offrir des services d'authentification, de chiffrement et de signature.
Certificat	Fichier électronique délivré par une Autorité de Certification attestant l'identité d'un porteur (personne physique, machine…). Le certificat est valide pendant une durée donnée précisée dans celui-ci.
Autorité de Certification (AC ou CA)	Service chargé de signer, émettre et maintenir les certificats d'une infrastructure à clés publiques, conformément à une politique de certification. Services applicatifs exploitant les certificats émis par l'Autorité de Certification du porteur du certificat.
Politique de certification (PC)	Ensemble de règles et d'exigences auxquelles est soumise une autorité de certification dans la mise en place et la fourniture de ses prestations.
Déclaration des pratiques de certification (PC)	Description des pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'autorité de certification applique dans le cadre de la fourniture de ses services de certification électronique, en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.
Liste de révocation des Certificats (CRL ou LCR)	Liste publiée par l'autorité de certification présentant les certificats n'étant plus dignes de confiance (révoqués, invalides…). Par simplicité on y associe également les listes de révocation d'autorités (appelées ARL)
Répondeur OCSP	Service de statut en ligne des certificats
Bi-clé	Couple de clés composé d'une clé privée et d'une clé publique.
X 509	Norme de l'Union internationale des télécommunications (UIT)

	relative aux infrastructures à clés publiques (PKI), entre autres les formats standards de ses composants : certificats électroniques, listes de révocation, algorithme de validation…
UTF-8	Codage des caractères définis par Unicode où chaque caractère est codé sur une suite de un à six mots de 8 bits (il n'existe pas actuellement de caractères codés avec plus de 4 mots).
Distinguished Name (DN)	Elément permettant d'identifier un porteur ou une autorité de certification de façon unique.
Object Identifier (OID)	Identifiant universel, représenté sous la forme d'une suite d'entiers associé dans le cadre d'une PKI à un élément de référence tel que la politique de certification ou la déclaration de pratiques de certification.

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 « BNPP Service CA » met en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats.

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

II.B. Informations devant être publiées

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

- La présente politique de certification : **http://bnpp.digitaltrust.morpho.com/cp/BNPP-FR-cp-bnpp-aatl-service.pdf** ;
- Les listes des certificats révoqués : **http://bnpp.digitaltrust.morpho.com/crl/bnpp-sealing-and-timestamping-ca.crl** ;
- Les certificats des autorités « BNPP Service CA », en cours de validité : **http://bnpp.digitaltrust.morpho.com/ca/bnpp-sealing-and-timestamping-ca.cer** .

ITG tient à disposition des entités les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, etc.).

II.C. Délais et fréquences de publication

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

II.D. Contrôle d'accès aux informations publiées

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

III. Identification et authentification

III.A. Nommage

III.A.1. Types de noms

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

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

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

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 par les opérateurs techniques de l'IGC.

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

Aucune exigence n'est stipulée en plus des règles spécifiées ci-dessus.

III.A.5. Unicité de Noms

Afin d'assurer l'identification unique du porteur au sein de l'IGC de BNP Paribas et pour éviter toute ambigüité, le champ « subject » de chaque certificat de porteur permet d'identifier de façon unique son usage au sein de l'IGC de BNP Paribas.

a) S'agissant d'un certificat d'entité

L'entité de BNP Paribas doit préciser dans le champ CN de sa demande un nom significatif en relation avec son service applicatif, c'est-à-dire à titre d'exemple de faire un choix parmi les possibilités suivantes :

- Sa raison sociale
- Le nom d'une de ses filiales
- Le nom d'une de ses offres commerciales

Si le nom proposé est ambigu ou litigieux, par exemple s'il s'agit d'inscrire une marque déposée existante, il est nécessaire dans ce cas de préfixer le nom par la raison sociale du client.

De plus, le gestionnaire de Certificats s'assure de l'unicité du champ DN du certificat, à l'aide du référentiel des certificats déjà émis.

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

b) S'agissant d'un certificat d'horodatage

Chaque unité d'horodatage est nommée « Timestamp Unit » suffixée par un numéro incrémental dont la gestion est assurée par BNP Paribas.

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

c) S'agissant d'un certificat OCSP

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

De plus, le champ CN du sujet (DN) du certificat est structuré de la façon suivante :

- CN (commonName) = OCSP Responder <N>

où <N> est une valeur incrémentale unique

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

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

ITG est la seule entité habilitée à demander la création d'un certificat d'entité ou d'horodatage.

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

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

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

III.B.2. Validation de l'identité de l'entité cliente de BNP Paribas

La présente PC n'autorise la délivrance de certificat entité que pour le compte d'entité du groupe BNP Paribas et aucunement pour un organisme extérieur au groupe BNP Paribas.

Lors de la demande d'un certificat de signature entité, la demande devra être approuvée par le RSSI (Responsable de Sécurité des Systèmes d'Information) de l'Entité en question, afin que le gestionnaire de certificat puisse émettre la demande auprès de l'Exploitant de l'IGC.

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

a) S'agissant d'un certificat entité de BNP Paribas

Seul le gestionnaire de certificats est habilité à demander la création d'un certificat d'entité.

b) S'agissant d'un certificat d'horodatage de BNP Paribas

Seul le gestionnaire de certificats est habilité à demander la création d'un certificat d'horodatage.

c) S'agissant d'un certificat OCSP

Seul le gestionnaire de certificats est habilité à demander la création d'un certificat OCSP.

III.B.4. Information non vérifiée du porteur

Sans objet.

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

a) S'agissant d'un certificat entité de BNP Paribas

La demande effectuée par le gestionnaire de certificats ne peut avoir lieu qu'après une demande émise par un membre de l'entité demandeuse, en conformité avec le §III.B.2

b) S'agissant d'un certificat d'horodatage de BNP Paribas

La confirmation de la validité du demandeur est confirmée lors des signatures du formulaire de demande de certificat d'horodatage.

c) S'agissant d'un certificat OCSP

La confirmation de la validité du demandeur est confirmée lors des signatures du formulaire de demande de certificat OCSP.

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.

En cas de changement de bi-clé, se reporter au §IV.G.

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

En cas de révocation de certificat pour cause de compromission ou suspicion de compromission de clé, perte ou vol, de nouvelles clés doivent être générées. La procédure d'authentification à mettre en œuvre est alors la même que lors d'un premier enregistrement conformément au §III.B.3.

Si le certificat est révoqué pour une autre cause (modification d'informations contenues dans le certificat, révocation de l'autorité de certification, etc.), de nouvelles clés doivent également être générées. L'utilisateur s'authentifie par la même procédure que lors de la première demande de certificat.

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

a) S'agissant de l'autorité de certification

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.

b) S'agissant de l'entité finale

La révocation d'un certificat émis par l'autorité « BNPP Service CA » est effectuée via un formulaire par :

- Certificat entité :
  - Le gestionnaire de certificats suite à un évènement particulier
  - L'opérateur de l'IGC en cas de rupture contractuelle.
- Certificat d'horodatage : Le gestionnaire de certificats suite à un évènement particulier
- Certificat OCSP : .
  - Le gestionnaire de certificats suite à un évènement particulier
  - L'opérateur de l'IGC en cas de rupture contractuelle.

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 le gestionnaire de certificat dans le cadre de l'activité commerciale de la société.

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

a) S'agissant d'un certificat entité ou d'horodatage de BNP Paribas

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.

b) S'agissant d'un certificat OCSP

Lors de la demande de certificat émise dans le cadre du certificat OCSP, le formulaire fourni par le gestionnaire de certificat contient les éléments nécessaires à la constitution du DN du certificat. L'Opérateur de l'IGC peut alors générer les bi clés et la preuve de possession de la clé à soumettre pour signature à l'AC.

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.

Le gestionnaire de certificat atteste de la conformité de la demande de création de certificats « entité », de certificat d'horodatage ou de certificat OCSP.

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

a) S'agissant d'un certificat entité ou d'horodatage de BNP Paribas

L'acceptation se matérialise par installation du certificat sur les serveurs de signature ou d'horodatage de BNP Paribas.

Le rejet se matérialise par un message électronique indiquant la raison du refus.

b) S'agissant d'un certificat OCSP

L'acceptation se matérialise par la validation du certificat généré par l'opérateur de l'IGC. Le rejet se matérialise par un message électronique indiquant la raison du refus.

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

Le délai maximal de traitement est de 1 semaine après réception et validation de la demande.

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, l'autorité « BNPP Service CA » en qualité de service technique, déclenche les processus de génération du certificat.

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

L'Administrateur de l'IGC informe le gestionnaire de certificat du bon déroulement de l'opération.

IV.D. Acceptation du certificat

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

ITG accepte formellement le certificat en vérifiant la conformité du certificat vis-à-vis du formulaire de demande.

IV.D.2. Publication du certificat

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

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

Se référer au chapitre correspondant de la DPC.

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

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

a) S'agissant d'un certificat entité de BNP Paribas

L'utilisation de la clé privée associée à un certificat d'entité est strictement limitée à la signature de documents pour le compte de cette entité et ne peut pas être employée à d'autre fin.

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.

b) S'agissant d'un certificat d'horodatage de BNP Paribas

L'utilisation de la clé privée par une unité d'horodatage est strictement limitée à la création de contremarques de temps conforme à la RFC 3161.

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.

c) S'agissant d'un certificat OCSP

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

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

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

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'ANSSI afin de minimiser les possibilités d'attaques cryptographiques ;
- En cas de fin de vie du certificat associée à l'autorité « BNPP Service CA » ;
- En cas de compromission, suspicion de compromission, vol ou perte des moyens de reconstitution de la clé privée de l'autorité « BNPP Service CA ».

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).

La délivrance d'un nouveau certificat entité, d'horodatage ou OCSP suit la même procédure que pour un certificat initial.

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 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).

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

IV.I. Révocation et suspension des certificats

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

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

Pour les certificats entité, d'horodatage émis par l'autorité « BNPP Service CA », 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
- Non-conformité révélée lors d'un audit.

Le gestionnaire de certificats peut préciser dans le formulaire adéquat le motif de la demande de révocation :

- Perte
- Compromission
- Dysfonctionnement
- Arrêt de la mise en production

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

Seul le gestionnaire de certificats est habilité à effectuer une demande de révocation.

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

La révocation d'un certificat entité, d'horodatage de BNP Paribas est réalisée par les équipes d'exploitation de IDEMIA sous le contrôle de ITG.

En cas de révocation d'un des certificats de la chaîne de certification au travers d'une cérémonie des clés, BNP Paribas informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble de ses clients.

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 de certification, du service de signature ou du service d'horodatage de BNP Paribas, ITG demande après confirmation du risque à révoquer le certificat de celle-ci.

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

Les demandes de révocation devront être traitées à réception par l'autorité correspondante.

Cette révocation est traitée dans les 24 heures après réception de la demande.

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

Sans objet.

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

Une CRL est générée régulièrement toutes les 24 heures et immédiatement lorsqu'un certificat fait l'objet d'une révocation.

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

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

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

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

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 mises en œuvre, la DPC les précisera.

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

Se référer au chapitre correspondant de la DPC.

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

Sans objet.

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

IV.J.1. Caractéristiques opérationnelles

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

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

- Pour les certificats de porteurs :
  - CRL : **http://bnpp.digitaltrust.morpho.com/crl/bnpp-sealing-and-timestamping-ca.crl**
  - OCSP : **http://bnpp.digitaltrust.morpho.com/ocsp/bnpp-sealing-and-timestamping-ca**
- Pour les certificats de l'autorité de certification « BNPP Service CA » elle-même :
  - **http://bnpp.digitaltrust.morpho.com/crl/bnpp-level2-ca.crl**

Ces informations sont accessibles depuis internet.
De par leur nature, les deux services de statut des certificats n'ont pas une information immédiatement synchrone à l'issue d'une révocation. En effet, le service OCSP répond en temps réel alors que la mise à jour d'une CRL est un processus nativement asynchrone (cf. IV.I.7 et IV.I.8) avec par conséquent un temps de latence entre les deux services.

Concernant le statut des certificats cachet ou d'horodatage, l'écart maximum entre les deux services tient compte du temps de génération de la CRL immédiatement après révocation plus le délai de publication, soit 30 minutes.

IV.J.2. Disponibilité de la fonction

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

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

IV.J.3. Dispositifs optionnels

Sans objet.

IV.K. Fin de la relation avec le porteur

En cas de fin de relation entre l'AC et le porteur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.

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

IV.L. Séquestre de clé et recouvrement

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

V. Mesures de sécurité non techniques

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que les autorités « BNPP Instant CA » doivent respecter dans le cadre de l'hébergement de la PKI BNP Paribas chez IDEMIA. 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

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

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

V.A.3. Alimentation électrique et climatisation

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

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

V.A.4. Vulnérabilité aux dégâts des eaux

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

V.A.5. Prévention et protection incendie

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

V.A.6. Conservation des supports

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

V.A.7. Mise hors service des supports

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

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

.

V.A.8. Sauvegardes hors site

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

V.B. Mesures de sécurité procédurales

V.B.1. Rôles de confiance

On distingue les rôles suivants :

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

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

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

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

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

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

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

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

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

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

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

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

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

L'AC et l'opérateur de certification (OC) 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 concerne :

- La politique de certification ;
- La déclaration des pratiques de certification ;
- Les procédures internes ;
- Les documents techniques relatifs aux matériels et logiciels utilisés.

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

Les personnels contractants travaillant pour IDEMIA 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 hébergée chez IDEMIA journalise les évènements suivants, automatiquement dès le démarrage d'un système et sous forme électronique, concernant les systèmes liés aux fonctions qu'elle met en œuvre dans le cadre de l'IGC :

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

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

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

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

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

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

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

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

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

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

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

Les journaux d'évènements sont conservés 7 ans.

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

L'IGC 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.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.

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

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

Sans objet.

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

L'archivage permet de :

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

Les données à archiver sont les suivantes :

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

V.E.2. Procédure de constitution des archives

Se référer au chapitre correspondant de la DPC.

V.E.3. Période de conservation des archives

La durée de conservation des archives électronique est la suivante :

- Durée de rétention des archives de journaux d'évènements : 7 ans
- Durée de rétention des archives de certificats, CRL après leur expiration : 10 ans

De la même façon, les données papier sont archivées.

V.E.4. Durée de restitution des archives

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

V.E.5. Protection des archives

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

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

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

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

Se référer au chapitre correspondant de la DPC.

V.E.7. Système de collecte des archives

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

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

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

V.F. Changement de clé de l'autorité

L'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.

L'autorité « BNPP Service CA » ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration de son propre certificat. 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 Service CA » fixe la durée de vie du certificat demandé de telle sorte qu'il ne soit jamais valable au-delà de la date de fin de validité du certificat de sa bi-clé utilisée pour la signature.

V.G. Reprise suite à compromission et sinistre

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

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

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

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

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

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

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

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

Dans le cas de compromission d'un algorithme employé dans un certificat d'autorité, Voir le chapitre correspondant dans la PC PDF Level 2.

Dans le cas de la compromission d'un algorithme portant sur un certificat cachet ou d'horodatage, le certificat associé sera révoqué (voir §IV.I) et un nouveau certificat n'employant pas l'algorithme compromis sera généré (voir §IV.A).

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

Les différentes composantes de 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 de l'autorité en 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 considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

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

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

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

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

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

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

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

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

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

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

VI. Mesures de sécurité techniques

VI.A. Génération et installation de bi clés

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

VI.A.1. Génération des bi-clés

a) Clés d'autorité

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

Les clés de signature de l'autorité « BNPP Service 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 de l'autorité « BNP Service CA » est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance, 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 de l'autorité « BNPP Service 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 Service 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.

b) Clés des porteurs

Les clés des certificats entité et horodatage sont générés sur des ressources cryptographiques (HSM) par le personnel de BNP Paribas dans le respect d'une procédure spécifique prévue à cet effet. Cette méthodologie contrôlée par des auditeurs permet de s'assurer de la confidentialité et de l'intégrité des clés.

c) Clés OCSP

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

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

a) Clés d'autorité

Se référer au chapitre correspondant de la DPC.

b) Clés des porteurs

Les clés privées sont générées sur une ressource cryptographique (HSM) de telle sorte que les clés ne sortent jamais de la ressource et restent ainsi protégées en confidentialité et intégrité.

c) Clés OCSP

Les clés privées sont générées sur une ressource cryptographique (HSM) de telle sorte que les clés ne sortent jamais de la ressource et restent ainsi protégées en confidentialité et intégrité.

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

a) Clés des porteurs

Les clés publiques des porteurs sont remises à l'AC à partir de demandes générées par un logiciel de signature dans un format qui permet de prouver la possession de clés, en signant la requête. La signature est vérifiée par l'AC. Celle-ci émet un certificat si cette vérification est correcte.

La délivrance est ainsi protégée en intégrité de bout en bout lors de la demande de génération du certificat.

b) Clés OCSP

Les clés publiques des certificats OCSP sont remises à l'AC à partir de demandes générées dans un format qui permet de prouver la possession de clés, en signant la requête. La signature est vérifiée par l'AC. Celle-ci émet un certificat si cette vérification est correcte.

La délivrance est ainsi protégée en intégrité de bout en bout lors de la demande de génération du certificat.

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

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

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

VI.A.5. Taille des clés

Les autorités utilisent des clés de 4096 bits.

Les porteurs utilisent des clés de 2048 bits minimum.

Les certificats OCSP utilisent des clés de 2048 bits minimum.

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

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

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

VI.A.7. Durée de vie des clés

Cf. §VI.C.2.

VI.A.8. Objectifs d'usage de la clé

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

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

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

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

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

a) Clés d'autorité

Voir le chapitre correspondant dans la PC PDF Level 2.

b) Clés des porteurs

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

c) Clés OCSP

La clé privée du porteur est protégée par un boitier cryptographique dont le niveau de résistance est a minima FIPS 140-2 level 3.

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

a) Clés d'autorité

Voir le chapitre correspondant dans la PC PDF Level 2.

b) Clés des porteurs

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

c) Clés OCSP

Les clés privées des répondeurs OCSP ne sont pas contrôlées par plusieurs personnes.

VI.B.3. Séquestre de la clé privée

a) Clés d'autorité

Voir le chapitre correspondant dans la PC PDF Level 2.

b) Clés des porteurs

Les clés privées d'horodatage et de signature cachet ne sont en aucun cas séquestrées.

c) Clés OCSP

Les clés privées des répondeurs OCSP ne sont pas séquestrées.

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

a) Clés d'autorité

Voir le chapitre correspondant dans la PC PDF Level 2.

b) Clés des porteurs

La copie de secours des clés liées aux certificats cachets ou d'horodatage utilisées par les services de signature de BNP Paribas est réalisée en utilisant les spécifications du boîtier cryptographique.

Le processus est décrit dans la DPC.

c) Clés OCSP

Les clés privées des répondeurs OCSP font l'objet de copies de secours, en utilisant les spécifications du boitier cryptographique.

VI.B.5. Archivage de la clé privée

a) Clés d'autorité

Voir le chapitre correspondant dans la PC PDF Level 2.

b) Clés des porteurs

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

c) Clés des porteurs

Les clés privées des répondeurs OCSP 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

a) Clés d'autorité

Voir le chapitre correspondant dans la PC PDF Level 2.

b) Clés des porteurs

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

a) Clés OCSP

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

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

a) Clés d'autorité

Voir le chapitre correspondant dans la PC PDF Level 2.

b) Clés des porteurs

Non applicable.

c) Clés OCSP

Non applicable.

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

a) Clés d'autorité

Voir le chapitre correspondant dans la PC PDF Level 2.

b) Clés des porteurs

Non applicable.

c) Clés OCSP

Non applicable.

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

a) Clés d'autorité

Voir le chapitre correspondant dans la PC PDF Level 2.

b) Clés des porteurs

La destruction des clés est effectuée lorsque le certificat lié aux bi-clés a expiré.

c) Clés OCSP

La destruction des clés est effectuée lorsque le certificat lié aux bi-clés a expiré.

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

a) Clés d'autorité

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 § XI ci-dessous.

b) Clés des porteurs

Voir le paragraphe précédent.

c) Clés OCSP

Voir le paragraphe précédent.

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

VI.C.1. Archivage des clés publiques

a) Clés d'autorité

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

b) Clés des porteurs

Elles ne sont pas archivées.

c) Clés OCSP

Elles ne sont pas archivées.

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

S'agissant d'un certificat d'AC,

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

S'agissant d'un certificat final :

- Concernant le certificat d'unité d'horodatage : 3 ans
- Concernant le certificat cachet : 3 ans

S'agissant d'un certificat OCSP la durée de vie est fixée à 1 an.

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

VI.D. Données d'activation

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

a) S'agissant des clés d'autorité

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

Elles ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués et leur accès est conditionné par une autorisation du management de IDEMIA.

b) S'agissant des clés de porteurs

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

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

c) S'agissant des clés OCSP

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

Elles ne sont connues que par les membres de IDEMIA dans le cadre des rôles qui leurs sont attribués.

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

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

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

Se référer au chapitre correspondant de la DPC.

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

Se référer au chapitre correspondant de la DPC.

VI.E. Mesures de sécurité des systèmes informatiques

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

Se référer au chapitre correspondant de la DPC.

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

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

VI.H. Horodatage / Système de datation

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

VII. Profils des certificats, OCSP et des CRL

VII.A. Profil des certificats

VII.A.1. Numéro de version

Les certificats émis dans le cadre de l'IGC 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 autorité.
Signature	Signature de l'autorité pour l'authentifier	Sha2WithRSAEncryption
Issuer	Nom de l'autorité	Contient le DN (X.500) de l'autorité. L'émetteur contient la valeur suivante : CN=BNP Paribas Group Sealing and Timestamping CA, OU=0002 662042449, O=BNP Paribas, C=FR
Validity	Période de validité du certificat	Contient les dates d'activation et d'expiration du certificat.
Subject	Nom du porteur	Contient le DN du porteur (voir le paragraphe III.A.5)
Subject Public Key Info	Informations sur la clé publique de l'abonné	Contient l'OID de l'algorithme et la clé publique de l'abonné
Extensions	Liste des extensions	Voir paragraphe suivant

d)

VII.A.3. Extensions du certificat

Les certificats émis par l'autorité de certification « BNPP Service CA » de l'IGC de BNP Paribas comportent les extensions X.509v3 suivantes. La DPC précise les valeurs utilisées.

a) S'agissant des certificats cachet et horodatage

Extension	Extension critique	Description
Authority Key Identifier	N	Elément d'identification de la clé publique de l'autorité signant le certificat
Basic Constraint	O	Indique que le certificat est une entité finale.
Certificate Policies	N	OID de la PC régissant le certificat et Intitulé de la PC : - 1.2.250.1.62.10.5.1.1.2 pour les certificats cachet - 1.2.250.1.62.10.5.1.2.2 pour les certificats d'unité d'horodatage
Subject Key Identifier	N	Elément d'identification de la clé publique du porteur
CRL Distribution Point	N	URL du point de distribution de la CRL (voir le paragraphe IV.J.1)
Authority Information Access	N	Informations d'accès au certificat de l'autorité.
Key Usage	O	Description des utilisations autorisées de la clé privée : digitalSignature
Extended Key Usage	O	Horodatage uniquement : timeStamping

b) S'agissant des certificats OCSP

Extension	Extension critique	Description
Authority Key Identifier	N	Elément d'identification de la clé publique de l'autorité signant le certificat
Basic Constraint	O	Indique que le certificat est une entité finale.
Key Usage	O	Description des utilisations autorisées de la clé privée : digitalSignature
Extended Key Usage	N	Indique que le certificat signe les réponses OCSP (ocspSigning)
Certificate Policies	N	OID de la PC régissant le certificat et Intitulé de la PC : 1.2.250.1.62.10.5.1.3.1
OCSP no Check	N	Indique au client OCSP de faire confiance au répondeur OCSP pour la durée de vie du

Extension	Extension critique	Description
		certificat.
Subject Key Identifier	N	Elément d'identification de la clé publique du porteur

VII.A.4. OID des algorithmes

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

L'algorithme de condensat utilisé dans le cadre de l'IGC 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.

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

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

a) Certificats d'autorité

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

b) Certificats des porteurs

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

c) Certificats OCSP

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

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

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

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

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

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

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

VII.B. Profil des CRL

VII.B.1. Numéro de version

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

VII.B.2. Champs de base

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

Champ	Description
Version	Version de la CRLX.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. L'émetteur est le suivant : CN=BNP Paribas Group Sealing and Timestamping CA, OU=0002 662042449, O=BNP Paribas, C=FR
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.B.3. Extensions de CRL et d'entrées de CRL

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

Extension d'entrée	Description
Authority Key Identifier	Identifie la clé publique de l'autorité ayant signé la CRL
CRL Number	Donne un nombre croissant séquentiel pour chaque CRL émise

MS "CA Version"	Extension Microsoft AD CS liée à la version des clés d'AC
MS "CRL Next Publish"	Extension Microsoft AD CS liée à la date de prochaine publication
Reason Code	Identifie la cause de révocation du certificat. La valeur pour chaque révocation est « unspecified » et n'est donc pas inscrite.

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, de l'ensemble de l'IGC de BNP Paribas est réalisé tous les deux ans. Un audit interne sera mené par BNP Paribas annuellement.

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

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, BNPP 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 non-publique de 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
- Le procès-verbal 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 d'enregistrement des différents rôles (Référents, Gestionnaire de Certificats, etc.)

IX.D.3. Données à caractère non personnel

Aucune exigence spécifique n'est 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 de 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 entités ou des certificats d'horodatage, 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

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

IX.H. Limite de responsabilité

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

IX.I. Indemnités

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

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. Une ancienne version de la PC restera, a minima, publiée tant qu'il restera au moins un certificat valide se référant à ladite version de la 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. Dispositions concernant la résolution de conflits

La présente PC prévoit différentes dispositions concernant la résolution des conflits émanant des entités pour lesquelles elle fournit des services électroniques de confiance ou d'autres points qui y sont liés, qui sont indiquées dans la DPC.

IX.N. Juridictions compétentes

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

IX.O. Conformités aux législations et réglementations

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

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

IX.P. Dispositions diverses

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

IX.Q. Autres dispositions

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

X. Annexe 2 – Documents cités en référence

X.A. Réglementation

Non applicable.

X.B. Documents techniques

Référence	Objet du document
FIPS140-2_LEVEL3_CERT	Certificat de qualification FIP 140-2 level 3 du boitier cryptographique Thales nShield

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 la Référentiel Général de Sécurité de l'administration française.