Service d'horodatage

SunTSA

Politique et Pratiques d'Horodatage

Version 1.1

Date d'entrée en vigueur : 15/12/2020

Technopole de l'Aube en Champagne - 2, rue Gustave Eiffel 10430 Rosières-près-Troyes - France
Tél. : +33 (0)3 25 43 90 78 – Fax : +33 (0)9 81 40 30 08 – www.lex-persona.com
SAS au capital de 26 739 euros – R.C.S. Troyes 480 622 257 – Code APE 5829C – TVA FR01480622257

Table des matières

1 Introduction

1.1 Présentation générale

L'objectif de ce document est de définir les engagements et les pratiques que Lex Persona, en tant qu'Autorité d'Horodatage (AH), respecte dans la délivrance et la gestion de Jetons d'horodatage, ainsi que les obligations des autres participants. Le respect de ces engagements permet, après audit de conformité selon les processus établis dans le règlement eIDAS (cf. [EIDAS]), la qualification par l'organe de contrôle national, du service d'horodatage de Lex Persona appelé « Service » dans la suite du document.

La structure de la présente Politique d'Horodatage (PH) est basée sur les documents issus de l'ETSI (cf. [ETSI_319421]).

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

Compte tenu de la complexité de lecture d'une PH pour des personnes non-spécialistes du domaine, l'AH définie également des Conditions Générale d'Utilisation (CGU) correspondant aux « TSA Disclosure Statement » définis dans l'annexe B de [ETSI_319421]. Ces CGU sont mises à disposition des Abonnés et des Utilisateurs (cf. 3.2).

1.2 Définitions

Abonné : Entité légale, ayant contracté avec Lex Persona pour bénéficier du Service, qui soumet ou fait soumettre par sa communauté d'utilisateurs des demandes de Jetons d'horodatage pour ses besoins propres.

Autorité de Certification (AC) : Entité qui délivre et est responsable des Certificats électroniques signés en son nom, conformément à sa Politique de Certification. Dans ce document le terme d'AC concerne plus particulièrement l'AC qui émet les certificats d'UH.

Autorité d'Horodatage (AH) : Entité en charge de l'émission et de la gestion des Jetons d'horodatage conformément à une PH.

Jeton d'horodatage : 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) : Échelle de temps, liée à la seconde, telle que définie dans la recommandation ITU - R TF.460-5 [TF.460-5].

Listes de Certificats Révoqués (LCR) : Liste des identifiants des certificats qui ont été révoqués ou invalidés à une certaine date et qui ne sont donc plus dignes de confiance à partir de cette date (cf. RFC 5280 et RFC 6818).

Lex Persona Trust Service Provider (LPTSP) : Entité, sous l'entière responsabilité de Lex Persona, gérant les services de confiance proposée par Lex Persona à ses clients.

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 ou à une classe d'applications avec des exigences de sécurité communes.

Politique d'Horodatage (PH) : Ensemble de règles définissant les objectifs et les engagements d'une AH pris pour assurer la fiabilité des services d'horodatage fournis. La PH est un document public accessible librement.

Service : Service de confiance, opéré par Lex Persona, sous la responsabilité de l'AH, qui émet des Jetons d'horodatage conformément à la présente PH.

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

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 : Entité (personne physique ou morale) qui dispose d'un Jeton d'horodatage émis par le Service selon la présente PH et qui a accepté les CGU du Service.

1.3 Acronymes

AC	Autorité de Certification
AH	Autorité d'Horodatage
CGU	Conditions Générales d'Utilisation
HSM	Hardware Security Module
LCR	Liste des Certificats Révoqués
LPTSP	Lex Persona Trust Service Provider
PC	Politique de Certification
PH	Politique d'Horodatage
UH	Unité d'Horodatage

1.4 Gestion du document

1.4.1 Identification de la PH

La présente PH peut être identifié par son numéro d'identifiant d'objet :

1.3.6.1.4.1.22542.100.2.1

La présente PH est conforme à la politique BTSP (best practices policy for time-stamp) de l'ETSI, identifiée par l'OID 0.4.0.2023.1.1 [ETSI_319421].

1.4.2 Amendement du document

La présente PH est sous la responsabilité de l'AH qui a en charge l'administration et la gestion de la PH, et qui est en particulier responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PH.

1.4.2.1 Procédure de mise à jour

Le document peut être mis à jour uniquement par l'AH, 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.

Pour ce faire l'AH doit, dans un premier temps, valider ou non le principe de cette modification en fonction de ses objectifs et de ses responsabilités vis-à-vis du Service fourni. L'AH peut s'appuyer autant sur des ressources propres, que sur des ressources externes ayant une expertise dans le domaine, notamment pour l'évaluation de la conformité aux exigences réglementaires et normatives applicables.

Dans certains cas, sur décision du LPTSP Board, un audit interne peut être diligenté pour s'assurer que les nouvelles évolutions ne remettent pas en cause des exigences prises par l'AH dans sa PH.

1.4.2.2 Circonstances selon lesquelles l'OID doit être changé

Toute évolution de la présente PH ayant un impact majeur sur le Service doit se traduire par une évolution de l'OID, afin que les Abonnés et les Utilisateurs puissent clairement identifier les exigences applicables aux Jetons d'horodatage.

1.4.3 Procédure d'approbation

La PH doit être approuvée par l'AH avant d'être promulguée.

La décision est consignée dans un procès-verbal signé par les membres du LPTSP.

La nouvelle version de la PH entre en vigueur à la date indiquée dans sa page de garde et reste valide jusqu'à l'entrée en vigueur d'une nouvelle version.

1.4.4 Publication et consultation

La mise à disposition des informations devant être publiées à destination des Abonnés et Utilisateurs est réalisée par Lex Persona.

La PH est publiée sur le site suivant : https://tsa2.sunnystamp.com/repository.

Lex Persona peut modifier la présente PH. Dans ce cas Lex Persona avisera les Abonnés de la nature des modifications apportées, par tous moyens à sa convenance dont notamment le site Internet de Lex Persona et la messagerie électronique, en fonction de la portée des modifications.

Lex Persona adresse annuellement à l'ANSSI une synthèse de l'ensemble des modifications apportées à la fourniture de ses services de confiance qualifiés.

1.5 Documents associés

1.5.1 Documents normatifs

[ANSSI_HOR]	Services d'horodatage électronique qualifiés – Critères d'évaluation de la conformité au règlement eIDAS, Version 1.1 du 3 janvier 2017
[ANSSI_PSCO]	Prestataires de services de confiance qualifiés – Critères d'évaluation de la conformité au règlement eIDAS, Version 1.2 du 5 juillet 2017
[ANSSI_TL]	Liste nationale de confiance de la France publiée par l'ANSSI. https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/liste-nationale-de-confiance/
[ETSI_319102]	ETSI EN 319 102-1 V1.1.1 (2016-05) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf
[ETSI_319421]	ETSI EN 319 421 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf
[ETSI_319422]	ETSI EN 319 422 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf
[EIDAS]	Règlement nº 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 nº 1999/93/CE. http://www.europa.eu
[GDPR]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 https://www.cnil.fr/fr/reglement-europeen-protection-donnees

[OPENSSL]	Time Stamping Authority command (OpenSSL, Cryptography and SSL/TLS Toolkit) https://www.openssl.org/docs/manmaster/man1/openssl-ts.html
[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
[SOGIS-CRYPTO]	SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms – Version 1.0 – May 2016. http://sogis.org

1.5.2 Conditions Générales d'Utilisation

[CGU]	Conditions Générales d'Utilisation du SunTSA https://tsa2.sunnystamp.com/repository

1.5.3 Politique Générale des Services de Confiance

[PGSC]	Politique Générale des Services de Confiance de Lex Persona https://pki2.sunnystamp.com/repository

1.5.4 Politique de Certification

[PC]	Politique de Certification de l'AC « Sunnystamp Legal Persons CA » délivrant des certificats de niveau ETSI EN 319 411 NCP+ pour les UH. https://pki2.sunnystamp.com/repository

2 Parties prenantes et obligations

2.1 Obligations de l'AH

Le Service est placé sous la responsabilité de l'AH à laquelle incombe les obligations suivantes :

- Garantir, via les mesures décrites ci-dessous et dans [PGSC], qu'elle possède la fiabilité nécessaire pour fournir des services d'horodatage ;
- Conduire une analyse des risques de son service d'horodatage ;
- Adresser l'ensemble des exigences décrites dans la PH ;
- Décrire toutes les exigences que doivent respecter les éventuelles tierces parties dans le cadre du service d'horodatage ;
- Générer et signer les Jetons d'horodatage conformément à la présente PH ;

- Respecter et se conformer aux exigences et procédures définies dans la présente PH ;
- Garantir la conformité des exigences et des procédures décrites dans la présente PH ;
- Mettre à disposition des Abonnés et Utilisateurs l'ensemble des informations nécessaires à la vérification des Jetons d'horodatage qu'elle aura émise, selon les modalités indiquées dans la présente PH (cf. 3.2) ;
- Respecter les conditions de disponibilité du Service convenues contractuellement avec les Abonnés ;
- Maintenir une information sur la compromission de la bi-clé des UH ;
- Utiliser des certificats pour les UH sous sa responsabilité, conformément aux exigences de la PC de l'AC émettrice de ces certificats ;
- Authentifier les demandes de Jetons d'horodatage soumises par les Abonnés à l'AH ;
- Garantir qu'elle mettra à jour la PH en cas de changements majeurs des pratiques d'horodatage de son service ;
- Garantir que tout changement majeur dans ses pratiques d'horodatage fera l'objet d'une notification auprès de l'organisme qui lui a délivré les différentes qualifications.

L'AH s'appuie sur une organisation opérationnelle interne de Lex Persona pour la mise en œuvre technique du Service, notamment l'installation et l'exploitation des UH.

2.2 Obligations pour l'AC fournissant les certificats des UH

Les certificats de signature des Jetons d'horodatage, mis en œuvre au sein de chaque UH, sont émis par une AC gérée par Lex Persona et certifiée ETSI EN 319 411-1 de niveau NCP+.

Cette AC assume les responsabilités suivantes :

- L'émission des certificats de signature des UH ;
- La mise à disposition de l'AH des services de révocation nécessaires ;
- La publication à destination des Abonnés et Utilisateurs des moyens de vérification des certificats, c'est à dire de la chaîne de certification et du statut de révocation des certificats.

2.3 Obligations de l'Abonné

L'Abonné doit respecter les obligations suivantes :

- Accepter et respecter les CGU ;
- Respecter les obligations de la présente PH qui lui sont applicables ;
- Envoyer des requêtes conformes à la [RFC_3161] et aux contraintes exposées dans cette PH, à partir d'une empreinte calculée avec un algorithme conforme à l'état de l'art et autorisé par la PH ;
- S'assurer de la validité des Jetons d'horodatage dès leur réception en vérifiant en particulier la valeur de l'empreinte contenue ainsi que la signature du Jeton d'horodatage.

Il est recommandé que l'Abonné vérifie que le certificat de l'UH ne soit pas révoqué au moment de l'obtention des Jetons d'horodatage.

D'autre part, l'Abonné assume les responsabilités suivantes :

- La cohérence entre l'empreinte soumise dans la requête et l'empreinte contenue dans le Jeton d'horodatage ;
- La conservation des Jetons d'horodatage selon ses besoins propres ;
- La transmission des CGU à ses utilisateurs ou l'obligation de faire figurer leurs obligations dans un document qui leur est opposable.

2.4 Obligations de l'Utilisateur

L'Utilisateur n'a pas d'obligations vis-à-vis de l'AH mais il lui est néanmoins recommandé de vérifier les Jetons d'horodatage (cf. 5.6.1.2) et de tenir compte des limitations, indiquées dans la présente PH et dans les CGU, sur l'utilisation des Jetons d'horodatage.

3 Responsabilités concernant la mise à disposition des informations devant être publiées

3.1 Entités chargées de la mise à disposition des informations

Voir chapitre 2 de la [PGSC].

3.2 Informations devant être publiées

Lex Persona s'engage à publier au minimum les informations suivantes à destination des Abonnés, des Utilisateurs et des tiers ayant à déterminer la validité des Jetons d'horodatage produits par le Service :

- Le présent document, décrivant la politique et les pratiques du Service ;
- La [PGSC] ;
- Les [CGU] ;
- Les certificats des UH en cours de validité.

3.3 Délais et fréquences de publication

Voir chapitre 2 de la [PGSC].

3.4 Contrôle d'accès aux informations publiées

Voir chapitre 2 de la [PGSC].

4 Gestion des risques

Voir chapitre 3 de la [PGSC].

5 Exigences opérationnelles

5.1 Organisation interne

5.1.1 Fiabilité

Voir chapitre 7.2 de la [PGSC].

5.1.2 Rôles de confiance

Voir chapitre 4.2 de la [PGSC].

5.2 Ressources humaines

Voir chapitre 4.3 de la [PGSC].

5.3 Gestion des actifs

Voir chapitre 4.1 de la [PGSC].

5.4 Contrôle d'accès

Voir chapitre 5.2 de la [PGSC].

5.5 Cryptographie

5.5.1 Génération de clé des UH

L'AH garantit que les clés cryptographiques des UH sont produites dans des circonstances et dans un environnement contrôlés, 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 et ne sont pas exportées. La longueur des clés de l'AH est d'au moins 2048 bits avec l'algorithme RSA.

5.5.2 Certification des clés des UH

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 identifiée en 1.5.4.

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 requête de certificat (au format PKCS#10) contenant la clé publique de l'UH (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, que la clé publique qu'il contient correspond bien à la clé privée de l'UH 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.

5.5.3 Protection des clés privées des UH

Les clés privées des UH sont stockées dans des HSM certifiés CC EAL4+ et qualifiés par l'ANSSI.

Les HSM sont hébergés dans les sites sécurisées de l'AH et sont gérés exclusivement par les personnes ayant les rôles de confiance requis.

Les clés privées sont contrôlées par des données d'activation stockées sur des cartes à puce remises à des porteurs de secrets lors d'une cérémonie des clés.

L'AH s'assure de la sécurité des HSM tout au long de leur cycle de vie. En particulier, l'AH met en place les procédures nécessaires pour s'assurer :

- De leur intégrité durant leur transport depuis le fournisseur ;
- De leur intégrité durant leur stockage précédant la cérémonie des clés ;
- Que les opérations d'activation des clés de signature sont réalisées sous le contrôle d'au moins deux personnes ayant les rôles de confiance appropriés ;
- Qu'ils sont en bon état de fonctionnement ;
- Que les clés qu'ils contiennent sont détruites lorsqu'ils sont décommissionnés.

5.5.4 Destruction des clés des UH

Les clés privées des UH sont détruites dès la fin de leur durée d'utilisation (cf. 6.4).

5.5.5 Exigences de sauvegarde des clés des UH

Les clés privées des UH ne sont pas sauvegardées.

5.6 Horodatage

5.6.1 Gestion des requêtes d'horodatage

5.6.1.1 Émission de Jetons d'horodatage

Le Service fournit un Jeton d'horodatage en réponse à une requête d'horodatage [RFC_3161] valide émise par l'Abonné, contenant au minima l'empreinte de la donnée à horodater.

Si la requête contient le champ `reqPolicy`, sa valeur doit être l'OID de la PH (voir 1.4.1), sinon une erreur `unacceptedPolicy` sera retournée.

Si la requête contient le champ `certReq` avec la valeur `TRUE` alors le Jeton d'horodatage contiendra le certificat de l'UH utilisé pour signer ce Jeton d'horodatage sinon il ne contiendra pas le certificat de l'UH.

Si la requête contient le champ `nonce`, sa valeur sera intégrée dans le champ `nonce` du Jeton d'horodatage produit.

Si la requête contient des `extensions`, elles seront ignorées par l'AH.

Les Jetons d'horodatage sont générés dans un environnement sûr et contiennent les informations suivantes :

- L'empreinte et l'algorithme d'empreinte de la donnée horodatée ;
- L'identifiant de l'UH contenu dans la propriété signée « SigningCertificate » de la signature du Jeton d'horodatage et dans le DN du certificat de l'UH dans le cas où il est présent dans le Jeton d'horodatage ;
- L'identifiant (OID) de la PH appliquée (voir 1.4.1) ;
- Un identifiant unique du Jeton d'horodatage ;
- La date UTC de génération du Jeton d'horodatage par l'UH ;
- La précision de la date UTC de génération du Jeton d'horodatage ;
- Le « nonce » (dans le cas où il a été renseigné dans la requête) ;
- L'extension `esi4-qtstStatement1` qui indique qu'il s'agit d'un Jeton d'horodatage qualifié.

Les Jetons d'horodatage sont signés par une UH avec sa clé privée, réservée à cet usage.

La fourniture d'un Jeton d'horodatage en réponse à une demande n'excède pas quelques secondes, ceci afin de ne pas nuire ni dégrader l'ergonomie de l'application de l'Abonné.

Le Service conserve les Jetons d'horodatage générés pour une durée de 10 ans.

5.6.1.2 Vérification d'un Jeton d'horodatage

Les Abonnés et, de manière générale, les Utilisateurs sont incités à vérifier la validité des Jetons d'horodatage générés par le Service (voir 2.4).

La vérification d'un Jeton d'horodatage se déroule de la façon suivante :

- Vérifier que le Jeton d'horodatage a été correctement signé, et que le certificat de l'UH est valide à l'instant de la vérification ;
- Vérifier que l'OID contenu dans le Jeton d'horodatage est bien celui qui s'applique pour la présente PH (cf. 1.4.1) ;
- Vérifier que le certificat de l'UH est contenu dans la liste de confiance [ANSSI_TL] publiée par l'ANSSI et référencé dans cette liste en tant que « service de génération d'horodatage électronique qualifié » (https://uri.etsi.org/TrstSvc/Svctype/TSA/QTST/) ;
- Vérifier la valeur de l'empreinte contenue dans le Jeton d'horodatage par rapport aux données à laquelle elle se rapporte.

Si le Jeton d'horodatage est contenu dans une signature électronique, il devrait normalement être vérifiée par l'application de vérification de signature utilisée conformément à [ETSI_319102]. Dans tous les cas, un Jeton d'horodatage peut être vérifié avec [OPENSSL].

L'AH garantit l'accès à l'information nécessaire pour vérifier la signature numérique des Jetons d'horodatage. En particulier :

- Les certificats des UH sont disponibles sur l'espace de publication de l'AH, et éventuellement sont joints au Jeton d'horodatage sur demande ;
- La chaîne de certification complète des certificats des UH est disponible sur l'espace de publication de l'AC ;
- Les informations sur le statut de révocation des certificats sont disponibles via les URL présentes dans les extensions *Authority Information Access* et *CRL Distribution Point* des certificats d'UH. Les LCR sont publiées sur l'espace de publication de l'AC.

L'AH garantit que les Jetons d'horodatage sont vérifiables pendant la période de validité des certificats des UH émettrices.

5.6.2 Synchronisation de l'horloge

L'heure intégrée dans un Jeton d'horodatage est donnée par l'horloge de l'UH produisant ce Jeton d'horodatage. Cette horloge est synchronisée avec le temps UTC via plusieurs sources de référence.

L'AH garantit que son horloge est synchronisée avec le temps UTC selon l'exactitude déclarée de 1 (une) seconde, et garantit les propriétés suivantes :

- 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 ;
- Les horloges des UH 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 ;
- Tout non-respect de l'exactitude déclarée par son horloge interne sera détecté ;
- Aucun Jeton d'horodatage ne sera généré par une UH dès lors que l'horloge de cette UH est détectée comme étant en dehors de l'exactitude annoncée, ou que l'exactitude ne peut plus être garantie ;
- 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.

5.7 Sécurité physique et environnementale

Voir chapitre 4 de la [PGSC].

5.8 Sécurité opérationnelle

Voir chapitre 4 de la [PGSC].

5.9 Sécurité réseau

Voir chapitre 5.4 de la [PGSC].

5.10 Gestion des incidents

Voir chapitre 4.6.1 de la [PGSC].

L'AH garantit, dans le cas d'événements qui affectent la sécurité du Service (incluant la compromission de la clé privée de signature d'une UH ou la perte détectée de calibrage qui pourrait affecter des Jetons d'horodatage émis), qu'une information appropriée est mise à la disposition des Abonnés et des Utilisateurs. En particulier :

a) 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 Jetons d'horodatage émis dans le cadre d'un plan de secours ;
b) Dans le cas d'une compromission, réelle ou suspectée, l'AH mettra à la disposition de tous ses Abonnés et Utilisateurs une description de la compromission survenue ;
c) Dans le cas d'une perte de calibrage d'une UH, qui pourrait affecter des Jetons d'horodatage émis, l'AH prendra les mesures nécessaires pour que les Jetons d'horodatage de cette UH ne soient plus générés jusqu'à ce que des actions soient faites pour restaurer la situation ;
d) Dans le cas d'une perte de connexion prolongée avec les serveurs de temps, l'AH prendra les mesures nécessaires pour que les Jetons d'horodatage de cette UH ne soient plus générés jusqu'à ce que des actions soient faites pour restaurer la situation ;
e) Dans le cas d'un événement majeur dans le fonctionnement de l'AH ou d'une perte de calibrage qui pourrait affecter des Jetons d'horodatage émis, chaque fois que cela sera possible, l'AH mettra à la disposition de tous ses Abonnés et Utilisateurs toute information pouvant être utilisée pour identifier les Jetons d'horodatage qui pourraient avoir été affectés, à moins que cela ne contrevienne à la vie privée des Abonnés ou à la sécurité du Service.

5.11 Procédure de constitution des données d'audit

Voir chapitre 4.4 de la [PGSC].

Les traces générées et collectées par le Service comprennent notamment les traces d'événements relatifs :

- Au cycle de vie des clés et des certificats d'UH ;
- À la synchronisation entre les UH et le temps UTC, y compris les sauts de seconde, les calibrations et les pertes de synchronisation ;
- Aux requêtes d'horodatage et aux Jetons d'horodatage produits.

Le Service conserve ces traces pour une durée de 10 ans.

Les traces sont protégées en intégrité et en confidentialité.

5.12 Continuité d'activité

Voir chapitre 4.6 de la [PGSC].

5.13 Fin de vie

L'AH dispose d'un plan de fin de vie qui sera déroulé en cas de cessation de l'activité du Service.

Les principales étapes de ce plan de fin de vie sont les suivantes :

- L'AH avisera, par tous moyens à sa convenance, les Abonnés et Utilisateurs, ainsi que tous les partenaires et parties concernées, de la fin d'activité ;
- L'AH préviendra directement et sans délai le point de contact de l'organe de contrôle national ;
- 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 Jetons d'horodatage ;
- L'AH s'efforcera de proposer à ses Abonnés un transfert du Service vers un autre prestataire de service de confiance qualifié d'horodatage ;
- 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 une période raisonnable ;
- L'AH maintiendra ou transférera à un organisme fiable ses obligations de rendre disponibles aux Utilisateurs, pendant leur période de validité, les certificats des UH.
- L'AH demandera à l'AC la révocation des certificats des UH et les clés privées associées des UH seront détruites de telle façon qu'elles ne puissent pas être recouvrées ;
- L'AH prendra les mesures nécessaires pour couvrir les dépenses nécessaires à l'accomplissement de ces exigences minimales dans le cas où l'AH serait en faillite ou dans l'incapacité de couvrir les dépenses par elle-même.

Le plan de fin de vie appliqué sera celui en vigueur au moment de l'annonce de la fin d'activité.

5.14 Conformité

Voir chapitre 6 de la [PGSC].

6 Exigences de sécurité techniques

6.1 Exactitude temps

L'AH garantit que les Jetons d'horodatage sont générés avec une exactitude de temps de 1 seconde par rapport au temps UTC.

Cette précision est obtenue par synchronisation et contrôle des horloges des UH en se basant sur des sources de temps externes de type GPS et références UTC(k).

6.2 Algorithmes obligatoires

L'AH accepte les empreintes calculées avec les algorithmes suivants :

- SHA256 ;
- SHA384 ;
- SHA512.

Les Jetons d'horodatage sont signés selon les algorithmes et les longueurs de clé conformes à l'état de l'art. Actuellement, la bi-clé des UH est une bi-clé RSA de 2048 bits et l'algorithme de signature des Jetons d'horodatage utilise une fonction de hachage SHA256.

6.3 Durée de validité des certificats de clé publique des UH

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.

La durée de validité des certificats des UH est de 3 ans.

6.4 Durée d'utilisation des clés privées des UH

La durée d'utilisation des clés privées des UH sera limitée en pratique à 2 ans afin de faciliter la vérification des Jetons d'horodatage grâce à une période adéquate de validité du certificat.

7 Profil des certificats et Jetons d'horodatage

7.1 Format du certificat des UH

Les certificats des UH, pour la signature des Jetons d'horodatage, sont des certificats au format X.509 v3 qui respectent le gabarit suivant :

Champs de base :

Champ	Valeur
Version	2 (correspond à la v3 de X.509)
Numéro de série	Défini lors de la création
Emetteur	CN = Sunnystamp Legal Persons CA OI = NTRFR-480622257 OU=0002 480622257 O = LEX PERSONA C = FR
Sujet	CN = Sunnyseal TSU**XX** Qualified eIDAS Timestamp *(où **XX** est l'identifiant de l'UH allant de 01 à 99)* serialNumber = Identifiant unique généré par l'AC OI = NTRFR-480622257 O = LEX PERSONA

	C = FR
Validité	3 ans
Signature	SHA256withRSA
Clé publique	RSA 2048 bits

Extensions :

Champ	Critique	Valeur
AuthorityInfoAccess	Non	id-ad-caIssuers= https://pki2.sunnystamp.com/certs/sunnystamp-legal-persons-ca.cer id-ad-ocsp= http://ocsp2.sunnystamp.com/sunnystamp-legal-persons-ca
AuthorityKeyIdentifier	Non	Empreinte SHA1 de la clé publique de l'émetteur
BasicConstraints	Oui	cA=false
CertificatePolicies	Non	OID=0.4.0.2042.1.2 OID=1.3.6.1.4.1.22542.100.1.1.2.2 URL=https://pki2.sunnystamp.com/repository
CRLDistributionPoints	Non	http://pki2.sunnystamp.com/crls/sunnystamp-legal-persons-ca.crl http://pki3.sunnystamp.com/crls/sunnystamp-legal-persons-ca.crl
ExtendedKeyUsage	Oui	id-kp-timeStamping
Key Usage	Oui	digitalSignature
SubjectKeyIdentifier	Non	Empreinte SHA1 de la clé publique du sujet

7.2 Format des Jetons d'horodatage

Les Jetons d'horodatage, conformes à la norme [RFC_3161] et au profil [ETSI_319422], respectent le gabarit suivant :

Champ	Commentaires	Valeur
version	Version du format	1
policy	OID de la PH	OID de la présente PH (cf. 1.4.1)
messageImprint	OID de l'algorithme d'empreinte et empreinte des données à horodater	Identiques aux valeurs inclues dans la demande

serialNumber	Identifiant unique du Jeton d'horodatage	Généré par l'UH
genTime	Heure du Jeton d'horodatage	Heure de l'UH au moment de la génération du Jeton d'horodatage
accuracy	Précision déclarée	1 seconde
nonce	Donnée anti-rejeu	Identique à celui présent dans la requête si `nonce` était présent
extensions	Extension supplémentaires optionnelles	Contient l'extension `qcStatements` avec la valeur `esi4-qtstStatement1`