Politique d'Horodatage

Dématérialisation des contrats et actes de gestion du Groupe BPCE

BPCE : Société anonyme à directoire et conseil de surveillance,

au capital de 155 742 320 €.

Siège social : 50 avenue Pierre Mendes France

75201 Paris Cedex 13.

RCS n° 493 455 042.

SOMMAIRE

1 INTRODUCTION

1.1 Présentation générale

Le Groupe BPCE, pour ses réseaux Caisse d'Epargne, Banque Populaire et Filiales, met en œuvre pour ses Clients un service de dématérialisation des contrats et des actes de gestion intégrant un processus de signature électronique. Ce service de signature peut avoir lieu à distance ou en face à face dans une agence du réseau. Dans le cadre de ce processus :

- Les Clients peuvent signer des contrats et des actes de gestion à l'aide des bi-clés associées des certificats générés à la volée et valables le temps de la transaction de signature électronique.

- Les Etablissements signent et horodatent les contrats et des actes de gestion en leur nom à l'aide de bi-clés associées à des certificats de type cachet serveur.

Dans ce cadre, le Groupe BPCE se positionne en tant qu'Autorité d'Horodatage (ci-après « AH ») et délivre des contremarques de temps.

La solution d'Horodatage est mise en œuvre par l'opérateur de service d'horodatage (OSH) pour le compte du Groupe BPCE.

Le présent document constitue la politique d'horodatage du Groupe BPCE (ci-après « PH») présentant ce service d'horodatage.

Dans le cadre de la présente PH, les utilisateurs du service d'horodatage sont :

- **Les clients des établissements du groupe** qui ont des besoins d'horodater des transactions de signature électronique durant leur processus de signature des contrats en agence.

- **Les applications du système de confiance** mis en œuvre qui a besoin d'horodater

    - des transactions de signature électronique durant leur processus de signature des contrats en agence.

    - des traces pour assurer notamment les opérations d'archivage des transactions.

A titre d'information, une contremarque de temps permet d'attester de la réalité, à une date et une heure donnée, de l'existence d'une empreinte numérique (ou « hash ») qui est soumise au service d'horodatage. Les contremarques de temps sont délivrées et signées électroniquement par l'AH à l'aide d'Unité(s) d'Horodatage (ci-après « UH »).

L'objectif de ce document est de définir les engagements que le Groupe BPCE, en tant qu'AH, respecte dans la délivrance et la gestion de contremarques de temps, ainsi que les obligations des autres participants.

Le présent document pourra ultérieurement être complété, dans sa partie mise en œuvre, par une Déclaration des Pratiques d'Horodatage (DPH) et des Conditions Générales d'utilisation du service d'horodatage (CGU).

Une DPH expose les mécanismes et les procédures mis en œuvre pour atteindre les objectifs de sécurité de la PH, en particulier les processus qu'une UH emploiera pour la création des contremarques de temps et le maintien de l'exactitude de ses horloges. L'AH du Groupe BPCE peut mettre en œuvre plusieurs UH pour supporter son service d'horodatage.

Cette PH n'impose pas d'exigences sur le lien entre l'empreinte numérique à horodater et le contenu de la donnée électronique qui en est à l'origine. Cette vérification est à la charge de l'utilisateur du service d'horodatage.

Dans le cadre de cette PH, la date et le temps de chaque contremarque de temps sont synchronisés avec le temps UTC avec une précision de 1 seconde. La présente PH applique un format de contremarque de temps standard défini par le [RFC 3161]. La gestion de la synchronisation de l'horloge du service d'horodatage est détaillée au chapitre 5.2.4.

La présente PH et la DPH associée sont élaborées sur la base des documents suivants :

- Electronic Signatures and Infrastructures (ESI), Policy and Security Requirements for Trust Service Providers issuing Time-Stamps, ETSI EN 319 421
- Electronic Signatures and Infrastructures (ESI);Time-stamping protocol and time-stamp profiles, ETSI EN 319 422

1.2 Identification du document

La présente PH appelée : « Politique d'Horodatage de Dématérialisation des contrats et actes de gestion du Groupe BPCE» est la propriété du Groupe BPCE.

Elle est identifiée par un numéro d'identification unique, l'OID : **1.3.6.1.4.1.40559.1.0.4.4.0.1.1**

Les contremarques de temps respectant la présente politique, la référenceront en utilisant ce numéro d'identification unique « OID » (cf. chapitre 5.2.5).

D'autres éléments, plus explicites, (nom, numéro de version, date de mise à jour) permettent également de l'identifier.

1.3 Publication du document

Avant toute publication officielle, la Politique d'Horodatage est validée par le comité de suivi des Autorités.

La présente Politique d'Horodatage est publiée à l'adresse www.dossiers-securite.bpce.fr .L'ensemble des informations associées (cf. 1.5.3) notamment les versions antérieures de ces documents avec leur période de validité, sont également publiées à l'adresse www.dossiers-securite.bpce.fr.

1.4 Approbation du document

La Direction de la Sécurité des Systèmes d'Information (DSSI-G) sous la responsabilité du RSSI-Groupe constitue l'Autorité de Gestion des Politiques (AP).

En tant qu'Autorité, l'AP a pour responsabilité de:

- Définir l'organisation des composantes du système d'horodatage.
- Définir les normes de constitution des numéros d'identifiant d'objet (OID) associés au système d'horodatage.
- D'autoriser les évolutions du système d'horodatage.
- Définir et faire approuver auprès de la Direction Juridique, la Direction Conformité et Sécurité Groupe et la Direction Informatique et Technologie Groupe (DIT-G), les Politiques d'Horodatage
- Faire approuver auprès de la Direction Juridique, la Direction Conformité et Sécurité Groupe et la Direction Informatique et Technologie Groupe (DIT-G), les Déclarations des Pratiques d'Horodatage associées.
- Définir les règles de nommage unique des unités d'horodatage (UH).
- Auditer périodiquement les composantes du système d'horodatage et leur organisation.
- Valider les demandes de révocation d'UH.
- Arbitrer les litiges relatifs aux services d'horodatage.
- Contrôler de la mise en œuvre de l'ensemble des points cités ci-dessus.
- Contrôler la validité et l'intégrité des informations publiées (liste des certificats d'AC ayant émis les certificats des UH, Liste des Certificats Révoqués et Politiques d'horodatage).

L'AP agît conformément à la présente PH et à la DPH associée.

1.5 Processus de mise à jour

1.5.1 Circonstances rendant une mise à jour nécessaire

La mise à jour de la Politique d'Horodatage est un processus impliquant tous les acteurs et faisant l'objet d'une démarche rigoureuse. Il est enclenché essentiellement pour procéder à des modifications importantes, pour prendre en compte de nouveaux besoins, de nouveaux acteurs, améliorer le cadre juridique ou combler des lacunes.

La Politique d'Horodatage est réexaminée a minima tous les ans.

1.5.2 Prise en compte des mises à jour

Les demandes d'information ou questions concernant la présente politique sont à adresser par courriel à l'adresse suivante :

- Groupe BPCE
- Directeur de la Sécurité des Systèmes d'informations Groupe
- 50 Avenue Pierre Mendes France
- 75201 Paris Cedex 13
- rssi-pssi-icg@bpce.fr

Ces remarques et souhaits d'évolution sont examinés par le Groupe BPCE, qui engage si nécessaire le processus de mise à jour de la présente Politique d'Horodatage et qui redirige les demandes vers les acteurs concernés.

Toutes les demandes d'évolutions concernant les phases opérationnelles seront soumises aux équipes de l'Opérateur Technique (OT).

1.5.3 Information des acteurs

Lorsqu'une mise à jour a été planifiée, les informations relatives à cette évolution sont mises en ligne sur les lieux de publication (cf.1.3).

Indépendamment de ce mode de communication, les acteurs peuvent à tout moment se renseigner auprès du Groupe BPCE pour obtenir plus d'informations, en envoyant un mail à rssi-pssi-icg@bpce.fr.

La publication d'une nouvelle version de la Politique d'Horodatage consiste à archiver la version précédente et mettre en ligne dans le répertoire prévu à cet effet, les éléments suivants :

- Document au format PDF ;
- OID du document ;
- Le hash de la PH
- Les certificats des Unités d'Horodatage couvertes par la PH
- Les certificats de la chaîne d'AC ayant émis les certificats des UH
- Les points de téléchargement des LCR générées par les AC ayant émis les certificats des UH.

1.6 Entrée en vigueur de la nouvelle version et période de validité

La nouvelle version de la Politique d'Horodatage entre en vigueur dès qu'elle est publiée sur le site identifié au paragraphe 1.3. Elle est publiée avant toute émission d'un jeton d'horodatage conforme à la présente Politique d'Horodatage, c'est-à-dire intégrant l'OID défini au paragraphe 1.2.

1.7 Cohérence de la documentation

Cette Politique d'Horodatage décrit le contexte de production de contremarques de temps et, de fait, ne constitue qu'une brique du référentiel documentaire du Groupe BPCE.

L'AP s'assure de la cohérence de ce référentiel documentaire et de l'adéquation de la présente Politique d'Horodatage avec les autres documents, plus particulièrement les politiques de signature, de certification et de gestion des preuves.

1.8 Principes de l'horodatage réalisé par le Groupe BPCE

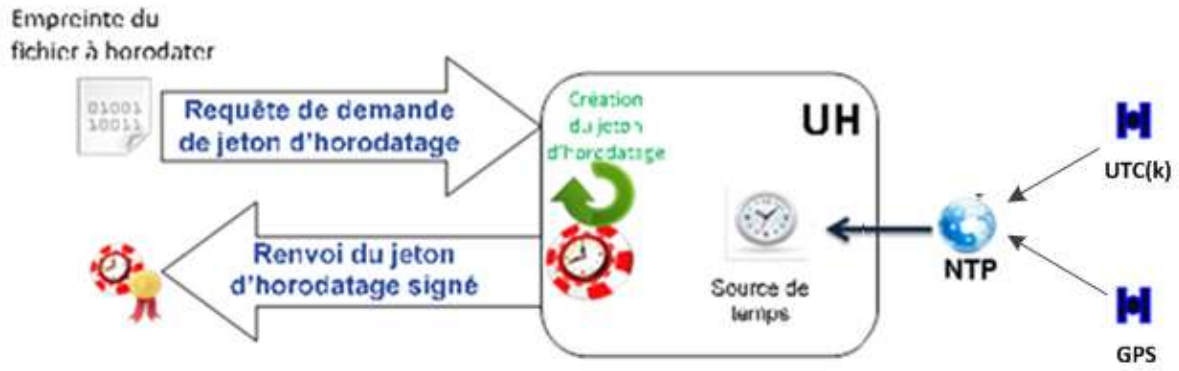
L'Autorité de certification (AC) qui délivre les certificats est l'AC « AC CACHET SERVEUR BANQUE POPULAIRE » pour les unités d'horodatage (UH) de Banque Populaire (BP) et l'AC « AC CACHET SERVEUR CAISSE D EPARGNE » pour les unités d'horodatage (UH) de Caisse d'Epargne (CE).

Le service d'horodatage est basé sur des serveurs connectés sur le réseau intranet de l'entreprise et installés sur des sites géographiques distincts.

L'horodatage est effectué par le DTSS (progiciel d'horodatage de l'ICG fournit par Morpho). Le DTSS utilise comme référence l'heure système du serveur où il est installé, basée sur deux serveurs NTP synchronisés sur l'heure GPS.

Préalablement à chaque horodatage, le DTSS valide la synchronisation de l'heure du serveur avec quatre serveurs NTP, deux reliés à une source UTC(k) et les deux autres à une source GPS.

Le schéma de principe est alors le suivant :



1.9 Etablissement de la confiance dans le service d'horodatage du Groupe BPCE

La garantie apportée par l'Autorité d'Horodatage s'appuie sur des éléments techniques (décrits précédemment) et des règles de gestion exposées dans la présente politique d'horodatage.

La politique d'horodatage (PH) présente aux utilisateurs les engagements pris par l'autorité d'horodatage, notamment en matière de sécurité, et décrit de façon macroscopique les moyens mis en œuvre pour tenir ces engagements.

La PH 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 la PH portent 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 de respecter ces exigences.

La présente PH est élaborée sur la base des documents issus de l'ETSI EN 319 421 et ETSI EN 319 422.

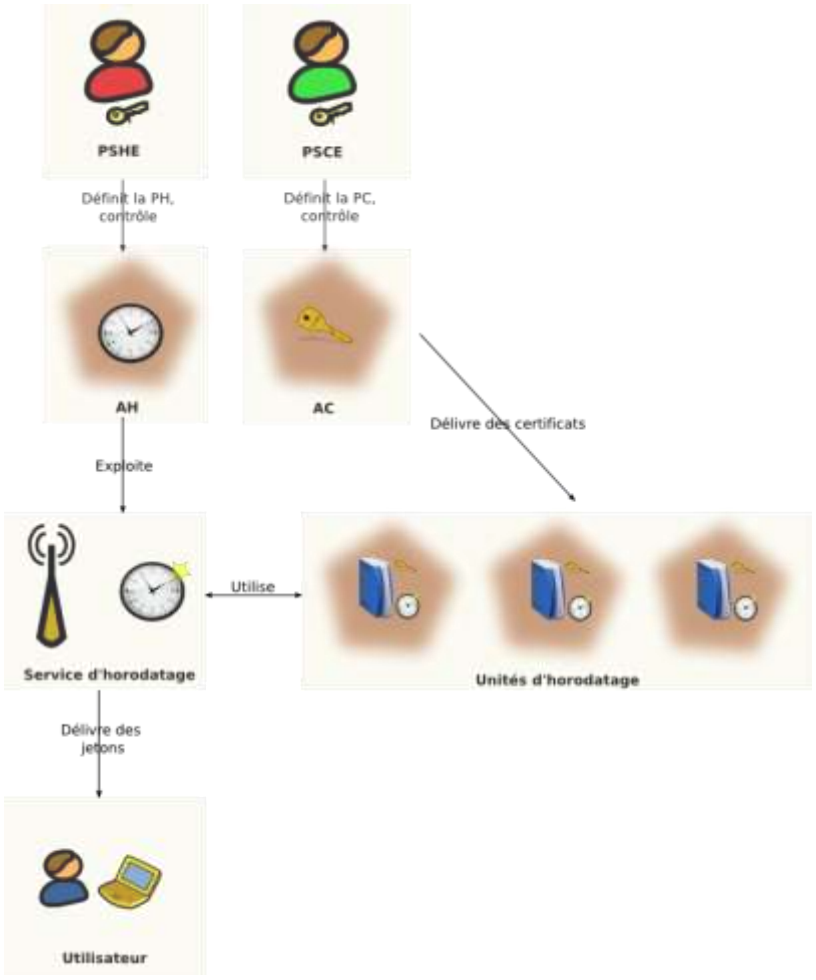
1.10 Entités intervenant dans le service d'horodatage

Le Groupe BPCE est le responsable de l'Autorité d'Horodatage qui est exploitée et maintenue en conditions opérationnelles par son Opérateur Technique.

L'Autorité d'Horodatage utilise un service d'horodatage qui assure un niveau de performance conforme aux exigences exprimées dans l'[ETSI_PH], notamment au niveau de la gestion de la dérive et de la précision de temps fournies dans les contremarques de temps.

Le Groupe BPCE est également le responsable de l'AC qui émet les certificats nécessaires aux unités d'horodatage du service d'horodatage.

La représentation schématique est alors la suivante :



1.11 Autres aspects

Les clés privées des unités d'horodatage sont générées et stockes dans des boîtiers cryptographiques matériels.

2 DÉFINITION ET ACRONYMES

Les définitions et acronymes sont référencés dans le document: « Mesures communes » publié à la même adresse que la présente politique.

3 POLITIQUE D'HORODATAGE

Pour cette politique, la date et le temps de chaque contremarque de temps doivent être synchronisés avec le temps *UTC* avec une exactitude de 1 seconde.

Cette politique impose l'usage d'un protocole d'horodatage spécifique pour demander et obtenir une contremarque de temps auprès d'une AH conforme à la RFC3161 et profilée dans le document ETSI EN 319 422.

Les caractéristiques principales de cette politique sont les suivantes :

- la protection des clés et de l'horloge respectent les exigences spécifiées dans [ETSI_PH] ;
- la sauvegarde et l'import des clés privées sont interdits ;
- l'AC générant les certificats de clé publique pour les unités d'horodatage doit gérer le service de révocation pour chaque certificat publié.

4 CONDITIONS GÉNÉRALES D'UTILISATION

Compte tenu de la complexité de lecture d'une PH pour des utilisateurs non-spécialistes du domaine, l'AH définie également des conditions générales d'utilisation correspondant aux *« TSA Disclosure Statement » (TDS)* définis dans l'annexe B de l'ETSI EN 319 421.

Ces conditions générales d'utilisation ne sont pas destinées à remplacer la politique d'horodatage mais sont destinées à des abonnés et à des utilisateurs de contremarques de temps non-techniciens afin qu'ils puissent facilement comprendre l'information essentielle dont ils doivent avoir connaissance.

Vis-à-vis des clients des banques du groupe, le processus d'horodatage est intégré au processus de signature électronique de contrat en agence.

Au moment de la signature électronique, l'établissement s'assure que le client a signé la dernière version des Conditions générales de Signature qui intègrent notamment les problématiques liées à l'horodatage.

5 EXIGENCES RESPECTÉES PAR L'AUTORITÉ D'HORODATAGE

5.1 Dispositions Générales

5.1.1 Obligation de l'Autorité d'Horodatage

Vis-à-vis de la présente Politique, le système d'horodatage validé par l'AH :

- Génère et signe les contremarques de temps conformément à la PH ;
- Respecte et se conforme aux exigences et procédures définies dans la présente PH ;
- Met à disposition de ses utilisateurs l'ensemble des informations nécessaires permettant de vérifier les contremarques de temps qu'elle aura émises. Cela comprend a minima :
  - Les certificats de la chaîne d'AC ayant émis les certificats des UH
  - Les certificats des UH
  - Les points de distribution des LCR générées par l'AC ayant émis les certificats des UH

5.1.2 Obligation du client

Le client est tenu d'accepter les conditions du service de signature qui intègrent notamment les aspects liés à l'horodatage.

5.1.3 Obligation de l'Utilisateur de Contremarque de Temps

Les utilisateurs de contremarques de temps doivent procéder de la manière suivant pour s'assurer de la validité du jeton d'horodatage qui a été délivré par l'AH :

- vérifier que la contremarque de temps a été correctement signée et que le certificat de l'UH est valide à l'instant de la vérification ;
- s'assurer que les contremarques de temps sont obtenues auprès des UH mises en œuvre par le Groupe BPCE.

5.1.4 Obligations des Autorités de Certification fournissant des certificats aux Unités d'Horodatage

Les Politiques de Certification des AC délivrant les certificats d'horodatage décrivent les obligations prises par l'Autorité de Certification. Ces documents sont accessibles à l'adresse www.dossiers-securite.bpce.fr.

Les AC délivrent des certificats de clés publiques pour les UH sous un OID particulier. Elles fournissent également un service de révocation mis à jour sur une base quotidienne en employant un mécanisme de publication de LCR sur un site HTTP.

Ces AC s'engagent à conserver pendant au moins 1 an après expiration des certificats des UH, tous les journaux d'événement liés à la délivrance des certificats d'UH.

5.1.5 Déclaration des Pratiques d'Horodatage

Au titre de ses pratiques d'horodatage, l'Autorité d'Horodatage réalise les actions suivantes :

- Mène une analyse de risques afin de déterminer les contrôles de sécurité nécessaires et les procédures opérationnelles d'émission des contremarques de temps par les UH ;
- Possède une DPH et des procédures associées pour adresser toutes les exigences identifiées dans la présente PH ;
- Identifie, dans la DPH, les obligations des organisations participant à la fourniture des services d'horodatage, y compris la politique et les pratiques applicables. Cela inclut les AC décrites au paragraphe 5.1.4 ;
- Met à la disposition des utilisateurs de contremarques de temps les éléments publics de sa DPH, s'il y a lieu, et toute autre documentation appropriée ;
- Met en œuvre une organisation de décision permettant d'approuver les moyens décrits dans la DPH ;
- S'assure que les pratiques mentionnées dans la DPH sont correctement mises en œuvre ;
- Définit une procédure de contrôle périodique de la conformité des pratiques mentionnées dans la DPH au regard de la présente PH.

5.1.6 Conditions Générales d'Utilisation

L'Autorité d'Horodatage publie également dans des Conditions Générales d'Utilisation du service d'horodatage les informations suivantes :

- Le cadre d'application de la DPH ;
- Les coordonnées de l'AH ;
- Les types et le cadre d'utilisation des contremarques de temps ;
- La précision de la date des contremarques de temps par rapport à l'échelle de temps UTC ;
- Les algorithmes de hachage autorisés pour constituer l'objet horodaté ;
- La durée minimum pendant laquelle il est possible de vérifier les contremarques de temps, à compter de leur date de génération ;
- Les obligations des abonnés ;
- Les obligations des utilisateurs de contremarque de temps ;
- Les informations permettant de vérifier la contremarque de temps ;
- Les limitations de responsabilité et les garanties de l'AH ;
- La PH et la DPH appliquée ;
- Les règles appliquées en matière de protection des informations confidentielles ;
- Les règles appliquées en termes d'assurance de l'AH ;
- Les lois applicables et les règles de règlement des litiges ;
- Les niveaux de certifications et les audits obtenus par l'AH.

5.1.7 Conformité avec les exigences légales

5.1.7.1 Juridictions compétentes

Les dispositions de la politique d'horodatage sont régies par le droit français.

En cas de litige relatif à l'interprétation, la formation ou l'exécution de la présente politique, et faute d'être parvenues à un accord amiable ou à une transaction, les parties donnent compétence expresse et exclusive aux tribunaux compétents de Paris, nonobstant pluralité de défendeurs ou d'action en référé ou d'appel en garantie ou de mesure conservatoire.

5.1.7.2 Dispositions concernant la résolution de conflits

En cas de contestation ou de litige, les parties décident de soumettre cette difficulté à une procédure amiable, préalablement à toute procédure devant un tribunal conformément aux conditions générales de signature et accord passé avec le Porteur.

L'AP s'assure que tous les accords qu'elle conclut prévoient des procédures adéquates pour le règlement des différends.

5.1.7.3 Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par l'AH sont protégés par la loi, règlements et autres conventions internationales applicables.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages Web, bases de données, textes originaux, …) est sanctionnée par le Code de la propriété intellectuelle et le Code pénal.

L'AH détient tous les droits de propriété intellectuelle : elle est propriétaire de la PH de la DPH associée et des certificats émis par l'AC.

5.1.7.4 Données personnelles

En conformité avec les dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le traitement automatisé des données personnelles, réalisé à partir des plates-formes du Groupe BPCE a fait l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés [CNIL].

Conformément à l'article 32 de la loi n° 78-17 du 6 janvier 1978, les utilisateurs sont informés que les données personnelles qu'ils communiquent pourront être transmises et exploitées par le groupe BPCE et les différents partenaires intervenant dans les échanges concernés.

Les utilisateurs des services du Groupe BPCE sont tenus de respecter les dispositions de la loi relative à l'informatique, aux fichiers et aux libertés, dont la violation est passible de sanctions disciplinaires et pénales.

Ils doivent notamment s'abstenir, s'agissant des informations nominatives auxquelles ils accèdent, de toute collecte, de toute utilisation détournée et, d'une manière générale, de tout acte susceptible de porter atteinte à la vie privée ou à la réputation des personnes.

5.2 Exigences opérationnelles

5.2.1 Gestion des requêtes

Les demandes de contremarques de temps sont réalisées par les UH de l'AH du Groupe BPCE selon le protocole défini par le [RFC 3161]. Ce protocole est conforme à [ETSI_TSP].

Le service d'horodatage peut recevoir des requêtes provenant de tous les composants de l'infrastructure mise en œuvre pour la dématérialisation des contrats et actes de gestion, notamment pour :

- L'horodatage des transactions de signature électronique
- L'horodatage des éléments de traces.

5.2.2 Fichiers d'audit

La journalisation effectuée par les UH concerne les évènements relatifs à l'administration (modification de la configuration, mise à jour d'une politique de confiance), à l'horloge (synchronisation, perte de calibrage, etc.) et à la gestion d'un jeton d'horodatage.

La confidentialité et l'intégrité des journaux 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.

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. Cela concerne :

- Tous les évènements enregistrés dans le fichier de trace permettent d'identifier l'instant précis d'un évènement concernant l'AH ;
- Les enregistrements relatifs à l'administration du service d'horodatage sont gardés, durant toute la durée de vie du service d'horodatage ;
- Cette journalisation concerne les actions effectuées par les administrateurs sur la configuration générale du module d'horodatage :
    - Ajout, modification ou suppression d'une application cliente pouvant demander des jetons d'horodatage
    - Ajout, modification ou suppression d'une autorité de certification

- Ajout, modification ou suppression d'un utilisateur (administrateur, …)

Les enregistrements concernant tous les événements touchant à une synchronisation de l'horloge des unités d'horodatage sont effectués :

- La configuration de l'horloge d'horodatage est définie dans le fichier de configuration du module d'horodatage qui précise la source de temps utilisée ;
- Les enregistrements concernant tous les événements touchant à la détection de perte de synchronisation sont effectués.

Les éventuelles dérives temporelles sont enregistrées par le module d'horodatage.

Les journaux sont intégrés dans la politique de sauvegarde de l'OT.

5.2.3 Gestion de la durée de vie de la clé privée

L'AH met en œuvre plusieurs UH pour assurer la continuité du service d'horodatage. Avant l'expiration de la clé privée d'une UH, l'opérateur technique organisera la génération et la mise en œuvre d'une nouvelle UH.

5.2.4 Synchronisation de l'horloge

Le système de synchronisation est basé sur le fonctionnement suivant :

- Le module d'horodatage (DTSS) synchronise son horloge interne avec des serveurs NTP.
- Les serveurs NTP sont synchronisés soit :
  - Avec une source GPS connectée et dédiée
  - Avec un relais NTP synchronisé avec une source UTC(k)

5.2.5 Contenu d'une Contremarque de Temps

Les contremarques incluent une date et une heure d'UH avec une précision donnée au regard du temps UTC.

Le tableau ci-dessous reprend les champs d'un TimeStampToken tels que définis dans le [RFC 3161].

Les contremarques de temps émises par l'AH du Groupe BPCE respectent les exigences correspondantes du [RFC 3161], moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	Description ou valeur	Elément contenant	
		Certificat	Jeton
version	1		X
Policy	OID de la PH		X
Pays de l'AH	FR	X	
AC Id	Identifiant de l'AC	X	
AH Id	Identifiant de l'AH	X	
UH Id	Identifiant de l'UH	X	
messageDigest	Condensat (hash) des données à horodater		X
serialNumber	Identifiant unique de la contremarque de temps		X
GenTime	Heure de génération de la contremarque de temps calculée par rapport à une source UTC(k)		X
accuracy	absent car égal à 1 seconde		X
nonce	Identique à celui présenté lors de la demande de génération si celui-ci est présent dans cette dernière		X

La contremarque de temps est signée par l'UH à l'aide du certificat délivré par une AC du Groupe BPCE. Ce certificat et la clé privée correspondante sont utilisés exclusivement pour cet usage.

5.2.6 Compromission de l'Autorité d'Horodatage

La compromission de l'AH peut être due :

- aux vols des serveurs des unités d'horodatage ;
- au vol des clés privées des UH ;
- à la compromission de la clé privée de l'AC ayant servi à générer les certificats des UH.

En cas de compromission de la clé privée de l'AC, la procédure mise en place est détaillée dans la PC/DPC en vigueur pour cette AC.

Dans le cadre du plan de continuité d'activité, le Groupe BPCE dispose de deux salles serveurs sur deux sites distincts.

Les deux sites disposent des mêmes équipements et des mêmes logiciels pour faire fonctionner le service d'horodatage. Notamment chaque site possède ses propres Unités d'Horodatage.

En cas de compromission de l'Autorité d'Horodatage et plus particulièrement des clés privées des Unités d'Horodatage, les équipes de l'Opérateur Technique exploitant le service d'horodatage déclenchent les procédures adéquates permettant de maintenir le service sur au moins 1 des 2 sites.

Les problèmes d'exploitation déclenchant une bascule des activités du service d'horodatage vers le site de secours sont définis dans les documents d'exploitation maintenus par l'Opérateur Technique.

Le détail des actions enclenchées par cette bascule ainsi que les délais de remise en activité des services sont précisés dans les documents d'exploitation maintenus par

l'Opérateur Technique. Ce fonctionnement permet à l'AH du Groupe BPCE de garantir un service d'horodatage avec un haut niveau de disponibilité.

En tout état de cause, l'Opérateur Technique :

- Mettra à disposition du Groupe BPCE et des utilisateurs de contremarque de temps une description de la compromission détectée ;
- Coupera l'unité d'horodatage suspectée de compromission ;
- Mettra à disposition quand cela est possible les éléments permettant d'identifier les contremarques de temps émises qui pourraient être compromises ou suspectées de compromission.

5.2.7 Fin d'activité

En cas de fin d'activité du service d'horodatage, l'Opérateur Technique :

- Rendra disponible au Groupe BPCE et aux utilisateurs des contremarques de temps l'information de la cessation d'activité ;
- Abrogera l'ensemble des autorisations délivrées à des tiers dans le cadre du service d'horodatage ;
- Conservera les informations d'audit ;
- Conservera les informations nécessaires à la vérification des contremarques de temps ;
- Détruira les clés privées de toutes les unités d'horodatage de son service d'horodatage.

5.3 Exigences physiques, environnementales, procédurales et organisationnelle

Les exigences de ce chapitre sont référencées dans le document suivant : «Mesures communes», publié à la même adresse que la présente politique.

5.4 Exigences de sécurité techniques

5.4.1 Exactitude du temps

L'ensemble du service d'horodatage est synchronisé avec l'heure UTC (Temps Universel Coordonné (ISO8601))

La gestion d'heure d'été et d'hiver n'est pas prise en compte, de même que les fuseaux horaires.
L'algorithme de sélection du temps de l'UH doit être synchronisé au minimum avec deux sources de temps pour délivrer des jetons d'horodatage.

Les sauts de secondes sont pris en compte automatiquement à travers le protocole NTP.

En cas de dysfonctionnement du traitement du saut de seconde programmé ou de la synchronisation, le service d'horodatage se verrouille et ne délivre plus de jetons d'horodatage.

5.4.2 Génération des clés

La génération des bi-clés cryptographiques des UH est réalisée à l'aide de ressources cryptographiques matérielles. A 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.

5.4.3 Certification des clés de l'UH

La certification des clés d'une UH revient à paramétrer le service d'horodatage pour qu'il utilise le certificat de signature de l'UH lors d'une demande de contremarque de temps.

Les informations suivantes font parties de la demande de certificat de l'UH :

- Le CN qui est complété par le profil de génération du certificat pour aboutir au DN du certificat de l'UH;
- La valeur de la clé publique correspondant à la clé privée générée dans les boitiers cryptographiques;

La vérification de ces informations lors de l'import du certificat est faite par le contact technique en contrôlant ces informations par rapport à celle fournies dans la demande de certificat.

L'import du certificat permet de valider et d'initialiser le contexte d'horodatage et ainsi permettre le démarrage du service d'horodatage.

5.4.4 Protection des clés privées des UH

Les clés privées des unités d'horodatage sont stockées dans un module cryptographique matériel respectant les exigences identifiées dans le référentiel FIPS PUB 140-2 niveau 3.

5.4.5 Exigences de sauvegarde des clés des UH

La présente PH ne comporte pas de politique de sauvegarde des clés des UH. Les clés des UH ne sont pas exportables et ne sont de fait pas sauvegardées.

5.4.6 Destruction des clés des UH

En fin de vie d'une clé privée d'UH, normale ou anticipée (révocation), cette clé est détruite par une opération d'administration du boîtier HSM. Elle n'est pas exportable et n'est pas sauvegardée.

5.4.7 Algorithmes obligatoires

L'AH, 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 des autorités compétentes en la matière comme par exemple [DCSSI_ALGO]. L'algorithme de calcul d'empreinte numérique accepté est SHA-1 au minimum ;
- Génère des contremarques de temps signées selon les algorithmes et les longueurs de clé conformes aux exigences des autorités compétentes en la matière comme par exemple [DCSSI_ALGO]. La bi-clé de l'UH est au minimum une bi-clé RSA de 2048 bits utilisant l'algorithme SHA-256.

5.4.8 Vérification des contremarques de temps

L'AH tient à disposition des clients les informations nécessaires à la vérification de la signature électronique des contremarques de temps. L'ensemble des informations et les moyens de leurs mise à disposition par l'AH sont précisés dans la documentation technique de l'opérateur.

La vérification d'une signature électronique de contremarque de temps peut être faite par une application utilisatrice et consiste en les opérations suivantes :

- Vérification du calcul de la contremarque de temps ;
- Vérification et extraction de la date et de l'heure contenues dans la contremarque de temps ;
- Identification et extraction du certificat de l'UH ayant émis la contremarque de temps ;
- Vérification que la date à laquelle la contremarque de temps a été émise est comprise dans la période de validité du certificat de l'UH ayant émis la contremarque de temps ;
- Vérification de l'état de validité du certificat de l'UH ayant émis la contremarque de temps au moment de la génération de la contremarque de temps ;
- Vérification que la date indiquée par l'AH dans la contremarque de temps est antérieure à la révocation éventuelle du certificat d'UH ayant émis la contremarque de temps.
- Si l'ensemble de ces opérations est positif, alors la contremarque de temps est considérée comme valide.

5.4.9 Durée de vie des clés publiques des UH

La durée de vie des clés publiques est positionnée à 3 ans.

5.4.10 Durée d'utilisation des clés privées des UH

La durée d'utilisation des clés privées est positionnée à 2 ans et demi.

6 DOCUMENTS CITÉS EN RÉFÉRENCES

6.1 Réglementations

Renvoi	Document
[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004

6.2 Documents techniques

Renvoi	Document
[DCSSI_ALGO]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, DCSSI, version 1.02 du 19 novembre 2004 N°2791 SGDN/DCSSI/SDS/Crypto du 19 novembre 2004 Les informations sont consultables sur le site http://www.ssi.gouv.fr
[ETSI_ALGO]	ETSI TS 119 312 : Cryptographic suites
[ETSI_PH]	ETSI EN 319 401 : General Policy Requirements for Trust Service Providers ETSI EN 319 421 : Policy & security requirements for TSP issuing time-stamps
[ETSI_TSP]	ETSI EN 319 422 : Time-stamping protocol and time-stamp profiles
[RFC 3161]	IETF - Internet X.509 Public Key Infrastructure - Time-Stamp Protocol - 08/2001

7 EXIGENCES SUR LES FORMATS DES CONTREMARQUES DE TEMPS, DES CERTIFICATS ET DES LCR ET SUR LES ALGORITHMES CRYPTOGRAPHIQUES

7.1 Contremarque de temps

Les contremarques de temps fournies par l'AH du Groupe BPCE ont une structure TimeStampToken conforme au [RFC3161].

Le tableau ci-dessous reprend l'ensemble des champs d'un TimeStampToken tels que définis dans le [RFC3161].

Une contremarque de temps conforme à la présente PH respecte, de base, les exigences correspondantes du RFC 3161, moyennant les compléments et/ou modifications d'exigences définis dans ce tableau.

Champ	Exigences
messageImprint	Valeur hachée du message suivant l'algorithme défini dans le paragraphe suivant
Accuracy	Ce champ est positionné et contient une valeur inférieure ou égale à 1 seconde.
Ordering	*Ce champ n'est pas positionné*
Tsa	*Ce champ n'est pas positionné*
certReq	Quelque soit la valeur de la requête, le jeton contient toujours la chaîne de certification associée
Extensions	*Aucune extension n'est marquée critique*

7.2 Certificats et LCR

Les gabarits des certificats d'UH sont conformes aux exigences des certificats de type « cachet » dont la clé privée associée est utilisée pour signer des jetons d'horodatage.

Il est rappelé ici que :

- L'extension « Extended Key Usage » est présente, marquée critique, et ne contient que l'identifiant « id-kp-timeStamping » à l'exclusion de toute autre ;
- Le champ « DN Subject » identifie l'AH de manière unique et l'identifiant propre à l'UH concernée, au sein de l'AH, est porté dans l'attribut commonName du DN de ce champ (au sein d'une AH, chaque UH a un identifiant unique) ;
- La durée de vie maximale est bornée selon le couple {durée de vie cryptographique de la clé ; fin de validité de la durée de vie de l'AC émettrice}.

7.3 Algorithmes cryptographiques

L'algorithme mis en œuvre pour la génération des certificats et le calcul des hachés dans les contremarques de temps est SHA-256. Cet algorithme respecte les recommandations en la matière et en vigueur en France.

8 AUDIT

Les exigences de ce chapitre sont référencées dans le document : « Mesures communes » publié à la même adresse que la présente politique.

9 EXIGENCES DE SÉCURITÉ DU MODULE D'HORODATAGE DES UH

9.1 Exigences sur les objectifs de sécurité

Le module d'horodatage, utilisé par l'AH pour générer et mettre en œuvre les clés de signature des UH et pour générer les contremarques de temps, répond aux exigences de sécurité suivantes :

- Garantir que la génération des bi-clés des UH est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- Assurer la confidentialité et l'intégrité des clés privées de signature des UH durant tout leur cycle de vie, et permettre leur destruction sûre en fin de vie ;
- Garantir l'authenticité et l'intégrité des clés publiques lors de leur export (à fins de certification par une AC) ;
- Vérifier la correspondance entre le certificat importé et la clé publique de l'UH ;
- 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, lors des phases d'initialisation, de personnalisation et d'opération, pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- Etre capable de détecter les tentatives d'altérations physiques et d'entrer dans un état sûr quand une tentative d'altération est détectée ;
- Permettre de créer une signature numérique, pour signer les contremarques de temps générées par l'UH, qui ne révèle pas les clés privées de l'UH 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 synchronisation de son horloge avec le temps UTC suivant la précision définie dans la PH ;
- Fournir des contremarques de temps conformes aux requêtes reçues.

9.2 Exigences complémentaires

Sans objet.

10 VÉRIFICATION DES CONTREMARQUES DE TEMPS

10.1 Empilement des contremarques de temps

Les contremarques de temps peuvent être validées en faisant une demande auprès du Groupe BPCE, demande à adresser par courriel à l'adresse suivante rssi-pssi-icg@bpce.fr.

Durant le processus de signature électronique, le système génère un dossier de preuve contenant les documents signés et les éléments de preuve.

Pour maintenir la capacité de vérifier une contremarque de temps après la durée de vie du certificat de l'UH qui a signé cette contremarque, l'AH conserve l'ensemble des listes de révocation.

10.2 Gestion de la révocation par l'AC

L'AC publie des CRL qui permettent d'attester de l'état du certificat d'une UH.

11 PRÉCISION DE LA SYNCHRONISATION DE L'HORLOGE

La précision de l'horloge est de 1 seconde par rapport au temps UTC(k).

12 PROTOCOLE D'HORODATAGE

12.1 Conformité RFC 3161

La validité de la conformité à la RFC 3161 est obtenue par :

- L'utilisation d'un boîtier d'horodatage conforme aux règlementations et normes en vigueur ;
- Le passage réussi à des outils de validation de la contremarque de temps.

12.2 Conformité ETSI EN 319 422

Le profil des contremarques de temps est conforme à l' [ETSI_TSP].

13 COMPATIBILITÉ AVEC [ETSI_PH]

La présente PH est conforme à l' [ETSI_PH].

14 GABARIT DE CERTIFICAT D'UNE UH

Chaque UH dispose d'un certificat généré à partir du gabarit « Certificat Horodatage » décrit dans la politique de certification de l'AC publiée sous www.dossiers-securite.bpce.fr.