Politique de signature et de validation de signature de BNP Paribas

Signature Cachet

itg

Revue		
Nom	Fonction	Date

Validation		
Nom	Fonction	Date

Suivi des versions			
Version	Date	Auteur	Nature des modifications
0.1	15/09/2015	Morpho DSA	Initialisation du document
0.5	19/01/2016	Cédric SZANIEC	Finalisation de la relecture globale des documents : version avant complétion par les différents contributeurs
1.0	09/05/2016	Cédric SZANIEC	Version validée par la PMA

Sommaire

I. Objet du document

La signature électronique apposée sur un ensemble de données permet de garantir l'intégrité de ces données et l'authenticité de leur émetteur.

Une politique de signature et de validation de signature est un document décrivant les règles à suivre pour créer et valider des signatures électroniques dans le cadre de transactions électroniques.

Ces politiques ont été élaborés en s'appuyant sur les recommandations du document ETSI TR 102 041 – V1.1.1: Signature Policies Report.

Ce document s'organise de la façon suivante :

- Chapitre I : Objet du document, le présent chapitre
- Chapitre II : Champ d'application
- Chapitre III : Obligations et recommandations générales
- Chapitre IV : Politique de signature 'Cachet'
- Chapitre V : Politique de validation de signature 'Cachet'

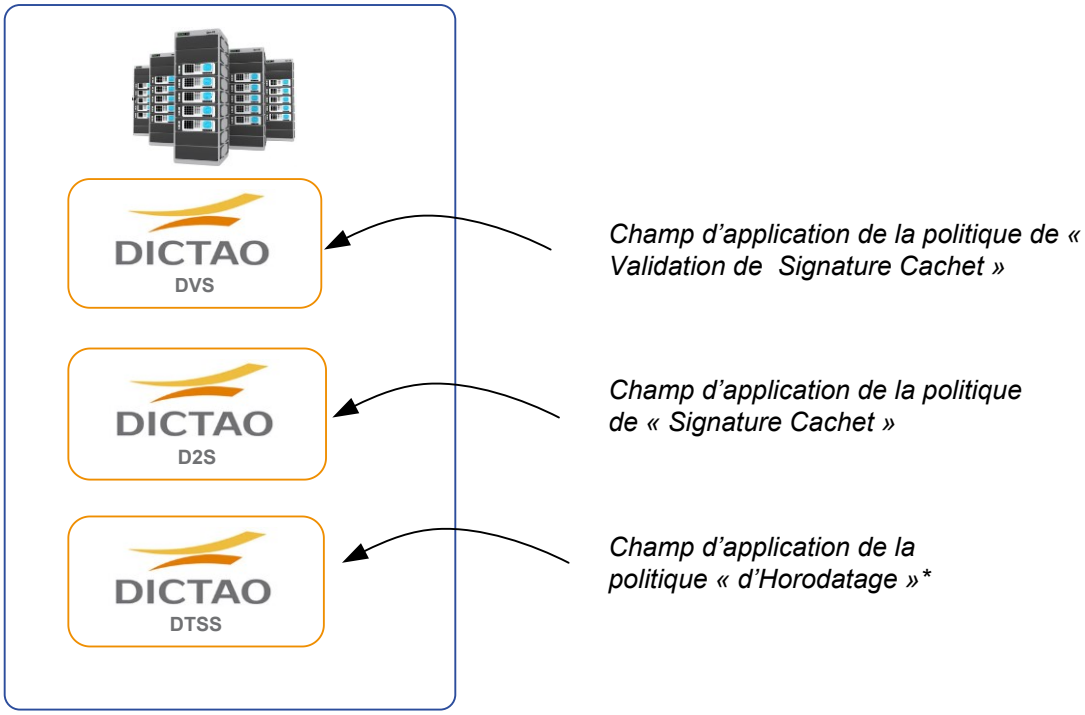
II. Champ d'application

II.A. Préambule

La présente politique de signature & de validation de signature s'applique aux :

- Processus de création de Signature Cachet pouvant être au nom
  - De BNP Paribas
  - D'une entité de BNP Paribas
- Processus de validation de signature de « Signature Cachet » et de création des « Preuves de Validation » au nom de BNP Paribas.

Les schémas ci-dessous mettent en évidence le lien entre les différentes briques composant le socle de signature et de validation de signature décrites dans le présent document.



Note : Les politiques décrites dans le présent document font référence à l'utilisation de données horodatées. Les contremarques de temps sont générées conformément à la politique d'horodatage de BNP Paribas publiée sous la référence 1.2.250.1.195.106.4.1.1 ci-après intitulée « PH-BNPP ».

II.B. Identification du document et date d'émission

Le présent document a été validé le 09 mai 2016 sous l'OID 1.2.250.1.195.107.3.1.1.

II.C. Période de validité

Le présent document entre en vigueur 7 jours ouvrés après la date de distribution ou de mise en ligne. Il reste en vigueur (sauf mention du contraire) tant que les services de signature électronique et de validation sont disponibles.

II.D. Mise à jour du document

II.D.1. Organisme responsable

Le présent document est maintenu par le service Technologie et Processus (ITP) / Informatique et Technologie Groupe (ITG).

ITP ITG peut être contactée pour toutes questions concernant la présente Politique de signature et de validation de signature.

Pour toute demande concernant la présente Politique d'Horodatage, 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).

II.D.2. Personnes physiques responsables

ITP ITG nomme les personnes (ou Services) déterminant la conformité de cette PSV.

II.D.3. Procédure

La mise à jour du présent document implique la présence de plusieurs acteurs et est déclenchée essentiellement pour :

- Procéder à des modifications importantes,
- Prendre en compte de nouveaux besoins ou de nouveaux acteurs,
- Améliorer un cadre juridique,
- Améliorer la qualité du document.

Toute publication d'une nouvelle version du document consiste à archiver l'ancienne version et distribuer et mettre en ligne les éléments suivants :

- Document au format PDF

- OID du document
- Date d'entrée en vigueur

II.D.4. Cohérence documentaire

Le document décrit le contexte de production des signatures de BNP Paribas et de leur validation.

Il revient au comité d'approbation de faire en sorte que ce document reste cohérent vis-à-vis de la politique de certification de l'autorité de certification de type « cachet » et les certificats identifiés par les OID 1.2.250.1.195.105.1.1.1 et 1.2.250.1.195.105.1.2.1, notamment en ce qui concerne la signature des preuves horodatée.

Les politiques définies par le présent document s'appuie sur la politique d'horodatage de BNP Paribas qui décrit le contexte de production des contremarques de temps.

II.D.5. Publication et consultation

BNP Paribas se doit de tenir ces politiques à l'usage des utilisateurs de fonctions de signature ou de son service de validation de signature.

Ce document peut être distribué à ses utilisateurs finaux, soit par courrier électronique soit en le mettant en ligne.

Cette politique est publiée à l'adresse : **http://bnpp.digitaltrust.morpho.com/psv.html**

II.E. Données nominatives

Les noms / prénoms et emails de la personne sont enregistrés dans le référentiel DTP.

II.F. Politique de confidentialité

Les informations suivantes auxquelles il peut être fait référence dans le présent document sont considérées confidentielles :

- Les données secrètes associées au certificat (clé privée, mot de passe, …)
- Les journaux des composants serveur (traces d'activité)
- Les rapports d'audit

III. Obligations et recommandations générales

III.A. Obligations appliquées aux signataires

III.A.1. Sécurité du serveur

Le serveur fait l'objet de protection d'accès décrits dans la politique de certification « BNP Paribas Group Sealing and Timestamping CA » pour plus de détails.

La responsabilité de cette protection en incombe à ITP ITG.

III.A.2. Sécurité des clés de signature cachet

Les clés de signature sont stockées dans des Boitiers cryptographiques opérés par BNP Paribas. Les clés de signature et leurs données d'activation sont gérées en conformité avec la politique de certification de l'AC « BNP Paribas Group Sealing and Timestamping CA » (dit 'Service') de BNP Paribas [BNPP_IGC_PC Service CA] pour les certificats cachet serveur.

En cas de compromission, le signataire doit immédiatement en avertir les responsables du service de signature afin que son accès à celui-ci soit fermé et/ou le certificat révoqué.

III.A.3. Données d'authentification

Le signataire (application interne de BNP Paribas) doit s'assurer que les données qu'il utilise pour s'authentifier auprès du service de signature restent sous son contrôle exclusif (confidentialité).

En cas de compromission, il doit immédiatement en avertir les responsables du service de signature afin que son accès à celui-ci soit fermé et/ou le certificat révoqué.

III.A.4. Publication des CRL

Certaines données, notamment les listes de révocations, ne peuvent être mises à jour en temps réel et il s'écoule plusieurs heures (24 au maximum) avant la publication de ces données par l'entité responsable (l'autorité de certification, dans le cas d'une liste de révocation).

Dans ces conditions, il se peut qu'une signature soit déclarée valide si les données ont été signées entre le moment où le certificat a été révoqué et le moment où sa révocation a été publiée par l'autorité de certification et prise en compte par le service.

La publication des CRL est décrite dans la DPC de l'AC « BNP Paribas Group Sealing and Timestamping CA » [BNPP_IGC_DPC Service CA].

III.A.5. Limites de responsabilité

Le service de signature de BNP Paribas n'est pas responsable du contenu des données signées.

III.B. Obligations appliquées à l'infrastructure de confiance

III.B.1. Sécurité

Les serveurs de signature et de validation de BNP Paribas sont les éléments les plus sensibles de la cinématique de signature. Il est donc nécessaire de limiter l'accès physique et technique à ces serveurs et aux informations qu'ils contiennent aux seules personnes ayant des droits adéquats.

Les mesures prises concernent :

- La protection des accès physiques aux serveurs
- Le choix d'un environnement d'hébergement adapté en termes de disponibilité aux exigences des clients de BNP Paribas (réseaux de climatisation et d'alimentation électrique secourus, systèmes de détection et d'extinction automatique de départs de feu, etc.)
- L'accès aux systèmes de signature et de validation de signature est restreint aux seules personnes habilitées. Le nombre de personnes ayant accès aux serveurs de signature et de validation est strictement limité et ces personnes sont identifiées et authentifiées.
- La surveillance de la plate-forme de BNP Paribas est assurée en vue de prévenir les tentatives de compromission, d'intrusion physique ou par les réseaux de télécommunications
- Le stockage des clés de signature des serveurs est effectué sur un boîtier cryptographique.

III.B.2. Administration de la plate-forme de BNP Paribas

Les administrateurs de la plate-forme de BNP Paribas et de ses composants doivent s'assurer que les données qu'ils utilisent pour s'authentifier auprès du service de signature ou de validation restent sous leur contrôle exclusif (confidentialité).

En cas de compromission/ perte / vol de leur carte à puce, pour les collaborateurs internes de BNP Paribas, ils doivent immédiatement en avertir leur manager afin que leur accès à celle-ci soit fermé ou modifié. Concernant les prestataires extérieurs, ils doivent prévenir le manager du domaine dans lequel s'exécute leur mission.

Le manager procédera ensuite aux requêtes appropriées afin de révoquer la carte à puce en question et ensuite effectuer une nouvelle demande.

III.B.3. Reprise en cas de sinistre

En cas d'un incident quelconque ayant pu affecter le processus de signature ou de validation, qu'il s'agisse d'un incident technique ou d'une action mal intentionnée, prouvée ou supposée, ITP ITG doit vérifier l'impact de cet incident sur le traitement des demandes de signature ou de validation en cours.

III.C. Recommandations aux destinataires

III.C.1. Vérifications complémentaires

Les services de signature cachet vérifient la validité des signatures des documents lorsque celles-ci sont produites.

Néanmoins, il appartient aussi au destinataire du document signé de vérifier la validité de la signature électronique conformément à ce document.

III.C.2. Période de grâce

Compte tenu des délais de publication des CRL, le présent document recommande au destinataire d'attendre le temps nécessaire avant de déclarer une signature valide pour son usage.

IV. Politique de signature Cachet

IV.A. Préambule

Ce chapitre, intitulé Politique de signature Cachet de BNP Paribas, décrit les prestations fournies par le service de signature électronique de BNP Paribas pour l'émission de documents signés au nom du BNP Paribas ou de ses entités.

Le service de signature cachet est de type client-serveur. Une application cliente envoie au service de signature, soit l'ensemble des documents qu'elle désire signer, soit l'empreinte de ces documents, ainsi que l'identifiant de la politique de signature à utiliser, conditionnant ainsi le certificat de signature électronique à utiliser par association préalable de celui-ci avec la politique de signature.

L'application cliente est identifiée et authentifiée par certificat électronique.

Le service de signature de BNP Paribas effectue la signature électronique des données reçues et renvoie à l'application appelante la signature du ou des documents.

IV.B. Acteurs

Les acteurs concernés par la présente politique sont les suivants :

- **L'administrateur de l'application appelante**
  - Est responsable de l'application métier et des documents qu'elle soumet au service pour signature Cachet.
  - Administre et gère notamment les données d'authentification de l'application métier auprès du service de signature.
- **Le service d'horodatage**, génère des contremarques de temps à valeur probante conformément à la politique d'horodatage.
- **Le service de signature**
  - Authentifie la source de la requête
  - Reçoit les documents à signer et les signe
  - Soumet la signature au service d'horodatage pour y apposer une contremarque de temps
  - Soumet la signature au service de validation
- **Le destinataire de la signature**, reçoit les documents signés par le service.
- **Les administrateurs des services de confiance de BNP Paribas**, allouent les ressources cryptographiques du service de signature et de validation de BNP Paribas. Ils définissent les politiques de signature et de validation. Toute modification de la configuration des services de confiance est tracée et signée par l'administrateur.

- **Les auditeurs**, consultent les journaux d'activités du service de validation de signature.

IV.C. Accès au service de signature

IV.C.1. Ouverture du service

Afin de raccorder l'application appelante au service de signature Cachet, celle-ci doit utiliser un certificat électronique d'identification et d'authentification. L'administrateur de l'application appelante dépose donc une demande d'ouverture (accès et droits) auprès du service gestionnaire de la plateforme.

ITP ITG peut procéder à la fermeture du service à tout moment, notamment pour des raisons de sécurité (compromission de clé ou de certificat).

IV.C.2. Authentification

Afin de sécuriser et d'authentifier les échanges entre les applications appelantes et le service de signature, la communication s'effectue grâce au protocole HTTPS. L'authentification du client auprès du serveur s'effectue grâce à un certificat d'authentification installé sur l'application appelante, et est mutuelle.

IV.C.3. Gabarit des certificats d'authentification

Le gabarit des certificats d'authentification au service de signature est conforme aux standards X.509 et possède un usage de clés de type « Digital Signature » et est conforme aux recommandations cryptographiques de l'état de l'art.

IV.C.4. Politique d'authentification

L'accès au service est soumis aux conditions suivantes :

- La requête est transmise via le protocole HTTPS assurant une authentification mutuelle par certificat des deux parties
- Le certificat d'authentification de l'application soumettant la requête est identifiée par son sujet (DN), n'est pas révoqué et est en cours de validité.

IV.C.5. Protection des secrets

Les secrets (clé de signature cachet) et clé de signature de preuve (comme vu en chapitre suivant) sont protégés et conservés dans un boitier cryptographique certifié suivant la norme « Critères communs » au niveau EAL4+.

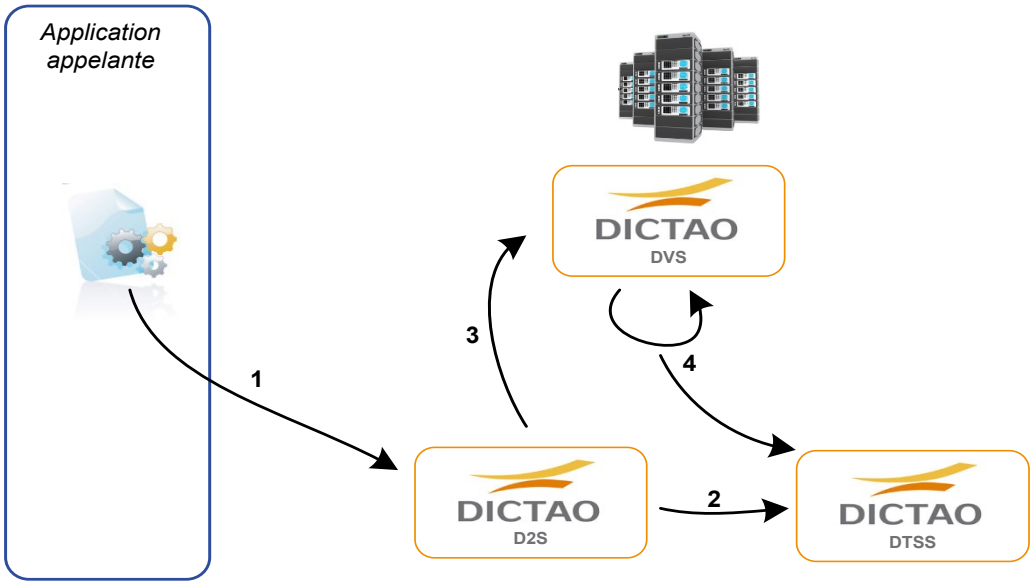
IV.D. Cinématique de création de signature Cachet

La cinématique de signature cachet consiste à créer une signature horodatée qui consiste en

- Un document PDF signé
- Une signature XADES version 1.3.2 jointe ou détachée

- Créer une preuve de validation de signature

Les étapes de cette cinématique sont décrites dans le schéma ci-dessous.



Les échanges et les données de confiance ainsi créées sont:

- Echange 1 : L'application appelante demande la création d'une signature au service de signature.
- Echange 2 : Le service de signature cachet de BNP Paribas procède aux opérations de signature en y associant un jeton d'horodatage.
- Echanges 3 et 4: Le serveur de signature demande une validation de signature avec une création de preuve au service de validation. La donnée de confiance créée est :
    - Une preuve de validation de la signature signée et horodatée à l'instant « T».
    - La preuve est conservée par le service de validation au moins pendant la période durée du service de signature

IV.E. Signature

IV.E.1. Données signées

Le service de signature de BNP Paribas signe électroniquement tout document électronique transmis par l'application appelante reconnue et authentifiées auprès du service de signature Cachet.

Ceci suppose au préalable une identification et authentification (via son certificat électronique client) de l'application appelante auprès du service de signature Cachet.

IV.E.2. Gabarit du certificat de signature Cachet

Les certificats dont les gabarits sont repris ci-dessous sont décrits dans la politique de certification de l'autorité de certification Services de BNP Paribas pour les certificats cachet serveur de l'AC « BNP Paribas Group Sealing and Timestamping CA ».

IV.E.3. Caractéristiques des signatures

Les signatures électroniques sont de type XAdES détaché, XAdES enveloppé ou PDF.

Conformément à la norme, les propriétés signées comprennent au moins les éléments suivants :

- Le certificat de signature (*SigningCertificate*)
- La date et l'heure de signature (*SigningTime*). La date et l'heure de référence pour cette opération sont précisées dans le document Déclaration des pratiques de signature.
- Une référence au présent document (*SigningPolicyIdentifier / SigPolicyIdType*)
    - OID (URI ou URN) de la présente politique de signature (*SigPolicyId*)
    - Valeur de l'empreinte de la politique de signature calculé et algorithme utilisé (*SigPolicyHash*) : SHA256.
- Un jeton d'horodatage délivré par le service d'horodatage.

IV.E.4. Algorithmes de signature

L'algorithme de signature recommandé par la présente politique est le SHA256withRSAEncryption.

IV.E.5. Vérification préalables à la signature

Le service de signature vérifie, avant chaque signature, que le certificat de signature est utilisé durant sa période de validité et qu'il n'est pas révoqué.

IV.E.6. Vérification lors de la signature

Le service de signature appelle automatiquement le service de validation de signature après la création de la signature, ce dernier réalisant alors une validation immédiate de la signature produite.

V. Politique de validation de signature Cachet

V.A. Préambule

La signature électronique apposée sur un ensemble de données permet de garantir l'intégrité de ces données et l'authenticité de leur émetteur.

La politique de validation de signatures décrit les règles à suivre pour valider des signatures électroniques émises dans le cadre de transactions électroniques, conformément à une politique de signature donnée.

V.A.1. Acteurs

Les acteurs concernés par la présente Politique de Validation de Signature Cachets ont les suivants :

- **Le service de validation de signature**, qui vérifie que :
  - les signatures Cachet sont conformes à ce même document
  - les contremarques de temps ont été générées conformément à la politique d'horodatage
- **Le service d'horodatage**, génère des contremarques de temps à valeur probante conformément à la politique d'horodatage de BNP Paribas
- **Les administrateurs**, alloue les ressources cryptographiques du service de signature et de validation. Ils définissent les politiques de signature et de validation. Toute modification de la configuration des services de confiance est tracée et signée par l'administrateur.
- **Les auditeurs**, consultent les journaux d'activités du service de validation de signature.
- **Le destinataire de la signature**, qui reçoit les documents signés après validation de la signature.

V.A.2. Champ d'application

La présente politique de validation s'applique à toutes les signatures effectuées par les services de signature de BNP Paribas.

V.A.3. Politique de signature associée

La présente politique de validation concerne les documents signés dont la signature comprend l'OID de ce document.

V.A.4. Période de validité

La présente politique entre en vigueur en même temps que la politique de signature associée.

V.A.5. Mise à jour de la politique

La présente politique doit être mise à jour selon les mêmes procédures et règles que la politique de signature associée.

V.A.6. Publication et consultation

La présente politique est mise à disposition de tous les responsables des services de signature et applications appelantes acceptant des documents signés sous le régime de la politique de signature associée.

V.A.7. Cohérence documentaire

La présente politique doit être mise à jour afin de correspondre aux règles définies dans la politique de signature associée.

V.B. Règles de validation

V.B.1. Conditions pour déclarer une signature valide

Une signature électronique Cachet émise par BNP Paribas est déclarée valide lorsque :

- Le format de la signature est conforme à la norme de signature utilisée et décrite au chapitre précédent.
- Le certificat de signature est conforme au gabarit décrit au chapitre précédent
- Le certificat de signature et sa chaîne de certification sont valides à l'instant « T » :
    - Validité temporelle
    - Le certificat n'est pas révoqué
    - La signature cryptographique est techniquement valide
- La vérification cryptographique de la signature conformément à la norme de signature utilisée donne un résultat positif
- Le jeton d'horodatage présent dans la signature ou accompagnant celle-ci est valide.

V.B.2. Données signées par l'application de signature

La politique de signature associée n'impose aucune restriction sur le type de document signé.

V.C. Création des preuves de validation de signature Cachet

Une preuve est générée par le service de validation à chaque opération de validation réalisée. La preuve de validation est signée électroniquement par le service de validation de BNP Paribas.

V.C.1. Sécurité des clés de signature de preuve

Ces clés sont hébergées dans un boîtier cryptographique dans un environnement sécurisé et contrôlé par ITP ITG.

V.C.2. Contenu de la preuve

Les informations contenues dans la preuve de validation de signature sont :

- Le hash des données applicatives caractérisant la transaction. La nature des données dont l'empreinte en utilisant l'algorithme SHA256.
- Les résultats de l'opération de validation de signature.
- Les données de confiance utilisées par le service de validation. Les données sont :
    - Les références aux certificats de la chaîne des autorités de certification,
    - Les références aux listes de révocation de certificat,
- La description de la politique de validation de signature appliquée.

V.C.3. Signature des preuves

a) Gabarit du certificat de signature Cachet

Le gabarit du certificat de signature est décrit dans la Politique de Certification de l'AC « BNP Paribas Group Sealing and Timestamping CA ».

b) Caractéristiques de la signature

La signature de la preuve de signature respecte la norme suivantes XAdES (ETSI TS 101 093), en version 1.1.1 ou supérieure.

Conformément à la norme, les propriétés signées comprennent au moins les éléments suivants :

- le certificat de signature (*SigningCertificate*)
- la date et l'heure de signature (*SigningTime*)
- une référence à la politique de signature associée (*SigningPolicyIdentifier / SigPolicyIdType*)
    - OID de la présente PS (*SigPolicyId*)
    - Valeur de l'empreinte de la politique de signature associée et algorithme utilisé (*SigPolicyHash*)

c) Algorithme de signature

L'algorithme de signature recommandé est le SHA256withRSAEncryption.

V.D. Conservation des preuves de validation

BNP Paribas conserve les preuves de validation durant toute la durée de vie de ses services, destinée à servir de preuve, le cas échéant, de la réalité de l'opération.

Le service de validation de signature s'engage à ne conserver aucune copie des données soumises pour validation de signature. En particulier, les journaux d'événements (traces d'activité) du service ne

contiennent aucune copie de ces données.

Le service de validation de signature de BNP Paribas s'engage à créer une preuve de validation signée.