Politique et déclarations des pratiques d'horodatage

Service Mailstone Timestamp

Version	Date	Description	Auteurs	Société
1.2	04/10/2022	Modification mineure	JR. Quiriconi	MAILSTONE
1.3	26/07/2024	• Correction de la description du service Mailstone Timestamp et son lien avec le service Mailstone • Ajustement de quelques libellés (Mailstone, client, …etc.) • Reformulation de certaines phrases • Correction de quelques fautes mineures • Mise à jour des obligations du client Mailstone • Suppression de la notion "d'utilisateur final", remplacement par client Mailstone • Renommage du document en "Politique et déclarations des pratiques d'horodatage" (anciennement "Politique d'horodatage") • Mise à jour d'une des déclarations de pratique en rapport avec la publication des documents • Ajout de la phrase "Mettre à dispo des clients les CGH et CGU" avant tout engagement contractuel, dans les obligations de l'AH • Ajout de la phrase "Prendre connaissance des CGH et CGU" avant tout engagement contractuel, dans les obligations des clients.	K. ELGUEBAIS	MAILSTONE

Etat du document – Classification	Référence
Valide – Public	1.3.6.1.4.1.57916.1.1.1.1.1

Table des matières

1 INTRODUCTION

1.1 PRESENTATION GÉNÉRALE

Mailstone est une solution simple de gouvernance des échanges numériques. Mailstone enregistre l'empreinte numérique d'emails, de pièces jointes et d'accusés de lecture, dans une contremarque de temps ainsi que dans une transaction blockchain. La solution délivre des preuves de leur intégrité et renforce ainsi leur valeur juridique.

Le service Mailstone Timestamp a pour objectif principal de délivrer des contremarques de temps conformes à la norme RFC 3161. Ces contremarques sont émises par l'Autorité d'Horodatage (AH) de Mailstone nommée Mailstone Timestamp, qui fait l'objet d'une qualification de service de confiance conformément au règlement eIDAS n° 2014/910 et aux normes ETSI (319/401 V2.3.1, 319/421 V1.2.1).

Le présent document, intitulé Politique et Déclaration des Pratiques d'Horodatage (PH-DPH), a pour objectif de définir les engagements pris par Mailstone, en tant qu'Autorité d'Horodatage (AH), pour la délivrance et la gestion des contremarques de temps qualifiées. Il contient aussi la Déclaration des Pratiques d'Horodatage (DPH).

La présente PH décrit les procédures techniques et organisationnelles mises en œuvre pour le respect de ces engagements, et définit les obligations des parties prenantes. En particulier, cette politique décrit les moyens mis en œuvre pour atteindre les objectifs de sécurité du service d'horodatage, notamment pour la création des contremarques de temps et le maintien de l'exactitude des horloges.

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

Le respect de cette politique permet la qualification du service d'horodatage de Mailstone par l'organe de contrôle national, après l'audit d'évaluation de la conformité selon les processus établis dans le règlement eIDAS et les normes ETSI (cf. [EIDAS] et [ETSI_TSP]). Les clauses principales de ce document sont synthétisées dans les Conditions Générales d'Utilisation du service d'horodatage (CGH), que les clients de Mailstone s'engagent à respecter. Ces CGH sont indépendantes des Conditions Générales du Service (CGS) Mailstone. Le service Mailstone Timestamp est distinct du service Mailstone.

2 IDENTIFICATION DU DOCUMENT

La présente Politique d'Horodatage (PH) est dénommée « *Politique d'Horodatage Mailstone Timestamp* ». Elle peut être identifiée par son numéro d'identifiant d'objet OID propre à Mailstone : 1.3.6.1.4.1.57916.1.1.1.1.1.

Ce présent document est conforme à la politique d'horodatage décrite dans le document [ETSI_TIMESTAMP] et identifiée par l'OID BTSP 0.4.0.2023.1.1 (itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)).

La décomposition de l'OID Mailstone est la suivante :

- Racine OID obtenue auprès de l'IANA : **1.3.6.1.4.1.57916**
    - 1 : Projet Mailstone Timestamp
        - 1 : Environnement technique Production
            - 1 : AH qualifiée
                - 1 : Politique d'horodatage
                - 1 : Version

2.1 GESTION DE LA POLITIQUE

L'entité en charge de l'administration et de la gestion de la politique d'horodatage (PH) est l'AH. Pour cela Mailstone met en place un comité de suivi des services de confiance (C2SC) composé de membres fondateurs, associés et collaborateurs de Mailstone, ayant reçu un rôle de confiance.

Le comité de suivi est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PH.

Des précisions sont données sur le processus d'amendement de la PH au §10.10.

L'organisation de l'AH est fiable. Les pratiques de service de confiance qu'opère l'AH ne sont pas discriminatoires.

2.2 POINT DE CONTACT

Toute demande relative à la présente Politique d'Horodatage est à adresser à :

MAILSTONE

IMMEUBLE LE MERCURE C POLE D'ACTIVITES,

485 RUE MARCELIN BERTHELOT,

13 290 AIX-EN-PROVENCE

contact@mailstone.fr

2.3 DÉFINITIONS ET ABRÉVIATIONS

2.3.1 Abréviations

Pour le présent document, les abréviations suivantes s'appliquent :

AC	Autorité de Certification
AH	Autorité d'Horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
BTSP	Best practices Time-Stamp Policy
CGH	Conditions Générales d'Horodatage
CGS	Conditions Générales du Service Mailstone
DN	Domain Name
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
PSHE	Prestataire de Services d'Horodatage Electronique
TSP	TimeStamp Provider
UH	Unité d'Horodatage
UTC	Coordinated Universal Time
DPH	Déclaration des Pratiques d'Horodatage

2.3.2 Définitions

Client– Client de la solution Mailstone.

Autorité de Certification (AC) – Entité qui délivre et est responsable des Certificats électroniques signés en son nom, conformément à sa Politique de Certification. Dans le contexte de la présente PH, l'AC est l'autorité qui produit les certificats d'horodatage mis en œuvre dans l'infrastructure Mailstone.

Autorité d'Horodatage (AH) – Entité en charge de l'émission et de la gestion des contremarques de temps conformément à une Politique d'Horodatage.

Contremarque de temps – Donnée signée 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) – Echelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-5 [TF.460-5].

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.

Liste de Certificats Révoqués (LCR) – Liste de certificats ayant fait l'objet d'une révocation avant la fin de leur période de validité.

Mailstone – Société immatriculée au RCS de Aix en Provence **n°**852 381 052 qui délivre et administre l'Autorité d'Horodatage (AH) de Mailstone, nommée Mailstone Timestamp.

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 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 les exigences de sécurité satisfaites. Une PH identifie également les obligations et exigences portant sur les autres intervenants, notamment les clients Mailstone. La PH identifie aussi les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AH applique dans le cadre de la fourniture de ses services d'horodatage pour respecter les exigences qui lui incombe.

Service d'horodatage – Ensemble des prestations nécessaires à la génération et à la gestion des 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 des 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 de contremarque de temps – Entité (personne morale ou physique) qui dispose d'une contremarque de temps émise par le Service d'Horodatage de Mailstone Timestamp dans le cadre de la présente Politique d'Horodatage et qui a accepté les Conditions Générales d'Horodatage du service Mailstone Timestamp.

Empreinte numérique - Valeur de hachage unique générée à partir du contenu d'un fichier ou d'un message.

Blockchain – v. norme ISO 22739 :2024 (Chaîne de blocs et technologies de registres distribués - ISO TC 307). La blockchain est une technologie appartenant à la catégorie des registres électroniques définis par le règlement n° 2024/1183 du 11 avril 2024 comme une "séquence d'enregistrements de données électroniques qui garantit l'intégrité de ces enregistrements et l'exactitude du classement chronologique de ces enregistrements".

2.4 LIEN ENTRE LE SERVICE MAILSTONE TIMESTAMP ET MAILSTONE

La solution Mailstone propose un service d'enregistrement d'empreintes numériques d'e-mails dans une contremarque de temps ainsi que dans une blockchain, permettant ainsi d'obtenir des preuves de l'intégrité d'un e-mail et de ses pièces jointes.

La mission du service Mailstone Timestamp, utilisé exclusivement en interne par le service Mailstone, est de délivrer les contremarques de temps pour ce dernier.

Mailstone Timestamp fournit une contremarque de temps en réponse à une requête contenant l'empreinte de la donnée à horodater.

L'empreinte de la donnée est établie par le service Mailstone lorsqu'il capture un e-mail.

La vérification des contremarques de temps émises par le service Mailstone Timestamp peut être effectuée depuis n'importe quel outil supportant la norme RFC3161 sur laquelle est basée la solution.

La fourniture d'un horodatage en réponse à une demande est à la discrétion de l'AH en fonction du niveau de service contractualisé avec le service Mailstone.

3 DISPOSITIONS GÉNÉRALES

3.1 OBLIGATIONS DE L'AUTORITÉ D'HORODATAGE

L'Autorité d'horodatage doit respecter les obligations suivantes :

- L'AH met à disposition des futurs clients du service Mailstone, l'ensemble des conditions générales d'utilisation, avant tout engagement contractuel.
- L'AH génère et signe les contremarques de temps conformément à la présente PH et aux CGH associées.
- L'AH garantit la conformité pour tout acteur intervenant dans la gestion des contremarques de temps par rapport aux exigences et aux procédures prescrites dans cette PH.
- L'AH remplit tous ses engagements tels que stipulés dans ses Conditions Générales d'Horodatage.
- L'AH met à la disposition de ses clients l'ensemble des informations nécessaires à la vérification des contremarques de temps.
- L'AH respecte les conditions de disponibilité du service d'horodatage convenues contractuellement avec les clients.
- L'AH maintient une information sur la compromission de la bi-clé des UH.

3.2 OBLIGATIONS DU CLIENT DU SERVICE MAILSTONE

Le client doit respecter les obligations suivantes :

- Prendre connaissance de l'ensemble des conditions générales d'utilisation du service Mailstone et Mailstone Timestamp, avant tout engagement contractuel.
- Accepter et respecter les CGH et les CGU ;
- Respecter les obligations de la présente PH qui lui sont applicables ;

- Vérifier la validité des contremarques de temps qu'il reçoit (selon les directives données au §5.45.4

3.3 OBLIGATIONS POUR LES ACS FOURNISSANT LES CERTIFICATS DES UHS

Les certificats doivent être délivrés par une AC conforme à la norme [ETSI_AC]. Mailstone fait le choix d'acquérir ce certificat auprès de la société Certinomis. Le certificat obtenu est généré par l'AC « Certinomis - Timestamp CA » et identifié par l'OID 1.2.250.1.86.2.6.5.24.1. Ce certificat est conforme à la norme [ETSI_AC], respecte les gabarits de certificats d'horodatage de la norme [ETSI_CERT_UH] et est qualifié selon le règlement eIDAS.

La Politique de Certification applicable est consultable ici :

http://www.certinomis.fr/publi/pc/2021/PC_SERVEUR_RGS2E_Qualifie_eIDAS_v1.94.pdf

La politique est téléchargeable sur le site Certinomis sur la page : https://www.certinomis.fr/nos-certificats-racines/nos-politiques-de-certification (et pour le lien « Politique Serveur RGS 2E » éventuellement).

L'AC doit assurer la publication et l'actualisation des données nécessaires à la vérification des certificats qu'elle délivre, y compris son propre certificat et la liste actualisée des certificats révoqués.

3.4 DÉCLARATIONS DES PRATIQUES D'HORODATAGE (DPH)

L'AH garantit qu'elle possède la fiabilité nécessaire pour fournir le service d'horodatage. En particulier :

a) L'AH a effectué une analyse de risques afin de déterminer les contrôles de sécurité nécessaires et les procédures opérationnelles.

b) L'AH a établi un ensemble de procédures internes pour répondre à toutes les exigences identifiées dans cette PH.

c) La PH identifie les obligations de toutes les organisations externes participant à la fourniture du service d'horodatage, y compris la politique applicable et les pratiques. Cela inclut l'AC fournissant les certificats aux UH.

d) L'AH met à la disposition des clients du service Mailstone tous les éléments publics de ses procédures opérationnelles dans sa PH, et, s'il y a lieu, toute autre documentation appropriée, tel que nécessaire pour évaluer la conformité à la PH.

e) L'AH dispose d'une organisation adéquate pour la vérification de concordance entre les procédures opérationnelles exposées dans la PH et les engagements pris dans la PH.

f) Le responsable opérationnel de l'AH garantit que les pratiques sont correctement mises en œuvre.

g) L'AH définit une procédure de contrôle périodique de la conformité des pratiques, y compris les responsabilités, à la politique d'horodatage.

h) L'AH informe le client de la mise à jour de sa politique d'horodatage, en respectant les délais du paragraphe 4.3.

i) L'AH ayant été évaluée conforme avec la présente PH, si une modification envisagée à l'initiative de l'AH pouvait entraîner une non-conformité avec ladite PH, alors l'AH soumettrait cette modification à l'organisme évaluateur indépendant pour avis.

3.5 CONDITIONS GÉNÉRALES D'HORODATAGE

L'AH définit des CGH qui reprennent les grands principes décrits dans la présente PH. Ces CGH sont conformes à l'annexe 1 du document [ETSI_TIMESTAMP].

Les CGH du service d'horodatage sont mises à la disposition des clients du service Mailstone (cf. §4.3).

4 PUBLICATION DES INFORMATIONS

4.1 RESPONSABLE DE LA PUBLICATION

L'AH est responsable de la publication des informations requises.

4.2 INFORMATIONS PUBLIÉES ET LOCALISATION

Les informations mises à disposition des clients du service Mailstone sont les suivantes :

- Le présent document, constituant à la fois la Politique d'Horodatage (PH) et les Déclarations des Pratiques d'Horodatage (DPH),
- Les Conditions Générales d'Horodatage (CGH),
- Les certificats des Unités d'Horodatage.

Les documents sont disponibles directement ici : https://www.mailstone.io/terms

Les Listes de Certificats révoqués par l'AC « Certinomis - Timestamp CA » ayant délivré les certificats d'UH et la chaîne de certification, sont publiées par Certinomis et disponibles sur les liens suivants :

https://www.certinomis.fr/nos-certificats-racines/nos-listes-de-revocations

4.3 DÉLAIS DE PUBLICATION

Les présentes PH et DPH, ainsi que les CGH sont publiés 24h au plus tard après validation d'une nouvelle version par le C2SC et avant la production d'une contremarque de temps sous les nouvelles conditions.

Cette validation est effective avec la signature du PV de la réunion du comité par l'ensemble des membres présents à ce comité.

5 EXIGENCES OPÉRATIONNELLES

5.1 SYNCHRONISATION DE L'HORLOGE

L'AH garantit que son horloge est synchronisée avec le temps UTC selon l'exactitude déclarée d'une seconde.

Mailstone met en œuvre dans son architecture des boîtiers de temps autonomes qui permettent de synchroniser en interne les différents systèmes via le protocole NTP.

La synchronisation externe des boîtiers de temps autonomes se basent sur :

- Boitier 1 : des sources NTP reliées à une source UTC(k). Les serveurs NTP utilisés sont les suivants :
  - ntp.obspm.fr
  - ntp1.jussieu.fr
  - fr.pool.ntp.org
- Boitier 2 : Une source GPS directement rattachée au boîtier de temps.

A travers son architecture mise en œuvre, Mailstone couvre les exigences suivantes en particulier :

a) Le calibrage de chaque horloge d'UH est maintenu de telle manière que les horloges ne puissent pas normalement dériver en dehors de l'exactitude déclarée.

b) 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.

c) L'AH s'assure que tout non-respect de l'exactitude déclarée par son horloge interne sera détecté.

d) Si l'horloge d'une UH est détectée comme étant en dehors de l'exactitude annoncée, ou que les serveurs de temps ne sont plus disponibles, alors les contremarques de temps ne seront plus générées.

e) L'AH garantit que la synchronisation de l'horloge est maintenue lorsqu'un saut de seconde est programmé comme notifié par l'organisme approprié. Le changement pour tenir compte du saut de seconde est effectué durant la dernière minute du jour où le saut de seconde est programmé. Un enregistrement du temps exact (à la seconde près) de l'instant de ce changement est effectué. Les contremarques de temps sont suspendues 5 minutes avant un saut de secondes, et sera à nouveau disponible 5 minutes après celui-ci.

Les mesures de sécurité techniques mises en place pour le respect de ces exigences sont décrites au §77.1.

En cas de désynchronisation des horloges système des UC, il peut être effectué des opérations de resynchronisation manuelles.

5.2 REQUÊTE ET RÉPONSE DU SERVICE D'HORODATAGE

L'AH fournit une contremarque de temps en réponse à une requête contenant l'empreinte de la donnée à horodater.

La requête spécifie également l'identifiant de la PH à utiliser. Le service d'horodatage s'assure que l'identifiant fourni dans la requête est bien autorisé avant de produire la réponse.

La fourniture d'une contremarque de temps en réponse à une demande n'excède pas quelques secondes[1], ceci afin de ne pas nuire ni dégrader l'ergonomie de l'application appelante.

L'AH Mailstone conserve la contremarque de temps générée.

Les précisions concernant le protocole et le format des requêtes au service d'horodatage, sont fournies au §8.38.3.8.2

5.3 CONTENU D'UNE CONTREMARQUE DE TEMPS

Les contremarques de temps sont générées dans un environnement sûr et contiennent les informations suivantes conformes à la norme [RFC_3161] :

- L'identifiant de l'UH fourni à travers le DN du certificat de l'unité d'horodatage,
- L'identifiant (OID) de la politique d'horodatage appliquée,
- Un identifiant unique de la contremarque,
- Un temps, celui du moment de génération de la contremarque, synchronisé avec le temps UTC avec une précision d'une seconde,
- L'empreinte et l'algorithme d'empreinte de la donnée horodatée.

La contremarque de temps est signée par l'UH avec sa clé privée, réservée à cet usage.

Les précisions concernant le format des contremarques de temps sont données au §8.38.3.

5.4 VÉRIFICATION DES CONTREMARQUES DE TEMPS

Comme évoqué au paragraphe §3.23.2, la vérification des contremarques de temps doit se faire de la manière suivante :

- Vérifier que l'OID porté dans la contremarque correspond bien à celui qu'il a demandé, et que cet OID est identifié dans la présente PH ;
- Vérifier que le format de la contremarque correspond à celui décrit au §8.38.3;
- Calculer l'empreinte de la donnée qui a été horodatée et vérifier que cette empreinte est celle contenue dans la contremarque ;

[1] Ce temps de réponse est le délai écoulé entre la réception de la requête et la signature de la contremarque de temps résultante.

- Vérifier que la contremarque de temps est qualifiée au titre du règlement eIDAS en s'appuyant sur la liste de confiance eIDAS publiée par l'ANSSI ;
- Vérifier que le certificat de l'UH porte bien l'OID indiqué au §23.3 ;
- Vérifier que le certificat de l'UH est signé par la bonne AC et n'était pas expiré au moment de la génération de la contremarque de temps ;
- Vérifier que le certificat de l'UH n'est pas révoqué par l'AC ayant émis le certificat d'UH, en utilisant la LCR publiée par l'AC ou son service OCSP. Dans le LCR, il faut vérifier que le numéro de série du certificat d'UH :
    - Soit n'est pas présent. Le certificat n'a donc pas été révoqué ;
    - Soit est présent mais avec une date de révocation postérieure à la date de production de la contremarque ;
- Vérifier le statut de la contremarque de temps en s'appuyant sur la Trusted List ANSIhttps://cyber.gouv.fr/sites/default/files/document/tl-fr.xml ainsi que la norme ETSI 319 422 (§4 et §5), norme qui elle-même se base sur les RFC 3161 et 5816).

6 MESURES DE SÉCURITÉ NON-TECHNIQUES

6.1 MESURES DE SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

Mailstone dispose d'une architecture répartie sur plusieurs sites physiques. Les composants applicatifs sont hébergés auprès d'un hébergeur SecNumCloud (https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/referentiels-exigences) et les composants sensibles (HSM et boîtiers de temps) sont hébergés sur un site certifié ISO 27001 dans un espace (baie) dédié à Mailstone.

Quel que soit le type d'hébergeur les exigences ci-dessous s'appliquent.

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

Des mesures de sécurité sont mises en place sur les sites d'hébergement de l'infrastructure du système d'horodatage, afin de protéger l'environnement et les composantes elles-mêmes. Ces mesures sont les suivantes :

a) Contrôle d'accès physique :

L'accès physique aux équipements du service d'horodatage est limité aux seuls individus autorisés. Si nécessaire, une personne non-autorisée peut accéder à certaines installations si elle est accompagnée de façon permanente par une personne habilitée. Dans le cas des composants applicatifs hébergés dans l'environnement SecNumCloud, l'accès physique est interdit pour le personnel Mailstone.

Les sites, accessibles 24H/24H, 7j/7j, sont sous la surveillance permanente d'une équipe de sécurité. Les accès sur les sites sont sécurisés et strictement règlementés. Une double vérification de l'identité et de l'autorisation d'accès de chaque intervenant sur le site est effectuée au poste de sécurité.

Un système d'accès par badge individuel complète ce dispositif en limitant l'accès aux zones autorisées et en permettant une traçabilité des personnes sur le site.

De plus, la sûreté des locaux est assurée par un système CCTV. Un nombre important de caméras filment et enregistrent numériquement les locaux et l'extérieur des bâtiments. Une batterie de moniteurs de contrôle enregistre et conserve les données filmées sur une période allant jusqu'à 6 mois.

L'accès à la zone serveur contenant la baie dédiée à Mailstone fait l'objet d'une surveillance vidéo 24H/24H, 7J/7J. Ces matériels sont placés dans des baies fermées à l'aide d'un code (connu seulement par le personnel Mailstone) et à l'aide d'une clé accessible que par le personnel du site. Cette clé n'est utilisée qu'à la suite d'une demande d'intervention demandée par le personnel Mailstone ou en cas d'intervention de sécurité majeure, pour lequel le personnel Mailstone est informé.

b) Protection vis-à-vis des catastrophes naturelles :

Les datacenters sont situés sur des sites non exposées à des risques naturels ou environnementaux majeurs. L'analyse de risque propre à ces sites prend en compte la situation géographique et propose les mesures de sécurité adaptées au contexte.

Les mesures mises en œuvre assurent la protection contre un écroulement du bâtiment.

c) Prévention et protection incendie :

La protection contre les incendies repose sur un ensemble de moyens :

- Un système de sécurité incendie de catégorie A
- Un système d'extinction par Azote
- Application des règles R7/R13/R4
- Maintenance de la norme NFS 940
- Formation régulière des équipes
- Moyens d'accueil et d'intervention pompiers
- Murs stables au feu 2 heures et portes coupe-feu 1 heure

d) Protection contre la défaillance d'alimentation électrique :

Les sites bénéficient de deux alimentions provenant de deux sous stations EDF différentes et cheminant par deux arrivées privatives distinctes. En cas de disparition d'une alimentation, le basculement sur le deuxième câble toujours sous tension est effectif au bout de 5 secondes.
Toute l'installation électrique est assurée de base en N+1 minimum.
Le site dispose de trois groupes électrogènes permettant une autonomie effective de cinq jours à pleine charge. En cas d'absence totale de tension sur les deux câbles EDF, les groupes électrogènes prennent le relais automatiquement en 20 secondes.

e) Protection contre la défaillance de connexions réseau :

Les sites disposent de deux arrivées réseau distinctes par des fournisseurs d'accès différents. Les équipements du site garantissent de façon transparente aux ressources hébergées un accès continu au réseau.

f) Climatisation :

Les salles sont climatisées par trois groupes froid, redondées en N+1, avec une configuration en allées chaudes et froides garantissant une température optimale de fonctionnement (maximum 30/35°C dans les allées chaudes).
La norme d'hygrométrie admise est de 50% avec + ou – 10% d'écart.

g) Protection contre les dégâts des eaux et les fuites de plomberie :

- Détection de l'eau dans les faux planchers
- Architecture de drainage (pompes de drainage et relevage dans les galeries en sous-sol)

h) Protection contre le vol, la casse et la pénétration :

Des contrôles sont mis en œuvre sur site pour empêcher des équipements, de l'information, des médias et du logiciel touchant aux services d'horodatage d'être enlevés du site sans autorisation.

i) Rétablissement de la sécurité après un désastre :

Les sites disposent de plans de continuité et de reprise d'activité à même de garantir une disponibilité de 99,8%.

6.2 MESURES DE SÉCURITÉ PROCÉDURALES

6.2.1 Sécurité des systèmes

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

- L'intégrité des composants du système d'horodatage et l'information sont protégés 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. Tout incident de sécurité sur le service d'horodatage est signalé aux autorités compétentes.
- 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.

6.2.2 Manipulation et sécurité des supports

Tous les supports sont traités de manière sécuritaire conformément aux exigences de la classification de l'information. Les supports contenant des données sensibles sont retirés de manière sécuritaire quand ils ne sont plus utiles. Cela concerne notamment les HSM et la destruction des clés privées lors de la fin d'utilisation.

6.2.3 Planification de système

Les charges sont contrôlées et des projections de charge dans le futur sont effectuées pour garantir que les puissances de traitement et de stockage adéquates resteront disponibles.

6.2.4 Rapport d'incident et réponse

L'AH 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.

6.3 PROCÉDURES DE FONCTIONNEMENT ET RESPONSABILITÉS

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

Les opérations de sécurité sont séparées des autres opérations. Elles 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.

Les opérations de sécurité sur les composantes du service d'horodatage sont réalisées par du personnel de confiance.

L'AH met en place un C2SC pour piloter et décider des choix importants liés au service d'horodatage. Le comité de suivi établit 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.

6.4 DÉPLOIEMENT ET MAINTENANCE

L'AH 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.

6.5 MESURES DE SÉCURITÉ VIS-À-VIS DU PERSONNEL

L'AH garantit que le personnel et les pratiques d'embauche améliorent et concourent à la fiabilité des opérations de l'AH. En particulier :

- L'AH emploie un personnel qui possède l'expertise, l'expérience et les qualifications nécessaires pour les services offerts, tels que l'exige la fonction.
- Les rôles de sécurité et les responsabilités, comme spécifié dans la politique de sécurité de l'AH, sont documentés dans des descriptions de poste. Les rôles de confiance, sur lesquels la sécurité du fonctionnement de l'AH repose, sont clairement identifiés.
- Le personnel met en œuvre des procédures administratives et de gestion ainsi que des processus en accord avec les procédures de gestion de sécurité de l'information de l'AH

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

- 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.
- Tout le personnel de l'AH dans des rôles de confiance est libre de conflit d'intérêt qui pourrait porter préjudice à l'impartialité des opérations de l'AH.
- Les rôles de confiance incluent les rôles qui impliquent les responsabilités suivantes :
  - **Responsable légal / Responsable AH** : personne disposant du pouvoir de décision sur les choix de l'AH ;
  - **Responsable opérationnel du service / responsable production** : personne en charge d'assurer le Maintien en Conditions Opérationnelles de la plateforme ;
  - **Responsable sécurité** : personne en charge d'assurer le Maintien en Conditions de Sécurité de la plateforme, la rédaction et l'application de la PSSI ;
  - **Membre du Comité de suivi** : personnes participant au suivi et aux décisions du service d'horodatage ;
  - **Les administrateurs des plateformes** : autorisés à installer, configurer et maintenir les unités d'horodatage de l'AH pour la gestion de l'horodatage ;

- **Les exploitants** : responsables du fonctionnement des unités d'horodatage de l'AH de manière quotidienne et autorisés à effectuer les opérations de sauvegarde et de secours ;
- **Les auditeurs de système** : autorisés à consulter les archives et les fichiers d'audit des unités d'horodatage ;
- **Les responsables des certificats d'UH** : personne disposant d'une délégation pouvant commander et obtenir un certificat pour une UH de Mailstone ;
- **Porteurs de secret** : personne disposant d'une part du secret permettant l'activation et l'utilisation du HSM et donc la mise en œuvre des clés privées des UH ;
- **Responsable juridique** : personne en charge d'assurer le suivi des points d'ordre juridique du service d'horodatage ;
- **Responsable d'audit** : personne en charge d'assurer le suivi des audits internes et des audits de qualification.

- Le personnel de l'AH est formellement nommé aux rôles de confiance par la direction.
- L'AH s'interdit de nommer 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.

6.6 CONSTITUTION DES DONNÉES D'AUDIT

L'AH enregistre les informations appropriées concernant le fonctionnement du service d'horodatage, en particulier :

- Les enregistrements d'audit relatifs à l'administration des services d'horodatage :
  - Gestion des opérateurs d'administration
  - Connexion / déconnexion des opérateurs d'administration (même en cas d'échec)
  - Configuration technique ou métier (définition d'une politique d'horodatage)
- Les enregistrements d'audit relatifs au fonctionnement du service d'horodatage :
  - Démarrage et arrêt des services
  - Traitement d'une demande de contremarque de temps
  - Défaillance / indisponibilité du service
- Les enregistrements d'audit concernant les événements touchant au cycle de vie des clés et certificats d'UH :
  - Génération de clés
  - Demande de certificat
  - Import du certificat
  - Désinstallation d'un certificat

- Destruction de la clé privée

- Les enregistrements d'audit concernant les événements touchant à une synchronisation de l'horloge des UH, y compris les événements touchant à la détection de perte de synchronisation :

  - Déclaration des sources de temps
  - Pertes d'accès à une source de temps
  - Détection de perte de synchronisation
  - Resynchronisation de l'horloge
  - Saut de seconde

Chacun de ces événements comprend au minimum les données suivantes :

- Type de l'événement
- Auteur (personne physique, système)
- Date et heure
- Résultat de l'évènement (échec ou réussite)

L'intégrité, la protection contre la suppression et la confidentialité des enregistrements d'audit sont assurés par une gestion d'accès physique, système et réseau appropriée.

Les traces techniques sont conservées sans purge sur les équipements du système d'horodatage. Une procédure de sauvegarde quotidienne permet d'exporter ces traces, protégées en intégrité (calcul d'empreinte) et confidentialité (chiffrement), vers des systèmes de conservation sur le long terme. Les journaux du service d'horodatage sont conservés pendant 7 ans au minimum après l'émission du certificat d'horodatage actif. Ces journaux comprennent les requêtes et réponses de contremarque de temps.

6.7 CONTINUITÉ D'ACTIVITÉ

Au-delà de la continuité d'activité assurée au niveau de l'hébergement, l'AH met en place son propre plan de continuité d'activité concernant les données et les secrets du système.

Les composantes du système d'horodatage disposent d'une sauvegarde hors site permettant une reprise rapide de ces fonctions à la suite de la survenance d'un sinistre ou d'un évènement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.). Les fonctions de sauvegarde et de restauration sont effectuées par des administrateurs autorisés conformément aux mesures de sécurité procédurales.

Les sauvegardes hors sites sont réalisées dans un environnement sécurisé en accès physique et logique et sécurisé contre les risques d'incendie et d'inondation.

6.8 GESTION DES INCIDENTS

L'AH 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 UH ou la perte détectée de calibrage qui pourrait affecter des contremarques de temps émises –, qu'une information appropriée est mise à la disposition des abonnés et des utilisateurs de contremarques de temps. En particulier :

- L'AH traite le cas de la compromission réelle ou suspectée de la clé privée de signature d'une UH ou la perte de calibrage de l'horloge d'une UH, qui pourrait affecter des contremarques de temps émises dans le cadre d'un plan de secours ;

- Dans le cas d'une compromission, réelle ou suspectée, l'AH mettra à la disposition de tous les abonnés et utilisateurs de contremarques de temps une description de la compromission qui est survenue ;

- Dans le cas d'une perte de calibrage d'une UH, qui pourrait affecter des contremarques de temps émises, l'AH prendra les mesures nécessaires pour que les contremarques de temps de cette UH ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation ;

- Dans le cas d'une perte de connexion prolongée avec les serveurs de temps, l'AH prendra les mesures nécessaires pour que les contremarques de temps de cette UH ne soient plus générées jusqu'à ce que des actions soient faites pour restaurer la situation ;

- Dans le cas d'un événement majeur dans le fonctionnement de l'AH 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 de tous ses abonnés et utilisateurs de contremarques de temps toute information pouvant être utilisée pour identifier les contremarques de temps qui pourraient avoir été affectées, à moins que cela ne contrevienne à la vie privée des abonnés ou à la sécurité des services d'horodatage ;

- L'AH prévient directement et sans délai le point de contact de l'organe de contrôle national.

6.9 CESSATION D'ACTIVITÉ DE L'AH

Des procédures de fin d'activité définies par l'AH garantissent que les dérangements potentiels aux abonnés et aux utilisateurs de contremarques de temps sont réduits au minimum à la suite de la cessation d'activité du service d'horodatage et assurent en particulier la maintenance continue des informations nécessaires pour vérifier la justesse de contremarques de temps.

En particulier :

- Avant que l'AH ne termine ses services d'horodatage, les procédures suivantes seront exécutées au minimum :

  - l'AH rendra disponible à tous ses abonnés et utilisateurs de contremarques de temps l'information concernant sa fin d'activité,

  - l'AH 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 contremarques de temps et mettra fin aux contrats de sous-traitance ;

- l'AH transférera à un organisme fiable ses obligations de maintien des fichiers d'audit et des archives nécessaires pour démontrer son fonctionnement correct durant la période contractuelle,

- l'AH maintiendra ou transférera à un organisme fiable ses obligations de rendre disponibles aux utilisateurs de contremarques de temps pendant une période raisonnable ses clés publiques ainsi que ses certificats,

- les clés privées des UH seront détruites de telle façon que les clés privées ne puissent pas être recouvrées,

- L'AH prend les mesures nécessaires pour couvrir les dépenses pour accomplir ces exigences minimales dans le cas où l'AH tomberait en faillite ou pour d'autres raisons serait incapable de couvrir les dépenses par elle-même ;

- L'AH prévient directement et sans délai le point de contact de l'organe de contrôle national.

7 MESURES DE SÉCURITÉ TECHNIQUES

7.1 CONTROLES RECURRENTS DE VALIDITE

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 Mailstone TimeStamp est bien présent dans la liste nationale de confiance publiée par l'ANSSI (https://cyber.gouv.fr/sites/default/files/document/tl-fr.xml). Et la Trusted List publiée par eIDAS (https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tl/FR).

7.2 GESTION DE LA SYNCHRONISATION DE L'HORLOGE

Chaque unité d'horodatage s'assure que les contremarques de temps sont produites avec une exactitude de temps de 1 seconde par rapport au temps UTC. Pour cela, elle utilise son horloge interne et des sources de temps.

7.3 GESTION DES SOURCES DE TEMPS

Les sources de temps utilisées par chaque unité d'horodatage sont au minimum :

- Le signal GPS reçu par une installation propre à l'AH
- Des serveurs de temps de référence, au minimum :
  - ntp.obspm.fr
  - ntp1.jussieu.fr
  - fr.pool.ntp.org

Le matériel permettant l'acquisition du signal GPS est maintenu et supervisé par l'infrastructure de l'AH. Ce matériel est lui-même doté d'une horloge interne précise.

7.4 SYNCHRONISATION DES UH

L'horloge interne des unités d'horodatage est synchronisée par le protocole NTP à partir de sources de temps fiables synchronisées sur UTC et distinctes des sources de temps de référence.

Toutes les minutes, la dérive de l'horloge de l'unité d'horodatage est contrôlée par rapport aux sources de temps.

L'algorithme de synchronisation considère le temps fiable lorsque l'horloge est synchronisée avec au minimum 2 sources de temps distinctes.

Les 3 sources de temps disponibles sont les suivantes :

- **Source de référence 1** : NTP d'une source fiable sur internet (pool.ntp.org) (suivi incidemment par l'horloge de l'UH du fait de la synchronisation du système)
- **Source de référence 2** : Un boitier de temps synchronisé en NTP avec des sources de temps externes (tel que citées dans le §7.3)
- **Source de référence 3** : Un boitier de temps synchronisé en GPS.

Dans le cas où une source de temps sur les 3 n'est pas disponible :

- La perte de disponibilité de la source de temps est journalisée,
- La perte de disponibilité de la source de temps est remontée par le système de supervision du service,
- L'unité d'horodatage recommence toutes les minutes un contrôle de disponibilité de la source de temps,
- L'unité d'horodatage maintient la délivrance de contremarques de temps tant qu'il n'est pas constaté de dérive de l'horloge de l'UH avec les deux sources de temps restantes.

Dans le cas où deux sources de temps ne sont pas disponibles :

- L'unité d'horodatage stoppe immédiatement la délivrance de contremarques de temps (il n'est plus possible de garantir l'absence de dérive de l'horloge de l'UH),
- La perte de disponibilité des sources de temps et l'arrêt du service sont journalisés,
- La perte de disponibilité des sources de temps et l'arrêt du service sont remontés par le système de supervision du service,
- Une intervention manuelle des équipes techniques est programmée, une fiche d'incident est reportée,
- L'unité d'horodatage recommence toutes les minutes un contrôle de disponibilité des sources de temps.
- Dès que au moins deux sources de temps sont disponibles et que l'horloge interne des unités d'horodatage est synchronisée, la délivrance des contremarques de temps est rétablie. Le rétablissement est journalisé et remonté par le système de supervision du service.

Pour éviter toute interruption de service due à une désynchronisation supérieure à 1 seconde, dès qu'une dérive de l'horloge de l'UH supérieure à 500ms (mais inférieure à la seconde) est détectée par rapport à au moins deux sources de temps disponibles :

- L'algorithme effectue une resynchronisation de l'horloge interne de l'unité d'horodatage sur ces sources de temps,
- La dérive de l'horloge (sans dépassement de la précision annoncée du service) est journalisée,
- La perte de synchronisation est remontée par le système de supervision du service,
- L'unité d'horodatage recommence toutes les minutes une mesure d'écart afin de vérifier l'écart constaté.

Si la dérive de l'horloge de l'UH perdure au-delà de trois tentatives de resynchronisation, les équipes techniques Mailstone sont informées afin d'effectuer une resynchronisation manuelle avant d'atteindre une dérive supérieure à 1 seconde qui engendrerait un arrêt de génération des contremarques de temps :

- L'unité d'horodatage est resynchronisée avec les sources de temps,
- La dérive de l'horloge est journalisée,
- La dérive de l'horloge est remontée par le système de supervision du service.

Dans le cas où l'horloge locale de l'unité d'horodatage est désynchronisée de plus de 900 ms par rapport à au moins deux sources de temps disponibles :

- L'unité d'horodatage stoppe immédiatement la délivrance de contremarques de temps,
- L'unité d'horodatage est resynchronisée avec les sources de temps,
- La perte de synchronisation est journalisée,
- La perte de synchronisation est remontée 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.

7.5 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. Lorsque l'équipe technique Mailstone prend connaissance d'un saut de seconde, elle effectue un arrêt manuel du service 5 minutes avant le saut de secondes et rétablit le service 5 minutes après.

Les unités d'horodatage utilisent la donnée envoyée par les serveurs NTP afin de gérer un saut de seconde et se resynchronisent automatiquement.

Toutefois, le service est interrompu pendant cet évènement pour garantir une délivrance de contremarques de temps en adéquation avec les engagements cités dans le §3.1.

7.6 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.

7.7 GESTION DES BI-CLÉS DES UNITÉS D'HORODATAGE

7.7.1 Génération de clé

L'AH garantit que les clés cryptographiques des UH sont produites dans des circonstances et un environnement contrôlé, au cours d'une cérémonie de clés faisant l'objet d'un procès-verbal.

Ces clés sont générées et protégées au sein d'un HSM cryptographique qualifié et ne sont pas exportées, excepté pour leur sauvegarde. La longueur des clés de l'AH est de 4096 bits basés sur l'algorithme RSA.

7.7.2 Certification des clés de l'unité d'horodatage

L'AH 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'UH sont égaux à ceux générés par l'UH.

Le certificat de l'UH est généré par l'AC Certinomis TimeStamp.

La demande de certificat envoyée auprès de l'AC contient, en plus des informations exigées dans la PC de l'AC pour la partie enregistrement, au moins les informations suivantes :

- Le nom (DN) de l'UH pour laquelle la demande de certificat est faite ;
- La valeur de la clé publique (et l'identifiant de l'algorithme).

L'AH vérifie lors de l'import du certificat de l'UH qu'il est bien émis par l'AC requise et qu'il est conforme au gabarit attendu. L'AH s'assure que l'UH ne peut être opérationnelle qu'une fois ces vérifications effectuées avec succès.

7.7.3 Durée de validité des certificats de clé publique des unités d'horodatage

La durée de validité des certificats des UH ne peut pas excéder :

- La durée de vie cryptographique de la clé privée associée,
- La date de fin de validité du certificat de l'AC émettrice.

Par défaut, cette durée est de 3 ans.

7.7.4 Protection des clés privées des unités d'horodatage

Les clés privées des UH sont stockées dans un moyen cryptographique décrit au §7.8.1.

7.7.5 Gestion de la durée de vie de la clé privée

Les clés privées des UH sont utilisées pendant 2 ans et 6 mois.

L'AH garantit que les clés privées de signature des UH ne sont pas employées au-delà de la fin de leur cycle de vie. En particulier :

a) Des procédures opérationnelles ou techniques assurent qu'une nouvelle paire de clés est mise en place quand la fin de la période d'utilisation d'une clé privée d'UH a été atteinte,

b) Le service d'horodatage détruit, de façon sécurisée, la clé privée si la fin de la période d'utilisation de cette clé privée a été atteinte.

7.7.6 Sauvegarde des clés des unités d'horodatage

Les clés privées des UH font l'objet d'une copie de secours (sauvegarde) qui ne peut être restaurée que par les administrateurs systèmes de l'AH. Au minimum 3 porteurs de secrets, désignés pendant la cérémonie des clés initiale, sont requis pour procéder à la restauration d'une clé privée d'UH dans une nouvelle partition du HSM. La sécurité de la sauvegarde est assurée par les mécanismes de sécurité intrinsèques au HSM, assurant un niveau de protection équivalent au stockage interne dans le HSM.

7.7.7 Destruction des clés des unités d'horodatage

Les clés de signature des UH sont détruites à la fin de leur cycle de vie.

7.8 CRYPTOGRAPHIE

7.8.1 Moyens cryptographiques

Les clés privées des UH sont stockées dans un HSM certifié CC EAL4+ et qualifié par l'ANSSI au niveau renforcé.

7.8.2 Gestion du cycle de vie

Le moyen cryptographique est déployé selon les préconisations d'emploi spécifiées dans sa cible de sécurité et rappelées dans le rapport de qualification du matériel. Ceci garantit en particulier :

- L'intégrité du HSM durant son transport depuis le fournisseur ou le cas échéant entre deux sites d'hébergement utilisés par Mailstone ;
- La sécurité physique (cf. §6.1) 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.

7.8.3 Gestion 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.

S'il y a 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.

La mise hors service des différents supports varie en fonction de leur nature. En ce qui concerne les documents papiers, les CD, les clés USB de stockage, les cartes à puce, seront broyés en fin de vie (fin d'utilisation ou obsolescence). Les supports de stockage seront vidés, puis détruits à l'aide d'un marteau. Les HSM seront mis hors service en suivant les directives du constructeur.

7.9 ALGORITHMES OBLIGATOIRES

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

- SHA-256 ;
- 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 4096 bits et l'algorithme de signature utilise une fonction de hachage SHA-512.

7.10 CONTRÔLE D'ACCÈS

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

a) 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.

b) 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.
c) 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.
d) 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.
e) Le personnel de l'AH est dûment identifié et authentifié avant d'utiliser des applications critiques liées à l'horodatage.
f) Le personnel de l'AH est tenu responsable de ses activités.

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

g) 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.
h) 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.
i) 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.

7.11 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.

7.12 DISPONIBILITE DU SERVICE

L'AH assure une disponibilité du service fourni en fonctionnement normal de 24h/24 et 7j/7, avec un minimum de 99 % de disponibilité globale par an. 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, sauf force majeure.

8 PROFIL DES CERTIFICATS ET CONTREMARQUES DE TEMPS

8.1 FORMAT DU CERTIFICAT D'HORODATAGE

Les certificats de signature des contremarques de temps respectent le gabarit suivant :

Champ		Valeur
version		2 (c'est-à-dire version3)
serialNumber		Nombre aléatoire à longueur fixe
signature		
🡐 algorithm		SHA256WithRSA
🡐 parameters		RSAParams : NULL
issuer Distinguished Name		*CN= Certinomis - Timestamp CA* *OI=NTRFR-433998903* *O=Certinomis* *C=FR*
validity		
🡐 notBefore		Date de génération du certificat
🡐 notAfter		3 ans après la date de génération
subject Distinguished Name		*DN : Timestamp Unit X (X) numéro instance de l'UH)*
subjectPublicKeyInfo		
🡐 algorithm **↳ algorithm** **↳ parameters**		rsaEncryption RSAParams : 05 00
🡐 subjectPublicKey		RSAPublicKey (4096 bits)
issuerUniqueID		Champ non utilisé
subjectUniqueID		Champ non utilisé

Extensions	Criticité	Valeur
← **authorityKeyIdentifier**	Non	Hash de la clé publique de l'émetteur
← **subjectKeyIdentifier**	Non	Hash de la clé publique du sujet
← **keyUsage**	Oui	digitalSignature (80)
← **extKeyUsage**	Oui	id-kp-timestamping (1.3.6.1.5.5.7.3.8)
← **authorityInformationAccess**	Non	accessMethod : id-ad-caIssuers accessLocation : https://www.certinomis.com/publi/cer/ac-ejb-timestamp.cer ocsp : http://ocsp-pki.certinomis.com/
← **privateKeyUsagePeriod**		Extension non utilisée
← **certificatePolicies**	Non	Stratégie du certificat : [1] Identificateur de stratégie = 1.2.250.1.86.2.6.5.24.1 https://www.certinomis.fr/documents-et-liens/nos-politiques [2] Identificateur de stratégie = 0.4.0.194112.1.1
← **basicContraints** ↳ **cA** ↳ **pathLenConstraint**	Oui	 false None
← **cRLDistributionPoints**	Non	Point de distribution de la liste de révocation de certificats Nom du point de distribution : Nom complet : https://www.certinomis.com/crl/ac-ejb-timestamp.crl
← **subjectInfoAccess**		Extension non utilisée
Instruction de certificat qualifié	Non	QcCompliance QcType : eSeal PDS : https://www.certinomis.fr/documents-et-liens/nos-conditions-generales-dutilisation

Tableau 1 : Format du certificat d'horodatage

8.2 FORMAT DES REQUÊTES DE CONTREMARQUE

Les requêtes de contremarques de temps doivent être envoyées en utilisant le protocole http et en respectant le format décrit par la RFC 3161 (dans son paragraphe §2.4.1).

Les requêtes doivent de plus répondre aux restrictions suivantes :

Champ	Commentaires	Valeur attendue

version	Version du format	1
messageImprint **← hashAlgorithm** **← hashedMessage**	OID de l'algorithme de hash (empreinte) Hash des données à horodater	Les seuls algorithmes d'empreinte autorisés sont définis au §7.8. La valeur du hash est libre.
reqPolicy	OID de la PH à appliquer (obligatoire)	
nonce	Optionnel : Donnée anti-rejeu	Absent ou valeur libre retournée dans la réponse
certReq	Optionnel : Demande à l'UH d'inclure son certificat de signature dans la réponse	Absent ou true/false
extensions	Interdites : La requête n'est pas traitée si une extension est présente	Absent

Tableau 2 : Format des requêtes de contremarque

Les requêtes ne sont pas signées par leur émetteur.

8.3 FORMAT DES CONTREMARQUES DE TEMPS

Les réponses envoyées par l'AH 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	Commentaires	Valeur
version	Version du format	1
policy	OID de la PH	1.3.6.1.4.1.57916.1.1.1.1.1
messageImprint **← hashAlgorithm** **← hashedMessage**	OID de l'algorithme de hash (empreinte) hash des données à horodater	Identiques aux valeurs inclues dans la demande (les algorithmes d'empreinte autorisés sont restreints par la politique)
serialNumber	Identifiant unique de la	Généré par l'UH

	contremarque de temps	
genTime	Heure de la contremarque de temps	Heure de l'UH au moment de la génération, donnée sans les millièmes de seconde
accuracy	Précision	1 seconde
nonce	Donnée anti-rejeu uniquement si nonce était présent dans la requête de jeton	Identique à celui présent dans la requête
tsa	DN du certificate de l'unité d'horodatage	Cf. subject Distinguished Name chap 7.1
extensions	Extension supplémentaires optionnelles	Aucune extension supplémentaire

Tableau 3 : Format des contremarques de temps

De plus, l'identifiant du certificat de l'unité d'horodatage est indiqué dans une structure de type **ESSCertIDv2** comme indiqué dans la RFC 5816 (dans son paragraphe §2.2.1).

Enfin, si et seulement 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**.

9 AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS

9.1 FRÉQUENCES ET / OU CIRCONSTANCES DES ÉVALUATIONS

Un contrôle de conformité est réalisé lors de la mise en service du système et à la suite de toute modification significative. De plus, un audit est réalisé au moins tous les 2 ans. Les audits sont réalisés en interne par du personnel de Mailstone ou bien sous la forme d'une prestation auprès d'acteurs spécialistes de la sécurité des systèmes d'information et ayant des compétences reconnues dans le domaine de l'horodatage électronique.

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

9.2 IDENTITÉS / QUALIFICATIONS DES ÉVALUATEURS

Les auditeurs internes sont des employés de la société Mailstone. Mailstone s'engage à mandater des personnes disposant des compétences en sécurité requises pour auditer et vérifier la conformité du système.

9.3 SUJETS COUVERTS PAR LES ÉVALUATIONS

Les contrôles de conformité portent sur une composante du système (contrôles ponctuels) ou sur l'ensemble de l'architecture du service d'horodatage (contrôles

périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la PH de l'AH ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

Pour ce faire, les auditeurs présenteront pour approbation au comité de suivi la liste des composantes et procédures qui seront auditées.

9.4 COMMUNICATIONS AUPRES DE L'ANSSI

Dans le cadre de l'activité de l'AH, la société Mailstone s'engage à informer directement l'ANSSI dans les cas suivants :

- Changements de sous-traitants
- Conditions d'hébergement
- Changement de matériel cryptographique
- Modification d'architecture
- Changement de procédure d'enregistrement et d'identification
- Changement de gouvernance

L'AH s'engage à informer l'ANSSI dans les meilleurs délais des modifications apportées à la fourniture de ses services de confiance et adresse une synthèse de l'ensemble de ces modifications une fois par an, dans le respect du processus de qualification de ces services.

9.5 ACTIONS PRISES A LA SUITE DES CONCLUSIONS DES ÉVALUATIONS

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AH, un avis parmi les suivants : "réussite", "échec", "à confirmer". Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AH qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation des certificats de la composante, la révocation de l'ensemble des certificats du service, etc. Le choix de la mesure à appliquer est effectué par l'AH et doit respecter ses politiques de sécurité internes.

- En cas de résultat "à confirmer", l'AH remet au responsable de la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.

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

10 AUTRES PROBLÉMATIQUES

10.1 TARIFS

10.1.1 Tarifs pour la fourniture des contremarques de temps

Se référer aux conditions contractuelles en vigueur.

10.1.2 Tarifs pour accéder aux informations publiées par l'AH

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

10.2 POLITIQUE DE REMBOURSEMENT

Se référer aux conditions contractuelles en vigueur.

10.3 RESPONSABILITÉ FINANCIÈRE

10.3.1 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.

10.3.2 Couverture et garantie concernant les entités utilisatrices

Sans objet.

10.4 CONFIDENTIALITÉ DES DONNÉES PROFESSIONNELLES

10.4.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- Les procédures internes de l'AH,
- Les clés privées des unités d'horodatage et des composantes de l'AH,
- Les données d'activation associées aux clés privées d'AH et des composantes,
- Tous les secrets de l'AH,
- Les journaux d'événements des composantes de l'AH.

10.4.2 Informations hors du périmètre des informations confidentielles

Sans objet.

10.4.3 Responsabilités en termes de protection des informations confidentielles

Mailstone applique des procédures de sécurité pour garantir la confidentialité des informations identifiées ci-dessus. Mailstone s'engage à respecter la législation et la réglementation en vigueur sur le territoire français.

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.

10.5 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.

10.6 DROITS SUR LA PROPRIÉTÉ INTELLECTUELLE ET INDUSTRIELLE

Tous les droits de propriété intellectuelle détenus par Mailstone 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 Mailstone 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.

10.7 LIMITE DE RESPONSABILITÉ

Mailstone ne pourra pas être tenue 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, Mailstone 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 ;

10.8 INDEMNITÉS

En toute hypothèse, la responsabilité de Mailstone sera limitée, tous faits générateurs confondus et tous préjudices confondus, à une indemnisation équivalente à un mois

d'abonnement au service Mailstone et ce, dans le respect et les limites de la loi applicable.

10.9 DURÉE ET FIN ANTICIPÉE DE VALIDITÉ DE LA PH

10.9.1 Durée de validité

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

10.9.2 Fin anticipée de validité

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

10.9.3 Effets de la fin de validité et clauses restant applicables

Sans objet.

10.10 AMENDEMENTS À LA PH

10.10.1 Procédures d'amendements

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.

10.10.2 Mécanisme et période d'information sur les amendements

Lors de tout changement important impactant la PH, Mailstone informera les clients Mailstone au travers d'un communiqué mis en ligne sur son site internet. Si besoin, une communication par courrier électronique pourra être réalisée.

10.10.3 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).

10.11 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.

10.12 JURIDICTIONS COMPÉTENTES

Se rapporter au §10.11.

10.13 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].

10.14 TRANSFERT D'ACTIVITÉS

Les procédures en cas de transfert d'activité du service Mailstone TimeStamp peuvent être demandés à l'AH en s'adressant à elle aux coordonnées mentionnées au §2.2.

11 ANNEXE 1: DOCUMENTS CITÉS EN RÉFÉRENCE

11.1 REGLEMENTATION

Renvoi	Document
[EIDAS]	Règlement Européen 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 1999/93/CE

Tableau 4 : Documents règlementaires

11.2 DOCUMENTS TECHNIQUES

Renvoi	Document
[ETSI_TSP]	ETSI EN 319 401 v2.3.1: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI_AC]	ETSI EN 319 411-2 v2.4.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI_TIMESTAMP]	ETSI EN 319 421 v1.1.1: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[ETSI_CERT_UH]	ETSI EN 319 422 v1.1.1: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
[RFC_3161]	IETF - Internet X.509 Public Key Infrastructure - Time-Stamp Protocol -08/2001
[RFC_5816]	IETF - ESSCertIDv2 Update for RFC 3161 – 03/2010

Tableau 5 : Documents techniques

11.3 DOCUMENTS MAILSTONE

DOC	Lien
CGH	https://service.mailstone.io/assets/docs/MailStone_TimeStamp_CGH.pdf
CGU	https://service.mailstone.io/assets/docs/CGV_Mailstone.html