Politique d'Horodatage

BPCE SA

Référence du document	
1.3.6.1.4.1.40559.1.0.4.4.0.1.0	01 Juillet 2013

BPCE : Société anonyme à directoire et conseil de surveillance,

au capital de 467 226 960 €.

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 met en œuvre une infrastructure de confiance pour ses projets de signature électronique de contrats en agence.

BPCE SA se positionne en tant qu'Autorité d'Horodatage (ci-après « AH ») et délivre des contremarques de temps pour les besoins des applications de dématérialisation des contrats en agence. La solution d'Horodatage est mise en œuvre par IT-CE, qui se positionne comme opérateur de service d'horodatage (OSH) pour le compte de BPCE SA.

Le présent document constitue la politique d'horodatage de BPCE SA (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 banques 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 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 BPCE SA, 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 de BPCE SA 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.

1.2 Identification du document

La présente « Politique d'Horodatage BPCE SA » est identifiée, au sein du référentiel documentaire de l'infrastructure de confiance, par un numéro d'identification unique, l'OID : **1.3.6.1.4.1.40559.1.0.4.4.0.1.0.**

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 Sécurité Groupe (COSSIG).

La présente Politique d'Horodatage est publiée sur l'URL : http://pro.d00.pki01.bpce.fr/PC_POLITIQUE_HORODATAGE_1.3.6.1.4.1.40559.1.0.4.4.0.1.0.pdf.

L'ensemble des informations associées (cf. 1.5.3) notamment les versions antérieures de ces documents avec leur période de validité, sont également publiées sur le site http://pro.d00.pki01.bpce.fr/.

1.4 Composition du comité d'approbation

L'approbation de la conformité de la DPC est mise à l'ordre du jour du COSSIG. Ce dernier se base sur des résultats d'audits menés par le contrôle RSSI IT-CE et sur les PV de mise en production. Deux niveaux de contrôles sont alors appliqués.

- Contrôle niveau 1 par les équipes opérationnelles d'IT-CE
- Contrôle niveau 2 par les équipes sécurité IT-CE

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 à minima tous les **7 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 :

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 BPCE SA, 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'OSH.

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 de BPCE SA pour obtenir plus d'informations, en envoyant un mail à rssi-politiques de sécurité-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 ;

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 site identifié au paragraphe 1.3.

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 de BPCE SA.

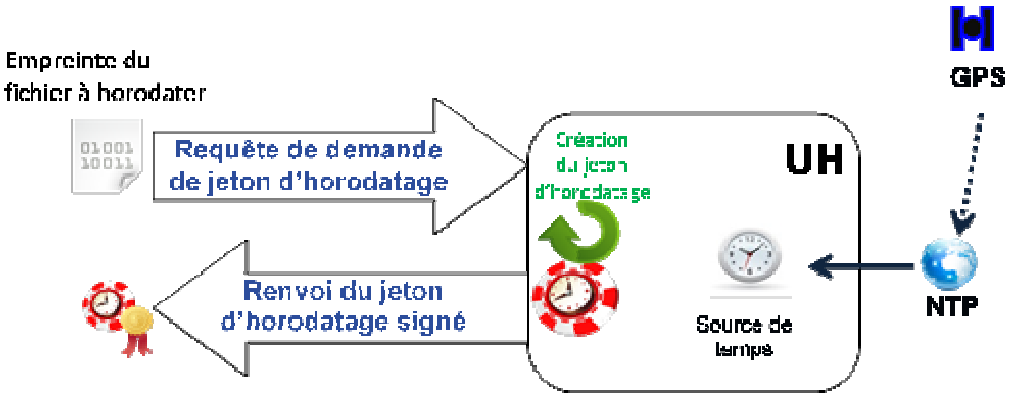
Le Comité Sécurité Groupe s'assure de la cohérence de ce référentiel documentaire et de l'adéquation de la présente Politique d'Horodatage avec les autres documents, plus particulièrement les politiques de signature, de certification et de gestion des preuves.

1.8 Principes de l'horodatage tel que réalisé par BPCE SA

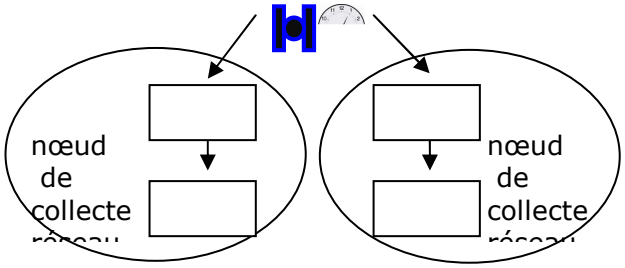
L'Autorité de certification qui délivre les certificats est l'AC SIGNATURE ICG D01-01.

L'horodatage est effectué par des UH (logiciel DTSS de l'éditeur DICTAO) qui prend sa source de temps sur un service NTP.

Le schéma de principe est alors le suivant :



Le service NTP est basé sur des serveurs situés sur le réseau intranet de l'entreprise et est installé sur deux sites géographiques distincts. Il y a deux niveaux de service au sein d'un nœud de collecte.



L'horloge de référence est GPS.

Les UH de l'infrastructure ICG accèdent à la source de temps sur le niveau dit « Strate 1 », le protocole est NTPv4.

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

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 présente 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 ce 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.

La présente PH est élaborée sur la base des documents issus de l'ETSI TS 102 023 ([ETSI_PH]) et de la Politique d'Horodatage Type (RGS – Politique d'Horodatage Type) définie par le Référentiel Général de Sécurité (RGS).

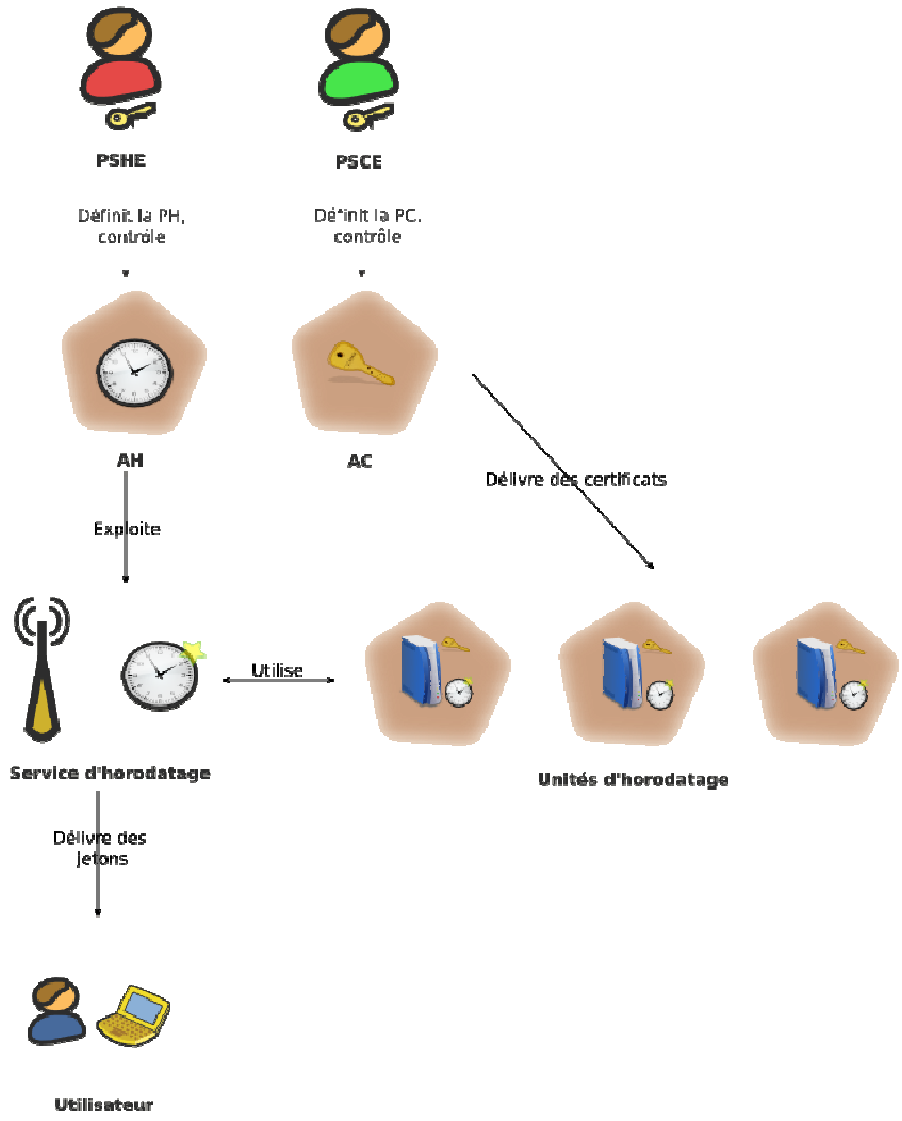
1.10 Entités intervenant dans le service d'horodatage

BPCE SA est le responsable de l'Autorité d'Horodatage qui est exploitée et maintenue en condition opérationnelle par IT-CE.

L'Autorité d'Horodatage utilise dans son service d'horodatage des boîtiers de temps qui assurent 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.

BPCE SA 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 unités d'horodatage utilisent des boîtiers cryptographiques matériels pour générer et stocker les clés privées des certificats électroniques.

2 DÉFINITION ET ACRONYMES

Les définitions et acronymes sont référencées dans le document annexe suivant : « Mesures communes, définitions et acronymes applicables à l'Infrastructure de ConfianceGroupe (ICG) ». Cette annexe est publiée au sein du même espace 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 définie dans le RFC3161 et profilée dans le document ETSI TS 101 861 V1.4.1.

Les caractéristiques principales de cette politique sont les suivantes :

- la protection des clés et de l'horloge respectent les exigences spécifiées au 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 102023.

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.

Il n'existe pas actuellement de CGU propre au service d'horodatage. 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 de son contrat, le client est tenu d'accepter les CGU du service de signature qui intègre 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, l'Autorité d'Horodatage :

- 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, à travers sons système d'archivage, l'ensemble des informations nécessaires permettant de vérifier les contremarques de temps qu'elle aura émises. Les demandes de vérifications font partie d'un processus tiers décrit dans la Politique d'Archivage de BPCE SA.

5.1.2 Obligation de l'abonné

Le client d'une des banques du groupe est tenu d'accepter les CGU 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 :

- 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 place par BPCE SA ;

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

L'Autorité de Certification qui délivre les certificats est l'AC SIGNATURE ICG D01-01. Cette AC respecte la politique de certification PC_BPCE_AC_SIGNATURE_ICG.

Cette AC délivre des certificats de clés publiques pour les UH fournit un service de révocation mis à jour sur une base quotidienne en employant au moins un mécanisme de publication de LCR.

Cette AC s'engage 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 l'AC SIGNATURE ICG D01-01 fournissant les certificats aux unités d'horodatage ;

- 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 ;

- 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 ;

- Informe préalablement les Clients de tout changement auquel elle a l'intention de procéder dans la partie publique de sa DPH et après mise en place du changement, met immédiatement à la disposition des Clients et des utilisateurs de contremarques de temps la partie publique révisée de la DPH

5.1.6 Conditions Générales d'Utilisation

Les éléments liés au service d'horodatage sont décrits dans les CGU acceptés par le client dans le cadre du processus de signature électronique en agence.

Les éléments suivants font partie de ces CGU :

- Les obligations de l'abonné ;

- Les obligations des utilisateurs de contremarques de temps ;

- Une information sur le point de contact du service d'horodatage ;

- Une référence et une description de la PH appliquée ;

- Au moins un algorithme de hachage ;

- La période de temps minimum durant laquelle les contremarques de temps seront vérifiables par l'utilisateur de contremarques de temps et l'abonné. Ce temps ne tient pas compte des éventuelles procédures de révocation du certificat d'une unité d'horodatage ;

- L'exactitude du temps fourni dans les contremarques de temps par rapport au temps UTC ;

- L'ensemble des limitations du service d'horodatage, notamment le périmètre applicatif pour lequel les contremarques de temps sont fournies ;

- Les informations nécessaires pour vérifier les contremarques de temps ;

- La période de conservation des données d'audit ;

- Le système légal applicable ;

- Les limitations de responsabilité de l'AH ;

- Les procédures pour les plaintes et le règlement des litiges ;
- L'ensemble de la chaîne de certification de l'AC qui émet les certificats des UH et les points de publications des CRL ;
- Le pays dans lequel l'AH est installée.

5.1.7 Conformité avec les exigences légales

5.1.7.1 Droit applicable

Le présent document est régi par la loi française.

5.1.7.2 Règlement des différends

Toutes contestations et litiges survenant dans l'interprétation et la mise en œuvre du présent document seront soumis à la juridiction des tribunaux de Paris.

5.1.7.3 Propriété intellectuelle des infrastructures

Les utilisateurs de ces services ne disposent d'aucun droit de propriété intellectuelle sur ces différents éléments. Toute utilisation ou reproduction, totale ou partielle, de ces éléments et/ou des informations qu'ils contiennent, par quelque procédé que ce soit, est strictement interdite et constitue une contrefaçon sanctionnée par le Code de la propriété intellectuelle, sauf accord préalable et écrit de BPCE SA.

5.1.7.4 Données nominatives

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 nominatives, réalisé à partir des plates-formes **BPCE SA** 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 **BPCE SA** et les différents partenaires intervenant dans les échanges concernés.

Les utilisateurs des services **BPCE SA** 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 BPCE SA 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 par IT-CE, notamment pour :

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

5.2.2 Fichiers d'audit

Les journaux du service d'horodatage sont conservés sur le serveur d'horodatage depuis sa mise en activité. 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 enregistrements d'audit courants et archivés relatifs au fonctionnement des services d'horodatage sont assurées.

L'intégrité des journaux d'audit est garantie par le serveur DTSS qui signe les enregistrements d'audit. L'intégrité des pistes d'audit est garantie par l'intermédiaire d'une signature PKCS#1. Un mécanisme de chainage des pistes est également présent afin de se protéger contre la suppression ou l'injection de log d'audit.

La confidentialité des journaux d'audit est garantie par le fonctionnement du serveur DTSS par les rôles fonctionnels d'accès aux enregistrements d'audit.

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.

Les enregistrements relatifs au fonctionnement des services d'horodatage sont enregistrés par DTSS dans un fichier de trace.

De plus,

- Les opérations effectuées par une application via DTSS donnent lieu à la génération de preuves. Ces preuves sont là pour garder une trace de l'opération effectuée et de la justification de la réponse qui a été faite.
- Une preuve n'est générée que lorsque DTSS a pu effectuer l'opération dans des conditions techniques satisfaisantes permettant de faire une réponse adéquate. Ainsi un manque d'informations sur le statut de révocation d'un certificat (CRL non disponible par exemple), ne permet pas de répondre de façon satisfaisante et ne génère donc pas de preuve.
- Ces preuves peuvent être recherchées via une interface graphique offrant plusieurs critères de recherche. Les preuves peuvent alors être affichées et exportées.
- Les preuves sont au format XAdES-T.

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.

- 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.

- Les enregistrements relatifs à l'administration du service d'horodatage sont contenus dans le fichier de configuration XML du serveur DTSS.

- Cette journalisation concerne les actions effectuées par les administrateurs sur la configuration générale de DTSS

    - Ajout, modification ou suppression d'une application

    - Ajout, modification ou suppression d'une autorité de certification

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

- Ces journaux sont consignés dans des fichiers plats, chaînés et signés par une clé dédiée du HSM (Hardware Security Module).

- Un outil permettant de vérifier la signature de ces journaux et de faire des recherches sur les actions des administrateurs est également mis à disposition.

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 serveur DTSS 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 serveur DTSS dans le fichier de trace.

Il n'y a pas actuellement de politique d'analyse de ces journaux.

Les journaux ne sont ni exportés ni archivés.

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, IT-CE 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 serveur d'horodatage DTSS est synchronisé sur une source interne via NTP. Cette source interne est le boîtier de temps mis en œuvre par IT-CE

- Le boîtier de temps se synchronise sur une source GPS externe.

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 BPCE SA respectent, de base, 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 BPCE SA. 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 à :

- Vols des serveurs des unités d'horodatage ;
- Vol des clés privées des UH ;
- 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.

Concernant les autres cas de compromission, dans le cadre du plan de continuité d'activité, **IT-CE** 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, chacune ayant des clés privées différentes.

En cas de compromission de l'Autorité d'Horodatage et plus particulièrement des clés privées des Unités d'Horodatage, les équipes d'IT-CE 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 **IT-CE**.

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 **IT-**

CE. Ce fonctionnement permet à l'AH BPCE SA de garantir un service d'horodatage avec un haut niveau de disponibilité.

En tout état de cause, IT-CE :

- Mettra à disposition de BPCE SA 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, IT-CE :

- Rendra disponible à BPCE SA 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 ;
- Transfèrera à un organisme fiable les informations d'audit ;
- Fournira à un organisme fiable 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.

Le choix de l'organisme qui récupèrera les données d'audit sera défini dans le cadre du plan de fin d'activité mis en œuvre par l'AH BPCE SA.

5.3 Exigences physiques, environnementales, procédurales et organisationnelle

Les exigences de ce chapitre sont référencées dans le document annexe suivant : «Mesures communes, définitions et acronymes applicables à l'ICG ». Cette annexe est publiée au sein du même espace 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'ensemble est basé sur la synchronisation d'une source de Strate 1 et sur l'utilisation d'un matériel Symmetricom SyncServer 200.

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 serveur d'horodatage pour qu'il utilise le certificat de signature de l'UH lors d'une demande de contremarque de temps.

La configuration du serveur utilisé dans l'AH garantit le lien entre le demandeur d'une contremarque et les droits dont dispose le serveur d'horodatage pour lui la délivrer.

Les informations suivantes font parties de la demande :

- Le CN qui sera complété par le profil de génération du certificat de la PKI pour aboutir au DN du certificat de l'UH;
- La valeur de la clé publique suivant (module et exposant) ;

La vérification de ces informations lors de l'import du certificat est faite par l'unité d'horodatage 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 de l'unité d'horodatage.

5.4.4 Protection des clés privées des UH

Les clés privées des unités d'horodatage sont au format logiciel stockées sur le serveur correspondant.

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 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.

Le principe de prolonger l'horodatage XAdES-T n'a pas été retenu, le choix retenu est de constituer une liste blanche. Le principe de cette liste blanche est de ne plus appuyer la vérification sur la clé publique utilisée pour signer les contremarques de temps, c'est-à-dire de ne plus prendre en compte la durée de vie du certificat et de ne plus faire de vérification sur la CRL.

La vérification s'appuie sur une liste blanche configurée au niveau du serveur de signature. Cette liste blanche des certificats est mise à jour lors de la création du certificat (et de sa révocation). Cet usage est utilisé pour des raisons de performance et d'exploitation il est indiqué dans la politique de signature. Le fichier de configuration utilisé au moment de la génération du jeton d'horodatage fait également partie des éléments de preuve permettant de garantir la validité du jeton.

5.4.9 Durée de vie des clés publiques des UH

La durée de vie des clés publiques est la suivante :

- 3 ans pour le certificat d'horodatage des pdf
- 5 ans pour le certificat d'horodatage des preuves

5.4.10 Durée d'utilisation des clés privées des UH

La durée d'utilisation des clés privées est la suivante :

- 3 ans pour le certificat d'horodatage des pdf
- 5 ans pour le certificat d'horodatage des preuves

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
[DécretRGS]	Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005
[Ordonnance]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électronique entre les usagers et les autorités administratives et entre les autorités administratives

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_PH]	ETSI TS 102 023 V1.2.1 (2003-01) Policy requirements for Time-Stamping Authority
[ETSI_TSP]	ETSI TS 101 861 V1.2.1 (2002-03) Time Stamping Profile
[RFC 3161]	IETF - Internet X.509 Public Key Infrastructure - Time-Stamp Protocol - 08/2001
[RGS]	http://www.ssi.gouv.fr/IMG/pdf/RGSv1-0.pdf
[PH_Type]	http://www.ssi.gouv.fr/IMG/pdf/RGS__P_Horodatage-Type_v2-3.pdf

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 BPCE SA 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 n'est pas positionné car la précision du temps délivré dans la contremarque de temps par rapport au temps UTC(k) est d'une seconde.
Ordering	Ce champ n'est pas positionné
Tsa	Ce champ n'est pas positionné
Extensions	Aucune extension n'est marquée critique

Les champs en italique, optionnels, ne sont pas contenus dans les contremarques de temps conformes à la présente PH.

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 EXIGENCES DE SÉCURITÉ DU MODULE D'HORODATAGE DES UH

8.1 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.

8.2 Exigences complémentaires

Sans objet..

9 VÉRIFICATION DES CONTREMARQUES DE TEMPS

9.1 Empilement des contremarques de temps

Les contremarques de temps peuvent être validées en faisant une demande auprès du système d'archivage de BPCE SA.

Ce système génère un dossier de preuve de la transaction et de la signature électronique du contrat en agence.

Pour maintenir la capacité de vérifier une contremarque de temps après la durée de vie du certificat de l'UH qui a signée cette contremarque, il est utilisé une liste blanche identifiant au moment de la génération du jeton :

- Le certificat utilisé
- Le fichier de configuration correspondant

9.2 Gestion de la révocation par l'AC

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

Suite à la révocation d'un certificat, la liste blanche est mise à jour.

10 PRÉCISION DE LA SYNCHRONISATION DE L'HORLOGE

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

11 PROTOCOLE D'HORODATAGE

11.1 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.

11.2 Conformité ETSI TS 101861

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

12 COMPATIBILITÉ AVEC [ETSI_PH]

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

13 GABARIT DE CERTIFICAT D'UNE UH

Chaque UH a deux certificats :

Un certificat d'horodatage des pdf, ces certificats seront générés à partir du gabarit décrit ci-dessous :

Paramètre	Valeur
AC émettrice	AC SIGNATURE ICG D01-01
DN du certificat	CN = **HPDF-***ee*-*99*-**D0***9* OU = 0002 552028839 O = **BPCE** C = **FR**
Taille de la clé	2048
Algorithme de signature	sha256RSA
Durée de validité	**1096** (3 ans)
Utilisation de la clé	Signature numérique, Non répudiation (critique)
Usage avancé de la clé	Enregistrement des informations de date (1.3.6.1.5.5.7.3.8)
CRL DP	Oui

Où :

- ee est utilisé pour indiquer l'enseigne (bp ou ce)
- *9* est utilisé pour indiquer le site (Data Center) D01 ou D02
- *99* est utilisé pour indiquer le numéro d'ordre dans ce site

Un certificat d'horodatage des preuves, ces certificats seront générés à partir du gabarit décrit ci-dessous :

Paramètre	Valeur
AC émettrice	AC SIGNATURE ICG D01-01
DN du certificat	CN = **HPRE** *enseigne* OU = 0002 552028839 O = **BPCE** C = **fr**
Taille de la clé	2048
Durée de validité	**1827** (5 ans)
Usage de la clé	Signature numérique, Non répudiation (critique)
Usage	Enregistrement des informations de date

avancé de la clé	(1.3.6.1.5.5.7.3.8)
CRL DP	Oui

Où

- enseigne donne l'enseigne
  - HPRE CAISSE D'EPARGNE
  - HPRE BANQUE POPULAIRE