Politique d'horodatage BNP Paribas

Revue		
Nom	Fonction	Date

Validation		
Nom	Fonction	Date

Suivi des versions			
Version	Date	Auteur	Nature des modifications
0.1	14/09/2015	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
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

Sommaire

I. Définitions et acronymes

I.A. Définitions

- **Abonné** – Entité ayant besoin de faire horodater des données par une Autorité d'horodatage et qui a accepté les conditions d'utilisation de ses services. Dans le cadre de la présente politique d'horodatage, seules les applications de BNP Paribas sont concernées.

- **Autorité de Certification (AC)** – Cf. les Politiques de Certification de BNP Paribas : **http://bnpp.digitaltrust.morpho.com/pc.html**

- **Autorité d'horodatage (AH)** – Une Autorité d'Horodatage ou AH est chargée d'émettre et de gérer des jetons d'horodatage. Elle est responsable de l'ensemble du processus d'horodatage et de la validité des jetons émis.

- **Contremarque de temps** – Donnée qui lie une représentation d'une donnée à un temps particulier, exprimé en heure UTC, établissant ainsi la preuve que la donnée existait à cet instant-là.

- **Coordinated Universal Time (UTC)** – Échelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-5 [TF.460-5].

Nota – Pour la plupart des usages, le temps UTC est équivalent au temps solaire au méridien principal (0°). De manière plus précise, le temps UTC est un compromis entre le temps atomique particulièrement stable (Temps Atomique International, TAI) et le temps solaire dérivé de la rotation irrégulière de la terre lié au temps moyen sidéral de Greenwich (GMST) par une relation de convention.

- **Déclaration des pratiques d'horodatage (DPH)** – Une DPH identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AH applique dans le cadre de la fourniture de ses services d'horodatage et en conformité avec la ou les politiques d'horodatage qu'elle s'est engagée à respecter.

- **Entité** – Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.

- **Jeton d'horodatage** – Voir contremarque de temps.

- **Module d'horodatage** – Produit de sécurité comportant une ressource cryptographique et qui est dédié à la mise en œuvre des fonctions d'horodatage de l'UH, notamment la génération, la conservation et la mise en œuvre de la clé privée de signature de l'UH ainsi que la génération des contremarques de temps.

- **Politique d'horodatage (PH)** – Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AH se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'une contremarque de temps à une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes. Une PH peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les abonnés et les utilisateurs de contremarques de temps.

- **Produit de sécurité** – Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

- **Qualification d'un produit de sécurité** – Acte par lequel l'ANSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les services de sécurité objet de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le [RGS].

- **Service d'horodatage** – Ensemble des prestations nécessaires à la génération et à la gestion de contremarques de temps.

- **Unité d'Horodatage (UH)** – Ensemble de matériel et de logiciel en charge de la création de contremarques de temps caractérisé par un identifiant de l'unité d'horodatage accordé par une AC, et une clé unique de signature de contremarques de temps.

- **Utilisateur final** – Client de BNP Paribas pour lequel une contremarque de temps est émise.

I.B. Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

- **AC** : Autorité de Certification
- **AH** : Autorité d'Horodatage
- **CG** : Conditions Générales d'utilisation du service d'horodatage
- **CRL** : *Certificate Revocation List*, Liste des Certificats Révoqués
- **ANSSI** : Direction Centrale de la Sécurité des Systèmes d'Information
- **DPH** : Déclaration des Pratiques d'Horodatage
- **IGC** : Infrastructure de Gestion de Clés
- **OID** : Object Identifier
- **PH** : Politique d'Horodatage
- **PSHE** : Prestataire de Services d'Horodatage Électronique
- **RGS** : Référentiel Général de Sécurité
- **UH** : Unité d'Horodatage
- **UTC** : *Coordinated Universal Time*

II. Références documentaires

Référence	Document
[RFC 3161]	Standard international définissant le protocole d'horodatage
[RGS_A_5]	Politique d'Horodatage Type version 3.0 de l'Agence Nationale de la Sécurité des Systèmes d'information
[BNPP_IGC_PC Service CA]	Politique de certification de l'autorité de certification Service de BNP Paribas

III. Politique d'horodatage

III.A. Présentation générale

Une politique d'horodatage (PH) est composée d'un ensemble de règles décrivant les conditions de recevabilité d'un jeton d'horodatage pour des Utilisateurs ayant des besoins de sécurité communs. Cette PH est émise par BNP Paribas et définie les conditions d'utilisation des certificats d'horodatage dans le cadre de la certification ETSI TS 102-042.

Une PH est définie indépendamment des modalités de mise en œuvre de l'infrastructure à laquelle elle s'applique. Elle décrit les exigences auxquelles une AH doit se conformer pour la mise en place et la fourniture de ses prestations. La déclaration des pratiques d'horodatage (DPH) rassemble les procédures qui permettent d'atteindre les exigences décrites dans la PH. Il s'agit d'un document distinct de la PH.

Cette PH est dérivée des politiques d'horodatage type élaborées l'ANSSI dans le cadre du Référentiel Général de Sécurité (RGS).

Les jetons d'horodatage ou contremarques de temps, objets de la présente PH sont conformes à la norme [RFC 3161].

Les certificats d'horodatage sont émis par l'autorité de certification « BNP Paribas Group Sealing and Timestamping CA » (« BNPP Service CA » dans la suite de ce document) qui est en charge 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).

III.B. Périmètre d'application

L'AH peut fournir des jetons d'horodatage à toute application de type transaction électronique ou archives électroniques.

III.C. Identification du document

La présente PH est dénommée Politique d'Horodatage de la société BNP Paribas. Elle peut être identifiée par son numéro d'identifiant d'objet (OID) :

1.2.250.1.195.106.4.1.1

Pour la mise à disposition des informations publiées à destination des abonnés et des Utilisateurs de jetons d'horodatage, l'Autorité d'Horodatage (AH) de BNP Paribas met en œuvre une fonction de publication. La mise à disposition des informations de publication est assurée à l'aide du protocole HTTP à l'URL suivante :

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

III.D. Qu'est-ce que l'horodatage ?

III.D.1. Définition

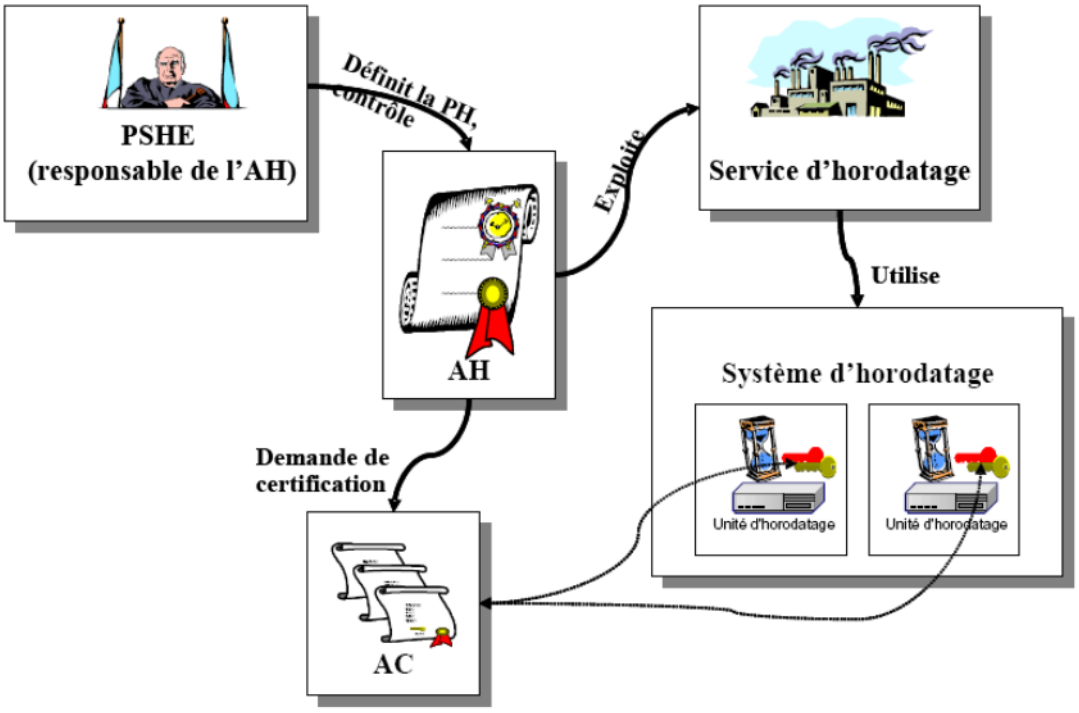
L'horodatage permet d'attester qu'une donnée existe à un instant donné. Pour cela, il convient d'associer une représentation sans équivoque d'une donnée, par exemple une valeur de hachage associée à un identifiant d'algorithme de hachage, à un instant dans le temps. La garantie de cette association est fournie au moyen d'une contremarque de temps qui est une structure signée qui contient en particulier :

- L'identifiant de la PH sous laquelle la contremarque de temps a été générée ;
- La valeur de hachage et l'algorithme de hachage de la donnée qui a été horodatée ;
- La date et le temps UTC ;
- L'identifiant du certificat de l'Unité d'horodatage (UH) qui a généré la contremarque de temps (qui contient aussi le nom de l'Autorité d'horodatage).

L'horodatage ne nécessite pas le déploiement d'une infrastructure étendue pour que la validité des certificats des unités d'horodatage puisse être vérifiée. En particulier, les utilisateurs finaux ne doivent pas nécessairement avoir des certificats eux-mêmes, mais doivent avoir accès aux informations de validité des certificats d'horodatage (chaîne de certification, CRL, …) pour vérifier les contremarques de temps.

La clé privée ou les clés utilisées pour générer les contremarques de temps sont gérées par l'Autorité d'horodatage qui conserve la pleine et entière responsabilité pour satisfaire aux exigences définies dans le document actuel. Une Autorité d'horodatage peut faire fonctionner plusieurs unités d'horodatage (UH). Chaque unité d'horodatage dispose de sa propre bi-clé.

III.D.2. Comment établir la confiance en horodatage



La garantie apportée par l'autorité d'horodatage s'appuie sur des éléments techniques (décrits précédemment) et des règles de gestion qui sont présentées dans la politique d'horodatage. La politique d'horodatage présente aux utilisateurs les engagements que prend l'autorité d'horodatage, notamment ceux pris en matière de sécurité, et décrit de façon macroscopique les moyens mis en œuvre pour tenir ces engagements. Elle revêt une grande importance car elle incarne le niveau de confiance atteint par le service d'horodatage. Elle traduit la reconnaissance formelle de l'importance accordée par l'autorité d'horodatage à la sécurité du service.

Les exigences pour les services d'horodatage décrits dans le document incluent des exigences portant, à la fois sur la gestion de l'horodatage et sur le fonctionnement des unités d'horodatage qui publient les contremarques de temps. L'Autorité d'horodatage, telle qu'identifiée dans la contremarque de temps, a la responsabilité d'assurer que ces exigences sont remplies. Elle peut sous-traiter à d'autres parties un sous-ensemble des services d'horodatage.

III.D.3. Présentation des rôles et relations

L'AH de BNP Paribas exploite l'ensemble des services d'horodatage qui regroupe les diverses prestations organisationnelles et techniques nécessaires à la génération et à la gestion des contremarques de temps.

Chaque UH signe ses contremarques de temps à l'aide d'une clé privée dont la clé publique correspondante a été certifiée au préalable par l'autorité de certification (AC) de BNP Paribas. Les clés privées sont conservées et mises en œuvre dans des boitiers cryptographiques certifiés.

III.E. Gestion de la PH

III.E.1. Entité responsable

L'AH est responsable de la validation et de la gestion de la PH répondant aux exigences de la présente PH.

III.E.2. Point de contact

ITP ITG peut être contactée pour toutes questions concernant la présente PH.

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).

III.E.3. Entité déterminant la conformité d'une DPH avec PH

ITP ITG nomme les personnes (ou Services) déterminant la conformité de la DPH avec cette PH.

III.E.4. Procédures d'approbation de la conformité de la DPH

L'approbation de la conformité de la DPH passe par :

- Une présentation des analyses par les personnes (ou services) désignées pour déterminer la conformité de la DPC et / ou
- Une validation des analyses par un tiers accrédité

Le document est mis à jour essentiellement lors de la modification importante des pratiques ou du service, pour prendre en compte de nouveaux besoins, de nouveaux acteurs, améliorer le cadre juridique, ou corriger toute non-conformité avec la PH correspondante.

Toute modification de la DPH entraine une modification de l'OID de ce document dans le cadre du suivi des versions du présent document.

III.E.5. Publication et consultation

Ce document est mis à la disposition des abonnés et des utilisateurs de contremarques de temps et, s'il y a lieu, toute autre documentation appropriée.

III.F. Conformité

Des audits sont réalisés périodiquement afin de garantir la conformité de la DPH par rapport à la PH correspondante.

IV. Dispositions générales

IV.A. Obligations

IV.A.1. Obligation de l'Autorité d'Horodatage

Dans le cadre de la présente PH, l'AH :

- Génère et signe les contremarques de temps conformément à la présente Politique d'Horodatage de BNP Paribas et à la DPH correspondante ;
- Respecte et se conforme aux exigences et procédures définies dans la présente PH et la DPH qui la supporte ;
- Garantit la conformité des exigences et des procédures décrites dans sa DPH avec la présente PH ;
- Met à disposition de ses abonnés et des utilisateurs l'ensemble des informations nécessaire à vérifier les contremarques de temps qu'elle aura émises, selon les modalités indiquées au paragraphe VII.H ;
- Maintient une information sur la compromission de la bi-clé des UH;
- Utilise des certificats pour les UH sous sa responsabilité qui sont délivrés par l'AC dénommée « BNP Paribas Group Sealing and Timestamping CA » [BNPP_IGC_PC Service CA].

IV.A.2. Obligations de l'abonné

On rappelle que dans le cadre de la présente PH, seul des groupes de l'organisation de BNP Paribas peuvent prétendre à ce rôle.

Dans le cadre de la présente PH, l'abonné :

- Identifie et habilite les applications qui vont demander des contremarques de temps auprès d'une ou des UH de l'AH ;
- Respecte les obligations de la présente PH applicables ;
- Indique à l'AH l'algorithme qu'il utilise pour calculer les empreintes numériques des données électroniques qu'il souhaite faire horodater parmi les algorithmes indiqués au paragraphe VIII.A ;
- Vérifie, conformément à la politique de certification de BNP Paribas au moment de l'obtention d'une contremarque de temps, que le certificat de l'UH est valide, et qu'il est délivré par l'AC [BNPP_IGC_PC Service CA] ;
- Utilise à sa convenance les mécanismes proposés par [RFC3161] pour éviter les possibilités de rejeu de contremarques de temps.

IV.A.3. Obligation de l'utilisateur de contremarque de temps

Dans le cadre de la présente PH, toute personne peut jouer ce rôle.

Les utilisateurs de contremarques de temps :

- Vérifient que la contremarque a été correctement signée et que le certificat de l'UH est valide à l'instant de la vérification ;
- Tiennent compte des limitations sur l'utilisation de la contremarque de temps indiquées dans la PH.

Traditionnellement, un jeton d'horodatage devient non vérifiable après l'expiration du certificat de l'UH car l'AC ayant émis ce certificat ne garantit plus la publication d'informations de révocation (CRL ou autre), y compris en cas de compromission de clés. Cependant, il est possible de vérifier un jeton d'horodatage après expiration du certificat de l'UH si, au moment de la vérification, il est possible de prouver que :

- La clé privée de l'UH n'a jamais été compromise jusqu'ici ;
- L'algorithme de hachage utilisé dans le jeton d'horodatage n'a pas encore de faiblesse cryptographique (attaque par collisions notamment) ;
- L'algorithme de signature et la taille de clé de signature du jeton d'horodatage sont toujours hors de portée d'attaques cryptographiques.

La notion d'expiration du certificat de l'UH traduit d'ailleurs justement l'incertitude sur une longue durée de ces affirmations et donc l'impossibilité pour une AC de les garantir à priori.

Notons que la première condition est la plus facile à assurer, notamment en contactant directement l'AH ou l'AC et/ou en s'assurant d'avoir la CRL correspondant à la fin de vie du certificat de l'UH exposant une non révocation ainsi qu'une garantie de destruction de la clé privée par l'AH.

Concernant les deux autres conditions, elles dépendent fortement de l'évolution de l'état de l'art des attaques cryptographiques. Il peut être utile de prévoir un nouvel horodatage (avec de nouveaux algorithmes de hachage et de signature) des jetons d'horodatage avant une telle évolution.

IV.A.4. Obligation pour l'AC fournissant les certificats des unités d'horodatage

L'AC délivrant des certificats de clés publiques pour les UH est **[BNPP_IGC_PC Service CA]** qui respecte sa propre PC. Elle fournit un service de révocation employant un mécanisme de publication de CRL.

IV.B. Déclaration des pratiques d'horodatage

Au titre de ses pratiques d'horodatage, l'AH de BNP Paribas :

- Possède une déclaration des pratiques et des procédures utilisées pour adresser toutes les exigences identifiées dans la présente PH.
- Met à la disposition des abonnés et des utilisateurs de contremarques de temps cette présente politique d'horodatage et, s'il y a lieu, et toute autre documentation appropriée.

- S'assure et garantit que les pratiques mentionnées dans la DPH sont correctement mises en œuvre et vérifie la concordance entre cette déclaration et la présente PH.

IV.C. Limite de responsabilité

La présente PH ne traite que le cas de la vérification des contremarques de temps pendant la période de validité du certificat de l'UH émettrice des contremarques de temps. La vérification en dehors de la période de validité d'un certificat d'UH n'est pas prise en compte dans le cadre de la présente PH.

L'AH n'est pas responsable de la conservation des contremarques de temps.

V. Exigences opérationnelles

V.A. Gestion des requêtes de contremarque de temps

Le service d'horodatage met en œuvre un contrôle d'accès basé sur l'utilisation de certificat SSL client. Les requêtes de contremarques de temps sont donc authentifiées et soumises à autorisation.

V.B. Fichiers d'audit

L'AH garantit que toutes les informations appropriées concernant le fonctionnement du service d'horodatage sont enregistrées pendant une période de temps suffisante et précisée dans la déclaration des pratiques d'horodatage), en particulier dans le but de fournir une preuve en cas d'enquêtes légales. En particulier :

- Les événements spécifiques et les données enregistrées sont documentés par l'Autorité d'horodatage.
- La confidentialité et l'intégrité des enregistrements d'audit courants et archivés relatifs au fonctionnement des services d'horodatage sont assurées.
- Les enregistrements relatifs au fonctionnement des services d'horodatage sont disponibles si exigé dans le but de fournir une preuve d'un fonctionnement correct des services d'horodatage en cas d'enquêtes légales.
- L'instant précis d'évènements significatifs concernant l'environnement de l'Autorité d'horodatage, la gestion des clés, et la synchronisation de l'horloge est enregistré.
- Les enregistrements relatifs à l'administration du service d'horodatage sont gardés, après la date d'expiration de la validité de la clé de signature de l'unité d'horodatage durant une période de temps appropriée pour fournir des éléments de preuves nécessaires et qu'indiqué dans les conditions générales d'utilisation de l'Autorité d'horodatage.
- Les événements sont enregistrés de telle façon qu'ils ne puissent pas être facilement supprimés ou détruits (sauf s'ils sont transférés sur un support de sauvegarde) durant la période de temps où l'on exige qu'ils soient conservés.
- Les enregistrements concernant tous les événements touchant au cycle de vie des clés sont effectués.
- Les enregistrements concernant tous les événements touchant au cycle de vie des certificats des unités d'horodatage sont effectués.
- Les enregistrements concernant tous les événements touchant à une synchronisation de l'horloge des unités d'horodatage sont effectués. Cela inclut l'information concernant des recalibrages ou des synchronisations normales.
- Les enregistrements concernant tous les événements touchant à la détection de perte de synchronisation sont effectués.

V.C. Gestion de la durée de vie de la clé privée

L'Autorité d'horodatage garantit que les clés privées de signature des unités d'horodatage ne sont pas employées au-delà de la fin de leur cycle de vie. En particulier :

- Des procédures opérationnelles ou techniques sont mises en place pour assurer qu'une nouvelle paire de clés est mise en place quand la fin de la période d'utilisation d'une clé privée d'unité d'horodatage a été atteinte.
- Le système d'horodatage détruit la clé privée si la fin de la période d'utilisation de cette clé privée a été atteinte.

V.D. Synchronisation de l'horloge

L'AH garantit que son horloge est synchronisée avec le temps UTC selon l'exactitude déclarée. En particulier :

- Le calibrage de chaque horloge d'unité d'horodatage est maintenu de telle manière que les horloges ne puissent pas normalement dériver à l'extérieur de l'exactitude déclarée.
- Les horloges des unités d'horodatage sont protégées contre les menaces relatives à leur environnement qui pourraient aboutir à une désynchronisation avec le temps UTC en dehors de l'exactitude déclarée.
- L'AH devra garantir que, si son horloge interne ne respecte plus l'exactitude déclarée, alors cela sera détecté.
- Si l'horloge d'une unité d'horodatage est détectée comme étant en dehors de l'exactitude annoncée, alors les contremarques de temps ne sont plus générées.

V.E. Exigences du contenu d'une contremarque de temps

L'AH garantit que les contremarques de temps sont générées en toute sécurité et incluent le temps correct. En particulier :

- La contremarque de temps inclut l'identifiant du certificat de l'unité d'horodatage. Ce certificat inclut :
  - un identifiant de l'Autorité d'horodatage,
  - une identification de l'unité d'horodatage qui génère les contremarques de temps.
- La contremarque de temps inclut un identifiant de la politique d'horodatage.
- Chaque contremarque de temps comporte un identifiant unique.
- Le temps inclus dans une contremarque de temps est synchronisé avec le temps UTC au moins avec l'exactitude définie dans la DPH.
- La contremarque de temps inclut une représentation de la donnée à horodater (c'est-à-dire la valeur de hachage et l'identifiant d'algorithme de hachage) telle que fournie par le demandeur.

- La contremarque de temps est signée en employant une clé produite exclusivement à cette fin. La contremarque de temps respecte de plus les exigences du paragraphe VIII.B ci-dessous.

V.F. Compromission de l'AH

L'AH garantit dans le cas d'événements qui affectent la sécurité des services d'horodatage, incluant la compromission de la clé privée de signature d'une unité d'horodatage ou la perte détectée de calibrage qui pourrait affecter des contremarques de temps émises, qu'une information appropriée sera communiquée aux entités de BNP Paribas utilisatrices du service d'horodatage.

En particulier, dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une unité d'horodatage, qui pourrait affecter des contremarques de temps émises, l'AH prendra les mesures nécessaires pour que les contremarques de temps de cette unité ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation.

V.G. Fin d'activité

A la fin de l'activité de l'UH, le service d'horodatage est arrêté et les procédures liées à la fin des certificats d'UH correspondants sont exécutées, conformément à. la politique de certification de l'AC « BNPP Service CA », § V.H et cf §VII.F.

VI. Exigences physiques et environnementales, procédurales et organisationnelles

VI.A. Exigences physiques et environnementales

L'Autorité d'Horodatage garantit que l'accès physique aux services critiques est contrôlé et que les risques physiques d'atteinte à ses actifs sont réduits au minimum. En particulier :

- A la fois pour la fourniture du service d'horodatage et la gestion de l'horodatage :
    - L'accès physique aux équipements concernés par les services d'horodatage est limité aux individus autorisés ;
    - Des contrôles sont mis en œuvre pour éviter la perte, des dégâts ou la compromission d'actifs et l'interruption des activités ;
- Des contrôles sont mis en œuvre pour éviter la compromission ou le vol d'informations ou d'équipements informatiques.
- Des contrôles d'accès sont appliqués aux modules d'horodatage pour remplir les exigences de sécurité des modules d'horodatage.

VI.B. Exigences procédurales

L'AH garantit que les composants du système d'Horodatage sont sûrs et correctement opérés, avec un risque minimal d'échec. En particulier :

- L'intégrité des composants du système d'horodatage et l'information sont protégés contre les virus, les logiciels malveillants et non autorisés.
- Les supports employés dans les systèmes d'horodatage sont manipulés de manière sécuritaire pour les protéger des dégâts, du vol, de l'accès non autorisé et de l'obsolescence. Nota – Chaque membre du personnel avec des responsabilités de gestion est responsable de la planification et de l'exécution effective de la politique d'horodatage et des pratiques d'horodatage.
- Des procédures sont établies et mises en œuvre pour tous les rôles de confiance et administratifs qui impactent la fourniture des services d'horodatage.

VI.B.1. Manipulation et sécurité des supports

Tous les supports sont traités de manière sécuritaire conformément aux exigences de la classification de l'information. Les supports contenant des données sensibles sont retirés de manière sécuritaire quand ils ne sont plus utiles.

VI.B.2. Rapport d'incident et réponse

L'AH agira d'une façon opportune et coordonnée pour répondre rapidement aux incidents et limiter l'impact des infractions à la sécurité. Tous les incidents sont rapportés aussitôt que possible après l'incident.

VI.C. Procédures de fonctionnement et responsabilités

Les opérations de sécurité sont séparées des autres opérations.

- les procédures opérationnelles et les responsabilités ;
- la protection vis-à-vis du logiciel malveillant ;
- la maintenance ;
- la gestion du réseau ;
- le contrôle actif des journaux d'audit, l'analyse des événements et les suites à donner ;
- le traitement et la sécurité des médias ;
- l'échange des données et du logiciel.

VI.D. Gestion d'accès au système

L'AH garantit que l'accès au système d'horodatage est limité aux individus dûment autorisés. En particulier :

- Des contrôles (Firewall à minima) sont mis en œuvre pour protéger le réseau interne de l'Autorité d'horodatage d'accès non autorisés incluant l'accès par des abonnés et des tierces personnes.
- L'AH garantit une administration efficace des utilisateurs (cela inclut les opérateurs, les administrateurs et les auditeurs), pour maintenir la sécurité du système, y compris la gestion des comptes des utilisateurs, l'audit, et la modification ou le retrait rapide d'accès.
- Le personnel de l'AH est correctement identifié et authentifié avant d'utiliser des applications critiques liées à l'horodatage.
- Le personnel de l'AH est tenu responsable de ses activités, par exemple en conservant des fichiers d'audit.
- L'abonné est authentifié auprès du service d'horodatage par un certificat SSL.

VI.E. Exigences organisationnelles

Les rôles de confiance incluent les rôles qui impliquent les responsabilités suivantes :

- Les officiers chargés de la sécurité : responsabilité complète d'administrer la mise en œuvre des pratiques de sécurité ;
- Les administrateurs système : autorisés à installer, configurer et maintenir les modules d'horodatage de l'Autorité d'horodatage pour la gestion de l'horodatage ;
- Les opérateurs système : responsables pour faire fonctionner les modules d'horodatage de l'Autorité d'horodatage de manière quotidienne

- Les auditeurs de système : autorisés à consulter les archives et les fichiers d'audit des modules d'horodatage.

VII. Exigences de sécurité techniques

VII.A. Exactitude temps

L'exactitude de temps de l'AH de BNP Paribas est de de la seconde (une seconde) par rapport au temps UTC. La précision des UH est assurée par la source de temps interne, le mécanisme de synchronisation et les sources de temps externes.

Des précisions quant aux modalités de la synchronisation sont fournies dans la DPH.

L'initialisation de la synchronisation des UH garantit que la source de temps interne des UH :

- Délivrent une date et une heure avec la précision de une seconde au regard de la ou des sources de temps externes ;
- Est uniquement synchronisée par rapport aux sources de temps externes précisées dans la DPH.
- L'exactitude de temps apparaît dans chaque contremarque de temps générée.

VII.B. Génération de clé

L'Autorité d'Horodatage garantit que toutes les clés cryptographiques sont produites dans des circonstances contrôlées.

Conformément à la PC **[BNPP_IGC_PC Service CA]**, la génération des bi-clés cryptographiques des UH est réalisée à l'aide de ressources cryptographiques matérielles. À aucun moment, lors de cette génération, les clés privées d'UH ne sont exportées de ces ressources.

Les clés privées d'UH ont une longueur de 2048 bits pour l'algorithme RSA.

VII.C. Certification des clés de l'unité d'horodatage

L'Autorité d'Horodatage s'assure que la valeur de la clé publique et l'identifiant de l'algorithme de signature contenus dans la demande de certificat de l'Unité d'Horodatage sont égaux à ceux générés par l'Unité d'Horodatage.

L'Autorité d'Horodatage s'assure qu'une demande de certificat d'Unité d'Horodatage auprès d'une Autorité de Certification contient au moins les informations suivantes :

- le nom (DN) de l'unité d'horodatage pour laquelle la demande de certificat est faite ;
- la valeur de la clé publique (et l'identifiant de l'algorithme) ;
- la durée d'utilisation souhaitée pour la clé privée, si non précisé, se référer à la valeur présente dans la politique de certification **[BNPP_IGC_PC Service CA]**

L'Autorité d'Horodatage permet à l'Autorité de Certification de vérifier que la demande de certificat pour

l'Unité d'Horodatage est valide, en lui fournissant notamment les informations et documents nécessaires lors de l'enregistrement. De manière générale, l'AH respecte les obligations qui lui incombent et qui découlent de la politique de certification de l'AC.

L'Autorité d'Horodatage vérifie, lors de l'import du certificat de l'Unité d'Horodatage, qu'il provient bien de l'Autorité de Certification auprès de laquelle la demande de certificat a été effectuée.

L'Autorité d'Horodatage s'assure que l'Unité d'Horodatage ne peut être opérationnelle qu'une fois que les quatre exigences ci-dessus sont remplies.

L'AH ne rend opérationnelle l'UH qu'une fois que l'ensemble des exigences liées à la gestion de la bi-clé de l'UH et à la synchronisation sont remplies.

VII.D. Protection des clés privées des unités d'horodatage

L'Autorité d'horodatage garantit que des clés privées des unités d'horodatage restent confidentielles et conservent leur intégrité. En particulier, les clés de signature des unités d'horodatage sont gardées et utilisées à l'intérieur d'un module cryptographique FIPS 140-2 Level 2 au niveau de l'état de l'art.

VII.E. Exigences de sauvegarde des clés des unités d'horodatage

Se référer à la PC **[BNPP_IGC_PC Service CA]** pour l'exigence de sauvegarde des clés des certificats d'horodatage et l'ETSI TS 102 042.

VII.F. Destruction des clés des unités d'horodatage

L'Autorité d'horodatage garantit que les clés de signature des unités d'horodatage ne seront plus utilisées à la fin de leur cycle de vie.

VII.G. Algorithmes obligatoires

L'Autorité d'horodatage, dans la limite des algorithmes qu'elle reconnaît :

- Accepte des valeurs de hachage générées par des clients et employant les algorithmes de hachage conformes aux exigences du chapitre VIII.B ci-dessous.
- Génère des contremarques de temps signées selon les algorithmes et les longueurs de clé conformes aux exigences du chapitre VIII.A ci-dessous.

VII.H. Vérification des contremarques de temps

L'Autorité d'horodatage garantit que les utilisateurs de contremarques de temps peuvent avoir accès à l'information utilisable pour vérifier la signature numérique des contremarques de temps. En particulier :

- Les certificats des unités d'horodatage sont disponibles, soit joints à la contremarque de temps, soit disponibles par d'autres moyens, par exemple un serveur.
- Un ou plusieurs certificats utilisables pour valider une chaîne de certificats se terminant par un certificat d'unité d'horodatage sont disponibles.

VII.I. Durée de validité des certificats de clé publique des unités d'horodatage

La durée de validité des certificats des unités d'horodatage ne doit pas être plus longue que la période de temps durant laquelle l'algorithme choisi et la longueur clé sont reconnus comme adéquat pour l'usage.

VII.J. Durée d'utilisation des clés privées des unités d'horodatage

La durée d'utilisation d'une clé privée sera au plus égale à la période de validité du certificat de clé publique correspondant. Toutefois elle sera en pratique réduite afin que la validité des contremarques de temps générées avec cette clé puisse être effectuée durant un laps de temps suffisant (qui sera supérieur ou égal à la différence entre la période de validité du certificat et la durée d'utilisation de la clé privée).

VIII. Formats des contremarques de temps, des certificats et des CRL et des algorithmes cryptographiques

VIII.A. Requêtes d'horodatage

Il existe deux façons d'effectuer une requête d'horodatage.

Au titre de la présente PH, les requêtes d'horodatage envoyées par l'abonné à l'AH de BNP Paribas doivent avoir une structure TimeStampReq conforme à la [RFC3161] et aux éléments suivants :

Champ	Valeur
`Version`	1
`messageImprint`	Le hash des données à horodater suivant l'un des algorithmes précisés au tableau suivant.
`Nonce`	Obligatoire

Les champs non précisés dans le tableau ne doivent pas être positionnés par l'abonné.

VIII.B. Algorithmes d'empreinte

Les OID des algorithmes d'empreinte autorisés sont :

Champ	Valeur
id-sha256	2.16.840.1.101.3.4.2.1
id-sha384	2.16.840.1.101.3.4.2.2
id-sha512	2.16.840.1.101.3.4.2.3

VIII.C. Contremarque de temps

Les contremarques de temps fournies par l'AH de BNP Paribas respectant la présente PH ont une structure TimeStampToken conforme à la [RFC3161].

Champ	Valeur
`version`	1
`policy`	1.2.250.1.195.7.4.1
`messageImprint`	Cf. (§ VIII.A)
`serialNumber`	Cf. [RFC3161]
`genTime`	Cf. [RFC3161]
`accuracy`	Cf.§ VII.A
`nonce`	Présent si présent dans la requête (voir ci-dessus)

VIII.D. Certificats et CRL

Le DN du certificat des unités d'horodatage est encodé en PrintableString.

Champ

CN = Timestamp Unit X[i]
OU = 0002 662042449
O = BNP Paribas
C = FR

Concernant la CRL, se reporter à la politique de certification **[BNPP_IGC_PC Service CA].**

[i] X désigne le numéro de l'UH de BNP Paribas