DIDeS
Direction de l'Innovation et du Développement des e-Services

Politique d'Horodatage

Version 4

Date version : 17 décembre 2003

Identification du document : 1.2.250.1.8.1.1.1.1.4

Documents de référence

Référence	Version	Titre du document de référence
ETSI TS 101 861	V 1.1.1	Time Stamping Profile
ETSI TS 102023	V 1.1.1	Policy Requirements for time-stamping authorities – January 2002
ETSI TS xxxx STF 178-T2	Draft E	Policy Requirements for Certification Authorities issuing public key certificates – 10 november 2001
ITU-R TF.460-5		Standard-Frequency and Time Signal emissions – 1997
ITU-R TF.536-1		Time-Scale Notations – 1998
RFC 3161		Internet X.509 Public Key Infrastructure : Time-Stamp Protocol (TSP) – 2001

1.2.250.1.8.1.1.1.4 –17/12/2003

SOMMAIRE

1. OBJECTIFS GENERAUX 5
2. DEFINITIONS ET ABREVIATIONS 6
2.1 DEFINITIONS 6
2.2 ABREVIATIONS 7
3. ACTEURS DE L'HORODATAGE 8
3.1 SERVICES D'HORODATAGE 8
3.2 AUTORITE D'HORODATAGE 8
3.3 SERVICE DEMANDEUR 8
3.4 COMMISSION D'APPROBATION DES POLITIQUES 8
4. POLITIQUE D'HORODATAGE 9
4.1 DEFINITION 9
4.2 IDENTIFICATION 9
4.3 CONFORMITE 9
4.4 CERTIFICATS D'HORODATAGE 9
5. OBLIGATIONS 10
5.1 OBLIGATIONS DE L'AH 10
5.2 OBLIGATIONS DE L'OPERATEUR DE SERVICE D'HORODATAGE 10
5.3 OBLIGATIONS ET RESPONSABILITES DES SERVICES DEMANDEURS 11
5.3.1 Vérification de la validité des jetons dès réception 11
5.3.2 Archivage des jetons d'horodatage 11
5.4 OBLIGATIONS DES UTILISATEURS FINAUX 11
6. EXIGENCES CONCERNANT LES PRATIQUES D'HORODATAGE 12
6.1 DECLARATION DES PRATIQUES D'HORODATAGE DE L'OSH ET RESUME PUBLIABLE DES POLITIQUES 12
6.1.1 Déclaration des Pratiques d'Horodatage (DPH) de l'OSH 12
6.1.2 Résumé publiable des politiques 12
6.2 CYCLE DE VIE DES CLES DE L'AH 13
6.2.1 Génération des clés de l'AH 13
6.2.2 Protection des clés privées de l'AH 13
6.2.3 Distribution des clés publique de l'AH 13
6.2.4 Renouvellement des clés de l'AH 14
6.2.5 Fin du cycle de vie des clés cryptographiques 14
6.2.6 Gestion du cycle de vie des UH utilisées pour la signature des jetons d'horodatage 14
6.3 PRODUCTION DES JETONS D'HORODATAGE 14
6.3.1 Jeton d'horodatage 14
6.3.2 Synchronisation avec l'UTC 15
6.3.3 Disponibilité du service 15
6.4 VALIDITE D'UN JETON D'HORODATAGE 15
6.4.1 Durée de validité d'un jeton d'horodatage 15
6.4.2 Vérification d'un jeton d'horodatage par le service demandeur 16
6.5 GESTION ET EXPLOITATION DE L'AH 16
6.5.1 Gestion de la sécurité 16
6.5.2 Classification des biens 17
6.5.3 Sécurité du personnel 17
6.5.4 Sécurité physique 18
6.5.5 Sécurité d'exploitation 19
6.5.6 Zonage des locaux 20
6.5.7 Gestion des accès aux composantes du système d'horodatage de l'AH 20
6.5.8 Maintenance et déploiement de l'AH 20
6.5.9 Mesures à prendre en cas de compromission 21
6.5.10 Fin du cycle de vie de l'AH 21
6.5.11 Données enregistrées par l'AH 22
6.6 ORGANISATION DE L'AH 23
6.7 CONTROLES DE CONFORMITE 24
7. ADMINISTRATION DE LA POLITIQUE D'HORODATAGE 25
7.1 PROCEDURES DE MODIFICATION DE LA POLITIQUE D'HORODATAGE 25
7.2 PROCEDURES DE PUBLICATION ET DE NOTIFICATION 25

1.2.250.1.8.1.1.1.1 4 –17/12/2003

AVERTISSEMENT

La présente Politique d'Horodatage (PH) est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables (notamment la convention de Berne de 1886). Ces droits sont la propriété exclusive de La Poste. La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement par écrit par La Poste ou ses ayants droit, sont strictement interdites.

Le Code de la Propriété Intellectuelle n'autorise, aux termes de l'article L.122-5, d'une part, que « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinés à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (article L.122-4 du Code de la Propriété Intellectuelle).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.

1.2.250.1.8.1.1.1.1 4 –17/12/2003

1. OBJECTIFS GENERAUX

Ce document constitue la PH de La Poste. Il développe les points suivants :

- Une description des services rendus par l'Autorité d'Horodatage (AH) La Poste ;
- Un ensemble d'exigences concernant l'exploitation de l'AH.

Il a pour but de fournir aux services demandeurs des services d'horodatage l'information nécessaire pour évaluer la confiance qu'ils placent dans une relation basée sur des jetons d'horodatage émis par l'AH La Poste.

La structure et le contenu de la présente PH sont inspirés du document « Policy Requirements for Time-Stamping Authorities » de l'ETSI qui donne des directives générales et définit des exigences pour la rédaction d'une PH, référencé sous l'Identifiant d'Objet (OID) suivant :

{itu-t(0) identified-organisation(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy(1)}

1.2.250.1.8.1.1.1.4 –17/12/2003

2. DEFINITIONS ET ABREVIATIONS

2.1 DEFINITIONS

Autorité de Certification (AC) : Entité émettant des Certificats après vérification de l'identité de la personne ou du représentant du système applicatif, ou de la procédure ayant mené à son identification. L'AC est responsable de l'ensemble des composantes matérielles, humaines et organisationnelles utilisées dans le processus de création et de gestion des Certificats. Il s'agit de CertiNomis dans le cadre de la présente PH.

Autorité d'Horodatage (AH) : Autorité responsable de la gestion de l'environnement d'horodatage et de la production des jetons d'horodatage de La Poste sur les données qui lui sont présentées afin d'attester de l'existence de ces données à la date de la marque de temps. Il s'agit de La Poste dans le cadre de la présente PH.

Commission d'Approbation des Politiques (CAP) : La CAP de La Poste est constituée de représentants désignés par La Poste pour créer, contrôler le respect et faire évoluer la documentation des politiques régissant l'infrastructure des Services Électroniques de Confiance.

Composante de l'AH : Plate-forme constituée d'au moins un poste informatique, une application, un moyen de cryptographie, un support réseau et jouant un rôle déterminé au sein du système.

Déclaration des pratiques d'horodatage (DPH) : Document conforme aux exigences de la PH, décrivant précisément les pratiques mises en place par l'AH ou par l'OSH pour la fourniture de jetons d'horodatage.

Echelle de temps Universal Time Coordinated (UTC) : Heure basée sur le méridien de Greenwich (+0, heure GMT). Cette heure est utilisée afin de ne pas avoir à prendre en compte les décalages horaires lorsque l'on s'adresse à plusieurs interlocuteurs situés dans des fuseaux horaires différents.

Echelle de temps UTC(k) : Heure fournie par la source de temps « k » avec une précision de ± 100 ns, conformément à la recommandation S5 du Comité Consultatif pour la Définition de la Seconde (référence : [ITU-R TF.536-1])

Empreinte (empreinte numérique ou condensat ou hash) : Résultat d'une fonction de hachage appliquée sur une chaîne de caractères de longueur quelconque visant à réduire celle-ci en une donnée de longueur fixe représentative de cette chaîne de caractères.

Jeton d'horodatage : Elément de données résultant de l'association de données à une date et une heure obtenues à partir d'une source de temps réputée fiable, le tout étant signé électroniquement par l'AH.

Opérateur de Service d'Horodatage (OSH) : Opérateur assurant les prestations techniques nécessaires au processus d'horodatage. Il est en charge du bon fonctionnement et de la sécurité des moyens informatiques et techniques. Il est en charge de la sécurité des personnels, des locaux et, plus généralement, du bon respect des procédures, toutes choses indispensables pour garantir un niveau de fiabilité.

Politique d'horodatage (PH) : Texte contractuel qui établit les obligations et responsabilités de l'Autorité d'Horodatage, de l'Opérateur des Services d'Horodatage, des services demandeurs et des utilisateurs finaux. Elle est librement consultable par les clients, les abonnés ainsi que par tous les tiers utilisateurs du service.

Résumé publiable des politiques : Document résumant les informations publiables des politiques et pratiques de l'AH destiné plus particulièrement aux services demandeurs des services d'horodatage.

Service demandeur : Entité demandant à l'AH la fourniture de service d'horodatage et ayant explicitement ou implicitement accepté les termes et conditions de cette fourniture.

Signature électronique : Résultat du chiffrement, à l'aide d'une clé privée, d'une empreinte des données à signer par utilisation des techniques de la cryptographie asymétrique. La clé privée est associée à une clé publique certifiée par un certificat émis par une AC.

Source de temps : Composante interne ou externe d'une AH fonctionnant comme une tierce partie de confiance chargée de restituer l'heure exacte.

Système d'horodatage : Ensemble des Unités d'horodatage et composantes de l'AH permettant la fourniture des services d'horodatage.

Unité d'horodatage (UH) : Ensemble de composants logiciels et matériels, géré comme une entité particulière et ayant une seule clé de signature des jetons d'horodatage active à un instant.

1.2.250.1.8.1.1.1.4 –17/12/2003

Utilisateur final : Personne physique ou morale identifiée ou non qui reçoit par l'intermédiaire du service demandeur un jeton d'horodatage correspondant à la fourniture d'un service d'horodatage par l'AH.

2.2 ABREVIATIONS

AH	Autorité d'Horodatage
CAP	Commission d'Approbation des Politiques
DPH	Déclaration des Pratiques d'Horodatage
ETSI	European Telecommunication Standards Institute
OID	Object IDentifier
OSH	Opérateur de Service d'Horodatage
RSSI	Responsable de la Sécurité des Systèmes d'Information
UH	Unité d'Horodatage
UTC	Universal Time Coordinated

1.2.250.1.8.1.1.1.4 –17/12/2003

3. ACTEURS DE L'HORODATAGE

3.1 SERVICES D'HORODATAGE

Les services d'horodatage se chargent d'émettre des jetons d'horodatage aux services demandeurs conformément au RFC3161. Ils assurent également l'exploitation de l'horodatage pour s'assurer que le service fourni est conforme aux spécifications de l'AH.

Les services d'horodatage sont assurés par l'Opérateur de Service d'Horodatage (OSH) sous la responsabilité de l'AH.

3.2 AUTORITE D'HORODATAGE

L'AH a la complète responsabilité de la fourniture des services d'horodatage définis au paragraphe 3.1.

Les clés de signature de l'AH sont utilisées pour signer les jetons d'horodatage et l'AH est identifiée comme l'émetteur de ces jetons.

L'AH peut faire appel à d'autres entités pour réaliser tout ou partie des services. Elle en conserve cependant l'entière responsabilité et s'assure que les exigences décrites dans la présente politique sont satisfaites.

3.3 SERVICE DEMANDEUR

C'est l'entité qui demande à l'AH la fourniture de service d'horodatage.

Les services demandeurs peuvent fournir les jetons d'horodatage à leurs utilisateurs. Ces derniers sont appelés « utilisateurs finaux » dans le présent document.

3.4 COMMISSION D'APPROBATION DES POLITIQUES

La CAP de La Poste pour les Services Électroniques de Confiance de La Poste est constituée de représentants désignés par La Poste pour créer, contrôler le respect et faire évoluer la documentation des politiques régissant l'infrastructure des Services Électroniques de Confiance de La Poste.

Les principales fonctions de la CAP sont de :

- Maintenir, corriger, faire évoluer, clarifier et remplacer les politiques en usage au sein des Services Électroniques de Confiance de La Poste ;
- Approuver les nouvelles politiques ;
- Publier les politiques.

La CAP a également pour rôle d'approuver la façon dont la sécurité a été prise en compte et mise en œuvre au sein de l'infrastructure. À ce titre, elle valide ou fait valider par une entité qu'elle désigne, la conformité des pratiques des opérateurs à la présente PH (voir paragraphe 6.7).

1.2.250.1.8.1.1.1.1.4 –17/12/2003

4. POLITIQUE D'HORODATAGE

4.1 DEFINITION

La Politique d'Horodatage est un texte contractuel qui établit les obligations et responsabilités de l'Autorité d'Horodatage, de l'Opérateur des Services d'Horodatage, des Services demandeurs et des Utilisateurs finaux. La Politique d'Horodatage est librement consultable par les clients, les abonnés ainsi que par tous les tiers utilisateurs.

Définissant un cadre clair, elle permet d'établir la confiance à l'égard des jetons émis par l'Autorité d'horodatage, selon l'usage et la finalité recherchés.

4.2 IDENTIFICATION

La présente PH est dénommée « Politique d'Horodatage de La Poste ».

La Poste s'est fait attribuer par l'AFNOR en 1991, l'identifiant **1.2.250.1.8** et peut depuis affecter des identifiants sous sa branche aux objets de son choix. La présente PH est identifiée par l'Identifiant d'Objet (OID) suivant :

{iso(1) member-body(2) france(250) type-org(1) la poste(8) Courrier(1) Services de Cachet Electronique(1) document(1) ph (1) version (3)}

Soit : **1.2.250.1.8.1.1.1.1.3**

Les jetons d'horodatage émis par les Services d'Horodatage comportent l'OID de la PH applicable.

4.3 CONFORMITE

L'AH met en place des audits périodiques des pratiques de l'OSH pour en garantir la conformité avec la présente PH.

4.4 CERTIFICATS D'HORODATAGE

Les certificats d'horodatage, certifiant les clés publiques associées aux clés privées (hébergées dans les UH) utilisées pour la signature des jetons d'horodatage générés dans le cadre de la présente PH, sont émis par l'AC CertiNomis (CertiNomis Horodatage DSA). Ces certificats sont dédiés à l'horodatage : le champ usage avancé des clés privée est positionné en conséquence.

Ils sont émis suivant la politique de certification (PC) : « Politique de Certification Horodatage ». L'OID de cette PC est : 1.2.250.1.86.2.1.10.1.

L'AH se déclare conforme aux obligations lui incombant définis dans cette Politique de Certification qui précise entre autre les limites de responsabilité de l'AH concernant les certificats d'UH.

1.2.250.1.8.1.1.1.1.4 –17/12/2003

5. OBLIGATIONS

5.1 OBLIGATIONS DE L'AH

L'AH :

- s'assure que toutes les exigences détaillées au chapitre 6, sont mises en place ;
- garantie l'application des procédures décrites dans la présente politique, que les fonctionnalités de l'AH soient sous-traitées auprès de sociétés externes ou non ;
- s'assure que les moyens mis en œuvre, décrits dans la Déclaration des Pratiques d'Horodatage (DPH) de l'OSH, répondent complètement aux exigences de la PH ;
- s'engage à respecter la confidentialité des éléments précisés dans la DPH de l'OSH.

5.2 OBLIGATIONS DE L'OPERATEUR DE SERVICE D'HORODATAGE

Concernant la génération des jetons d'horodatage, l'OSH s'engage à :

- Respecter et à répondre aux exigences de la présente PH telles que traduits dans la DPH ;
- Accepter les audits périodiques de contrôle de conformité par rapport à la présente PH réalisés par l'AH ou par des entités d'audit externes tel que précisé au paragraphe 6.7.

En outre l'OSH s'engage au respect des obligations suivantes :

- Respecter le contrat de prestation de services qui le lie à l'AH ;
- N'utiliser les clés privées de l'AH que pour la signature des jetons d'horodatage destinés à des Services Demandeurs ayant contractualisés avec l'AH dans le cadre de la présente PH et ce, selon les règles et avec les moyens spécifiés dans la Politique de Certification et le contrat de service de l'AC émettrice des certificats associés ;
- Protéger contre toute compromission les clés privées de l'AH utilisées pour la signature des jetons d'horodatage ;
- Assurer le bon fonctionnement et la sécurité des moyens informatiques et techniques mis en œuvre dans le cadre des services d'horodatage ;
- Garantir le respect des caractéristiques opérationnelles de la fonction d'horodatage qui lui est confiée par l'AH dans le cadre des services d'horodatage ; Ces caractéristiques sont détaillées dans le présent document et dans le contrat de prestation de services associé ;
- Se conformer aux résultats des contrôles de conformité effectués sur demande de l'AH, conformément au paragraphe 6.7, et remédier aux non-conformités que ceux-ci révéleraient ;
- Documenter ses procédures internes d'exploitation ;
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles il s'engage.

1.2.250.1.8.1.1.1.4 –17/12/2003

5.3 OBLIGATIONS ET RESPONSABILITES DES SERVICES DEMANDEURS

5.3.1 Vérification de la validité des jetons dès réception

Le service demandeur s'engage à vérifier la validité d'un jeton d'horodatage dès sa réception selon la procédure de vérification décrite au paragraphe 6.4.2. Le service demandeur s'engage également à vérifier que les données sur lesquelles portent le scellement d'horodatage sont bien celles transmises pour horodatage.

5.3.2 Archivage des jetons d'horodatage

L'archivage des jetons d'horodatage émis pour un service demandeur relève de la responsabilité dudit service demandeur.

5.4 OBLIGATIONS DES UTILISATEURS FINAUX

Les utilisateurs finaux n'ont pas d'obligation dans le cadre de la présente politique.

Il leur est cependant recommandé de valider (ou faire valider par les services demandeurs) les jetons d'horodatage. Dans ce cas, ils doivent appliquer les procédures de vérification de la validité des jetons d'horodatage définies au paragraphe 6.4.2.

1.2.250.1.8.1.1.1.1 4 –17/12/2003

6. EXIGENCES CONCERNANT LES PRATIQUES D'HORODATAGE

6.1 DECLARATION DES PRATIQUES D'HORODATAGE DE L'OSH ET RESUME PUBLIABLE DES POLITIQUES

6.1.1 Déclaration des Pratiques d'Horodatage (DPH) de l'OSH

L'AH peut démontrer qu'elle possède la fiabilité nécessaire pour la fourniture de service d'horodatage.

En particulier :

- L'OSH dispose d'une DPH décrivant les procédures utilisées pour assurer sa conformité à toutes les exigences identifiées dans la présente PH ;
- La DPH, de nature confidentielle, est la propriété de l'OSH ;
- La DPH identifie les obligations de tous les organismes externes sur lesquels s'appuient ses services. Ces obligations comprennent les politiques et pratiques applicables ;
- La DPH contient les modalités des éventuels audits effectués par une entité d'audit indépendante ;
- La DPH, ainsi que toute information pertinente, est rendue disponible à la Commission d'Approbation des Politiques (CAP) de l'AH afin de lui permettre d'estimer la conformité avec la politique et ainsi d'approuver ses pratiques ;
- L'AH fournit aux entités responsables des services demandeurs les conditions d'utilisation de ses services d'horodatage ;
- La CAP s'assure que les pratiques sont correctement mises en place ;
- L'AH définit un processus et les responsabilités associées pour la revue des pratiques d'horodatage ;
- L'OSH s'engage à informer la CAP de toute modification qu'il a l'intention d'effectuer dans sa DPH dans des délais suffisants, et à rendre immédiatement disponible la DPH révisée aux éventuelles entités effectuant des audits.

6.1.2 Résumé publiable des politiques

L'AH se réserve le droit de publier, en complément des éléments de la présente PH, un résumé des informations suivantes contenues dans la DPH de l'OSH :

- Le cadre d'application de la DPH :
  - Les coordonnées de l'AH ;
  - La PH appliquée ;
- La fonction de hachage utilisée pour constituer l'objet horodaté ;
- La durée de vie attendue des clés privées de signature utilisées pour signer le jeton d'horodatage ;
- La période de validité des clés privées utilisées pour signer les jetons d'horodatage ;
- La période d'activité des clés privées utilisées pour signer les jetons d'horodatage ;
- La précision de la date des jetons d'horodatage par rapport à l'échelle de temps UTC ;
- Les obligations des services demandeurs (cf. 5.3) ;
- Les obligations des utilisateurs finaux (cf. 5.4) ;
- Les informations permettant de vérifier le jeton d'horodatage (cf. 7.2) ;
- La périodicité de rétention des journaux de l'AH ;
- Les limitations de responsabilité.

1.2.250.1.8.1.1.1.4 –17/12/2003

6.2 CYCLE DE VIE DES CLES DE L'AH

6.2.1 Génération des clés de l'AH

L'AH s'assure que la génération des clés cryptographiques est effectuée en conformité avec les normes existantes en la matière.

En particulier :

- La génération des clés de signature de l'AH est réalisée dans un environnement physiquement sécurisé (voir section 6.5.4) par du personnel autorisé ayant des rôles définis ;
- La procédure de génération des clés de signature de l'AH est exécutée sous double contrôle (OSH et AH) et elle fait l'objet d'une trace systématique.
- Les propriétés du module cryptographique permettant la génération des clés de signature de l'AH sont parmi les suivantes :
    - La conformité aux exigences définies par le FIPS 140-1 Level 3 ou plus ; ou
    - La conformité aux exigences définies par le CEN Worfkshop Agreement 14167-2 ; ou
    - La conformité aux critères de sécurité EAL 4 ou plus, ou tout autre critère de sécurité équivalent.

  NOTE : En attente des textes réglementaires applicables à ce domaine, une dérogation précisée dans la DPH est accordée par l'AH à l'OSH pour la génération des clés de signature de l'AH.
- L'algorithme de génération des clés, la longueur des clés obtenue et l'algorithme de signature utilisés pour la signature des jetons d'horodatage sont en concordance avec l'état de l'art existant.

6.2.2 Protection des clés privées de l'AH

L'AH s'assure de la confidentialité des clés privées de signature et maintient leur intégrité.

En particulier :

- Les clés privées de signature de l'AH sont conservées et utilisées par un module cryptographique conforme à l'un des Critères suivants :
    - FIPS 140-1 Level 3 ou plus ;
    - CEN Worfkshop Agreement 14167-2 ;
    - EAL 4 ou plus, ou tout autre critère de sécurité équivalent.

  NOTE : En attente des textes réglementaires applicables à ce domaine, une dérogation précisée dans la DPH est accordée par l'AH à l'OSH pour la conservation et l'utilisation des clés de signature de l'AH.

Il n'existe pas de copie de sauvegarde des clés privées de l'AH.

6.2.3 Distribution des clés publique de l'AH

L'AH s'assure de l'intégrité et de l'authenticité de ses clés publiques de signature, ainsi que du maintien de tous les paramètres associés à ces clés lors de sa mise à disposition aux services demandeurs.

Les clés publiques de signature sont rendues disponibles aux services demandeurs au moyen de certificats de clés publiques.

1.2.250.1.8.1.1.1.1.4 –17/12/2003

6.2.4 Renouvellement des clés de l'AH

La durée de vie des bi-clés d'horodatage de l'AH, qui correspond à la durée de vie du certificat associé, est de 4 ans.

La période d'activité des clés privées d'horodatage de l'AH, qui correspond à la période durant laquelle les clés privées d'horodatage de l'AH sont utilisées pour émettre des jetons dans le cadre de la présente PH, est de 1 an. Elle coïncide avec la période de renouvellement des clés de l'AH qui est également de 1 an.

6.2.5 Fin du cycle de vie des clés cryptographiques

L'AH s'assure que ses clés privées d'horodatage ne sont pas utilisées au-delà de la fin de leurs périodes d'activité. En fin de sa période d'activité, une clé privée de signature de l'AH est détruite sans possibilité de reconstruction. La partie publique, contenue dans le certificat d'horodatage, reste elle accessible.

Les procédures techniques et opérationnelles de l'OSH permettent la mise en place d'un nouveau bi-clé sur demande de l'AH.

6.2.6 Gestion du cycle de vie des UH utilisées pour la signature des jetons d'horodatage

L'AH assure la sécurité des modules cryptographiques (UH) durant leur cycle de vie.

En particulier, l'AH prend les mesures nécessaires visant à :

- Assurer que chaque UH utilisée pour la signature des jetons d'horodatage n'est pas modifié durant sa livraison ;
- Assurer que chaque UH utilisée pour la signature des jetons d'horodatage n'est pas altéré avant et lors de sa mise en fonction et lors de toute mise à jour ultérieure effectuée sur ce module ;
- Garantir que l'activation des clés de signature de l'AH dans chaque UH n'est réalisée que par du personnel autorisé ayant des rôles définis et au moins sous double contrôle (Cf. 6.2.1*)*, au sein d'un environnement physiquement sécurisé ;
- Assurer le fonctionnement correct des UH de signature des jetons d'horodatage ;
- Assurer que la clé privée de signature de l'AH conservée dans une UH est effacée à la fin du cycle de vie du module cryptographique.

6.3 PRODUCTION DES JETONS D'HORODATAGE

6.3.1 Jeton d'horodatage

L'AH s'assure que les jetons d'horodatage sont émis de manière sécurisée et qu'ils présentent une garantie suffisante de fiabilité de l'heure.

En particulier :

- Le jeton d'horodatage contient un identifiant de la PH ;
- Chaque jeton d'horodatage contient un identifiant unique ;
- La précision de l'heure contenue dans le jeton d'horodatage vis-à-vis de l'échelle de temps UTC est de plus ou moins une seconde ;
- Le jeton d'horodatage contient l'empreinte numérique de l'objet horodaté, cet objet étant fourni par le service demandeur.
- Les clés utilisées pour signer les jetons d'horodatage ne servent qu'à cet usage ;

1.2.250.1.8.1.1.1.4 –17/12/2003

- L'AH est identifiée dans le certificat d'horodatage contenu dans le jeton d'horodatage. Cette identification comprend :
  - Un identifiant du pays dans lequel l'AH est établi (champ DN du certificat).
  - Un identifiant de l'AH : La Poste en l'occurrence.
  - Un identifiant de l'UH.

6.3.2 Synchronisation avec l'UTC

L'AH s'assure de la précision de l'horloge des services d'horodatage vis-à-vis de l'échelle de temps UTC.

En particulier :

- Les propriétés du module de sécurité opérant l'horloge sont évaluées selon des critères de sécurité internationaux (critères de sécurité EAL 4 ou plus, ou tout autre critère de sécurité équivalent).

  NOTE : En attente de produits du marché conformes à ces critères et applicables à ce domaine, une dérogation est accordée par l'AH à l'OSH pour la sécurité de l'horloge de l'AH.

- L'AH s'assure que l'étalonnage de l'horloge des services d'horodatage de façon à ce que l'horloge ne dévie pas de la précision annoncée ;
- Les horloges sont protégées contre tout facteur pouvant impacter leur précision au-delà de la dérive maximale acceptée;

  NOTE : Les facteurs incluent notamment les dommages effectués par du personnel non autorisé, les dommages électriques ou électromagnétiques.

- L'AH s'assure de la détection de toute dérive par rapport à sa référence de temps. En cas de dérive des caractéristiques de précision de l'horloge des services d'horodatage par rapport cette échelle de temps, les jetons d'horodatage ne sont pas émis par l'AH ;
- Les entités responsables des services demandeurs sont averties par l'AH de toute dérive de l'horloge des services d'horodatage supérieure à une seconde par rapport à l'échelle de temps UTC.
- Les ajustements effectués par le Bureau International des Poids et Mesures concernant la synchronisation de l'échelle de temps UTC avec les échelles de temps UTC(k) sont pris en compte par l'AH (cas des sauts de seconde programmés). Les sauts de secondes (ajustements par rapport au temps UTC) programmés par le BIPM sont pris en compte.

6.3.3 Disponibilité du service

Pour accroître la disponibilité du service d'horodatage, l'AH dispose de plusieurs UH.

La disponibilité du service d'horodatage dépend du niveau de service souscris par le service demandeur. Ce niveau de service est défini au travers d'une convention de service ne faisant pas partie du cadre de la présente PH.

6.4 VALIDITE D'UN JETON D'HORODATAGE

6.4.1 Durée de validité d'un jeton d'horodatage

L'AH s'engage à ce que les jetons d'horodatage émis dans le cadre de la présente PH aient une durée de validité de 10 ans.

La validité d'un jeton d'horodatage est vérifiable de façon autonome par le service demandeur pendant la période de publication en ligne des CRLs délivrées par l'AC émettant les certificats d'horodatage de l'AH :

- La vérification d'un jeton d'horodatage s'effectue à partir des informations publiées par l'AC émettrice du certificat d'UH qu'il comprend ;

1.2.250.1.8.1.1.1.4 –17/12/2003

- Les CRLs de l'AC, qui comportent tous les certificats révoqués depuis le début de l'existence de l'AC, sont accessibles sur son site Internet pendant leur période de publication ;
- La période de vérification autonome d'un jeton d'horodatage par le service demandeur est au minimum de 3 ans après sa date d'émission.

Au-delà de cette période, le service demandeur peut s'assurer de la validité d'un jeton d'horodatage par requête expresse auprès de l'AH. Les conditions financières de traitement de cette requête faisant intervenir un huissier sont détaillées dans le contrat de service liant l'AH et le service demandeur.

6.4.2 Vérification d'un jeton d'horodatage par le service demandeur

La procédure de vérification de la validité d'un jeton d'horodatage, réalisée par le service demandeur à l'aide d'outils appropriés, doit au minimum permettre de garantir que :

- Le jeton d'horodatage émane bien des services d'horodatage de l'AH concernée par la présente PH en contrôlant :
  - La provenance du certificat d'horodatage (i.e. de l'AC émettrice par rapport à celle attendue).
  - La correspondance du champ OID du jeton d'horodatage (Champ *Policy* de *TSTInfo)* avec l'OID de la présente PH ;
- La signature apposée sur le jeton d'horodatage est correcte (vérification de l'intégrité du jeton d'horodatage) ;
- Les attributs du certificat d'horodatage sont bien spécifiques à l'horodatage.
- Le certificat d'horodatage est valide en contrôlant :
  - Sa non-révocation auprès de l'AC émettrice (interrogation de CRLs) ;
  - La signature apposée sur le certificat par l'AC émettrice (vérification de l'intégrité des données du certificat) ;
  - La période de validité du certificat ;
- Les certificats de l'ensemble de la chaîne de certification sont valides ;
- L'empreinte présente dans le jeton d'horodatage est bien celle des données présentées au Service d'horodatage.

6.5 GESTION ET EXPLOITATION DE L'AH

6.5.1 Gestion de la sécurité

L'AH s'assure que les procédures administratives et les procédures de gestion de l'OSH sont mises en œuvre, et correspondent aux normes et bonnes pratiques existant en la matière.

En particulier :

- L'AH assume la responsabilité de la fourniture du service d'horodatage au regard de la présente PH, quelles que soient les fonctions sous-traitées ;
- Les responsabilités des tierces parties auprès desquelles des fonctions de l'AH sont sous-traitées sont fixées contractuellement ;
- La gestion de la sécurité est maintenue à toute heure. Tout changement ayant un impact sur le niveau de sécurité fourni est approuvé par la CAP de l'AH ;
- Les contrôles de sécurité et les procédures opérationnelles concernant la fourniture du service d'horodatage sont documentés, mis en place et maintenus à jour ;
- L'AH s'assure que la sécurité des informations est assurée lorsque des fonctions de l'AH ont été sous-traitées à une autre organisation ou entité.

1.2.250.1.8.1.1.1.1 4 –17/12/2003

6.5.2 Classification des biens

L'AH réalise une classification de sécurité des biens (clés privées, …) et s'assure que les moyens de production ont été mis en place par rapport à cette classification.

En particulier l'AH maintient un inventaire de tous les biens et leur affecte des exigences de protection adéquates.

6.5.3 Sécurité du personnel

L'AH s'assure que les pratiques appliquées au personnel permettent d'apporter la crédibilité concernant les opérations de l'AH et de l'OSH. Le personnel employé par l'AH et l'OSH comprend le personnel engagé contractuellement pour réaliser certaines tâches sur lesquelles reposent les services d'horodatage. Le personnel impliqué dans le contrôle des services d'horodatage n'est pas nécessairement considéré comme du personnel de l'AH.

En particulier :

- L'AH et l'OSH emploient le personnel possédant les connaissances, l'expérience et les qualifications requises pour occuper les fonctions relatives à la fourniture du service. Les connaissances, l'expérience et les qualifications requises peuvent être obtenues par la formation, l'expérience actuelle ou une combinaison des deux ;
- Les rôles et responsabilités concernant la sécurité, spécifiés dans la politique de sécurité de l'OSH, sont documentés par des descriptions de postes. Les fonctions sensibles sur lesquelles repose la sécurité de l'exploitation de l'OSH sont clairement identifiées ;
- Les employés et prestataires externes de l'AH et de l'OSH possèdent le minimum de privilèges leur permettant d'accéder aux informations qui leur sont destinées. Les niveaux de privilèges sont accordés aux utilisateurs en fonction de la sensibilité de leur poste.

Les contrôles complémentaires suivants peuvent être appliqués par l'OSH :

- Le personnel ayant des responsabilités de direction des fonctions d'horodatage :
    - Possède des connaissances sur les techniques d'horodatage ;
    - Possède des connaissances sur les techniques de signature numérique ;
    - Possède des connaissances sur les mécanismes d'étalonnage et de synchronisation de l'horloge de l'AH avec l'UTC ;
    - Est familiarisé avec les procédures de sécurité appliquées au personnel ;
    - Possède l'expérience relative à la sécurité de l'information et l'estimation des risques.
- L'AH a pris les mesures adéquates visant à éviter tout conflit d'intérêt qui pourrait porter préjudice à l'impartialité dans la gestion de l'horodatage ;
- Les fonctions sensibles incluent les rôles ayant les responsabilités suivantes :
    - Responsable de la Sécurité des Systèmes d'Information (RSSI) de l'AH : La personne responsable du contrôle de la sécurité physique et fonctionnelle, de la mise en œuvre de la politique de sécurité, de l'analyse des journaux d'événements et de la remontée des incidents à l'autorité de sécurité compétente. Il participe également à l'initialisation des fonctions cryptographiques ;
    - Administrateurs (de l'OSH) : Les personnes responsables des services délivrés et de l'initialisation de ces services, de la supervision des actions des opérateurs, de la configuration des journaux et de la remontée des incidents au RSSI ;
    - Ingénieurs systèmes (de l'OSH) : Les personnes responsables de la mise en route, de la configuration, de l'administration et de la maintenance du système, et de la remontée des incidents de sécurité aux administrateurs ;

- Opérateurs (de l'OSH) : Les personnes responsables des opérations, de l'exploitation des services délivrés, de l'initialisation des fonctions cryptographiques et de la remontée des incidents de sécurité aux administrateurs.

- Les fonctions sensibles sont précisément définies par le RSSI ;
- Les procédures de recrutement du personnel de l'AH et de l'OSH comprennent les éléments suivants :
  - L'AH et l'OSH se renseignent sur le passé judiciaire des personnes qu'elle compte employer ;
  - Le personnel n'a pas accès à des fonctions sensibles sans que les vérifications nécessaires aient été effectuées.

6.5.4 Sécurité physique

L'AH s'assure que l'accès physique aux services critiques est contrôlé et que les risques physiques concernant ses biens sont minimisés.

En particulier :

- Les contrôles suivants sont appliqués aux services d'horodatage :
  - Les accès physiques aux moyens permettant de rendre les services d'horodatage sont limités aux seules personnes autorisées ;
  - Des contrôles empêchant la perte, l'altération ou la compromission des biens et l'interruption de l'activité sont mis en place ;
  - Des contrôles empêchant la compromission ou le vol des informations et des moyens de traitement des informations sont mis en place ;
- L'accès physique aux locaux hébergeant les UH est contrôlé et limité aux seules personnes autorisées ;
- Les contrôles complémentaires suivants sont appliqués aux services d'horodatage :
  - Les outils de gestion de l'horodatage sont opérationnels au sein d'un environnement protégeant les services de la compromission par des accès non autorisés aux systèmes ou aux données ;
  - Les locaux hébergeant les UH sont séparés des locaux hébergeant les moyens d'exploitation courants ;
  - Des contrôles de sécurité physique sont mis en place pour protéger les moyens mis en œuvre pour héberger les ressources du système, les ressources du système elles-mêmes et les moyens mis en œuvre pour opérer sur ces ressources ;
  - La politique de sécurité physique destinée aux services d'horodatage développe au minimum les points suivants :
    - les contrôles d'accès physiques,
    - la protection contre les désastres naturels,
    - la protection contre l'incendie,
    - les mesures à prendre en cas de défaillance des systèmes électriques ou électromagnétiques,
    - les mesures à prendre en cas d'effondrement des structures,
    - les mesures à prendre en cas de dégâts des eaux,
    - la protection contre le vol,
    - le recouvrement après sinistre.
  - Des contrôles protégeant de toute sortie hors-site les équipements, l'information, les médias et les logiciels relatifs aux services d'horodatage sont mis en place.

1.2.250.1.8.1.1.1.1.4 –17/12/2003

6.5.5 Sécurité d'exploitation

L'AH s'assure que les composantes du système d'horodatage de l'AH sont exploitées correctement et de façon sûre, en minimisant les risques de défaillance.

En particulier :

- L'intégrité des composantes du système d'horodatage de l'AH et des données est protégée contre les virus et les logiciels non autorisés ;
- Des comptes-rendus d'incident sont réalisés et des procédures de réponse à incident sont appliquées pour tout incident de sécurité ou de défaut de fonctionnement ;
- Les supports de stockage utilisés pour la conservation des enregistrements d'audit des composantes du système d'horodatage de l'AH sont exploités de façon sûre afin de protéger ces supports des dommages, du vol, et des accès non autorisés. Tout membre du personnel ayant des responsabilités de gestion est responsable de la planification et de la mise en place effective de la PH et des pratiques associées décrites dans la DPH ;
- Des procédures sont établies et mises en place pour chacune des fonctions sensibles et des fonctions administratives ayant une incidence sur la fourniture de l'horodatage ;

Traitement et sécurité des supports de stockage d'information

- Tous les supports de stockage d'information sont manipulés avec précaution en conformité avec les exigences définies par le schéma de classification de l'information (voir 6.5.2). Les médias contenant des données sensibles sont conservés de manière sûre.

Planification des systèmes

- Les demandes en termes de capacités sont contrôlées et des planifications concernant les futures exigences en termes de capacité sont effectuées de façon à s'assurer de la disponibilité des capacités.

Compte-rendu d'incident et réponse à incident

- L'AH s'engage à fournir une réponse rapide, opportune et coordonnée aux incidents afin de limiter les impacts provenant d'incidents de sécurité. Des comptes-rendus d'incidents sont effectués dès que possible après les incidents.

L'AH applique les contrôles additionnels suivants aux services d'horodatage :

Responsabilités et procédures d'exploitation

- Les responsabilités d'exploitation de la sécurité de l'AH incluent les éléments suivants :
    - Les procédures opérationnelles et les responsabilités associées ;
    - La définition de l'architecture de sécurité et moyens permettant de réaliser cette architecture ;
    - La protection contre les logiciels dangereux ;
    - L'entretien des locaux ;
    - La gestion des réseaux ;
    - Le contrôle actif des journaux d'événements, l'analyse et le suivi des événements ;
    - La sécurité de l'utilisation des supports ;
    - Le changement de données ou de logiciels ;
- L'exploitation de la sécurité est séparée des autres procédures d'exploitation ;
- Les procédures d'exploitation sont gérées par du personnel spécifique dédié à cette fonction. Dans le cas où elles seraient appliquées par du personnel non qualifié, les politiques, les rôles et les responsabilités appliqués sont également définis.

1.2.250.1.8.1.1.1.4 –17/12/2003

6.5.6 Zonage des locaux

Les locaux d'exploitation des services d'horodatage sont découpés en zones concentriques d'accès contrôlés. Les équipements opérationnels (Unités d'horodatage) contenant des clés de signature sont situés dans la zone réputée la plus sensible. L'accès à une zone de plus grande sensibilité ne peut se faire que par une zone de sensibilité immédiatement inférieure.

6.5.7 Gestion des accès aux composantes du système d'horodatage de l'AH

L'OSH s'assure que l'accès aux composantes du système d'horodatage de l'AH est limité aux seules personnes autorisées.

En particulier :

- Des contrôles sont mis en place afin de protéger le réseau d'accès aux unités d'horodatage des accès non autorisés des services demandeurs et des tiers ;
- L'OSH assure une administration effective des accès des utilisateurs (qui comprennent les opérateurs, les ingénieurs systèmes et les administrateurs) afin de garantir la sécurité des composantes. L'administration des accès des utilisateurs comprend la gestion des comptes utilisateurs, l'audit, la modification et la suppression des accès ;
- L'OSH s'assure que l'accès aux informations et aux fonctionnalités systèmes sensibles est défini en accord avec la politique de contrôle d'accès ;
- Les contrôles mis en place par l'OSH permettent de garantir la séparation des fonctions sensibles définie dans la DPH, comme la séparation de l'administration de la sécurité et de l'exploitation. En particulier, l'exploitation des logiciels utilitaires systèmes est restreinte et fortement contrôlée ;
- Le personnel de l'OSH est identifié et authentifié avant toute réalisation de fonctions critiques relatives à l'horodatage ;
- L'OSH met en place des mesures permettant d'effectuer des contrôles a posteriori sur l'utilisation par le personnel des applications critiques relatives à l'horodatage. Ces mesures comprennent :
    - L'identification des applications ;
    - L'authentification du personnel ;
    - Les contrôles d'accès aux applications ;
    - La journalisation des événements relatifs aux applications.

L'OSH applique les contrôles complémentaires suivants aux services d'horodatage :

- L'OSH s'assure que les composantes réseau sont conservées dans un environnement sécurisé et que leur configuration est périodiquement auditée pour assurer la conformité avec les exigences de l'AH ;
- Des mécanismes d'alerte et de contrôle permanent permettent à l'OSH de détecter, d'enregistrer et de réagir à toute tentative irrégulière d'accès à ses ressources.

6.5.8 Maintenance et déploiement de l'AH

Les services critiques nécessitant des systèmes de confiance et les niveaux d'assurance requis sont identifiés par une analyse des risques (voir 6.1.1).

En particulier :

- Les projets de développement des systèmes de l'AH contiennent une analyse des exigences de sécurité ;
- Les procédures de contrôle des changements sont appliquées pour toute modification, mise en place d'une nouvelle version ou mise en place de correctifs pour tout logiciel d'exploitation.
- Le processus de gestion en configuration du cœur cryptographique de l'AH permet d'en assurer une maintenance suivie. La première fois qu'il est chargé, un contrôle est opéré pour garantir qu'il :

1.2.250.1.8.1.1.1.1.4 –17/12/2003

- vient de la société qui l'a mis au point ;
- n'a pas été modifié avant d'être installé ;
- correspond bien à la version voulue.

- L'AH doit prévoir un mécanisme permettant de vérifier périodiquement l'intégrité des logiciels.
- L'AH doit également mettre en place des mécanismes et (ou) des politiques lui permettant de contrôler et de surveiller la configuration du système de l'AH.
- Toute évolution est documentée et doit apparaître dans les procédures de fonctionnement interne et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.
- La procédure de maintenance des composantes sensibles (*accès par des opérateurs de maintenance, voire sortie physique du site*), assure la protection des informations confidentielles contre tout risque de divulgation.

6.5.9 Mesures à prendre en cas de compromission

En cas d'événement affectant la sécurité des services de l'AH, comme la compromission des clés privée de signature de l'AH ou une perte détectée de la précision de l'horloge de l'AH, l'AH s'assure que l'information appropriée est fournie aux entités responsables des services demandeurs.

En particulier :

- Le plan de reprise après sinistre concerne la compromission, la suspicion de compromission des clés privée de signature de l'AH et la perte de la précision de l'horloge de l'AH, qui pourraient avoir affecté les jetons d'horodatage qui ont été émis ;
- Dans le cas d'un incident majeur de l'exploitation de l'AH, d'une suspicion de compromission ou de la perte de la précision de l'horloge de l'AH, l'AH doit rendre disponible une description des événements aux entités responsables des services demandeurs, avec l'accord de l'OSH pour ce qui la concerne ;
- Dans le cas d'un incident majeur de l'exploitation de l'AH, d'une suspicion de compromission ou de la perte de la précision de l'horloge de l'AH, l'AH n'émet pas de jetons d'horodatage avant la résolution définitive de l'incident ;
- Dans le cas d'un incident majeur de l'exploitation de l'AH ou de la perte de la précision de l'horloge de l'AH, l'AH doit rendre disponible aux entités responsables des services demandeurs toute information permettant d'identifier les jetons ayant été affectés ;
- L'OSH met en place une datation des journaux d'anomalies de fonctionnement ou d'événements remarquables relatifs à l'émission des jetons d'horodatage. Cette datation est réalisée au moyen d'une horloge distincte de l'horloge de l'AH, et en synchronisation avec l'horloge de l'AH selon une précision dépendant du niveau d'assurance et du volume de jetons émis durant une période de 2 ans. En conséquence, en cas de compromission des clés privée, les journaux d'audits concernant l'émission des jetons d'horodatage par l'AH peuvent être examinés de façon à distinguer la période de temps critique durant laquelle des jetons d'horodatage ont été émis.

6.5.10 Fin du cycle de vie de l'AH

En cas de cessation des services d'horodatage, l'AH continue à maintenir l'information requise pour vérifier l'exactitude des jetons d'horodatage, dans un délai de 2 ans.

En particulier :

- Avant de fermer ses services d'horodatage, les procédures suivantes sont appliquées :
  - L'AH rend disponible aux entités responsables des services demandeurs toute modalité concernant la fin de ses activités (date prévue de fin d'activité, etc.) ;
  - Les autorisations données aux sous-traitants de l'AH intervenant dans le processus de création des jetons d'horodatage sont révoquées ;

1.2.250.1.8.1.1.1.1.4 –17/12/2003

- L'AH prend les mesures nécessaires afin de :
  - soit continuer à assurer les fonctions de vérification de la validité des jetons d'horodatage,
  - soit transférer contractuellement les fonctions permettant cette vérification ;
- L'AH prend les mesures nécessaires afin de continuer à rendre disponible ses clés publiques ;
- Les clés privées, sont détruites de manière à rendre impossible leur recouvrement ;

- L'AH prend les dispositions financières permettant de couvrir les frais relatifs à ces exigences ;
- Les pratiques de l'AH prévoient les mesures à prendre à la fermeture des services. Ces mesures comprennent :
  - La notification des entités affectées ;
  - La transmission des obligations de l'AH à d'autres parties.

6.5.11 Données enregistrées par l'AH

L'AH s'assure que toute donnée concernant l'exploitation des services d'horodatage est enregistrée pour une période de 2 ans, en particulier pour fournir des preuves légales.

En particulier :

Général

- Les événements et les données enregistrées sont documentés par l'AH ;
- L'AH assure la confidentialité et l'intégrité des enregistrements concernant l'exploitation des services d'horodatage ;
- L'AH met en place les moyens permettant d'assurer la confidentialité des enregistrements concernant l'exploitation des services d'horodatage ;
- Les enregistrements concernant les services d'horodatage peuvent être rendus disponibles pour des raisons légales ;
- Les heures précises des événements relatifs à l'environnement de l'AH, à la gestion des clés et à la synchronisation de l'horloge sont enregistrées ;
- Les enregistrements concernant les services d'horodatage sont conservés durant une période définie après expiration de la validité des clés de signature de l'AH afin de permettre des vérifications pour raisons légales ;
- Les événements sont enregistrés de façon à être difficilement effacés ou détruits (excepté s'ils sont transférés de façon sûre sur des supports de stockage de longue durée) durant la période de temps pendant laquelle ces enregistrements sont conservés. Cela peut être obtenu, par exemple par l'enregistrement de chacun des supports amovibles ou l'utilisation de site de sauvegarde hors-site.
- La confidentialité de toute information enregistrée concernant les services demandeurs est assurée à moins qu'un accord ait été obtenu concernant sa plus large diffusion.

Gestion des clés de l'AH

L'AH assure l'enregistrement des événements relatifs :

- Au cycle de vie des clés de l'AH ;
- Au cycle de vie du certificat de l'AH.

1.2.250.1.8.1.1.1.1 4 –17/12/2003

Synchronisation de l'horloge

- Les événements relatifs à la précision de l'horloge de l'AH vis-à-vis de l'échelle de temps UTC sont enregistrés. Ces enregistrements contiennent l'information relative au re-étalonnage ou la synchronisation de l'horloge vis-à-vis des échelles de temps UTC(k) ;
- Les événements relatifs à la détection de perte de synchronisation sont enregistrés.

6.6 ORGANISATION DE L'AH

L'AH s'assure que son organisation satisfait les exigences suivantes :

- L'AH s'engage à rendre ses services accessibles à tous ceux dont l'activité cadre avec son domaine d'exploitation et qui reconnaissent se soumettre aux obligations qui leur incombent et qui sont spécifiées dans le présent document ;
- L'AH possède un ou plusieurs systèmes de gestion de la qualité et de la sécurité des informations appropriés aux services d'horodatages ;
- L'AH a spécifié dans un contrat d'assurance les moyens lui permettant de supporter les risques liés à son exploitation et défini les responsabilités financières associées ;
- L'AH a la stabilité financière et les ressources requises pour exploiter le système d'horodatage conformément à cette politique ;

  NOTE : Ceci comprend les exigences concernant la fin de vie de l'AH (6.5.10).

- L'AH emploie suffisamment de personnes ayant les connaissances requises pour effectuer le type de travail nécessaire à la fourniture de service d'horodatage ;

  NOTE : Le personnel employé par l'AH comprend les personnes engagées contractuellement pour réaliser des fonctions sur lesquelles s'appuient les services d'horodatage de l'AH. Le personnel seulement engagé pour contrôler les services n'a pas la nécessité d'être considéré comme du personnel de l'AH.

- L'AH a des politiques et des procédures pour la résolution des réclamations et des contestations reçues des consommateurs ou d'autres parties concernant la fourniture du service d'horodatage ;
- L'AH a mis en place et documenté les accords et contrats la liant à des sous-traitants ou d'autres parties tierces.

1.2.250.1.8.1.1.1.1 4 –17/12/2003

6.7 CONTROLES DE CONFORMITE

Les mesures de contrôle décrites dans le présent chapitre s'appliquent aux composants du service d'horodatage sur lesquels La Poste s'appuie dans le cadre de la fourniture des Services Électroniques de Confiance. Les contrôles de conformité sont réalisés annuellement. Ils visent à s'assurer du respect des pratiques énoncées dans la DPH. La CAP de La Poste dans le cadre des Services Électroniques de Confiance désignera un organisme d'audit afin de procéder au contrôle de conformité. La société de l'auditeur ne doit pas avoir d'activité directement concurrente à celle de l'opérateur et éventuellement à celle du Service Demandeur. L'Opérateur des services d'horodatage a un droit de premier refus. Le cas échéant, la CAP lui proposera une liste de trois autres auditeurs, dans laquelle l'OSH devra choisir. L'organisme d'audit communique ses résultats à la Commission d'Approbation des Politiques (CAP). L'organisme d'audit désigné par la CAP rend un rapport qui fait apparaître le degré de conformité aux normes en vigueur et aux exigences de La Poste décrites dans la présente PH. La CAP prend les mesures adaptées au résultat de l'audit, à savoir :

- **en cas d'échec**, et selon l'importance des non-conformités, elle prend des sanctions. Les sanctions peuvent aller de la mise en demeure à effectuer immédiatement les modifications nécessaires, à la résiliation du contrat qui la lie à ses opérateurs ;
- **en cas de résultat « À confirmer »**, elle remet à la composante un avis précisant sous quel délai les non-conformités sont réparées. Puis, un contrôle de « Confirmation » permettra de vérifier que tous les points critiques ont bien été résolus ;
- **en cas de réussite**, elle remet à la composante contrôlée un avis d'autorisation d'exercice de sa fonction.

1.2.250.1.8.1.1.1.1 4 –17/12/2003

7. ADMINISTRATION DE LA POLITIQUE D'HORODATAGE

7.1 PROCEDURES DE MODIFICATION DE LA POLITIQUE D'HORODATAGE

La présente PH sera réactualisée selon besoin, après validation de la Commission d'Approbation des Politiques.

Les corrections d'erreurs ou changements suggérés à lecture de ce document sont à adresser à la Commission d'Approbation des Politiques à l'adresse mentionnée au chapitre 3.4.

7.2 PROCEDURES DE PUBLICATION ET DE NOTIFICATION

La présente PH est disponible sur le site de La Poste à l'URL suivante : www.laposte.fr/lre.

1.2.250.1.8.1.1.1.4 –17/12/2003