Service d'horodatage électronique de La Poste

Politique d'Horodatage La Poste

Résumé

Le présent document constitue la Politique d'Horodatage électronique de La Poste et définit les exigences techniques, organisationnelles et juridiques de l'Autorité d'Horodatage de La Poste, conformément aux exigences [PH-TYPE], [ETSI-PH] et [ANSSI-QTSP]. L'objet de la présente Politique d'Horodatage est de formaliser les engagements de l'AH. Cette Politique d'Horodatage, qui définit donc les « objectifs et les engagements » de l'AH pour assurer la fiabilité des services d'horodatage fournies, est un document public accessible librement par les services demandeurs et les utilisateurs finaux. La PH fait partie du référentiel documentaire de la Politique de Sécurité des Systèmes d'Information de La Poste (PSSI-G).

Version

Statut	Approuvé
Version	7.3
OID	1.2.250.1.8.1.1.1.1.7
Date d'enregistrement	25/09/2020
Responsable du document	Direction des Systèmes d'Information Groupe (DSI-G)
Valideur (s)	Direction des Systèmes d'Information Groupe (DSI-G) Direction des Systèmes d'Information Branche Service Colis Courrier (DSI-BSCC)
Approbateur (s)	Comité d'Approbation des Politiques et Homologation (CAPH)
Nom fonctionnel	Politique d'Horodatage de La Poste

Sommaire

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. Objectifs généraux

L'horodatage électronique est un service de sécurité qui permet d'attester que des données sous forme électronique existaient bien à un instant donné. Ce service contribue à d'autres services à valeur ajoutée (lettre recommandée électronique, validation de dépôt d'une offre dans le cadre d'un appel d'offre, etc.).

Ce service consiste à associer à une représentation sans équivoque des données concernées, un instant dans le temps suivant une précision prédéfinie par rapport au temps universel.

Cette association est réalisée à travers un mécanisme de signature numérique, la « représentation sans équivoque » des données concernées étant réalisé grâce à un algorithme de hachage. Les données ainsi horodatées peuvent être de n'importe quel type (texte brut, fichier bureautique, document électronique comportant une signature électronique, fichier multimédia, etc.), le type dépendant du service à valeur ajoutée qui s'appuie sur l'horodatage électronique.

L'horodatage électronique est réalisé sous le contrôle et sous la responsabilité d'une « Autorité d'Horodatage » (AH). Techniquement, l'horodatage électronique est réalisé par une ou plusieurs « Unité d'Horodatage » (UH), comportant chacune un « module d'horodatage ». Les unités d'horodatage sont mises en œuvre par un « Opérateur de Services d'Horodatage » (OSH), qui peut être interne ou externe à l'AH. Quelle que soit l'organisation retenue, l'AH reste responsable vis-à-vis des utilisateurs du service d'horodatage électronique rendu.

Le service d'horodatage électronique est sollicité par des « services demandeurs » qui ont en charge la fourniture, à leurs « utilisateurs finaux », des services à valeur ajoutée qui intègrent le service d'horodatage électronique.

Ainsi, l'AH est en relation directe avec les services demandeurs, et indirectement avec les utilisateurs finaux.

Un service d'horodatage est un service électronique de confiance. Il est nécessaire que les services demandeurs et, indirectement, les utilisateurs finaux puissent avoir confiance dans l'AH pour la fourniture de services d'horodatage fiables.

Cette fiabilité nécessite la mise en œuvre de moyens techniques, humains et organisationnels adéquats.

L'AH s'engage et est responsable vis-à-vis des services demandeurs sur la mise en œuvre des ces moyens.

L'objet de la présente Politique d'Horodatage est de formaliser ces engagements de l'AH. Cette Politique d'Horodatage, qui définit donc les « objectifs et les engagements » de l'AH pour assurer la fiabilité des services d'horodatage fournies, est un document public accessible librement par les services demandeurs et les utilisateurs finaux. Contractuellement, ce document engage l'Autorité d'Horodatage vis-à-vis des services demandeurs. Il appartient ensuite aux services demandeurs de retranscrire les éléments pertinents de la présente Politique d'Horodatage dans leurs propres relations contractuelles avec leurs utilisateurs finaux.

La présente Politique d'Horodatage est conforme au plan du document [ETSI-PH], au [RGS] et au règlement eIDAS.

2. Documents de référence

[ANSSI-QTSP]	*Services d'horodatage électronique qualifiés – Critères d'évaluation de la conformité au règlement eIDAS*, Version 1.1 du 3 janvier 2017
[ETSI-PH]	ETSI EN 319421 v1.1.1 – 03/2016 – Policy and security requirements for TSP issuing time-stamps
[ETSI-TSP]	ETSI EN 319422 v1.1.1 – 03/2016 – Time Stamping Protocol and Time Stamp token profile
[ETSI-TSP]	ETSI EN 319401 v2.2.1 – 04/2018 – General Policy Requirements for Trust Service Providers
[PC-UH]	*Politique de certification, Certificat de serveur, Authentification (Serveur & Client) / Cachet et UH*, réf.: DT-FL-0310/020, version 1.4 du 10 mars 2015. Certinomis. OID : 1.2.250.1.86.2.3.3.24.1
[PH-TYPE]	*Référentiel Général de Sécurité – Annexe A5 – PH Type*, version 3.0 du 27 février 2014
[RFC3161]	IETF – Time Stamp Protocol – 08/2001
[RGS]	*Référentiel Général de sécurité*, v.2.0.
[eIDAS PSC]	*Prestataires de services de confiance qualifiés - Critères d'évaluation de la conformité au règlement eIDAS* - Version 1.2 du 05 juillet 2017
[PCA]	Plan de continuité des activités des services de l'Horodatage

3. Définitions et abréviations

3.1. Définitions

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.

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 et Homologation (CAPH) - La CAPH 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.

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

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

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

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

Jeton d'horodatage - Voir contremarque de temps.

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

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

Prestataire de services d'horodatage (PSHE) – Un PSHE est un type de prestataire de services de confiance particulier. Un PSHE se définit comme toute personne ou entité qui est responsable de la génération et de la gestion de contremarques de temps, vis-à-vis de ses abonnés et des utilisateurs de ces contremarques de temps. Un PSHE peut fournir différentes familles de contremarques de temps correspondant à des finalités différentes ou des niveaux de sécurité différents. Un PSHE comporte au moins une AH mais peut en comporter plusieurs en fonction de son organisation. Un PSHE est identifié dans les certificats de clés publiques des UH dont il a la responsabilité au travers de ses AH.

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

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.

Système d'horodatage - Ensemble des unités d'horodatage et des composants d'administration et de supervision utilisés pour fournir des services d'horodatage.

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

UTC(k) - Temps de référence réalisé par le laboratoire "k" et synchronisé avec précision avec le temps UTC, dans le but d'atteindre une précision de ±100 ns, selon la recommandation S5 (1993) du Comité Consultatif pour la définition de la Seconde (Rec. ITU-R TF.536-1 [TF.536-1]).

Nota - Une liste des laboratoires UTC(k) est indiquée dans la section 1 de la Circulaire T publiée par le BIPM et est disponible sur le site web du BIPM (www.bipm.org).

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.

3.2. Abréviations

AC	Autorité de Certification
AH	Autorité d'Horodatage
CAPH	Commission d'Approbation des Politiques et Homologation
CGU	Conditions Générales d'utilisation du service d'Horodatage
DPH	Déclaration des Pratiques d'Horodatage
ETSI	European Telecommunications Standards Institute
LCR	Liste des Certificats Révoqués
IGC	Infrastructure de Gestion de Clés
OID	Object Identifier
OSH	Opérateur de Services d'Horodatage
PH	Politique d'Horodatage
PP	Profil de Protection
PSHE	Prestataire de service d'horodatage
RSSI	Responsable de la Sécurité des Systèmes d'Information

UH	Unité d'Horodatage
UTC	Coordinated Universal Time

4. Concepts généraux

4.1. Services d'horodatage

Les services d'horodatage se chargent d'émettre des jetons d'horodatage aux services demandeurs.

Un jeton d'horodatage est une structure signée numériquement et qui contient en particulier :

- l'identifiant de la Politique d'Horodatage sous laquelle le jeton d'horodatage a été généré ;
- la valeur de hachage et l'algorithme de hachage de la donnée qui a été horodatée ;
- la date et le temps UTC, suivant une précision sur laquelle l'AH s'engage ;
- l'identifiant du certificat de l'Unité d'Horodatage (UH) qui a généré la contremarque de temps (certificat qui identifie aussi l'AH).

La signature numérique est réalisée par un algorithme cryptographique asymétrique. Chaque UH dispose de sa propre bi-clé : la clé privée de signature est mise en œuvre au sein du module d'horodatage de l'UH, la clé publique est certifiée dans les conditions fixées par la présente PH.

Les services d'horodatage sont mis en œuvre par un « Opérateur de Services d'Horodatage » (OSH), sous la responsabilité de l'AH.

L'OSH a également en charge la surveillance et le contrôle du fonctionnement des services d'horodatage afin d'assurer la conformité avec les exigences et engagements de l'AH (synchronisation adéquate des horloges des modules d'horodatage avec le temps UTC, mise en œuvre des mesures de sécurité, etc.).

4.2. Prestataire de services d'horodatage

Le PSHE est La Poste.

En tant que prestataire de services de confiance particulier, La Poste est responsable de la génération et de la gestion de contremarques de temps vis-à-vis de ses abonnés et des utilisateurs de celles-ci.

4.3. Autorité d'Horodatage

L'AH a la complète responsabilité de la fourniture des services d'horodatage et de la conformité aux engagements définis dans le présent document.

Les clés de signature de l'AH sont utilisées, au sein des UH, 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.

L'AH est la DSI Courrier du groupe La Poste.

4.4. Service demandeur

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

Les services demandeurs utilisent ensuite ces jetons d'horodatage soit pour eux-mêmes, soit pour les fournir à leurs utilisateurs dans le cadre de services à valeur ajoutée. Les utilisateurs des services demandeurs sont appelés « utilisateurs finaux » dans le présent document.

4.5. Utilisateurs finaux

Les utilisateurs finaux sont les utilisateurs des services demandeurs. L'AH n'a pas de relations directes avec ces utilisateurs finaux.

4.6. Politique d'Horodatage et Déclaration des Pratiques d'Horodatage de l'AH

Une PH définit les engagements de l'AH en matière de niveau de service d'horodatage et de niveau de sécurité correspondant. Une PH identifie ainsi le « qu'est-ce qui est visé, quels sont les objectifs à atteindre », indépendamment de toute implémentation des services d'horodatage.

Une DPH identifie les pratiques d'horodatage qui doivent être mises en œuvre dans le fonctionnement des services d'horodatage. Une DPH identifie le « qu'est-ce qu'il faut faire » pour être conforme aux engagements pris dans la (ou les) PH applicables. Une DPH dépend de l'implémentation des services d'horodatage.

5. Politique d'Horodatage

5.1. Définition

La présente PH couvre les services d'horodatages fournis par La Poste.

5.2. 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 (x)}

Soit : **1.2.250.1.8.1.1.1.1.7**

Les jetons d'horodatage émis par les services d'horodatage de La Poste comportent l'OID ci-dessus.

5.3. Points de contact

5.3.1. Entité gérant la PH

Les questions relatives à la présente PH sont à adresser à :

Direction de la Cyber-Sécurité Groupe La Poste

9, RUE DU COLONEL PIERRE AVIA 75015 PARIS

direction.cyber@laposte.fr

5.3.1. Entité gérant l'AH

L'adresse de l'Autorité d'horodatage est la suivante :

Direction des Systèmes d'Information Courrier

111 boulevard Brune 75014 PARIS

ld-horodatage-mco@laposte.fr

5.4. Communauté d'utilisateurs et applicabilité

Les services demandeurs peuvent être internes (services ou filiales) ou externes au groupe La Poste, de même que les utilisateurs finaux.

5.5. Conformité

La Commission d'Approbation des Politiques et Homologation (CAPH) 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.

La CAPH approuve les nouvelles versions des politiques.

La CAPH se réunit aussi souvent que nécessaire, afin de valider toute nouvelle version d'un document de politique.

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

Les mesures de contrôle décrites ci-dessous 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 engagements pris dans la présente PH et des pratiques correspondantes énoncées dans la DPH.

L'AH, 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 des services demandeurs. L'Opérateur des Services d'Horodatage a un droit de premier refus. Le cas échéant, l'AH lui proposera une liste de trois autres auditeurs, dans laquelle l'OSH devra choisir.

L'organisme d'audit communique ses résultats à l'AH. L'organisme d'audit désigné 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. L'AH 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.

le PSHE dispose d'un PCA qui garantit aux clients utilisateurs du Service la continuité des Services de l'Horodatage de la Poste.

6. Obligations et responsabilités

6.1. Obligations de l'AH

6.1.1. Obligations générales

L'AH :

- s'assure que toutes les exigences détaillées dans les chapitres qui suivent sont mises en place ;
- garantit l'application des procédures découlant de 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 DPH, répondent complètement aux exigences de la PH ;
- s'engage à respecter la confidentialité des éléments précisés dans la DPH.

Concernant la génération des jetons d'horodatage, l'AH s'assure que l'OSH :

- Respecte et répond aux exigences de la présente PH telles que traduits dans la DPH ;
- Accepte les audits périodiques de contrôle de conformité par rapport à la présente PH réalisés par l'AH ou par des entités d'audit externes.

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 oeuvre 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 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.

6.1.2. Obligations vis-à-vis des services demandeurs

L'AH s'engage à respecter ses engagements vis-à-vis des services demandeurs tels que définis dans la présente PH et dans les Conditions Générales d'Utilisation (CGU) correspondantes.

6.2. Obligations des services demandeurs

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

L'archivage des jetons d'horodatage émis pour un service demandeur relève de la responsabilité dudit service demandeur. Par défaut, le service d'horodatage ne réalise aucun archivage des jetons d'horodatage produits. À la demande du client, moyennant des accords contractuels adéquats, le service d'horodatage peut fournir un service d'archivage des jetons d'horodatage générés.

6.3. Obligations des utilisateurs finaux

Les utilisateurs finaux n'ont pas d'obligation vis-à-vis de l'AH 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 dans la présente PH.

6.4. Responsabilités

Les responsabilités respectives de l'AH et des services demandeurs sont définies dans les Conditions Générales d'Utilisation (CGU) et dans chaque contrat entre La Poste et un service demandeur.

6.5. Conformité avec les exigences légales

6.5.1. Droit applicable

Le présent document est régi par la loi française.

6.5.2. Règlement des différends

Tout litige qui surviendrait concernant l'interprétation et l'exécution de la présente Politique d'Horodatage devra faire l'objet d'une tentative de règlement amiable. À défaut de règlement amiable, le litige sera soumis au droit français, et porté devant le tribunal compétent dans le ressort de la cour d'appel de Paris statuant en droit français.

6.5.3. Données nominatives

Les informations nominatives qui seraient contenues sur les plates-formes du service d'horodatage feront l'objet d'une déclaration auprès du Correspondant Informatique et Libertés (CIL) de La Poste.

7. Exigences concernant les pratiques d'horodatage

7.1. Déclaration des Pratiques d'Horodatage de l'OSH et conditions générales d'utilisation

7.1.1. Déclaration des Pratiques d'Horodatage (DPH) de l'AH

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

En particulier :

- Elle dispose d'une DPH décrivant les procédures utilisées pour assurer sa conformité à toutes les exigences identifiées dans la présente PH ;
- 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 et Homologation (CAPH) 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 ;
- L'AH 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 ;
- Toute entité intervenant dans la mise en œuvre des services d'horodatage s'engage à informer l'AH de toute modification qu'elle a l'intention d'effectuer dans ses pratiques dans des délais suffisants, et à rendre immédiatement disponible les éléments nécessaires à la mise à jour de la DPH.

7.1.2. Conditions Générales d'Utilisation

L'AH publie, en complément des éléments de la présente PH, des Conditions Générales d'Utilisation (CGU) comportant notamment les informations suivantes issues de la DPH :

- 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 minimum pendant laquelle il est possible de vérifier les jetons d'horodatage ;
- 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 ;
- Les obligations des utilisateurs finaux ;

- Les informations permettant de vérifier le jeton d'horodatage ;
- La périodicité de rétention des journaux de l'AH ;
- Les limitations de responsabilité.

Les CGU sont disponibles sur le site de Certinomis à l'URL suivante : https://www.certinomis.fr/nos-certificats-racines/nos-conditions-generales-dutilisation

7.2. Cycle de vie des clés de l'AH

7.2.1. 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 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 d'horodatage dans lequel est réalisée la génération des clés de signature de l'AH sont conformes aux exigences de la [PH-TYPE] et [ANSSI-QTSP]. En particulier, le matériel cryptographique est évalué CC EAL4+, (EAL4 augmenté par ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, ALC_FLR.3, AVA_VAN.5), rapport de certification : ANSSI-CC-2016/07.
- 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 conformes au minimum aux exigences du RGS pour les certificats de cachet serveur horodatage niveau 1*.

7.2.2. Protection des clés privées des UH

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 dans le même module d'horodatage que celui utilisé pour leur génération (*cf.* chapitre 7.2.1)

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

7.2.3. Distribution des clés publiques des UH

Les clés publiques d'UH sont distribuées au travers de certificats fournis par une AC qualifiée vis-à-vis du RGS pour les certificats cachet serveur horodatage au niveau 1* ou supérieur.

7.2.4. Renouvellement des clés des UH

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.

7.2.5. Fin du cycle de vie des clés des UH

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'une nouvelle bi-clé sur demande de l'AH.

7.2.6. Gestion du cycle de vie des modules d'horodatage utilisés pour la génération des jetons d'horodatage

L'AH assure la sécurité des modules d'horodatage (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.* 7.2.1), 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 d'horodatage.

7.2.7. Certification des clés de l'unité d'horodatage

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

L'Autorité d'Horodatage s'assure qu'une demande de certificat d'Unité d'Horodatage auprès d'une Autorité de Certification contient, en plus des informations exigées dans la PC Type « cachet » pour la partie enregistrement, au moins les informations suivantes :

- le nom (DN) de l'unité d'horodatage pour laquelle la demande de certificat est faite ;
- la valeur de la clé publique (et l'identifiant de l'algorithme) ;
- la durée d'utilisation souhaitée pour la clé privée.

L'Autorité d'Horodatage vérifie, lors de l'import du certificat de l'Unité d'Horodatage, qu'il provient bien de l'Autorité de Certification auprès de laquelle la demande de certificat a été effectuée. Cette vérification est effectuée dans le cadre de la cérémonie des clés de l'U.H.

L'Autorité d'Horodatage s'assure que l'Unité d'Horodatage ne peut être opérationnelle qu'une fois ces exigences remplies.

7.3. Production des jetons d'horodatage

7.3.1. 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 la seconde.

En particulier :

- Le jeton d'horodatage contient un identifiant de la PH (son OID : 1.2.250.1.8.1.1.1.1.7) ;
- 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 (une seconde) n'est pas indiquée dans le jeton d'horodatage ;
- 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 ;
- Le protocole utilisé pour les demandes et les réponses de fourniture de jetons d'horodatage est le protocole défini dans [RFC3161] et profilé dans [ETSI-TSP] ;
- 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.

7.3.2. Synchronisation des horloges 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 d'horodatage opérant l'horloge sont conformes aux exigences de la [PH-TYPE] et [ANSSI-QTSP] ;

  NOTE - Le matériel cryptographique utilisé est évalué CC EAL4+, (EAL4 augmenté par ADV_IMP.2, ALC_CMC.5, ALC_DVS.2, ALC_FLR.3, AVA_VAN.5), rapport de certification : ANSSI-CC-2016/07.

- 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 ;
- La précision par rapport au temps UTC est d'une seconde.
- 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 la précision annoncée par rapport au 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.

7.3.3. Vérification d'un jeton d'horodatage

La vérification d'un jeton d'horodatage est réalisable de façon autonome par le service demandeur pendant la période de publication en ligne des LCR 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 ;
- Les LCR 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 d'un an après sa date d'émission.

7.3.4. Procédure de vérification autonome d'un jeton d'horodatage

La procédure de vérification autonome d'un jeton d'horodatage 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 CRL) ;
  - 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.

7.3.5. Algorithmes de production du jeton d'horodatage

Les algorithmes suivants sont acceptés pour l'empreinte numérique des données horodatées (cette empreinte est réalisée par le demandeur et transmise dans la requête) :

- SHA-256 ;

- SHA-384 ;
- SHA-512.

Les contremarques de temps sont signées en utilisant des algorithmes et des longueurs de clés conformes à l'état de l'art et aux exigences de [ANSSI-QTSP] et [RGS]. Les biclés RSA des unités d'horodatage ont une longueur de 2048 bits. La signature des contremarques utilise une fonction de hachage de la famille SHA-2.

7.4. Gestion et exploitation de l'AH

7.4.1. Management de la sécurité

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

En particulier :

- L'AH réalise ou fait réaliser une évaluation de risques pour évaluer les actifs et les menaces pour ces actifs afin de déterminer les mesures de sécurité nécessaires et les procédures opérationnelles ;
- 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 CAPH 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 ;
- L'analyse de risques est revue et révisée tous les ans ;
- La direction du service d'horodatage approuve l'évaluation des risques et accepte les risques résiduels identifiés.

7.4.2. Classification et gestion des actifs

L'AH réalise une classification de sécurité des biens (clés privées, etc.) 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.

7.4.3. Sécurité liée au personnel

L'AH s'assure que les pratiques appliquées au personnel permettent d'apporter la crédibilité concernant les opérations de l'AH et s'assure que l'OSH fait de même pour son personnel. Le personnel impliqué dans les audits internes et externes des services d'horodatage n'est pas nécessairement 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 demandés par l'AH :

- 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 oeuvre 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.
  - Auditeurs de système : Les personnes autorisées à consulter les archives et les fichiers d'audit des modules d'horodatage.
- Les fonctions sensibles sont précisément définies par le RSSI ;
- Les tâches et les domaines de responsabilité conflictuels sont séparés pour réduire les possibilités de modification/utilisation non autorisées ou non intentionnelle des actifs.
- Des mises à jour sur les nouvelles menaces et pratiques de sécurité affectant le personnel sont effectuées au moins tous les 12 mois.

- Des sanctions disciplinaires appropriées seront appliquées au personnel qui enfreint les politiques et/ou procédures.
- 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.
- Les rôles sont validés par la direction de l'AH.

7.4.4. Sécurité physique et environnementale

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 oeuvre pour héberger les ressources du système, les ressources du système elles-mêmes et les moyens mis en oeuvre 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.

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.

7.4.5. Gestion de l'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 codes malveillants 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 7.4.2). 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 de celles-ci.

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 la résolution des 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.
- L'exploitation de la sécurité est séparée des autres procédures d'exploitation.
- L'AH vérifie que les correctifs de sécurité soient appliqués dans un délai raisonnable après leur mise à disposition. De même l'AH doit s'assurer que les dits correctifs ne soient pas appliqués s'ils entraînent des vulnérabilités ou instabilités supplémentaires qui l'emportent sur les avantages à les appliquer. L'AH documente les raisons pour lesquelles un correctif de sécurité n'a pas été déployé.
- L'AH traitera toute vulnérabilité critique dans un délai de 48h maximum. Toute vulnérabilité sera notifiée dans une analyse de risque ou dans un plan de réduction de risque et une mesure de reduction y sera associée.
- Les procédures de signalement et de réponse aux incidents sont utilisées de manière à ce que les dommages, consécutifs aux incidents de sécurité et dysfonctionnements soient minimisés.

7.4.6. Gestion des accès aux systèmes

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 création, 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 ;
- Les activités de surveillances sont mises en place par l'OSH et tiennent compte de la sensibilité de toute information collectée ou analysée.
- L'OSH surveille le démarrage et l'arrêt des fonctions de journalisation ainsi que la disponibilité et l'utilisation des services nécessaires au service.

- 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 demandes de service ;
  - Les contrôles d'accès aux applications ;
  - La journalisation des événements relatifs aux applications.
- L'OSH applique les même contrôles de sécurité à tous les systèmes colocalisés dans la même zone et restreint l'accès aux communications entre les zones au strict nécessaire. Cela inclut la désactivation ou l'interdiction des connexions aux services inutiles.
- L'OSH sépare les systèmes de production des systèmes utilisés dans le développement et les tests.
- L'OSH s'assure que la communication entre systèmes fiables est uniquement effectuée au travers de canaux de confiance qui sont logiquement distincts des autres canaux de communication . Les canaux de confiance permettent de garantir la protection des données transmises contre toute modification ou divulgation.
- L'OSH garantit un niveau élevé de disponibilité de l'accès externe au service de confiance via la mise en place de technologies permettant la redondance du service en cas de défaillance unique.
- L'OSH effectue une analyse de vulnérabilité régulière sur les adresses IP publiques et privées identifiées pour le service et enregistre les preuves de ces analyses (sous forme de rapports). L'OSH s'assure également que ces tests sont réalisés par une personne habilitée, compétente et indépendante et en conserve la preuve.
- L'OSH subit un test de pénétration sur ses systèmes à l'installation du service et après les mises à niveau ou modifications d'infrastructure qu'il juge importantes.

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

- L'OSH s'assure que les composants réseaux sont conservées dans un environnement sécurisé et que leur configuration est périodiquement auditée pour assurer la conformité avec les exigences de l'AH.

7.4.7. 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.Déploiement et maintenance de systèmes fiables

Les services critiques nécessitant des systèmes de confiance et les niveaux d'assurance requis sont identifiés par une analyse des risques (voir 7.4.1).

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 :
  - provient 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.

7.4.8. Compromission des services de l'AH

En cas d'événement affectant la sécurité des services de l'AH, comme la compromission des clés privées des unités d'horodatage 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 privées des unités d'horodatage 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'AH prévient également directement et sans délai l'ANSSI.
- 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.
- Lorsque l'atteinte à la sécurité ou la perte d'intégrité est susceptible de nuire à une personne à qui le service de confiance a été fourni, l'AH notifie la personne physique ou morale de la violation de la sécurité ou de la perte d'intégrité dans les plus bref délais.

7.4.9. Fin 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 ;
  - 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.

Tous les supports sont manipulés en toute sécurité conformément aux exigences de la classification des informations. Les supports contenant des données sensibles sont éliminés en toute sécurité lorsqu'ils ne sont plus nécessaires. L'AH a établi un document décrivant les pratiques de fin de vie de l'AH.

7.4.10. Conformité avec les exigences légales et règlementaires

L'AH est établie sur le territoire français. La présente PH est régie par le droit français.

Les informations nominatives qui seraient contenues sur les plates-formes du service d'horodatage feront l'objet d'une déclaration auprès du Correspondant Informatique et Libertés (CIL) de La Poste.

Afin d'assurer la conformité des services d'horodatage avec les exigences légales et règlementaire, l'AH peut s'appuyer sur les expertises juridiques nécessaires, internes ou externes au groupe La Poste.

7.4.11. Enregistrement des informations concernant l'exploitation des services d'horodatage

L'AH s'assure que toute donnée concernant l'exploitation des services d'horodatage est enregistrée pour une période de 10 ans.

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.

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 réétalonnage 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.

7.5. 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'horodatage ;
- 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 ;

  Remarque : Ceci comprend les exigences concernant la fin de vie de l'AH (cf. 7.4.9).

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

  Remarque : 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.
- Les pratiques de l'AH et de l'OSH sont non discriminatoires

7.6. Politique de sécurité

L'AH et le PSHE s'assurent que les exigences suivantes concernant la Politique de Sécurité sont appliquées :

- Les modifications à la politique de sécurité de l'information seront communiquées aux abonnés, parties de confiance, organismes d'évaluation, autorité de surveillance et organismes de réglementation.
- L'AH publiera et communiquera la politique de sécurité de l'information à tous les employés qui en sont affectés.
- L'AH prévoit de revoir la politique de sécurité de l'information et l'inventaire des actifs de sécurité au moins une fois par an. L'AH prévoit également de revoir ces éléments en cas de changement majeurs.
- L'AH s'assure que l'intervalle maximum entre deux vérification est documenté dans la DPH.

8. Administration de la Politique d'Horodatage

8.1. Procédures de modification de la Politique d'Horodatage

La présente PH est réactualisée selon le besoin, après validation de la Commission d'Approbation des Politiques et Homologation.

Les corrections d'erreurs ou changements suggérés à lecture de ce document sont à adresser à la Commission d'Approbation des Politiques et Homologation à l'adresse mentionnée au chapitre 5.3.1.

Dans le cas où l'AH serait certifiée conforme au [RGS], si une modification envisagée à l'initiative de l'Autorité d'horodatage pouvait entraîner une non-conformité avec la politique d'horodatage [PH-TYPE] ou avec la déclaration des pratiques d'horodatage, alors l'Autorité d'horodatage soumettra cette modification à l'organisme évaluateur indépendant pour avis.

De même, toute modification susceptible d'entraîner un écart par rapport aux exigences de [ANSSI-QTSP] fera l'objet d'une soumission pour avis par l'Autorité d'horodatage à l'organisme évaluateur indépendant et à l'organe de contrôle au sens du règlement eIDAS.

8.2. Procédures de publication et de notification

La présente PH est disponible sur le site de Certinomis à l'URL suivante :

https://www.certinomis.fr/nos-certificats-racines/nos-politiques-de-certification.

En cas de changement de la PH ayant un impact sur les utilisateurs et abonnés du service, ceux-ci sont avertis au moins un mois à l'avance de la nature et la portée de ces changements à travers la publication, sur le site ci-dessus, de la future version de la PH.

8.3. Organisme indépendant de contrôle de conformité

À la date de rédaction de la présente PH, l'organisme de qualification indépendant retenu pour valider la conformité de la PH avec les exigences du R.G.S. et au sens de l'article 42 du Règlement N° 910/2014 du Parlement européen et du conseil du 23 juillet 2014 (règlement eIDAS).est la société LSTI (453 867 863 RCS Saint-Malo).

9. Profils des certificats et des contremarques de temps

9.1. Profil des certificats

9.1.1. Champs de base

Les parties du profil marquées comme « *XXX* » dépendent de l'unité d'horodatage et les parties du profil marquées comme « ZZZ » dépendent de l'AC.

Champ	Valeur
Version	3
Numéro de série	défini par l'AC
Signature	sha256WithRSAEncryption
Issuer DN	CN = Certinomis - Prime CA OU = 0002 433998903 O = Certinomis C = FR
Validité	4 ans
Subject DN	CN = LA_POSTE_UNITE_HORODATAGE_ 81610_0050000XXX_XXX SERIALNUMBER = 50063IGB106 OU = 0002 356000000 2.5.4.97 = NTRFR-356000000 O = LA POSTE - DSI COURRIER L = PARIS S = 75 C = FR
Clé publique	RSA 2048 bits

9.1.2. Extensions

X509v3 Basic Constraints:	CA:FALSE
X509v3 Key Usage: (critical)	Digital Signature
X509v3 Extended Key Usage: (critical)	Time Stamping
X509v3 Authority Key Identifier:	keyid:70:89:80:FC:13:B5:74:C3:BF:3E:99:8C:4B:52:84:30:9E:30:ED:9E
X509v3 Subject Key Identifier:	Dépend de l'UH (keyid)
X509v3 CRL	URI:http://crl.igc-

Distribution Points:	g3.certinomis.com/INSTANCE_SHA2/crl/AC_PRIME-crl-1.crl URI:http://www.certinomis.com/crl/acg3-PRIME.crl
Authority Information Access:	OCSP - URI:http://igc-g3.certinomis.com/INSTANCE_SHA2/ocsp/OCSP_PRIME
X509v3 Subject Alternative Name:	DirName:/CN=LA_POSTE_UNITE_HORODATAGE_ *XXX*_ *XXX*
X509v3 Certificate Policies: Policy:	1.2.250.1.86.2.3.3.24.1

9.2. Profil des contremarques de temps

generation time	Date de l'horodatage
nonce	Valeur incluse dans la requête, si présente
policy	1.2.250.1.8.1.1.1.1.7
serial number	Numéro de série de la contremarque
accuracy	(absent)
gentimeaccuracy	(absent)
messageimprint	Empreinte des données et OID de l'algorithme utilisé (voir ci-dessous)

Les OID des algorithmes d'empreinte pouvant apparaître dans le champ « imprint alg oid » sont les suivants :

SHA256	2.16.840.1.101.3.4.2.1
SHA384	2.16.840.1.101.3.4.2.2
SHA512	2.16.840.1.101.3.4.2.3