Identification du document

Nom / référence	Politique d'Horodatage
Objet	Politique et pratiques d'horodatage

Auteur / propriétaire	Rémi BLANCHER
Relecteur	Olivier CLEF, Michaël FRANCK
Version actuelle	1.3
Statut actuel	Publié
Destinataire de l'information	Public
Date d'application	06/05/2023
Périodicité de contrôle	1 fois par an

Historique des versions

Révision	Nbr de pages	Objet de la modification	Date
1.0	34	Version initiale du document	23/05/2023
1.1	34	Modification suite à Audit interne : - Précision sur règles de non-cumul des rôles	11/07/2023
1.2	34	Modification des références de chapitre	17/08/2023
1.3	34	Mise à jour URL du site de publication	10/10/2023

Table des matières

1. Introduction

1.1. Présentation générale

APP Solutions (ci-après nommée « la Société ») est un tiers de confiance spécialisé dans la protection d'actifs immatériels.

Afin de répondre aux besoins, tant internes que de ses clients, APP Solutions a mis en place une solution d'horodatage électronique.

L'horodatage électronique est un service qui permet d'attester que des données sous forme électronique existaient bien à un instant donné.

Le présent document constitue la Politique d'Horodatage (ci-après « PH ») du service « VAULTINUM TIMESTAMPING » proposé par « la Société », ainsi que la Déclaration des Pratiques d'Horodatage (DPH) associées à sa mise en œuvre.

La présente politique vise à être conforme aux référentiels suivants :

- Référentiels ETSI EN 319401 et ETSI EN 319421,
- Référentiels de qualification des services de confiance de l'ANSSI.

Cette conformité permet de viser la reconnaissance du service par l'ANSSI comme service d'horodatage électronique qualifié au sens du Règlement eIDAS.

L'objectif de ce document est de définir les engagements pris par « la Société », en tant que fournisseur de services de confiance (Trust Service Provider au sens eIDAS) et qu'Autorité d'Horodatage (AH), pour la délivrance et la gestion de contremarques de temps et de définir les obligations des autres participants. Ce document décrit les moyens déployés pour atteindre les objectifs de sécurité du service d'horodatage, en particulier les mécanismes qu'une unité d'horodatage emploiera pour la création des contremarques de temps et le maintien de l'exactitude des horloges.

L'Autorité d'Horodatage met en œuvre plusieurs Unités d'Horodatage pour supporter son service d'horodatage.

Le présent document reprend le plan de la politique d'horodatage type du RGSv2 de l'ANSSI.

Le présent document spécifie l'ensemble des engagements pris par l'Autorité d'Horodatage et spécifie l'ensemble des politiques et pratiques appropriées à la fourniture du service.

1.2. Identification du document

La présente Politique d'Horodatage (PH) est dénommée « Politique d'Horodatage APP SOLUTIONS ».

Elle est identifiée par un numéro d'identifiant unique (OID) : 1.3.6.1.4.1.60053.2.1.1.1.1

1.3. Publication du document

Le présent document est publié sur une page accessible à l'URL suivante https://vaultinum.com/fr/publication-autorite-horodatage.

Le site de publication comporte également :

- Les Conditions Générales d'Utilisation à destination des utilisateurs ;
- Les certificats des unités d'horodatage ;
- Les éventuelles certifications de conformité obtenues.

Il est à noter que les informations confidentielles de la Déclarations des Pratiques d'Horodatage (DPH) ne sont pas publiées.

Le document ne peut être publié qu'après approbation du document par le comité de Direction de « la Société » (voir Gestion de la politique).

Le document est également communiqué aux employés et à une liste de tiers définie dans la DPH confidentielle.

L'accès en écriture au site de publication est réservé aux personnes habilitées avec une authentification à deux facteurs.

1.4. Gestion de la politique

L'Autorité d'Horodatage a en charge l'administration et la gestion de la Politique d'Horodatage, elle est en particulier responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente politique.

Le document peut être mis à jour uniquement par l'Autorité d'Horodatage, ou par les personnes mandatées par celle-ci, lors de modifications importantes des pratiques ou du service pour prendre en compte de nouveaux besoins, de nouveaux acteurs, améliorer le cadre juridique, ou corriger toute non-conformité.

Toute évolution de la présente politique ayant un impact majeur sur le service se traduira par une évolution de l'OID, afin que les utilisateurs puissent clairement identifier les exigences applicables aux contremarques.

La Politique d'Horodatage est approuvée par l'Autorité d'Horodatage avant d'être promulguée. La décision est consignée en comité de pilotage du service d'horodatage.

La nouvelle politique est publiée sans délai après l'approbation (voir chapitre 1.3 Publication du document).

La nouvelle version de la Politique d'Horodatage entre en vigueur après sa mise en ligne et reste valide jusqu'à l'entrée en vigueur d'une nouvelle version.

La politique est revue annuellement et lors de chaque changement majeur. Cette revue de la politique et des pratiques mises en œuvre est faite sous la responsabilité de la Direction de « la Société ».

1.5. Point de contact

Toute demande relative au service est à adresser au point de contact fourni à l'adresse suivante :

APP SOLUTIONS
Autorité d'Horodatage
25, rue de la Plaine
75020 PARIS

APP Solutions peut également être contacté au travers du formulaire de contact disponible sur son site internet : https://vaultinum.com.

2. Définitions et abréviations

2.1. Définitions

Termes	Définition
Abonné ou Client	Entité ayant besoin de faire horodater des données par une Autorité d'horodatage et qui a accepté les conditions d'utilisation de ses services.
Autorité de Certification (AC)	Entité qui délivre et est responsable des Certificats électroniques signés en son nom, conformément à sa Politique de Certification.
Autorité d'horodatage (AH)	Entité en charge de l'émission et de la gestion des contremarques de temps conformément à une Politique d'Horodatage.
Client	Cf Abonné
Contremarque de temps	Donnée signée qui lie une représentation d'une donnée à un temps, exprimé en heure UTC, établissant ainsi la preuve que la donnée existait à cet instant-là.
Coordinated Universal Time (UTC)	Echelle de temps, liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-5
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.
Horodatage	Service qui associe de manière sûre un événement et une heure afin d'établir de manière fiable l'heure à laquelle cet événement s'est réalisé.
Jeton d'horodatage	Voir contremarque de temps
Liste de Certificats Révoqués (LCR)	Liste de certificats ayant fait l'objet d'une révocation avant la fin de leur période de validité.
Module d'horodatage	Ensemble constitué d'un serveur applicatif d'horodatage, d'un module cryptographique permettant de manipuler les clés privées et d'un boitier de temps permettant de gérer la synchronisation du temps vis-à-vis de sources externes.
Politique de certification (PC)	Ensemble de règles identifiées, définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes.
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 utilisateurs de contremarques de temps.

Service d'horodatage	Ensemble des prestations nécessaires à la génération et à la gestion de Contremarques de temps.
Système d'horodatage	Ensemble des Unités d'horodatage et des composants d'administration et de supervision utilisés pour fournir le 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]).
Utilisateur final	Entité (personne ou système) qui fait confiance à une Contremarque de temps émise sous une Politique d'horodatage donnée par une Autorité d'horodatage donnée.

2.2. Abréviations

AC	Autorité de Certification
AH	Autorité d'Horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
BTSP	Best practices Time-Stamp Policy
DN	Distinguished Name
DPH	Déclaration des Pratiques d'Horodatage
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
LCR	Liste des Certificats Révoqués
NTP	Network Time Protocol
OID	Object Identifier
PH	Politique d'Horodatage
PSCO	Prestataire de Services de Confiance
PSHE	Prestataire de Services d'Horodatage
SSI	Sécurité des Systèmes d'Information
TSP	TimeStamp Provider
UH	Unité d'Horodatage
UTC	Coordinated Universal Time

3. Dispositions générales

3.1. Obligations de l'Autorité d'Horodatage

Le service d'horodatage est placé sous la responsabilité de l'Autorité d'Horodatage.

L'AH vise à respecter l'ensemble des obligations décrites :

- Dans la norme ETSI EN 319421 ;
- Dans la procédure de qualification de l'ANSSI applicable aux prestataires de service d'horodatage.

L'AH a les obligations suivantes :

- Générer et signer des contremarques de temps conformément à la présente Politique d'Horodatage ;
- S'assurer que l'ensemble des acteurs et sous-traitants intervenant dans l'AH respecte la présente Politique d'Horodatage, les exigences et dispositions de la DPH confidentielle et les différentes procédures associées ;
- Garantir que l'ensemble des pratiques sont conformes à la présente Politique d'Horodatage ;
- Respecter l'ensemble des exigences complémentaires inscrites dans les conditions générales d'utilisation du service (CGU) ;
- Mettre à disposition des abonnés et utilisateurs l'ensemble des informations nécessaires à la vérification des contremarques de temps.

3.2. Obligations de l'abonné

L'abonné doit :

- Accepter et respecter les conditions générales d'utilisation du service,
- Respecter les obligations de la présente Politique d'Horodatage qui lui sont applicables,
- Envoyer des requêtes conformes à la RFC 3161 et aux contraintes exposées dans cette Politique d'Horodatage, à partir d'une empreinte calculée avec un algorithme conforme à l'état de l'art et autorisé par la Politique d'Horodatage,
- S'assurer de la validité des contremarques de temps dès leur réception en vérifiant en particulier la valeur de l'empreinte contenue ainsi que la signature de la contremarque de temps. Il est recommandé que les clients vérifient que le certificat de l'unité d'horodatage ne soit pas révoqué au moment de l'obtention des contremarques.

L'abonné est responsable :

- Du lien entre l'empreinte soumise dans la requête et les données horodatées par la contremarque de temps,
- De la conservation des contremarques de temps selon ses besoins propres,
- De la transmission des Conditions Générales d'Utilisation à ses utilisateurs ou de faire figurer leurs obligations dans un document qui leur est opposable.

3.3. Obligations de l'utilisateur de contremarques de temps

Pour faire confiance à une contremarque de temps, l'utilisateur devra :

- Comparer le haché des données horodatées avec le haché présent dans la contremarque de temps,
- Vérifier que la contremarque de temps a été correctement signée, et que le certificat de l'Unité d'Horodatage (UH) est valide à l'instant de la vérification,
- Vérifier la validité du certificat d'horodatage. Cette vérification est réalisée en s'appuyant sur la chaîne de certification et la liste de certificats révoqués (LCR) émis par l'autorité de certification,

- Tenir compte des limitations sur l'utilisation de la contremarque de temps indiquées dans la présente Politique d'Horodatage et dans les conditions générales d'utilisation,
- Prendre en compte d'éventuelles consignes ou obligations contractuelles s'appliquant à leur utilisation des services.

3.4. Obligations de l'AC fournissant les certificats des unités d'horodatage

Les certificats de signature des contremarques de temps, mis en œuvre au sein de chaque unité d'horodatage, sont émis par une autorité de certification interne à « la Société ».

Cette autorité de certification est l'entité garante des conditions d'émission des certificats, selon sa Politique de Certification. Elle met en œuvre des pratiques conformes aux exigences prévues par la norme ETSI EN 319411-1.

L'Autorité de Certification est responsable de :

- L'émission des certificats de signature des unités d'horodatage,
- De la mise à disposition de l'Autorité d'Horodatage des services de révocation nécessaires,
- De la publication à destination des clients et utilisateurs des contremarques de temps des moyens de vérification des certificats, c'est à dire de la chaîne de certification et du statut de révocation des certificats.

3.5. Déclarations des pratiques d'horodatage

Le présent document contient la version publique de la déclaration des pratiques d'horodatage. Les pratiques jugées confidentielles sont précisées dans une déclaration des pratiques confidentielles associées au présent document et référant l'ensemble des pratiques et procédures de l'AH. L'AH garantit qu'elle possède la fiabilité nécessaire pour fournir des services d'horodatage. En particulier :

- L'AH a fait une évaluation de risques pour évaluer les actifs et les menaces pour ces actifs afin de déterminer les contrôles de sécurité nécessaires et les procédures opérationnelles (voir chapitre 5.2.6.1 Analyse de risque) ;
- L'AH dispose, comme mentionné plus haut, d'une déclaration des pratiques (dont la partie non-confidentielle est incluse dans le présent document) ainsi que des procédures documentées. Cette DPH et ces procédures visent à adresser toutes les exigences de la politique d'horodatage ;
- La DPH identifie les obligations de toutes les éventuelles organisations externes participant à la fourniture des services d'horodatage, y compris la politique applicable et les pratiques. Cela inclut l'AC fournissant les certificats aux unités d'horodatage ;
- L'AH met à la disposition des utilisateurs de jetons d'horodatage, les éléments publics de sa déclaration des pratiques d'horodatage au travers du présent document et à travers des conditions d'utilisation à l'intention des tiers publiés sur son site (voir chapitre 1.3 Publication du document).
- L'AH dispose d'une organisation adéquate permettant l'approbation de la présente PH/DPH ainsi que de la DPH confidentielle, ainsi que l'approbation de la concordance entre les deux documents ;
- Le responsable de l'AH garantit que les pratiques sont correctement mises en œuvre ;
- L'AH définit une procédure de contrôle périodique (audit interne) de la conformité des pratiques, y compris les responsabilités, à la déclaration des pratiques d'horodatage.
- L'AH ayant été évaluée pour être en conformité avec la présente PH/DPH, si une modification envisagée à l'initiative de l'AH pouvait entraîner une non-conformité avec ladite PH/DPH ou avec la version confidentielle DPH, alors l'AH soumettra cette modification à l'organisme évaluateur indépendant pour avis.
- L'AH informera au préalable les abonnés du service d'horodatage de tout changement qu'elle a l'intention de faire dans la partie publique de sa DPH. Cela prendra la forme d'une notification par email à l'ensemble des abonnés.

3.6. Conditions générales d'utilisation

L'Autorité d'Horodatage définit des Conditions Générales d'Utilisation du service d'horodatage qui reprennent les principales dispositions de la présente Politique d'Horodatage. Les Conditions Générales d'Utilisation répondent aux exigences de contenu des « Disclosure Statement » de l'ETSI 319421 et intègrent ainsi les engagements respectifs du fournisseur du service ainsi que des clients et des utilisateurs.

Les conditions générales d'utilisation sont publiées sur le site de publication (voir chapitre 1.3 Publication du document).

Elles sont fournies au format PDF en Français et en Anglais.

3.7. Conformité avec les exigences légales

L'AH garantit la conformité avec les exigences légales. En particulier :

- Des mesures techniques appropriées et organisationnelles sont prises pour assurer un niveau adéquat de protection des données à caractère personnel, conformément au RGPD ;
- Les informations fournies au service d'horodatage ne sont pas divulguées, sauf dans le cas :
    - D'un accord express du propriétaire des données ;
    - D'une décision judiciaire ;
    - D'une exigence légale.
- Les pratiques de l'AH sont non-discriminatoires. Chaque fois que cela est possible, « la Société » met en œuvre tous les moyens nécessaires pour rendre accessible son service aux personnes en situation de handicap. En particulier, les recommandations sur l'accessibilité sont prises en compte.

4. Exigences opérationnelles

4.1. Gestion des requêtes de contremarques de temps

L'AH fournit une contremarque de temps en réponse à une demande. La fourniture d'une contremarque de temps est quasi immédiate et se fait de façon synchrone.

Les réponses de la part d'une AH à une Demande de contremarque de temps n'excède pas quelques secondes, ceci afin de ne pas nuire ni dégrader l'ergonomie de l'application appelante.

Les engagements de qualité de service relatifs à la fourniture d'une contremarque de temps en réponse à une demande sont définis dans les CGU définies par l'AH.

Les demandes de contremarques de temps sont réalisées par les applications utilisatrices de l'AH selon le protocole défini par la norme RFC 3161. Ce protocole est conforme au document ETSI EN 319422.

La contremarque de temps générée est conservée par l'AH pour une durée de 7 ans.

4.2. Fichiers d'audit

Afin d'assurer la traçabilité de son service, l'AH enregistre et conserve des traces dans des fichiers d'audit.

En particulier, sont conservées :

- Les traces des demandes reçues par le service et des réponses retournées ;
- Les traces pertinentes relatives à l'administration du service d'horodatage ;
- Les traces pertinentes relatives au fonctionnement du service d'horodatage ;
- Les traces pertinentes concernant les événements liés au cycle de vie des clés d'UH et au cycle de vie des certificats associés ;
- Les traces pertinentes concernant la synchronisation des horloges et serveurs de temps utilisés par l'UH, y compris la perte de synchronisation ou le recalibrage/la resynchronisation des horloges.

Des mesures de sécurité (au niveau physique, réseau et système) sont mises en place afin d'assurer l'intégrité, la disponibilité et la confidentialité des traces. Il doit être particulièrement difficile, voire impossible, d'altérer ou détruire les traces d'événements. La DPH confidentielle décrit les moyens mis en œuvre.

La durée de conservation des journaux du service est conservée pendant une période minimale de 7 ans, conformément aux exigences de l'ANSSI, en particulier dans le but de fournir une preuve en cas d'enquête légale. Cette durée de 7 ans est applicable même après arrêt d'activité de l'AH.

Tous les événements sont datés. Les horloges utilisées pour dater les événements sont synchronisées avec UTC au moins une fois par jour.

4.3. Gestion de la durée de vie de la clé privée

L'AH garantit que la clé privée ne sera pas utilisée au-delà de la date de validité du certificat. Cela est obtenu par la mise en place de mesures techniques et organisationnelles. En particulier :

- La clé privée d'UH est renouvelée par anticipation avant la fin de la période d'utilisation de la clé précédente ;
- La clé privée d'UH est détruite en fin de période d'utilisation (voir chapitre 6.7 Destruction des clés des unités d'horodatage et chapitre 6.11 Durée d'utilisation des clés privées des UH).

4.4. Synchronisation de l'horloge

Conformément aux exigences eIDAS, l'AH garantit que son horloge est synchronisée avec le temps UTC selon l'exactitude déclarée de 1 (une) seconde, et garantit en particulier :

- Le calibrage de chaque horloge d'unité d'horodatage est maintenu de telle manière que les horloges ne puissent pas normalement dériver à l'extérieur de l'exactitude déclarée ;
- Les horloges des unités d'horodatage sont protégées contre les menaces relatives à leur environnement qui pourraient aboutir à une désynchronisation avec le temps UTC en dehors de l'exactitude déclarée.
    - Les menaces identifiées sont décrites dans l'analyse de risques. Les menaces étudiées prennent en compte : les modifications par du personnel non autorisé, les ondes radio et les chocs électriques ;
- L'Autorité d'horodatage garantit que, si son horloge interne ne respecte plus l'exactitude déclarée, alors l'anomalie est automatiquement détectée.
    - En cas de désynchronisation entraînant la production d'horodatages erronés, l'information sur de tels événements est publiée à destination des utilisateurs sur le site de publication (voir chapitre 1.3 Publication du document) ;
- Si l'horloge d'une unité d'horodatage est détectée comme étant en dehors de l'exactitude annoncée, les contremarques de temps ne sont plus générées ;
- L'Autorité d'horodatage garantit que la synchronisation de l'horloge est maintenue lorsqu'un saut de seconde est programmé. Le changement tient compte du fait que le saut de seconde est effectué durant la dernière minute du jour où le saut de seconde est programmé. Un enregistrement du temps exact (selon l'exactitude déclarée) de l'instant de ce changement est effectué.

4.5. Contenu d'une contremarque de temps

L'AH garantit que les jetons d'horodatage sont générés en toute sécurité et incluent le temps correct. Le jeton d'horodatage inclut également le certificat d'unité d'horodatage sur demande de l'abonné. Ce certificat indique les informations suivantes :

- L'identifiant du pays dans lequel l'AH est établie. Cette information est fournie dans le champ C du certificat ;
- L'identifiant de l'Autorité d'horodatage. Cette information est fournie par les champs O et OI du certificat ;
- L'identification de l'unité d'horodatage. Cette information est fournie par le champ CN du certificat.

Le jeton d'horodatage contient également l'OID de la présente PH/DPH (voir chapitre 1.2 Identification du document). Chacun des jetons d'horodatage contient :

- Un identifiant unique ;
- La date inscrite dans le jeton d'horodatage est reliée à un temps fourni par un laboratoire UTC(k) grâce au mécanisme de synchronisation décrit dans le chapitre 6.2.1 Synchronisation de l'horloge. Le temps est synchronisé avec UTC avec la précision décrite dans le chapitre 4.4 Synchronisation de l'horloge ;
- La valeur de hachage et l'identifiant d'algorithme de hachage ;
- La signature produite par la clé privée de l'UH.

Les jetons sont conformes aux exigences du chapitre ANNEXE Exigences sur les formats des contremarques de temps, des certificats et des LCR et sur les algorithmes cryptographiques .

Dans le cas de demande de contremarque de temps survenant durant un intervalle de temps correspondant à l'exactitude de l'horloge de l'UH, l'ordonnancement des contremarques de temps à l'intérieur de cet intervalle n'est pas requis.

4.6. Compromission de l'AH

L'Autorité d'horodatage garantit, dans le cas d'événements qui affectent la sécurité des services d'horodatage (incluant la compromission de la clé privée de signature d'une unité d'horodatage ou la perte détectée de calibrage qui pourrait affecter des jetons d'horodatage émis) qu'une information appropriée est mise à la disposition des utilisateurs de contremarques de temps. Cette notification se fera au travers d'une publication (voir chapitre 1.3 Publication du document).

Les dispositions suivantes sont prises en compte en cas de compromission :

- Le plan de secours (PCA/PRA) de l'Autorité d'horodatage traite le cas de la compromission réelle ou suspectée de la clé privée de signature d'une unité d'horodatage ou la perte de calibrage de l'horloge d'une unité d'horodatage, qui pourrait affecter des contremarques de temps émises ;
- Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une unité d'horodatage, qui pourrait affecter des contremarques de temps émises, l'AH met à la disposition de tous les utilisateurs de contremarques de temps une description de la compromission qui est survenue. Cette notification se fait via une publication sur le site référencé dans chapitre 1.3 Publication du document ;
- Dans le cas d'une compromission, réelle ou suspectée, ou d'une perte de calibrage d'une unité d'horodatage, qui pourrait affecter des contremarques de temps émises, l'AH prendra les mesures nécessaires pour que les contremarques de temps de cette unité ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation. Ces dispositions prennent la forme d'une suspension de l'activité de l'unité d'horodatage et en cas de compromission avérée, de son décommissionnement.
- En cas d'un événement majeur dans le fonctionnement de l'Autorité d'horodatage ou d'une perte de calibrage, qui pourrait affecter des contremarques de temps émises, chaque fois que cela sera possible, l'AH mettra à la disposition des utilisateurs de contremarques de temps toute information pouvant être utilisée pour identifier les contremarques de temps qui pourraient avoir été affectées4.
- L'AH préviendra directement et sans délai l'ANSSI (voir chapitre 5.2.3 Rapport d'incident et de réponse).

4.7. Fin d'activité de l'AH

En cas de cessation d'activité de son AH, « la Société » s'assurera que l'impact sur les utilisateurs soit réduit au maximum et assurera la maintenance continue des informations nécessaires pour vérifier la justesse des contremarques de temps.

À ce titre, « la Société » a mis en œuvre un plan d'arrêt d'activité (PAA) adressant l'ensemble des actions à exécuter :

- L'AH notifiera l'ANSSI de son plan d'arrêt d'activité ;
- L'AH rendra disponible sur son site internet (voir chapitre 1.3 Publication du document) l'information concernant son arrêt d'activité ;
- L'Autorité d'horodatage abrogera les autorisations données aux sous-traitants d'agir pour son compte dans l'exécution de n'importe quelles fonctions touchant au processus de génération des jetons d'horodatage ;
- « La Société » maintiendra les obligations de maintien des fichiers d'audit et des archives nécessaires pour démontrer son fonctionnement correct durant une période raisonnable. En cas d'arrêt total de l'activité, « la Société » transférera à un organisme fiable ses éléments pour la même durée de conservation cible ;
- « La Société » maintiendra ou transférera à un organisme fiable ses obligations de rendre disponible aux utilisateurs de contremarques de temps pendant une période raisonnable ses clés publiques ainsi que ses certificats ;
- L'AH détruira de façon définitive les clés privées de telle façon que celles-ci ne puissent être recouvrées ;
- L'ensemble des certificats d'unité d'horodatage seront révoqués.

Le plan d'arrêt d'activité est tenu à jour. Il est revu annuellement et lors de tout changement majeur.

« La Société » prend les mesures nécessaires pour couvrir les dépenses pour accomplir ses exigences minimales dans le cas où l'AH tomberait en faillite ou pour d'autres raisons où « la Société » serait incapable de couvrir les dépenses par elle-même.

5. Exigences physiques et environnementales, procédurales et organisationnelles

5.1. Exigences physiques et environnementales

« La société » dispose d'une architecture répartie sur deux sites physiques localisés en France. Un des sites est certifié ISO 27001, le second est en cours de certification ISO 27001. Les serveurs applicatifs et les composants sensibles (HSM et boîtiers de temps) sont hébergés dans des baies dédiées à « La société ».

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

- L'accès physique aux équipements concernés par les services d'horodatage est limité aux individus autorisés ;
- Des contrôles sont mis en œuvre pour éviter la perte, des dégâts ou la compromission d'actifs et l'interruption des activités et ;
- Des contrôles sont mis en œuvre pour éviter la compromission ou le vol d'informations ou d'équipements informatiques.

Les composants critiques pour l'opération sécurisée du service de confiance sont localisés dans un environnement de sécurité muni d'une protection physique contre les intrusions et de mécanismes d'alarme.

Des contrôles d'accès sont appliqués aux modules d'horodatage pour remplir les exigences de sécurité des modules d'horodatage.

Les contrôles suivants complémentaires sont appliqués à la gestion du service d'horodatage :

- Le système d'horodatage fonctionne dans un environnement qui protège physiquement les services de la compromission. Des moyens sont mis en œuvre pour se protéger d'un accès non autorisé aux systèmes ou aux données ;
- La protection physique est réalisée par la création d'un périmètre de sécurité dédié clairement défini (c'est-à-dire des barrières physiques) autour des UH ;
- Le service d'horodatage est séparé logiquement des autres services afin d'être protégé des compromissions et des accès non autorisés.
- Toute entrée dans la zone de sécurité physique est soumise à des moyens de surveillance. Cette surveillance est réalisée en toute indépendance. Toute personne non autorisée est obligatoirement accompagnée par une personne autorisée dans la zone sécurisée. Toutes entrées et sorties sont tracées.
- Des contrôles de sécurité physique et environnementale sont mis en œuvre pour protéger l'environnement qui abrite les ressources du système, les ressources du système elles-mêmes et les équipements utilisés pour remplir leur fonction ; la politique de sécurité physique et environnementale de l'AH pour les systèmes concernés par la gestion de l'horodatage concerne au minimum le contrôle d'accès physique, la protection vis-à-vis des catastrophes naturelles, les facteurs de sécurité liés au feu, la défaillance des services de base (par exemple le secteur, les télécommunications), l'écroulement de la structure, des fuites de plomberie, la protection contre le vol, la casse et la pénétration et, le rétablissement de la sécurité après un désastre.
- Des contrôles sont mis en œuvre pour empêcher des équipements, de l'information, des médias et du logiciel touchant aux services d'horodatage d'être enlevés du site sans autorisation.

5.2. Exigences procédurales

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

- L'intégrité des composants du système d'horodatage et l'information sont protégées contre les virus, les logiciels malveillants et non autorisés ;
- Un rapport d'incident et des procédures de réponse aux incidents sont employés d'une telle façon que les dégâts liés aux incidents de sécurité et aux défaillances soient réduits au minimum ;
- Les supports employés dans les systèmes d'horodatage sont manipulés de manière sécuritaire pour les protéger des dégâts, du vol, de l'accès non autorisé et de l'obsolescence.
- Des procédures sont établies et mises en œuvre pour tous les rôles de confiance et administratifs qui impactent la fourniture des services d'horodatage.

5.2.1. **Manipulation et sécurité des supports**

L'AH assure un niveau approprié de protection des biens et des supports de ces biens, y compris les biens dématérialisés.

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

En fin de vie, en fonction du niveau de confidentialité des informations qu'ils contiennent, les supports sont soit détruits, soit réinitialisés en vue d'une réutilisation.

Des mesures sont mises en œuvre afin de prévenir l'obsolescence, la perte, des dégâts ou l'altération ou la compromission des actifs nécessaires au bon fonctionnement du service d'horodatage électronique et à l'archivage des preuves, et ce pendant toute la durée de conservation prévue. Des contrôles sont également mises en œuvre pour éviter la perte, la compromission ou le vol d'informations ou d'équipements informatiques.

5.2.1.1. Gestion du cycle de vie des HSM

L'AH met en place des mesures spécifiques relatives au HSM afin de garantir que :

- L'intégrité du HSM durant son transport depuis le fournisseur ou le cas échéant entre deux sites d'hébergement utilisés par « la Société » ;
- La sécurité physique (voir chapitre 5.1 Exigences physiques et environnementales) et logique du matériel pendant son exploitation ;
- La sécurité des opérations d'administration, réalisées lors de cérémonies de clés par des porteurs de secret sous le contrôle de l'AH et du responsable de sécurité.

Les clés sont effacées avant la mise au rebut du matériel de façon qu'il soit quasiment impossible de permettre leur récupération.

5.2.1.2. Gestion du cycle de vie des secrets

Les sites dans lesquels sont conservées les sauvegardes sont protégés contre les risques d'incendies et d'inondation. De plus, les accès physiques et logiques sont protégés et soumis à une gestion des droits et à une authentification forte.

Dans le cas d'une utilisation de documents papiers, ou de supports amovibles telles qu'un CD, une clé USB de stockage, un disque dur externe ou une carte à puce, ceux-ci seront conservés dans un coffre-fort.

Des procédures de gestion protègent les supports contre l'obsolescence et la détérioration pendant la période durant laquelle l'AH s'engage à conserver les informations qu'ils contiennent.

5.2.2. **Planification de Système**

Les charges des différents composants sont contrôlées et des projections de charge dans le futur sont effectuées pour garantir que des puissances de traitement et des stockages adéquats seront disponibles.

5.2.3. **Rapport d'incident et réponse**

L'ensemble des systèmes font l'objet d'une surveillance (monitoring), en particulier des accès et de l'utilisation/charge des systèmes (voir section précédente). Ces activités de surveillance prennent en compte la sensibilité des données manipulées.

Les événements suivants sont surveillés à minima :

- Les démarrages et arrêts des fonctions de création de traces des systèmes ;
- La disponibilité et le niveau d'utilisation des services.

L'Autorité d'horodatage agit d'une façon opportune et coordonnée pour répondre rapidement aux incidents et limiter l'impact des infractions à la sécurité. Tous les incidents seront rapportés aussitôt que possible après l'incident en suivant les procédures définies. La gestion des incidents est réalisée par des personnes en rôle de confiance.

En particulier, en cas d'incident de sécurité grave (atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées), l'ANSSI sera notifiée de l'incident en suivant la procédure de notification d'incident dédiée, et au plus tard dans les 24 heures après la découverte de l'incident.

Cette notification est réalisée au moyen du formulaire mis en ligne sur le site de l'ANSSI. Les utilisateurs et/ou clients du service impactés seront également notifiés.

En cas d'incident majeur concernant les données personnelles, les personnes physiques impactées seront notifiées chaque fois que cela est possible. La CNIL sera informée dans les 72 heures.

La surveillance des systèmes inclut une revue des traces du système. L'objectif de cette revue est de découvrir des comportements malicieux. Ces revues s'appuient sur des mécanismes automatiques et permettent d'alerter de potentielles failles de sécurité ou d'événements critiques.

Toutes vulnérabilités critiques sont adressées dans une période de 48h après leur découverte. Pour toute vulnérabilité, l'AH :

- Créé et met en œuvre un plan de mitigation de la vulnérabilité ;
- Documente sur une base factuelle le choix de ne pas traiter une vulnérabilité.

La réponse à incident est mise en œuvre de façon à minimiser les impacts des incidents et dysfonctionnements.

5.2.4. **Procédures de fonctionnement et responsabilités**

Des procédures sont établis et mises en œuvre pour tous les rôles de confiance et administratifs qui impactent le fourniture des services d'horodatage.

Les opérations de sécurité sont séparées des autres opérations. Les opérations de sécurité incluent :

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

Ces opérations sont gérées par du personnel de confiance de l'Autorité d'horodatage.

L'AH met en place un comité de suivi pour piloter et décider des choix importants liés au service d'horodatage. Le comité de suivi établir les différents rôles de confiance et s'assure que chaque porteur d'un rôle de confiance est conscient de ses responsabilités et les accepte formellement.

5.2.5. Gestion d'Accès au Système

L'AH suit l'ensemble des recommandations définies dans le guide d'hygiène informatique publié par l'ANSSI, pour le niveau « standard ». Les règles de niveau renforcées sont mises en œuvre chaque fois que cela est possible. La PSSI rappelle l'ensemble de ces règles.

5.2.5.1. Réseau

L'AH protège ses systèmes et réseaux des attaques.

Pour se faire, l'AH a segmenté ses systèmes en réseaux et zones séparées en se basant sur l'analyse de risque. La séparation prend en compte la séparation des systèmes sur les plans à la fois fonctionnels, logiques et physiques.

L'AH applique des niveaux de sécurité et de contrôle similaire pour tous les systèmes localisés au sein d'une même zone.

Les accès et communications entre chaque zone sont contrôlés et limités. Elles sont réduites au minimum nécessaire à l'opération du service.

Ces contrôles - en particulier des pare-feu (firewalls) - sont mis en œuvre pour protéger le réseau interne de l'Autorité d'horodatage des accès non autorisés. Les accès non-autorisés incluent l'accès par des abonnés mais également des tierces personnes au réseau interne.

Les pare-feu (firewalls) sont configurés pour bloquer tous les protocoles et les accès non nécessaires au fonctionnement de l'Autorité d'horodatage.

Les règles réseau font l'objet de revues régulières. La revue est réalisée à minima de façon annuelle.

Tous les systèmes critiques sont regroupés au sein des zones les plus sécurisées. Les réseaux opérationnels et les réseaux d'administration sont séparés. Les services d'administration sont dédiés à cet effet et ne peuvent être utilisés pour d'autres besoins. L'AH s'assure que toute communication entre deux composants de sécurité est obligatoirement établie au travers d'un canal sécurisé. Ce canal est isolé des autres canaux. Cette séparation peut être obtenue par des moyens physiques, logiques ou cryptographiques. Le canal sécurisé permet l'identification de l'origine et du destinataire, ainsi que la protection en intégrité et confidentialité du contenu échangé.

L'AH réalise de façon régulière des scans de vulnérabilité. La régularité ciblée est trimestrielle. Les éléments de preuve relatifs à la qualité, l'éthique, l'expertise et l'indépendance des personnes réalisant les scans sont conservés afin de démontrer la pertinence des rapports.

L'AH réalise des tests de pénétration avant la mise en place de l'infrastructure technique et après chaque mise à jour significative de l'infrastructure. Ces tests de pénétration seront réalisés annuellement.

De même que pour les scans, les éléments de preuve relatifs à la qualité, l'éthique, l'expertise et l'indépendance des personnes réalisant les tests sont conservées afin de démontrer la pertinence des rapports

5.2.5.2. Gestion des comptes

L'Autorité d'horodatage garantit une administration efficace des utilisateurs (cela inclut les opérateurs, les administrateurs et les auditeurs), pour maintenir la sécurité du système, y compris la gestion des comptes des utilisateurs, l'audit, et la modification ou le retrait rapide d'accès. Le principe du moindre privilège est appliqué lors de la configuration des accès.

5.2.5.3. Contrôle d'accès

L'Autorité d'horodatage garantit que l'accès aux fonctions du système, à l'information et aux applications est limité conformément à la politique de contrôle d'accès et que le système d'horodatage possède les contrôles informatiques de sécurité suffisants pour la séparation des rôles de confiance identifiés dans les pratiques d'horodatage, y compris la séparation des fonctions d'administrateur de sécurité et des fonctions opérationnelles. En particulier, l'utilisation de programmes système utilitaires sera limitée et très contrôlée.

5.2.5.4. Identification et authentification du personnel

Le personnel de l'Autorité d'horodatage est correctement identifié et authentifié avant d'utiliser des applications critiques liées à l'horodatage.

5.2.5.5. Responsabilité des personnels

Le personnel de l'Autorité d'horodatage sera tenu responsable de ses activités. Une traçabilité des actions est mise en œuvre.

5.2.5.6. Gestion de l'horodatage

L'Autorité d'horodatage garantit que des composants de réseaux locaux (par exemple les routeurs) sont placés dans un environnement physiquement sûr et que leurs configurations sont périodiquement vérifiées pour la conformité avec les exigences indiquées par l'Autorité d'horodatage.

5.2.5.7. Surveillance

Une surveillance permanente et des équipements d'alarme est mise en œuvre pour permettre à l'Autorité d'horodatage de détecter, d'enregistrer et de réagir rapidement à n'importe quelle tentative non autorisée et/ou irrégulière d'accès à ses ressources.

5.2.6. Déploiement et Maintenance

L'Autorité d'horodatage emploie des produits et systèmes de confiance.

Des procédures de contrôle sont appliquées pour les nouvelles versions, les modifications et les corrections d'anomalies de n'importe quel logiciel opérationnel.

Les HSM font l'objet d'une veille particulière pour s'assurer que le niveau de qualification du produit est maintenu dans le temps et des actions sont prises pour assurer les montées de version logicielle fournies par le fournisseur.

5.2.6.1. Analyse de risque

Une analyse des exigences de sécurité est effectuée au moment de la conception et de l'étape de spécification des exigences pour tout projet de développement de systèmes entrepris par l'Autorité d'horodatage ou pour le compte de l'Autorité d'horodatage pour assurer que la sécurité fait partie du système d'information.

L'AH réalise cette analyse de risque afin d'identifier, analyser et évaluer les risques. Les risques techniques, mais également les risques métiers sont pris en compte.

L'AH sélectionne des mesures appropriées de traitement du risque, en s'appuyant sur les résultats de l'analyse de risque. Les mesures de traitement du risque permettent de s'assurer que le niveau de sécurisation est approprié vis-à-vis du niveau de risque.

L'AH détermine l'ensemble des exigences de sécurité et les procédures opérationnelles qui sont nécessaires à la mise en œuvre des mesures retenues. Ces éléments sont documentés dans la PSSI, ainsi que dans la présente PH/DPH, ainsi que dans la version confidentielle de la DPH.

L'analyse de risque est revue et mise à jour de façon régulière. Celle-ci est revue à minima annuellement et lors de tout changement majeur (voir chapitre 5.2.6.3 Gestion des changements), notamment en cas de modification des politiques ou pratiques relatives à la fourniture du service d'horodatage.

L'analyse de risque fait l'objet d'une approbation formelle par le comité de Direction de « la Société » qui accepte, au travers de cette approbation, le risque résiduel identifié.

En outre, l'analyse de risque fait l'objet d'une procédure d'homologation. Cette procédure d'homologation est réalisée préalablement à la fourniture du service de confiance qualifié puis révisée au moins tous les deux ans.

5.2.6.2. Politique de sécurité du système d'information

« La Société » a défini une politique de sécurité du système d'information (PSSI). La PSSI est approuvée formellement par le comité de Direction de « la Société ». La PSSI définit l'approche générale de l'organisation pour sa gestion de la sécurité de l'information.

Tout changement de la PSSI sera notifié aux tiers impactés, si cela s'avère nécessaire. Ces tiers peuvent inclure des abonnés, les utilisateurs, l'organisme d'évaluation ou l'organe de contrôle.

La PSSI est documentée, mise en œuvre et tenue à jour. Pour cela, des mesures de contrôle de sécurité et des procédures opérationnelles sont mises en place. Ces mesures couvrent les sites, les systèmes d'information et les biens impliqués dans la délivrance du service d'horodatage.

La PSSI est communiquée à l'ensemble des employés entrant dans son périmètre.

L'AH a l'entière responsabilité de la conformité de ses procédures à la PSSI, même dans le cas où de la sous-traitance est mise en œuvre.

En cas de sous-traitance, les responsabilités de chacun sont définies contractuellement. En particulier, le sous-traitant est tenu de mettre en œuvre l'ensemble des règles de sécurité qui lui sont applicables.

Lorsque l'AH a recours à un sous-traitant, elle s'assure que l'interface avec le sous-traitant est sécurisée et qu'elle est utilisée en conformité avec les recommandations du sous- traitant.

La PSSI est revue régulièrement, à minima de façon annuelle et à chaque changement majeur dans le système d'information. Cela afin d'assurer la continuité de son application, de sa cohérence et de son efficacité, même en cas de changement significatif. Tout changement ayant un impact sur le niveau de sécurité devra obligatoirement être validé par le comité de Direction de « la Société ».

Les configurations des systèmes mis en œuvre par l'AH fait régulièrement l'objet de vérification afin de s'assurer qu'ils sont en ligne avec la politique de sécurité. L'intervalle maximum entre deux vérifications est documenté dans la version confidentielle de la DPH.

5.2.6.3. Gestion des changements

Des procédures de contrôle de changement sont appliquées pour les nouvelles versions, les modifications et les corrections d'anomalies de n'importe quel logiciel opérationnel.

En cas d'intentions de changements dans la présente PH/DPH qui impacterait l'usage du service, le changement sera préalablement notifié :

- Auprès des utilisateurs de jetons d'horodatage par une publication sur le site (voir chapitre 1.3 Publication du document) ;
- Auprès des clients de « la Société » par un message électronique envoyée à leur adresse de contact.

Les changements apportés sont documentés.

En cas de modification importante dans la fourniture de son service de confiance, l'AH informe l'ANSSI selon les modalités convenues.

Ces modifications importantes comprennent notamment, sans s'y limiter :

- Les changements induits par une modification de la politique de service ou des conditions générales d'utilisation associées ;

- Les changements de sous-traitants ;
- Les modifications des conditions d'hébergement ;
- Les changements de matériels cryptographiques ;
- Les modifications d'architecture technique ;
- Les changements de procédures d'enregistrement et d'identification ;
- Les changements dans la gouvernance de l'AH.

Les modifications entraînant des changements dans la liste de confiance publiée par l'ANSSI sont notifiées dans les meilleurs délais.

L'AH adresse à l'ANSSI une synthèse de l'ensemble des modifications apportées à la fourniture de son service, impactant les constats présentés dans le rapport d'évaluation de la conformité, à une fréquence annuelle.

5.2.6.4. Gestion des vulnérabilités

L'AH définit et applique des procédures permettant d'assurer :

- Que les mises à jour de sécurité sont appliquées dans un temps raisonnable après leur mise à disposition ;
- Que les mises à jour de sécurité ne sont appliquées que si elles n'introduisent pas de nouvelles vulnérabilités additionnelles ou des instabilités qui ne seraient pas contrebalancées par les bénéfices de la mise en œuvre.

Les raisons de ne pas appliquer une mise à jour de sécurité sont documentées.

5.3. Exigences organisationnelles

L'Autorité d'horodatage garantit que le personnel (interne ou contractuel) et les pratiques d'embauche améliorent et concourt à la fiabilité des opérations de l'Autorité d'horodatage.

5.3.1. Expertise

L'Autorité d'horodatage emploie un personnel qui possède l'expertise, la formation, l'expérience et les qualifications nécessaires pour les services offerts, tels que l'exige la fonction. En particulier, le personnel a réalisé des formations sur la sécurité informatique et la protection des données à caractère personnel avec la spécificité d'un service d'horodatage et les fonctions occupées au sein de ce service.

Le personnel est en nombre suffisant pour assurer le volume de travail nécessaire pour la fourniture du service.

L'expertise des employés est acquise au travers de l'expérience, de formations spécifiques ou d'une combinaison des deux. La formation continue des employés inclut une mise à niveau, à minima annuelle, de la connaissance des nouvelles menaces et pratiques de sécurité.

Le personnel de gestion employé possède :

- La connaissance de la technologie de l'horodatage et ;
- La connaissance de technologie de la signature numérique et ;
- La connaissance des mécanismes pour le calibrage ou la synchronisation des horloges des unités d'horodatage avec le temps UTC et ;
- Pour le personnel avec des responsabilités de sécurité, une bonne connaissance des procédures de sécurité, et ;
- L'expérience avec la sécurité de l'information et l'évaluation des risques.

Le personnel d'encadrement possède également, au travers de son expérience ou d'une formation relative au service d'horodatage, une familiarité avec les procédures de sécurité applicable à son personnel. Il est également familié des notions relatives aux responsabilités en matière de sécurité et disposer d'une expérience en sécurité de l'information et en analyse de risque suffisante pour être en mesure d'assurer la fonction d'encadrement.

5.3.2. **Rôles et responsabilités**

Les rôles de sécurité et les responsabilités, comme spécifiées dans la politique de sécurité de l'Autorité d'horodatage, sont documentés dans des descriptions de poste. Les rôles de confiance, sur lesquels la sécurité du fonctionnement de l'Autorité d'horodatage repose, sont clairement identifiés au travers de fiches de poste mises à disposition des personnels.

L'AH distingue les rôles de confiance suivants (équivalents aux Trusted Roles de la norme ETSI [EN 319401]) :

- **Responsable sécurité / Officier de Sécurité** : L'officier de sécurité est chargé de la mise en œuvre de la politique de sécurité du système d'information pour le service d'horodatage. Il gère notamment les contrôles d'accès physiques aux équipements des systèmes sensibles. Ce rôle correspond au rôle Security Officer définit dans la norme [ETSI_TSP].
- **Administrateur des plateformes** : Les administrateurs des plateformes ont la charge de l'installation, de la mise en route, de la configuration, de la restauration et de la maintenance technique des équipements informatiques. Ils assurent l'administration technique des systèmes et des réseaux de la composante, ainsi que leur surveillance (détection d'incident). Ce rôle correspond au System Administrator définit dans la norme [ETSI_TSP].
- **Exploitant** : Les opérateurs systèmes (ou exploitants) ont la charge du fonctionnement technique quotidien du service : supervision, sauvegarde, gestion de tickets pour la maintenance et la continuité de service. Ce rôle correspond au System Operator définit dans la norme [ETSI_TSP].
- **Contrôleur / Auditeur de système** : L'auditeur de système a la charge de l'analyse récurrente des événements intervenant sur les composantes de l'Autorité d'Horodatage. Il dispose d'un accès aux journaux d'audit et aux archives afin de s'assurer du respect des conditions de sécurité et de la légitimité des opérations réalisées sur le système. Ce rôle correspond au System Auditor définit dans la norme [ETSI_TSP].
- **Porteur de secret** : Un porteur de secret est le détenteur exclusif d'une information ou d'un bien nécessaire pour l'accès aux opérations sensibles sur le boîtier cryptographique stockant les clés privées des unités d'horodatage. Le regroupement d'un sous-ensemble de ces porteurs est nécessaire pour la réalisation de ces opérations. Les porteurs de secrets sont responsables de la conservation et de la protection des secrets qui leur sont confiés, et reçoivent pour cela les moyens appropriés.

Le personnel de l'AH est formellement nommé aux rôles de confiance par la direction responsable de la sécurité. La personne nommée en rôle de confiance accepte également formellement son rôle et ses responsabilités.

L'AH met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté de ses personnels.

L'AH ne nomme pas aux rôles de confiance ou de gestion toute personne connue pour avoir une condamnation pour un crime sérieux ou une autre infraction qui affecte son adéquation avec la position. Le personnel n'a pas accès aux fonctions de confiance avant que les contrôles nécessaires ne soient achevés.

Le contrôle inclut une vérification de l'extrait de casier judiciaire (bulletin n°3).

APP SOLUTIONS peut décider en cas de refus de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions de la personne, de lui retirer ces attributions. Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans)

Des sanctions disciplinaires sont prévues en cas de non-respect des consignes énoncées dans la DPH ou dans la PSSI.

5.3.3. **Séparation des rôles**

Des descriptions de fonctions sont définies pour le personnel de l'Autorité d'horodatage (aussi bien provisoire que permanent) du point de vue de la séparation des responsabilités et du principe du privilège minimum, selon la sensibilité de la fonction sur la base des responsabilités et des niveaux d'accès.

À ce titre, les rôles pouvant présenter des conflits d'intérêts ainsi que les aires de responsabilité feront l'objet, chaque fois que cela est possible, d'une séparation des rôles pour réduire les opportunités d'atteinte, volontaire ou non, à l'intégrité du SI ou d'une mauvaise utilisation des biens.

Les fiches de poste indiquent le type d'enquête à effectuer sur le passé, le type de formation appropriée et les particularités de la fonction. Quand cela est nécessaire, ces descriptions de fonctions font la différence entre les fonctions générales et les fonctions spécifiques à l'Autorité d'horodatage. Ces descriptions de fonctions incluent des exigences d'expérience et de compétences.

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- Le responsable de sécurité ne peut pas être administrateur système ou exploitant ;
- Le contrôleur ne peut pas être administrateur système ou exploitant.

Les porteurs de secret ne doivent jamais détenir deux parts différentes d'un même secret.

5.3.4. **Conflit d'intérêts**

Tout le personnel de l'AH dans des rôles de confiance est libre de conflits d'intérêt qui pourrait porter préjudice à l'impartialité des opérations de l'AH.

5.3.5. **Suivi des procédures**

Afin d'assurer le suivi des procédures, « la Société » a mis en place un Système de Management de la sécurité de l'information et de la qualité qui est certifié ISO 27001.

Le personnel effectue des procédures administratives et de gestion ainsi que des processus en accord avec les procédures de gestion de sécurité de l'information de l'Autorité d'horodatage.

6. Exigences de sécurité techniques

La présente section contient les exigences de sécurité techniques, en particulier relatives à l'exactitude du temps et à la cryptographie. En particulier, des mesures de contrôles appropriées sont mises en place pour toutes clés cryptographiques ou tout dispositif cryptographique tout a long de leur cycle de vie.

6.1. Contrôles récurrents de validité

Chaque unité d'horodatage effectue des contrôles récurrents (plusieurs fois par jour) sur la validité des certificats utilisés.

Ce contrôle effectue une vérification que le certificat n'est pas présent dans la LCR (Liste des Certificats Révoqués) et que le service « VAULTINUM TIMPESTAMPING » est bien présent dans la liste nationale de confiance publiée par l'ANSSI (https://www.ssi.gouv.fr/uploads/tl-fr.xml).

6.2. Exactitude temps

Les unités d'horodatage fournissent une exactitude de 1 seconde par rapport au temps UTC. La précision des horloges des UH est assurée par le mécanisme de synchronisation de l'horloge d'UH avec les sources de temps externes.

Le mécanisme de synchronisation des UH garanti que l'horloge des UH :

- Délivrent une Date et une heure avec la précision de 1 seconde par rapport au temps UTC ;
- Est uniquement synchronisée par rapport à plusieurs types de sources de temps externes UTC(k).

6.2.1. **Synchronisation de l'horloge des UH avec source de temps UTC(k)**

L'horloge de l'unité d'horodatage est simplement l'horloge du serveur (physique ou virtuel) exécutant l'application d'horodatage. C'est cette horloge qui fournit les dates et heures incluses dans les jetons d'horodatage.

La synchronisation de cette horloge est faite via le protocole NTP et s'appuie sur les serveurs de temps matériels de l'infrastructure de l'AH. Ces matériels sont eux-mêmes dotés d'une horloge interne précise. Le quartz interne des serveurs de temps matériels assure à son horloge une précision bien supérieure aux horloges standard des serveurs, capable de conserver l'heure malgré l'absence de synchronisation aux sources externes.

Deux serveurs de temps matériels sont maintenus et supervisés par l'infrastructure de l'AH, chacun d'eux sur un site géographique distinct (site principal et site de secours).

En cas de défaillance du serveur de temps du site principal, la bascule est réalisée de manière automatique sur le serveur de temps de secours. Une supervision est mise en place afin détecter cette panne et alerter les administrateurs. Une panne prolongée des deux serveurs de temps matériel entraînera l'arrêt de l'unité d'horodatage impactée.

La synchronisation de chaque serveur de temps matériels est faite sur trois sources de temps externes UTC(k) suivantes :

UTC(k)	Laboratoire	Serveurs NTP
UTC(OP)	Observatoire de Paris (FRANCE)	ntp.obspm.fr
UTC(PTB)	Physikalisch-Technische Bundesanstalt (GERMANY)	ptbtime1.ptb.de ptbtime4.ptb.de
UTC(ROB)	The Royal Observatory of Belgium (BELGIUM)	ntp1.oma.be ntp2.oma.be

En cas d'indisponibilité d'une source de temps de synchronisation,

- Le serveur utilise automatiquement une des autres sources disponibles,

- La perte de disponibilité de la source de temps est journalisée par le serveur de temps,
- La perte de disponibilité de la source de temps est remontée par le système de supervision du service,
- Le serveur de temps recommence toutes les minutes un contrôle de disponibilité de la source de temps. Le rétablissement est journalisé et remonté par le système de supervision du service.

6.2.2. **Contrôle de la dérive de l'horloge des UH**

Les exigences de la norme EN 319 422 imposent une surveillance de l'horloge (dérive de l'horloge) par rapport au temps UTC.

L'horloge des UH, synchronisée sur une source de temps fiable, est contrôlé en permanence pour être capable de détecter une dérive ou un saut hors de la précision annoncée qui pourrait faire suite à une défaillance matérielle du serveur de temps ou une attaque externe sur le matériel ou sur sa source.

La méthode adoptée est de comparer l'heure du serveur avec au moins 3 sources de temps externes synchronisées sur UTC et distinctes des sources de temps utilisées par les serveurs de temps.

Ces vérifications sont à réaliser toutes les minutes sur les sources de temps externes de contrôles.

Si l'heure du serveur d'horodatage est désynchronisée de plus de 500 ms par rapport à la majorité des sources de temps de contrôle, alors une alerte doit être levée. La dérive de l'horloge est journalisée et est remontée par le système de supervision du service.

Si l'heure du serveur d'horodatage est désynchronisée de plus de 900 ms par rapport à la majorité des sources de temps de contrôle, l'unité horodatage est dans ce cas arrêtée car l'écart met en danger la garantie de précision d'une seconde des jetons d'horodatage. La dérive de l'horloge et l'arrêt du service sont journalisés et sont remontés par le système de supervision du service. L'unité d'horodatage recommence toutes les minutes une mesure d'écart afin de reprendre l'émission de contremarques de temps dès que son horloge est revenue à la précision souhaitée.

Ces sources sont choisies parmi des serveurs de laboratoires UTC(k) diffusant l'heure sur Internet et parmi des serveurs français de temps de strate 2 (une liste des serveurs français est proposée sur https://services.renater.fr/ntp/serveurs_francais).

Les sources de contrôles externes UTC(k) utilisées sont les suivantes :

UTC(k)	Laboratory	Ntp servers
UTC(CH)	Federal Institute of Metrology (SWITZERLAND)	ntp.metas.ch
UTC(ROA)	El Real Instituto y Observatorio de la Armada (ESPANA)	hora.roa.es
UTC(IT)	Istituto Nazionale di Ricerca Metrologica (ITALIA)	ntp1.inrim.it
UTC(SP)	SP Technical Research Institute of Sweden (SWEDEN)	ntp1.sptime.se
UTC(NIST)	The National Institute of Standards and Technology (UNITED STATES)	time.nist.gov

6.2.3. **Gestion des sauts de seconde**

La gestion des sauts de seconde est entièrement automatisée par le service.

La survenue d'un saut de seconde est une information déclarée par les serveurs NTP, dès la première heure du jour de son occurrence. Les unités d'horodatage utilisent la donnée envoyée par les serveurs NTP afin de gérer un saut de seconde, et sont à tout moment synchronisées sur l'heure UTC.

Toutefois, en cas d'ajout de seconde intercalaire, le service ne produira pas de jeton pendant la seconde intercalaire (« 23:59:60 ») pour ne pas perturber une application utilisatrice qui ne saurait pas gérer cette seconde intercalaire.

6.2.4. **Prise en compte de menaces**

L'horloge de l'unité d'horodatage ne peut pas être modifiée, exceptée par un administrateur système de confiance. Une modification non autorisée de cette horloge serait détectée dès la prochaine comparaison de l'horloge de l'unité avec les sources de temps. Afin de se protéger contre une falsification des réponses NTP d'une source de temps non authentifiée, l'unité d'horodatage se base toujours au minimum sur deux sources de temps pour évaluer la dérive de sa propre horloge.

6.3. Génération de clé

L'AH garantit que toutes les clés cryptographiques sont produites dans des circonstances contrôlées. Cette génération est réalisée par des personnes en rôle de confiance, et sous contrôle double (dual control), c'est-à-dire que deux personnes en rôle de confiance sont requises pour toute opération de création de clés.

Le personnel autorisé à réaliser cette opération est limité à celle requise pour cette opération. La DPH confidentielle précise les moyens mis en place pour limiter cette capacité.

En particulier, la génération des clés de signature des unités d'horodatage est effectuée dans un module cryptographique (HSM)

- Certifié au niveau EAL4+ des critères communs ;
- Répondant aux exigences de qualification de l'ANSSI.

Les clés cryptographiques ne sont pas importées dans différents modules cryptographiques, sauf à des fins éventuelles de sauvegarde. En tout état de cause, une clé privée ne pourra être associée qu'à un et un seul certificat (voir chapitre 6.4 Certification des clés de l'unité d'horodatage). Seule une clé cryptographique peut être active à un instant.

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

Les clés publiques de vérification des unités d'horodatage sont mises à disposition des utilisateurs au travers d'un certificat d'unité d'horodatage rendu public sur le site de publication (voir chapitre 1.3 Publication du document).

Pour l'émission des certificats, l'AH utilise une Autorité de certification interne pour délivrer les certificats d'horodatage. Cette AC est conforme à la norme EN 319 411-1 comme le recommande la norme EN 319 421.

L'AH vérifie, lors de l'import du certificat de l'UH, qu'il provient bien de l'Autorité de Certification auprès de laquelle la demande de certificat a été effectuée. L'AH vérifie également que le certificat a été signé correctement. Cette vérification inclut la vérification de la chaîne complète de certificat jusqu'à l'autorité racine.

L'AH s'assure que l'UH ne peut être opérationnelle qu'une fois ces exigences remplies.

6.5. Protection des clés privées des unités d'horodatage

L'Autorité d'horodatage garantit que des clés privées des unités d'horodatage restent confidentielles et conservent leur intégrité. En particulier, les clés de signature des unités d'horodatage sont gardées et utilisées à l'intérieur d'un HSM aux caractéristiques définies dans chapitre 6.3 Génération de clé.

6.6. Exigences de sauvegarde des clés des unités d'horodatage

Les clés privées des unités d'horodatage peuvent faire l'objet de copies de secours, soit dans un module d'horodatage qualifié au niveau renforcé par l'ANSSI, soit hors d'un module d'horodatage, mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant doit offrir un niveau de sécurité équivalent ou supérieur au stockage au sein du module d'horodatage et, notamment, s'appuyer sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. L'évaluation de la robustesse cryptographique et le choix de l'algorithme s'appuient sur les normes référencées dans chapitre 6.8 Algorithmes obligatoires.

Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module d'horodatage de telle manière que les clés privées des unités d'horodatage ne soient à aucun moment en clair en dehors du module d'horodatage.

6.7. Destruction des clés des unités d'horodatage

L'AH garantit que les clés de signature des unités d'horodatage sont détruites à la fin de leur cycle de vie.

6.8. Algorithmes obligatoires

L'AH accepte de générer des contremarques de temps pour les empreintes calculées avec les algorithmes suivants :

- SHA-256
- SHA-384
- SHA-512

Les contremarques de temps sont signées selon les algorithmes et les longueurs de clé conformes à l'état de l'art. Actuellement, la bi-clé de l'UH est une bi-clé RSA de 3072 bits et l'algorithme de signature utilise une fonction de hachage SHA-512.

6.9. Vérification des contremarques de temps

L'AH garantit que les utilisateurs de contremarques de temps ont accès à l'information utilisable pour vérifier la signature numérique des contremarques de temps. En particulier les certificats des unités d'horodatage sont joints à la contremarque de temps, ils sont également publiés sur le site de « la Société » (voir chapitre 1.3 Publication du document).

L'AH garantit que les utilisateurs de contremarques de temps ont accès, pour une durée minimale d'un an à compter de la création de la contremarque, à l'information utilisable pour en vérifier la signature numérique. En particulier :

- Les certificats des UH sont disponibles, joints à la contremarque de temps sur demande et toujours disponibles sur l'espace de publication de l'AH (voir chapitre 1.3 Publication du document).
- La chaîne de certification complète est disponible sur l'espace de publication de l'AH (cf. chapitre Publication des informations).
- Les informations sur le statut de révocation des certificats sont disponibles en activant les URL disponibles dans les certificats des Unités d'Horodatage (extensions Authority Information Access et cRLDistributionPoint).

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

La durée de validité des certificats des UH ne doit pas être plus longue que :

- La durée de vie cryptographique de la clé privée associée ;
- La fin de validité du certificat d'AC qui l'a émis.

Par défaut, cette durée est de 3 ans.

6.11. Durée d'utilisation des clés privées des UH

La durée d'utilisation d'une clé privée sera au plus égale à la période de validité du certificat de clé publique correspondant. Toutefois elle sera en pratique réduite afin que la validité des contremarques de temps générées avec cette clé puisse être effectuée durant un laps de temps suffisant. En tout état de cause, la durée d'utilisation de la clé privée ne pourra dépasser 3 ans. Dans la pratique, elle sera renouvelée de façon anticipée afin de garantir un recouvrement entre nouvelles et anciennes UH.

Les clés privées ne peuvent être utilisées au-delà de leur période de validité. En particulier,

- Des mesures techniques et opérationnelles sont mises en œuvre de façon à mettre en place une nouvelle clé avant que la clé courante n'expire ;
- Les clés privées sont alors détruites, ainsi que toutes les copies de sauvegardes, afin que la clé ne puisse être restaurée.

6.12. Contrôle d'Accès

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

- Des contrôles (par pare-feu) sont mis en œuvre pour protéger le réseau interne de l'AH d'accès non autorisés incluant l'accès par des abonnés et des tierces personnes. Les pares-feux sont aussi configurés pour bloquer tous les protocoles et les accès non nécessaires au fonctionnement de l'AH ;
- Les liens entre les sites d'hébergement sont sécurisés et garantissent l'intégrité et la confidentialité des données échangées, notamment les flux vers les HSM ;
- L'AH effectue une administration efficace des utilisateurs (exploitants, administrateurs et auditeurs), pour maintenir la sécurité du système, y compris la gestion des comptes des utilisateurs, l'audit, et la modification ou le retrait rapide d'accès ;
- L'AH garantit que l'accès aux fonctions du système, à l'information et aux applications est limité conformément à la politique de contrôle d'accès et que le système d'horodatage possède les contrôles informatiques de sécurité suffisants pour la séparation des rôles de confiance identifiés dans les pratiques d'horodatage, y compris la séparation des fonctions d'administration des fonctions d'exploitation ;
- Le personnel de l'AH est dûment identifié et authentifié avant d'utiliser des applications critiques liées à l'horodatage ;
- Le personnel de l'AH est tenu responsable de ses activités.

Les contrôles complémentaires suivants sont appliqués à la gestion de l'horodatage :

- L'AH garantit que des composants de réseau locaux (par exemple les routeurs) seront mis dans un environnement physiquement sûr et que leurs configurations sont périodiquement vérifiées pour la conformité avec les exigences indiquées par l'AH ;
- Une surveillance permanente et des équipements d'alarme sont mis en œuvre pour permettre à l'AH de détecter, d'enregistrer et de réagir rapidement à n'importe quelle tentative non autorisée et/ou irrégulière d'accès à ses ressources ;
- L'AH garantit que les opérations d'administration système des plateformes sont réalisées exclusivement sur un réseau dédié, depuis un poste d'administration sans accès au réseau extérieur.

6.13. Sécurité des plateformes informatiques

L'AH applique la politique de sécurité des systèmes d'information sur toute l'infrastructure informatique du service d'horodatage. Cette politique garantit en particulier :

- Une organisation interne de la sécurité pilotée par un comité de suivi,
- La mise en place de système de contrôle de flux (détection d'intrusion, fermeture des ports non explicitement autorisé),
- La mise en place systématique de contrôle d'accès logique dont le niveau de sécurité est adapté au contexte d'emploi,
- Le passage obligatoire par un bastion pour tous les accès d'administration aux plateformes hébergées,

- L’interdiction de la connexion au réseau d’administration de l’entreprise sans connexion VPN,
- La traçabilité systématique des accès pour garantir entre autres l’imputabilité des actions,
- Le déploiement de solutions de sécurité pour lutter contre les virus et autres logiciels malveillants sur les plateformes du service,
- La gestion des vulnérabilités par analyse des alertes de sécurité communiquées par différentes sources,
- La conduite régulière de tests de vulnérabilité réseau,
- La conduite périodique, et au moins annuelle, de tests d’intrusion sur le système d’horodatage.

6.14. Disponibilité du service

L’AH assure une disponibilité du service de 99%. En cas de sinistre, l’AH s’engage à rétablir le service dans les 96h suivant l’identification du sinistre. En cas de sinistre majeur, l’AH s’engage à rétablir le service dans les 90 jours suivant l’identification du sinistre.

7. Audit de conformité et autres évaluations

7.1. Fréquences et / ou circonstances des évaluations

Un contrôle de conformité à la PH lors de la mise en œuvre opérationnelle du système, et lors de toute modification significative est effectué à travers un audit interne biannuel.

Cet audit interne est mené par des équipes internes de la « Société » ou bien à travers des prestations externes.

Dans le cadre d'obtention de qualification du service d'horodatage, l'audit d'évaluation de la conformité est réalisé par une société externe dûment accréditée.

7.2. Identités / qualification des évaluateurs

« La société » s'engage à mandater des personnes disposant des compétences en sécurité requises pour auditer et vérifier la conformité du système.

7.3. Relations entre évaluateurs et entités évaluées

L'auditeur est désigné par l'AH. Il est indépendant de l'entité opérant les composantes du système d'horodatage.

7.4. Périmètre des évaluations

L'auditeur s'assure que les politiques, déclarations et services sont correctement mis en œuvre et détecte les cas de non-conformités qui pourraient compromettre la sécurité du service offert.

L'auditeur procède de manière régulière à des contrôles de conformité de la mise en œuvre :

- De la politique d'horodatage
- Des déclarations de pratique d'horodatage
- Des services mis en œuvre

Il a notamment pour objectif de s'assurer que les pratiques mises en œuvre permettent de répondre aux exigences attendues par les niveaux de qualification obtenus par l'AH. Il s'assure également que les processus d'horodatage sont conformes aux procédures rédigées.

7.5. Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'auditeur rend à l'AH un avis qui peut être « réussite, échec, ou à confirmer ».

En cas d'échec, l'équipe d'audit remet des recommandations à l'AH ; le choix des mesures à appliquer appartient à l'AH.

En cas de résultat « à confirmer », l'équipe d'audit identifie les non-conformités, et les hiérarchisent ; il appartient au COPIL de proposer un calendrier de résolution des non-conformités ; un contrôle de vérification permettra de lever les non-conformités identifiées.

En cas de réussite, l'AH confirme à la composante contrôlée la conformité aux exigences de la PH.

7.6. Communication des résultats

Dans le cas d'une qualification de l'AH, les résultats d'audits sont tenus à la disposition de l'organisme en charge de la qualification.

8. Autres problématiques métiers et légales

8.1. Tarifs

8.1.1. Tarifs pour la fourniture de contremarques de temps

Se référer aux conditions contractuelles en vigueur.

8.1.2. Tarifs pour accéder aux informations publiées par l'AH

L'accès aux informations publiées par l'AH est gratuit.

8.2. Politique de remboursement

Se référer aux conditions contractuelles en vigueur.

8.3. Responsabilité financière

8.3.1. Couverture par les assurances

L'AH applique des niveaux de couverture d'assurance raisonnables et a souscrit à cet effet une assurance responsabilité civile au titre de la réalisation de son activité professionnelle.

8.3.2. Autres ressources

« La société » déclare disposer d'une garantie financière suffisante spécialement affectée à la couverture des risques financiers sur les activités de l'AH.

8.3.3. Couverture et garantie concernant les entités utilisatrices

Sans objet.

8.4. Confidentialité des données professionnelles

8.4.1. Périmètre des informations confidentielles

L'AH met en place un inventaire de tous les biens informationnels et procèdent à une classification de manière à définir des exigences de protection en accord avec les besoins.

En particulier, les informations suivantes sont traitées comme confidentielles :

- Les clés privées d'UH ;
- Les scripts de cérémonies ;
- Les codes d'activation des parts de secrets ;
- Les journaux d'événements ;
- La DPH et les procédures internes de l'AH.

8.4.2. Informations hors du périmètre des informations confidentielles

Sans objet.

8.4.3. Responsabilités en termes de protection des informations confidentielles

L'AH s'engage à traiter (et à faire traiter par les différentes parties prenantes) les informations confidentielles recueillies dans le respect des lois et règlements en vigueur.

Les informations fournies par les abonnés à l'AH ne sont pas divulguées, à moins de leur accord, d'une décision judiciaire ou d'une exigence légale.

8.5. Protection des données personnelles

Dans le cadre du service d'horodatage, l'AH ne traite aucune donnée personnelle et n'a donc pas de relations avec la CNIL pour ce service.

Les informations fournies par les abonnés à l'AH ne sont pas divulguées, à moins de leur accord, d'une décision judiciaire ou d'une exigence légale.

8.6. Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par « la Société » sont protégés par la législation et réglementation en vigueur.

Les utilisateurs ne disposent d'aucun droit de propriété intellectuelle sur les différents éléments mis en œuvre par « la Société » pour assurer son service d'horodatage.

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

8.7. Limite de responsabilité

« La Société » ne pourra pas être tenu pour responsable d'une utilisation non autorisée ou non conforme des contremarques de temps.

De plus, dans la mesure des limitations autorisées par la loi française, « la Société » ne saurait être tenu responsable :

- D'aucune perte financière ;
- D'aucune perte de données ;
- D'aucun dommage indirect lié à l'utilisation d'une contremarque de temps.

En toute hypothèse, la responsabilité de « la Société » sera limitée, tous faits générateurs confondus et pour tous préjudices confondus, au montant payé à « la Société » pour l'accès au service d'horodatage et ce, dans le respect et les limites de la loi applicable.

8.8. Indemnités

Sans objet.

8.9. Durée et fin anticipée de validité de la PH

8.9.1. **Durée de validité**

Cette PH reste en application jusqu'à la publication d'une nouvelle version.

8.9.2. **Fin anticipée de validité**

Cette PH reste en application jusqu'à la publication d'une nouvelle version.

8.9.3. **Effets de la fin de validité et clauses restant applicables**

Sans objet.

8.10. Amendements à la PH

8.10.1. **Procédures d'amendements**

Tout amendement de la PH devra être soumis au comité de suivi.

L'AH contrôlera que tout projet de modification de sa PH reste conforme aux exigences de la norme [ETSI_TIMESTAMP]. En cas de changement important, l'AH pourra faire appel à une expertise technique externe, si elle le juge nécessaire.

8.10.2. Mécanisme et période d'information sur les amendements

Lors de tout changement important impactant la PH, « la Société » informera les abonnés et les utilisateurs au travers d'un communiqué distribué par voie électronique sur son site internet. Si besoin, une communication par courrier électronique ou postal pourra être réalisée.

8.10.3. Circonstances selon lesquelles l'OID doit être changé

L'OID de la PH de l'AH peut être spécifié par un abonné dans les requêtes de contremarques de temps et est systématiquement inscrit dans les contremarques de temps générées par l'AH. Cet OID, en lien avec la PH qui est publique, permet aux abonnés et aux utilisateurs de connaître les conditions de génération des contremarques de temps et en particulier les exigences de sécurité associées.

Si ces conditions sont modifiées de façon importante (par exemple changement d'algorithme cryptographique, augmentation de la précision du temps contenu dans les contremarques, augmentation significative des exigences de sécurité opérationnelle), alors l'AH fera alors évoluer l'OID. Ainsi les abonnés et les utilisateurs pourront clairement distinguer quelles contremarques de temps correspondent à quelles conditions de génération et quelles exigences de sécurité associées.

En particulier, l'OID de la PH de l'AH évoluera dès lors qu'un changement majeur intervient dans les exigences de la norme [ETSI_TIMESTAMP] (et qui sera signalé comme tel, notamment par une évolution de l'OID BTSP de cette norme).

8.11. Dispositions concernant la résolution de conflits

Les présentes politiques sont soumises au droit français.

En cas de litige entre les parties découlant de l'interprétation, l'application et/ou l'exécution du contrat et à défaut d'accord amiable entre les parties ci-avant, la compétence exclusive est attribuée au tribunal de commerce de Paris.

8.12. Juridictions compétentes

Se rapporter au paragraphe précédent 8.11.

8.13. Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente PH sont, notamment, ceux de la loi française et du règlement européen eIDAS [EIDAS].

8.14. Transfert d'activités

Voir chapitre 4.7 Fin d'activité de l'AH.

9. Documents cités en référence

9.1.1. **Réglementations**

[eIDAS]	Règlement n°910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n°1999/93/CE https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32014R0910
[GDPR]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27avril 2016

9.1.2. **Documents normatifs**

[ETSI_TSP]	ETSI EN 319 401 V2.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.03.01_60/en_319401v020301p.pdf
[ETSI_TIMESTAMP]	ETSI EN 319 521 V1.1.1 (2019-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers. https://www.etsi.org/deliver/etsi_en/319500_319599/319521/01.01.01_60/en_319521v010101p.pdf
[ANSSI_PSCO]	Prestataires de services de confiance qualifiés – Critères d'évaluation de la conformité au règlement eIDAS, Version 1.2 du 5 juillet 2017 https://www.ssi.gouv.fr/uploads/2017/01/eidas_psc-qualifies_v1.2_anssi.pdf
[ANSSI_HORODATAGE]	Services d'horodatage électronique qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, Version 1.1 du 3 janvier 2017 https://www.ssi.gouv.fr/uploads/2016/06/eidas_horodatage-qualifie_v1.1_anssi.pdf
[ANSSI_RGS_HOR]	Référentiel Général de Sécurité version 2.0 - Annexe A5 Politique d'Horodatage Type, Version 3.0 du 27 février 2014 https://www.ssi.gouv.fr/uploads/2016/06/eidas_horodatage-qualifie_v1.1_anssi.pdf
[RFC_3161]	Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP) https://www.ietf.org/rfc/rfc3161.txt
[RFC_5816]	ESSCertIDv2 Update for RFC 3161 https://www.ietf.org/rfc/rfc5816.txt

10. Formats des contremarques de temps, des certificats et des LCR

10.1. Contremarque de temps

Les réponses envoyées par le service d'horodatage respectent le format décrit par la [RFC_3161] (dans son paragraphe §2.4.2) amendée par la [RFC_5816]. Elles sont signées par la clé privée de l'unité d'horodatage qui les produit.
En particulier, les champs significatifs (structure TSTInfo) sont définis comme suit :

Champ	Valeur
Version	1
Policy	OID de la PH applicable (1.3.6.1.4.1.60053.2.1.1.1.1)
MessageImprint	Contient l'identifiant de l'algorithme d'empreinte utilisé par l'Application pour calculer une représentation de la donnée à horodater.
SerialNumber	Renseigné par l'UH avec un numéro de série unique
GenTime	Contient la date et l'heure UTC
Accuracy	Précision 1 seconde.
Ordering	Ce champ est absent et donc non renseigné.
Nonce	Renseigné seulement si l'Application utilisatrice transmet une valeur pour ce champ qui est en ce cas reprise à l'identique dans ce champ
Tsa	Non renseigné
Extensions	Extension non critique qcStatements (1.3.6.1.5.5.7.1.3) contenant l'attribut « esi4-qtstStament-1 » (0.4.0.19422.1.1)
ESSCertIDv2	Identifiant du certificat de l'unité d'horodatage.

Si la requête demande la fourniture du certificat de l'unité d'horodatage par le champ certReq, alors ce certificat est fourni dans le champ certificates de la structure SignedData

10.2. Certificats et LCR

Les gabarits des certificats d'UH sont conformes à la PC de l'AC émettrice (voir chapitre 7 de la PC AC Horodatage) : suivante https://vaultinum.com/fr/publication-autorite-horodatage

L'OID du profil est 1.3.6.1.4.1.60053.1.2.1.1.1

Les LCR sont conformes à la PC de l'AC émettrice.

Philippe THOMAS

Certified by yousign